Forensic Readiness for Wireless Medical Systems: Designing for User Safety

AR KAR KYAW
M.F.I.T. (1st Class Honours, AUT, NEW ZEALAND), B.Eng.Tech. (Massey University, NEW ZEALAND), B.E. (Mandalay Technological University, BURMA)

A thesis submitted to the Graduate Faculty of Design and Creative Technologies
AUT University
in fulfilment of the
requirements for the Degree of
Doctor of Philosophy

School of Engineering, Computer and Mathematical Sciences

Auckland, New Zealand
2019

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

.....

Ar Kar KYAW

Acknowledgements

This PhD thesis was completed at the Faculty of Design and Creative Technologies of AUT University in New Zealand. While conducting this research project I received support from many people in one way or another, without whose support, this thesis would not have been completed in its present form. It is my pleasure to take this opportunity to thank everyone who assisted me in the journey to complete my thesis. I would like to apologise to those who I do not mention by name here; however, I highly valued their kind support.

First, I would like to express my heartfelt gratitude to my primary supervisor, Dr Brian Cusack for his invaluable support and encouragement throughout this PhD study. Dr Cusack provided me with the freedom to explore research directions and choose the routes that I wanted to investigate. Dr Cusack's encouragement, excellent guidance, creative suggestions, and critical comments have greatly contributed to this thesis. I enjoyed our discussions and had learned a great deal from you. Dr Cusack, I would like to thank you wholeheartedly for constantly advising me to move forward and steering me in the right direction when needed most. I also would like to thank my secondary supervisor, Professor Dave Parry, for his help and support. I strongly believe that what I have learned during the PhD study period will be infinitely valuable in my life. For this I am eternally grateful. Thank you, from the depth of my heart!

I would like to acknowledge the friendship and mentorship of my fellow PhD students for their support. Similarly, I would like to thank my colleagues at Whitireia Polytechnic (New Zealand) for their support. Without their support and encouragement, my study life at AUT would have been more difficult. I would like to thank all of you.

In addition, I am extremely grateful to my late father, (U Kyaw Myint), and my beloved mother, Daw Tin Tin Win, whose continual support, encouragement, love, praying for my progress and for teaching me the values in life that brought me to where I am today. I greatly appreciate my younger brother and two sisters in Burma for fulfilling my duty of taking care of my mum while I was pursuing the PhD degree.

Abstract

The focus of this research is on the risks associated with wireless medical systems (WMedSys) and devices in the healthcare environment. The deployment of wireless communications in medical healthcare environments has rapidly increased to meet the clinical requirements, and to have the benefits of mobility and accessibility for everyone. Many medical devices such as telemetry, pulse oximetry monitors, electrocardiography (ECG) carts, neuro-stimulators, infusion pumps, insulin pumps, pacemakers, implantable cardioverter defibrillators (ICD) and drug pumps use the wireless communication technologies for practical service advantages. The wireless medical devices (WMedDs) allow mobility, continuous monitoring of users' health in real-time, and other service advantages. However, these technology innovations are vulnerable to unplanned failure and intentional disruption. In this thesis, the concern for patient safety is addressed by evaluating current systems, designing improved systems, and advocating for better security provisions.

The nature of wireless networking has inherited security and privacy problems that transfer theoretically and practically to the medical healthcare industry. The growth in wireless network deployments and devices has created the problem of security vulnerabilities leading to potential patient harm. Many incidences have been reported where service functionality, patient harm, and intentional damage have occurred. For instance, Radcliffe (2011) demonstrated hacking a commercially available wireless insulin pump, which controls the insulin dosages for patients who have diabetes. Likewise, Halperin et al. (2008, p. 1) have performed a number of "software radio-based attacks" on implantable cardioverter defibrillators (ICDs). Chapter 2 also reports three such cases. Such types of attacks can compromise patient safety, patient privacy and negate the expected benefits from using wireless technologies. Hence, the risks and concerns in the problem area require detailed research and mitigation from working solutions.

Design Science (DS) is adopted as the research methodology. DS has the benefit of managing theory to build artefacts. These artefacts may be investigated in context, and improvement by design and functionality through continuous

iterations and testing. Depending on the characteristics and the goals of the research, a researcher can shape the processes to deliver innovative or confirmatory outcomes. In this research, the DS research methodology is applied to a design artefact extracted from the review of relevant past literature. It is then put through rounds of testing that include confirmation, improvement, and expert feedback. The purpose of DS is not only to develop an artefact but also to answer the research questions and give solutions for problems. The main research question is: “What can be improved to make digital forensic investigation more effective in a wireless medical system?” The entry point of problem solving has been adopted and the methods of testing, experiment and expert feedback are used to formulate the artefact design. The key contribution of the research is to innovate a forensically ready system that will preserve and make available digital evidence (a costing of the system is provided in Appendix C).

The thesis is structured to provide a substantial literature review (see the reference list pp. 187-246), a methodological explanation, the reported findings from the confirmatory tests (see Appendix B data), reported findings from the scenario tests (see Appendix E and Appendix F), and reported findings from the expert feedback (see Appendix D). The research hypotheses are tested, and the research questions are answered (see Chapter 8). The design for WMedSys is presented as an improved solution to the research problem. The thesis concludes with a summary and recommendations for further research.

Table of Contents

Chapter – 4 Security Risks

Chapter – 5 Wireless Network Architecture and Standards

Chapter – 6 Research Methodology

Chapter – 7 Pilot Study Findings

Chapter – 8 Expert Feedback Evaluation, Analysis of Findings and Answers to Research Questions

Chapter – 9 A Proposed Two-Tier Security Model

Chapter – 10 Summary and Conclusion

Appendices

List of Tables

List of Figures

List of Abbreviations

ACR-NEMA	American College of Radiology – National Electronic Manufacturers' Association
AD	Active Directory
AD DS	Active Directory Domain Services
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
ASIC	Application-Specific Integrated Circuit
ASTM	American Society for Testing and Materials
AUTH	Authentication
BCC	Body-Coupled Communication
BMDs	Bedside Medical Devices
BroIDS	Open-source UNIX based Bro Intrusion Detection System
BSN	Body Sensor Node
BSSID	Basic Service Set Identification
C1WSN	Category 1 Wireless Sensor Network
C2WSN	Category 2 Wireless Sensor Network
CCMP	Counter Cipher Mode with Block Chaining Message Authentication Code Protocol
CE	Clinical Engineer
CEN/TC 251	European Committee for Standardisation/Technical Committee 251
CEO	Chief Executive Officer
CERT	Computer Emergency Readiness Team
CGMIDS	Continuous Glucose Monitoring and Insulin Delivery System
CH	Channel
CIAA	Confidentiality, Integrity, Availability and Authentication
COWs	Computer-on-Wheels
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CS	Central Server
CTIA	Cellular Telecommunications Industry Association
CU	Capture Unit
CVD	Cardiovascular Disease

DDoS	Distributed Denial of Service
DE	Digital Evidence
DES	Data Encryption Standard
DFI	Digital Forensic Investigation
DFR	Digital Forensic Readiness
DHCP	Dynamic Host Configuration Protocol
DICOM	Digital Imaging and Communications in Medicine
DNS	Domain Name Service
DoS	Denial of Service
DS	Design Science
DSRM	Design Science Research Methodology
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EBSS	Extended Basic Service Set
ECG	Electrocardiography
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMR	Electronic Medical Record
ES	Evidence Store
ESSID	Extended Service Set Identification
EU	European Union
FCC	Federal Communication Commission
FDA	Food and Drug Administration
FHSS	Frequency Hopping Spread Spectrum
FIs	Forensic Investigators
FS	Forensic Server
GCM	Continuous Glucose Monitor
GCMP	Galios Counter Mode Protocol
GPRS	General Packet Radio Service
GPS	Global Positioning System
GPU	Graphics Processing Unit
HCFA	Health Care Financing Administration
HIPAA	Health Insurance Portability and Accountability Act
HIPC	Health Information Privacy Code
HL7	Health Level 7 Standard
HS	Hash Store
HTTPS	Hypertext Transfer Protocol Secure

HW	Hardware
IBSS	Independent Basic Service Set
IC	Integrated Circuit
ICD	Implantable Cardioverter Defibrillators
ICU	Intensive Care Unit
ICU-BMDs	Intensive Care Unit-Bedside Medical Devices
ICV	Integrity Check Value
ID	Identification
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineering
IMDs	Implantable Medical Devices
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IS	Information System
ISM	Industrial, Scientific and Medical
ISO	International Organisation for Standardisation
ISO/TC215	International Organisation for Standardisation/Technical Committee 215
ISP	Internet Service Provider
IV	Initialisation Vector (Used for Data Confidentiality)
KRACK	Key Reinstallation Attack
KSA	Key Scheduling Algorithm
LEA	Law Enforcement Agencies
LPU	Local Processing Unit
MAC	Medium Access Control
MAN	Metropolitan Area Network
MD5	Message Digest Version 5 (Hashing Algorithm)
MEDIX	Medical Data Interchange
MGEN	Multi-Generator (Application Used for Generating Network Traffic)
MIB	Medical Information Bus
MIC	Message Integrity Check
MIS	Management Information System
MITM	Man-in-the-Middle
MODEM	Modulator-Demodulator

MS-CHAPv2	Microsoft Challenge Handshake Authentication Protocol Version 2
NCPDP	National Council of Prescription Drug Programs
NHI	National Health Index
NIC	Network Interface Card
NTP	Network Time Protocol
OOK	On-Off Keying
OpenEMR	Open-source Electronic Health Records and Medical Practice Management Solution
OS	Operating System
OSI	Open System Interconnection
P2P	Peer-to-Peer
PACS	Picture Archiving and Communication Systems
PAN	Personal Area Network
PC	Personal Computer
PD	Patient Database
PDA	Personal Digital Assistant (Handheld Personal Computer)
PEAP	Protected Extensible Authentication Protocol
PHD	Personal Health Data
PHY	Physical Layer
PMK	Pairwise Master Key
PMSta	Patient Monitoring Station
POC	Point-of-Care
PPS	Packet per Second
PRTG	Passler Router Traffic Grapher (Network Monitoring Software)
PSK	Pre-Shared Key
PWR	Power
QoS	Quality of Service
RADIUS	Remote Authentication Dial in User Service
RAM	Random Access Memory
RAP	Rogue Access Point
RC4	Rivest Cipher 4 (Cryptographic Algorithm)
RF	Radio Frequency
RFID	Radio Frequency Identification
RFMON	Frequency Monitoring or Scanning
ROM	Read Only Memory
RSN	Robust Security Network

RTLS	Real-Time Location Systems
SCADA	Supervisory Control and Data Acquisition
SDR	Software Defined Radio
SN	Sensor Network
SNORT	Free and Open-source Network Intrusion Prevention System and Network Intrusion Detection System
SOHO	Small Office and Home Office
SPIN	Standard Prescriber Identification Number
SpO2	Peripheral Capillary Oxygen Saturation (an estimate amount of oxygen in the blood)
SRD	Short Range Device
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSN	Social Security Number
STA	Station or Device (may be a desktop, laptop or access point)
SW	Software
SYN	Synchronisation
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TKIP	Temporal Key Integrity Protocol
UbiMon	Ubiquitous Monitoring
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
UPIN	Universal Physician Identifier Number
USRP	Universal Software Radio Peripheral
VPN	Virtual Private Network
VTA	Vulnerabilities, Threats and Attacks
WAN	Wide Area Network
WAP	Wireless Access Point
WBAN	Wireless Body Area Network
WD	Wireless Drone
WEP	Wired Equivalent Privacy
WFRM	Wireless Forensic Readiness Model
WFS	Wireless Forensic Server
Wi-Fi	Wireless Fidelity or A Popular Wireless Networking Technology based on IEEE 802.11 Standards

WIPS	Wireless Intrusion Prevention System
WISE	Wireless Intelligent Sensor
WLAN	Wireless Local Area Network
WMS	Wireless Medical Network
WMedDs	Wireless Medical Devices
WMedSys	Wireless Medical System
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Areal Network
WPA-PSK	Wi-Fi Protected Access-Pre-Shared Key
WPA2	Wi-Fi Protected Access II
WPS	Wi-Fi Protected Setup
WS	Workstation
WSN	Wireless Sensor Network
WWAN	Wireless Wide Area Network
X73PHD	X73 Personal Health Data
XAMPP	Cross-Platform, Apache, MariaDB (Database), PHP, Perl (P)
XOR	Exclusive OR

List of Publications

Peer-reviewed Journal Articles & Book Chapter

Kyaw, A. K., Tian, Z., & Cusack, B. **(2020)**. Design and evaluation for forensic ready wireless medical systems. [***Accepted*** *for HealthyIoT 2019: Internet of Things Technology for Healthcare; To be published as part of the Lecture Notes of the Institute of Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST) book series by Springer in 2020.*]

Kyaw, A. K., Truong, H. P., & Joseph, J. (**2018**). Low-cost computing using Raspberry Pi 2 Model B. *Journal of Computers, 13*(3), 287-299.

Cusack, B., Tian, Z., & **Kyaw, A.K. (2017).** Identifying DoS and DDoS Attack Origin: IP traceback methods comparison and evaluation for IoT. In: Mitton, N., Chaouchi, H., Noel, T., Watteyne, T., Gabillon, A., Capolsini, P (Eds.), *Interoperability, Safety and Security in IoT* (pp. 127-138. InterIoT 2016, SaSeIoT 2016. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 190. Springer, Cham. doi: 10.1007/978-3-319-52727-7_14

Kyaw, A. K., Tian, Z., & Cusack, B. (**2016**). Wi-Pi: a study of WLAN security in Auckland City. *IJCSNS International Journal of Computer Science and Network Security, 16*(8), 68-80.

Refereed Conference Proceedings

Kyaw. A. K., Fernandez, S., Vasava, V., Truong, H. P., & Joseph. J. **(2019)**. Teaching network security through penetration testing using the experiential learning approach. In *Proceedings of the ISERD – International Conference on Education and E-Learning (ICEEL)*, February 24-25, 2019, Bali, Indonesia.

Cusack, B., & **Kyaw. A. K**. **(2018)**. Treating wireless medical system risks for usability and safety. In *Proceeding of the 2018 Cyber Forensic & Security International Conference*, August 21-23, 2018, Nuku'alofa, Kingdom of Tonga, pp. 265-276.

Kyaw, A. K., Agrawal, P., & Cusack, B. (**2016**). Wi-Pi: A study of WLAN security in Auckland CBD. In *Proceedings of the Australasian Computer Science Week Multiconference* (ACSW 2016). New York, United States of America: ACM.

Kyaw, A. K., Chen, Y., & Joseph, J. (**2015**). Pi-IDS: evaluation of open-source intrusion detection systems on Raspberry Pi 2. In *Proceedings of the 2nd International Conference on Information Security and Cyber Forensics (InfoSec2015)*, (pp. 165-170). United States of America: IEEE.

Kyaw, A. K., Sioquim, F., & Joseph, J. (**2015**). Dictionary attack on Wordpress: Security and forensic analysis. In *Proceedings of the 2nd International Conference on Information Security and Cyber Forensics (InfoSec2015)*, (pp. 158-164). United States of America: IEEE.

Kyaw, A. K., & Cusack, B. (**2014**). Security challenges in pervasive wireless medical systems and devices. In *Proceedings of the 11th International Conference on High-capacity Optical Networks and Emerging/Enabling Technologies (HONET-PfE 2014)*, (pp. 178 – 185). United States of America: IEEE.

Cusack, B., & **Kyaw, A. K**. (**2014**). Managing wireless security risks in medical services. In P. A. H. Williams (Ed.), *Proceedings of the 3rd Australian eHealth Informatics and Security Conference (AeHIS)*, (pp. 14-21). Perth, Western Australian: Security Research Centre (SECAU), Edith Cowan University.

Cusack, B., & **Kyaw, A. K**. (**2012**). Forensic readiness for wireless medical systems. In A. Woodward (Ed.), *Proceedings of the 10th Australian Digital Forensics Conference*, (pp. 21-32). Perth, Western Australia: SECAU – Security Research Centre, Edith Cowan University.

International Conference Presentations

Cusack, B., Tian, Z., & **Kyaw, A. K**. (**2016**). Identifying DoS and DDoS attack origins: IP traceback methods comparison and evaluation for IoT. Paper presented at *the 3rd EAI Conference on Safety and Security in Internet of Things*, October 26-27, 2016. Paris, France.

Kyaw, A. K., Agrawal, P., & Cusack, B. (**2016**). Wi-Pi: A study of WLAN security in Auckland CBD. Paper presented at *the Australasian Computer Science Week Multiconference* (ACSW 2016), February 2-5, 2016. Australian National University, Canberra, Australia.

Kyaw, A. K., & Cusack, B. **(2014)**. *Security challenges in pervasive wireless medical systems and devices*. Paper presented at the Proceedings of the 11th International Conference on High-capacity Optical Networks and Emerging/Enabling Technologies (HONET-PfE 2014), December 15-17, 2014. University of North Carolina, Charlotte: North Carolina, United States of America.

New Zealand Conference Paper

Shah, Z., Cosgrove, S., & **Kyaw, A. K**. (**2017**). *Investigating security and networking issues in the Internet of Things (IoT).* Abstract paper presented at the WelTec Whitireia Research Symposium 2017, Wellington, New Zealand.

International Journal/Conference Papers (to be submitted)

Kyaw, A. K., & Cusack, B. (2019). Compromising a wireless medical system with different attacks: An empirical study.

Kyaw, A. K., & Cusack, B. (2019). Digital forensic investigation: Evidential recovery in a compromised wireless medical system.

Chapter One

INTRODUCTION

1.0 INTRODUCTION

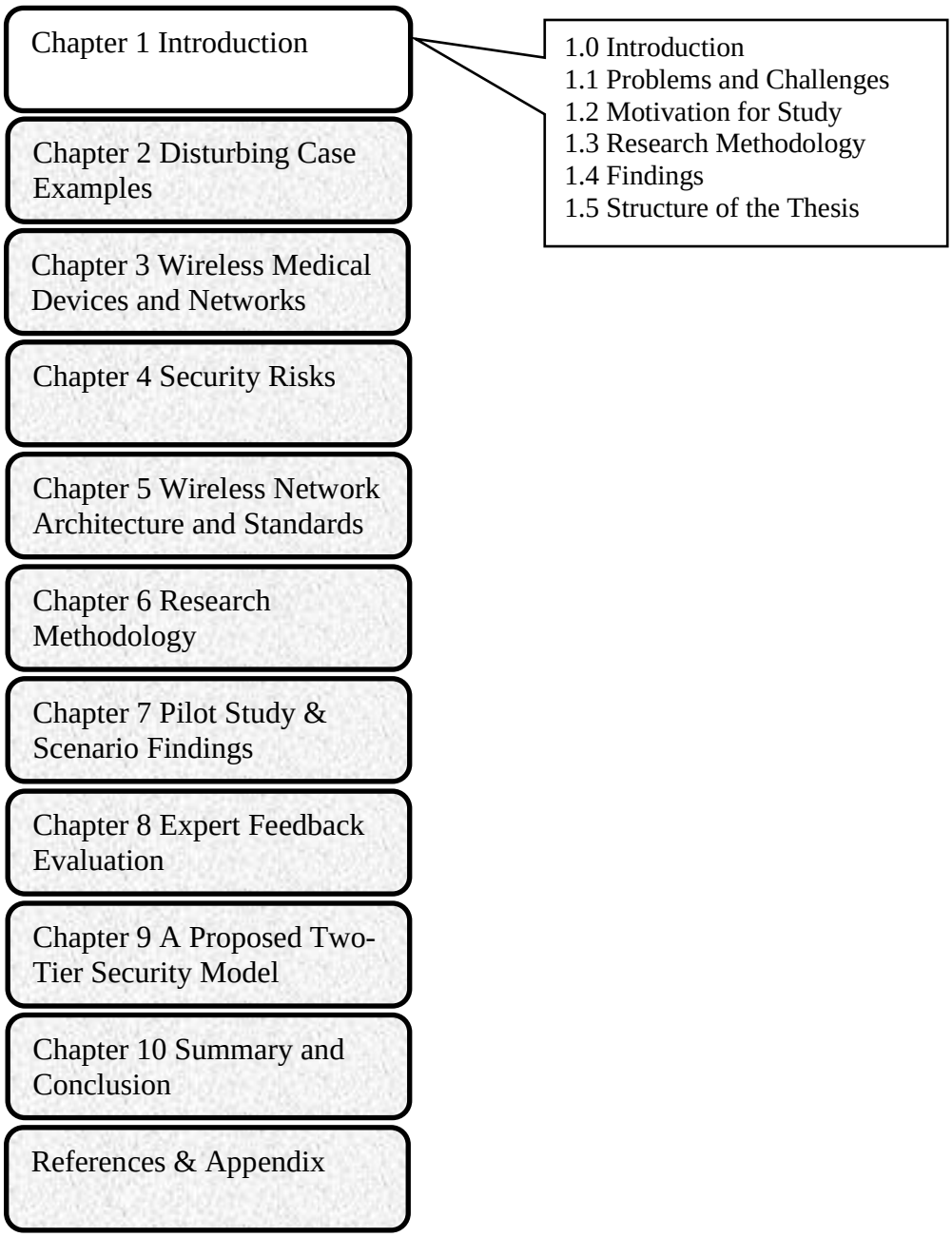


Figure 1.1: Roadmap of Chapter 1

Chapter 1 introduces the study and gives an overview of the plan and objectives. Section 1 overviews the problems and challenges faced when wireless technologies are introduced to medical environments. Section 2 elaborates the motivation for this study which is patient safety. Section 3 presents the design

science methodology, the entry level artefact, and the data collection requirements. Section 4 presents a brief review of the findings and the value of the improved artefact which is a framework for better security and forensic practice. Section 5 concludes the Introduction by outlining the structure of the thesis.

1.1 PROBLEMS AND CHALLENGES

The focus of this research is on the risks associated with wireless medical devices (WMedDs) in the medical healthcare environment. The deployment of wireless communications in a medical healthcare environment has been rapidly increasing to meet clinical requirements (Nita et al., 2011; Paquette, 2011; Topol, 2011). Many medical devices such as telemetry, pulse oximetry monitors, electrocardiography (ECG) carts, neuro-stimulators, infusion pumps, insulin pumps, pacemakers, implantable cardioverter defibrillators (ICD) and drug pumps use the wireless communication technologies for practical service advantages. The WMedDs allow mobility, continuous monitoring of users' health in the real-time, and other service advantages (Arney et al., 2011; Sagahyroon et al., 2011; Ren et al., 2010; Censi et al., 2010; Petković, 2009; Meingast et al., 2006).

However, the nature of wireless networking has inherited security and privacy problems that transfer at least theoretically to the medical healthcare industry (Hanna et al., 2011; Devaraj & Ezra, 2011; Censi et al., 2010). As a result of the growth in wireless network deployments, and device usage, the WMedDs have generated security vulnerabilities. Many have been reported where service functionality, incidents to patients, intentional exploitation, and other predictable compromise of the wireless devices and communication protocols, are elaborated in detail. For instance, Radcliffe (2011) has demonstrated hacking wirelessly in a commercially available insulin pump, which controls the insulin dosages for patients who have diabetes. Likewise, Halperin et al. (2008, p. 1) have performed a number of "*software radio-based attacks*" on implantable cardioverter defibrillators (ICDs). Such types of attack can compromise patient safety, patient privacy, and the expected benefits to be gained from the wireless systems. Hence, the risks and concerns being raised as researchable issues have been noted by others and cited as important risks to mitigate.

Currently, all level of policy and disciplinary protection is afforded to medical practices to manage risk, but deaths can still occur through the mis-use of IT systems. The security risk of WMedDs and WMedSys used in the medical healthcare sector have been established in the literature (Cagalaban & Kim, 2011; Gollakota et al., 2011; Arney et al., 2011; Hanna et al., 2011; Huang & Segal, 2011; Maisel & Kohno, 2010; Al Ameen et al., 2010; Denning et al., 2010; Saleem et al., 2010; Fu, 2009; Malasri & Wang, 2009; Denning et al., 2009; Zhang et al, 2003). Hence it is an area that requires further study and evaluation; and reconsideration in terms of material risk to intended beneficial health services. However, the current literature reviewed concerns preventing events occurring and yet the same literature identifies serious shortcoming for protection when using wireless networks and devices. Consequently, there needs to be post-event capability in the form of forensically ready preparations.

This study offers evaluation for the design of another layer of security protection for wireless medical systems and devices. The current literature is concerned with pre-event protection and has little on post-event protection. The literature supports the view that it is likely unintended events will occur more frequently in a wireless system than a wired system, and that the occurrence in a wireless system has a high probability. Post-event actions are generally termed as "*forensic investigations*" (Rowlingson, 2004). A design science approach is to be taken to design a more secure medical services system that includes both pre and post event protection.

1.2 MOTIVATION FOR STUDY

The reading of literature alerted me to serious problems arising from the rush to implement wireless medical systems (WMedSys) and the problems coming from easy access to the systems. Of course vendors were keen to sell their products and the medical community to use them because of the outstanding benefits provided. Then, however, more than mistakes and incorrect usage became apparent in press reports and academic research reports. Suspicious cases of irregular performance of implantable devices and the case of a patient in a Paris hospital suffering overdoses of insulin as the pump malfunctioned became news. Further investigation showed external influence in these cases that may have had a

malicious intent. The entertainment industry then picked up these stories and turned them into “who dunit” scripts. This meant TV had a series of CSI events based on malicious hacking of WMedDs and also movies began to include the concepts.

My motivation was to explore the factuality of these stories and to find by laboratory research evidence for or against. My initial attempts to obtain used hospital systems for research purposes was prevented by the lack of co-operation from the vendors. Several high profile vendors were approached formally and informally but they would not provide test equipment. They also viewed such research as being unhelpful because all their medical equipment was being produced under compliance conformance (for Health Insurance Portability and Accountability Act or HIPAA of 1996). However, I persisted and set up a test bed with simulated equipment as close as possible to the real context.

Principally my concern was to assure patient safety by providing knowledge and information to inform best security practices. To do this I had to extend the current literature knowledge base and do empirical testing and design formulation. This was achieved by identification, exploitation and mitigation. Most of the literature covered wireless security topics but only a small amount forensic mitigation. Hence, I focused on the forensic capability and the readiness of system for forensic investigation. My motivation was high as it was obvious little had been done in this area and a significant contribution could be made. I had a strong sense that patient wellbeing and protection could be improved by the design of effective forensic capabilities.

1.3 RESEARCH METHODOLOGY

A design science research methodology (DSRM) is adopted and customised as the most appropriate for a study that is at design level. The DSRM will deliver an improved security artefact that includes forensic capability. Peffers et al. (2007, p. 1) has “a commonly accepted framework for design science research (DSR)” by integrating “principles, practices, and procedures required to carry out DSR” in information systems. The process elements are based on peer review and are derived from previously published papers (Nunamaker et al., 1991; Walls et al.,

1992; Archer, 1984; Eekels & Roozenburg, 1991; Takeda et al., 1990; Rossi & Sein, 2003; Hevner et al., 2004; Peffers, 2007).

The first process of the DSRM is the "problem identification and motivation" as it is important to define the particular research problem that will be employed in the development of an artefact and effective solution. The second process of DSRM is to "define the objectives for a solution" from the definition of the problem and knowledge of its feasibility. The objectives should be deduced from the problem specification and they can be quantitative or qualitative. For instance, the quantitative objective can be "a desirable solution would be better than current ones" (Peffers et al., 2007, p. 55). Similar to the first process stage, the knowledge of the state of problems and current solutions, if any, and their efficacy are required as resources in the process stage. The third process is to "design and develop" the artefact, which can be "constructs, models, methods, or instantiations" or "new properties of technical, social or informational resources" (Jarvinen, 2007, p. 49 cited in Peffers et al., 2007, p. 55). According to Peffers et al. (2007), a conceptual design science (DS) artefact is an artefact in which a research contribution is embedded in the design. The architecture and desired or required functionality of the artefact is indispensable for creating the tangible artefact, and therefore the theory knowledge is an essential resource in a solution.

The fourth process is the "demonstration" of the artefact application in order to answer one or more cases of the problem by using "experimentation, simulation, case study, proof or other appropriate means" (Peffers et al., 2007, p. 55). Thus, the effective knowledge of utilising the artefact to answer the problem is an important resource in this process stage. The fifth process is the "evaluation", in which the artefact is assessed as to how well it provides a solution to the problem. The effectiveness and efficiency can be observed and measured by evaluating "the objectives of a solution to actual observed results from the use of an artefact in the demonstration" (Peffers et al., 2007, p. 56). The evaluation should be conceptually consistent with any suitable empirical or pragmatic evidence or plausible proof. After completing the evaluation process, the researchers can make a decision as to whether to iterate back to the third process phase "to try to improve the effectiveness of the artefact or to continue on to communication and leave further improvement to subsequent projects" (Peffers et

al., 2007, p. 56). The final process of the DSRM process model is the "communication" (Archer, 1984; Hevner et al., 2004; Peffers, 2007, p. 56). Thus, the problem, the significance of the problem, the artefact design, the utility and novelty, the rigour of the artefact design and its effectiveness should be communicated "to researchers and other relevant audiences such as practicing professionals, when appropriate" (Peffers et al., 2007, p. 56). Similarly, the outcome of DSR can be communicated in scholarly research publications.

The DSRM has four research entry points. These are: a problem-centred initiation, an objective-centred solution, a design-and-development-centred initiation and client-/context-initiated solution. Researchers can start their research from any entry point although the proposed DSRM process model is planned in a nominally sequential order (Peffers et al., 2007). In this research the vulnerability problem of WMedSys is taken as the starting entry point and the identification of previous designs the first artefact for improvement processes.

The research question that guides the investigation is:

"**What can be improved to make digital forensic investigation more effective in a wireless medical system?**"

Subsequently, several related secondary or subordinate (sub) questions are formulated in order to answer the main question.

Sub-Question 1: What are the potential risks (security and privacy) of current WMedDs and WMedSys?

Sub-Question 2: What are current protection mechanisms to mitigate security attacks related to a WMedSys?

Sub-Question 3: What are feasible protection mechanisms to improve the design of WMedDs to mitigate security attacks related to a WMedSys?

Sub-Question 4: What are the hardware and software required for the successful acquisition of Digital Evidence (DE) from a WMedSys?

1.4 FINDINGS

The deliverable from this research is an improved digital forensic readiness framework for use and implementation in WMedSys. It has been tested, costed and industry appraised so that it is ready for implementing in practice. It was also found that factual awareness of the vulnerability problem had been marginalised by all the hype and dramatisation of the problem. I am now hopeful it can be taken seriously again, and a working solution is presented. The continuous publications during the course of this Thesis research have also promoted awareness of solutions and gained credibility as a solvable research topic.

The evaluated artefact was further analysed in thematic groupings using NVIVO software. Thematic analysis is a commonly used approach in conducting qualitative data analysis in DS research. Qualitative methodologies aim to explore complex phenomena (Vaismoradi, Turunen, & Bondas, 2013). Vaismoradi et al. (2013) accept multiple realities and have a commitment to identifying an approach to in-depth understanding of the phenomena, a commitment to participants' viewpoints, conducting inquiries with the minimum disruption to the natural context of the phenomenon, and reporting findings in a literary style rich in participant commentaries. Thematic analysis is a process for encoding qualitative information (Boyatzis, 1998). This type of analysis looks mainly at "what and how" the data say and aims at identifying patterns within the data.

The main contribution of this research is to present a novel conceptual design for a DFR Framework which can be easily implemented and integrated to the existing wireless networks in the healthcare sector. Thematic expert evaluation analysis shows that the proposed artefact is efficient and effective in providing better security for patient's safety. The proposed artefact uses Pi-drones to collect any user's wireless attacks including successful, unsuccessful wireless login attempts to the WMedSys and forwards them to a centralised logging system in order to preserve digital forensic evidence. In addition, it provides low resource requirements, with cost-effective and customisation benefits by adapting free open-source software (See Appendix C financial analysis). Hence, it is suitable for additional security risk mitigation and better patient safety. Nevertheless, it also has several limitations. Although experts believe that the proposed framework is only designed for WMedSys in 2.4 GHz band, the proposed

framework can easily apply to both 2.4 GHz and 5GHz by replacing the hardware of the Pi-drone. For future work, the experts suggest that the proposed DFR Framework needs to be implemented and tested in a controlled medical environment to prove the functionality and reliability with big data sets.

1.5 STRUCTURE OF THESIS

The Thesis is structured to present a logical account of the completed research. First there is a formalities section that introduces a reader to the topic and a brief overview in the Abstract. To access the contents of the Thesis tables are provided and a definitions listed for all abbreviations used. The body of the Thesis is followed by the substantial list of references used, and Appendix that contain specific technical detail of the experimental and compliance work undertaken in testing. The content of each chapter is as follows:

- Chapter 1 provides an overview and introduction to the Thesis.
- Chapter 2 provides three case study reviews.
- Chapter 3 specifies wireless network and device features.
- Chapter 4 defines the security risks.
- Chapter 5 addresses related legislation and standards.
- Chapter 6 specifies the methodology used.
- Chapter 7 reports the Pilot Study and Scenario findings.
- Chapter 8 reports the expert feedback evaluation and improved artefact.
- Chapter 9 addresses the key issue of patient safety and propose a two-tier security model.
- Chapter 10 concludes the Thesis and lists topics for further research.

Chapter Two

DISTURBING CASE EXAMPLES

2.0 INTRODUCTION

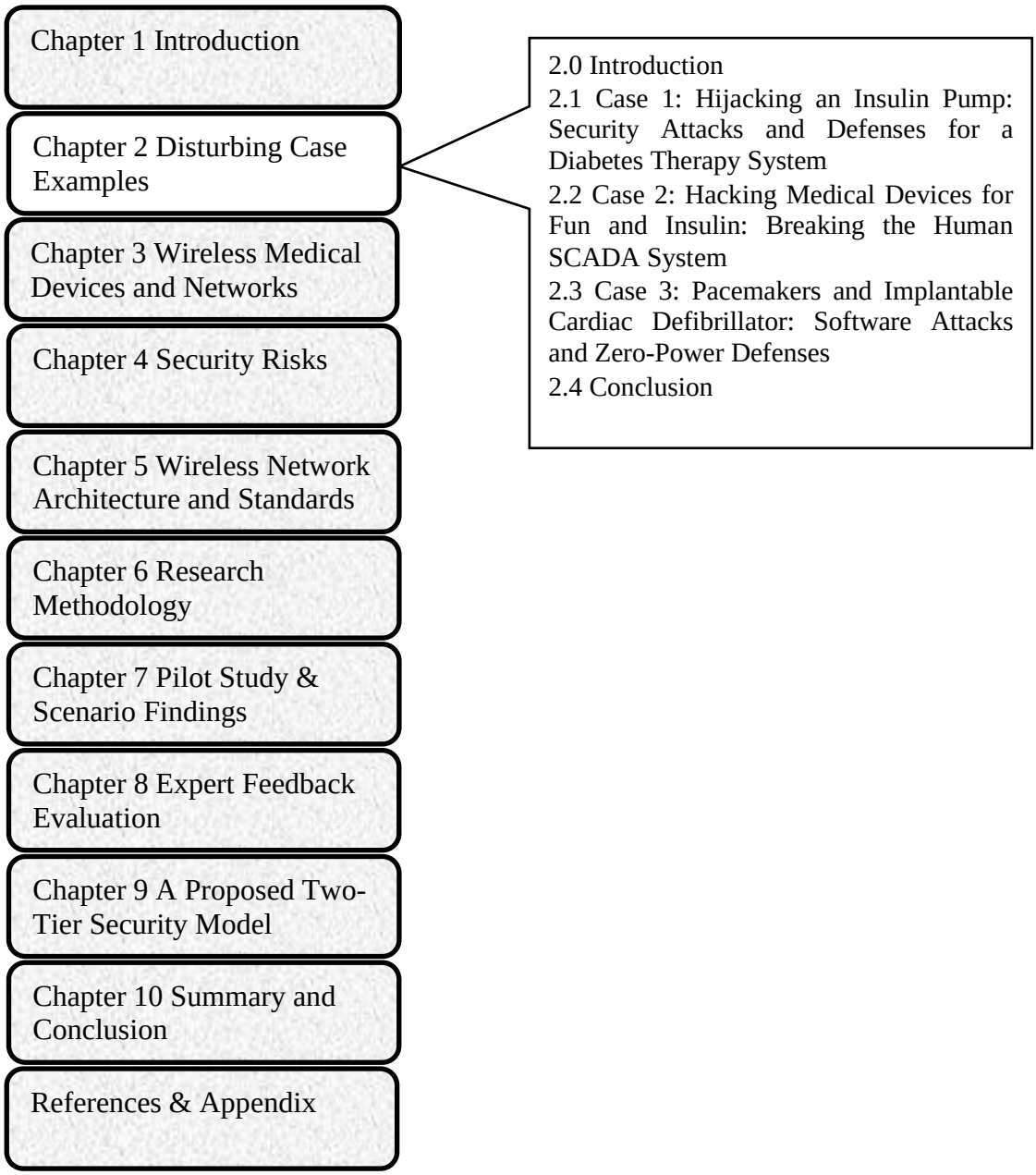


Figure 2.1: Roadmap of Chapter 2

Chapter 2 starts the substantial literature review required for this thesis by identifying disturbing failures in wireless medical systems. Each example is taken from public reports of vulnerabilities in the medical systems, and how the

vulnerabilities have been exploited. Patient safety is paramount but in these examples the medical implanted and support equipment is shown to be vulnerable to outsiders and to have unplanned consequences for well-being. .Hence, the literature review in this chapter reviews three cases that demonstrate risk and potential failure in WMedSys. These tangible concerns motivate the research, define the problem area, and present the challenges for research.

2.1 CASE 1: Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System

The research study was conducted by Li, Raghunathan and Jha (2011). According to the *national diabetes fact sheet* (Centers for Diseases Prevention and Control, 2007, cited in Li et al., 2011, p. 150), there were "*25.8 million people (8.3% of population) live with diabetes*" in the United States. Li et al. (2011, p.150) state that "*there were around 245,000 insulin pump users in 2005*" and the insulin pump market was "*expected to grow at a compound rate of 9% from 2009 to 2016*". Hence, the wireless-enabled continuous glucose monitoring and insulin delivery systems (CGMIDS) are currently being used for treating those patients with diabetes (Figure 2.2).

Figure 2.2: Insulin delivery system (Li et al., 2011, p. 152)

Even though such systems provide patients or users with “a better control over blood glucose levels” and “a better quality of life” (Li et al., 2011, p. 151), the wireless links are vulnerable to security attacks. Wireless enabled systems are well known for allowing security attacks by malicious computer users. However, the security attacks on wearable and implantable medical devices can be dangerous and have significant life-threatening or fatal consequences for patients.

As a result, the vulnerabilities of such personal healthcare systems require mitigation (Li et al., 2011, p. 150). The relevant questions are: "*what if incorrect blood glucose results are sent to the insulin pump wirelessly by malicious attackers*" and "*what if the attackers can control the insulin pump remotely and stop the required insulin injection, or inject insulin at a much higher dose than necessary*". As a proof of concept Li et al. (2011) successfully launched planned security attacks (both passive and active) on a wireless medical system (CGMIDS).

One of the components of a CGMIDS is the insulin pump that autonomously administers and supplies insulin in bolus and basal doses. According to the requirements, the patient or device user can programme its infusion time, rate and dosage. In order to "*offer greater convenience and control over blood glucose levels*", modern insulin pumps are usually equipped with four programming and communication interfaces (as shown in Figure 2.2) such as "*buttons on the pump itself*", "*wireless connection to a remote control*", "*wireless connection to a computer, used to upload data and/or manage the programming*" and "*wireless connection to a blood glucose monitor*" (Li et al., 2011, p. 151). However, these wireless links are vulnerable to malicious attacks that can affect the confidentiality, integrity and availability of the insulin delivery system. However, when correctly used it can deliver a better quality of life for patients.

The research report goes in detail to explain the components used in the descriptive experimental method that was used to perform passive and active attacks on a commercial insulin delivery system. The components (Li et al., 2011, p. 152) such as "*a glucose meter, an insulin pump, a remote control, and a Universal Software Radio Peripheral (USRP)*" were used for experimental setup. Hence, the frequency used by medical device under experiment was determined by checking its Federal Communications Commission (FCC) identification. Then, "*a 915 MHz daughter board and antenna were attached to the USRP board*" to intercept and produce the frequency of 915 MHz for communication between the insulin pump and the remote control (Figure 2.3). The modulated wireless signal was intercepted and down-converted to the baseband in order to find the *on-off* key used in the communication (Li et al., 2011).

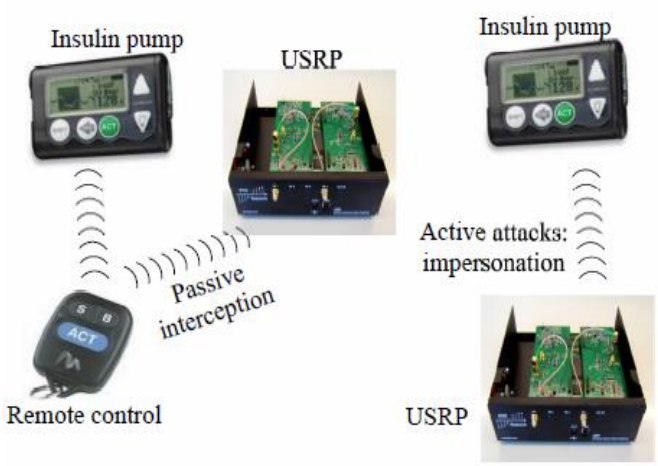


Figure 2.3: Security attacks on an insulin delivery system (Li et al., 2011, p. 152)

For an insulin pump to receive data or accept control commands, the six digits or PIN number (*printed on the back of glucose meter or remote control*) has to be manually entered by the CGMIDS users. Hence, the researchers (Li et al., 2011, pp. 152-153) intercepted the *plaintext* data from remote control to the glucose meter after entering the PIN and were able to get access and to analyse the format of 80-bits communication packet (Figure 2.4) used in the *insulin delivery system* as soon as the sequence of *on* and *off* bits were synchronised. The 80-bit communication packet comprises the first 40-bit representing the device type and PIN. Likewise, the last 40-bit contains the payload *information*, *counter*, *cyclic redundancy check* (CRC) and packet trailer (4 bits).

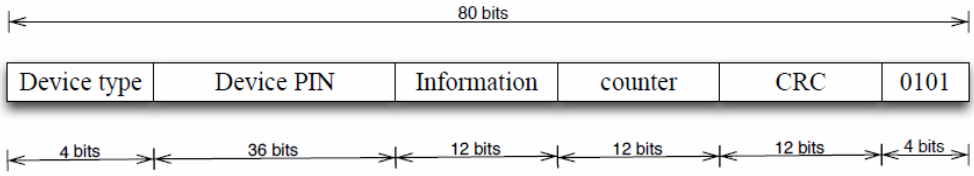


Figure 2.4: Format of the communication packet (Li et al., 2011, p. 153)

The first 40-bits of the packet can be decoded during the experiment, but deciphering the last 40-bits is not a simple task. In fact, the deciphering a 36-bit PIN can be performed by mappings between the *information* bits and the corresponding hexadecimal digits (Li et al., 2011). Similarly, the authors mentioned that the 12-bit *counter* could be found after the signal pattern repeated 256 counts and parameters for CRC calculation (Table 2.1) could be obtained after several experiments were completed. Hence, the CRC parameters are required to perform a replay attack or to reproduce "*a legitimate packet that will be accepted by the insulin pump*" (Li et al., 2011, p. 153). However, the authors

did not disclose some of the CRC parameters (CRC polynomial and final XOR values) due to security reasons and replaced the symbols with "***x***". Moreover, the researchers did not validate the communication protocol format between the insulin pump and glucose monitor, although the format of communication packet between the remote control and glucose meter was successfully parsed in the research.

Table 2.1: CRC parameters for the remote control and glucose meter (Li et al., 2011, p. 153)

Parameters	Remote Control	Glucose Metre
CRC order	8	8
CRC polynomial	*x*	*x*
Initial value	0	0
Final XOR value	*x*	*x*
Reverse data bytes	N	N
Reverse CRC	N	N

Li et al. (2011, pp. 153-154) classified potential attacks into two categories as "*attacks without the knowledge of the device PIN*" and "*attacks with the knowledge of the device PIN*". Such attacks could compromise the privacy of patients, data integrity and availability. Furthermore, the authors (Li et al., 2011, 154) documented the ways in which the medical device PIN could be obtained through "*peeking at the printed PIN*" and "*insider information from the device manufacturing or supply chain*", instead of eavesdropping on the wireless communication links.

In the research, the attack experiments were first initiated by determining the maximum distance (*4.5 metres*) from where the insulin pump could be programmed by the remote control. Then, the passive eavesdropping attack was conducted when the remote control was communicating with the insulin pump within *7-8 meters* (without having any obstacle between the devices). The "*device type, device PIN and control command sent to the insulin pump*" were successfully extracted (Li et al., 2011, p. 154). Subsequently, an active attack was performed by using an off-the-shelf USRP device and PIN (extracted by eavesdropping in a passive attack) to control the pump with unauthenticated commands. Unlike a passive attack, the active attack could be carried out from *20 meters* away to manipulate the injection of insulin to the patient (Li et al., 2011). Afterwards, the authors discussed two possible countermeasures against such

security attacks. One of the proposed countermeasures (Li et al., 2011, p. 154) is applying rolling code base cryptography (used in current security protocols in automobile keyless entry) to the insulin delivery system (Figures 2.5a and 2.5b). The purpose of applying the proposed cryptographic method is to protect the extraction of medical device's PIN from eavesdropping wireless links and replay attacks. The transmitted information can be encrypted, and the rolling code can be changed every time (Li et al., 2011). However, the authors did not implement or verify the proposed cryptographic method in this article.

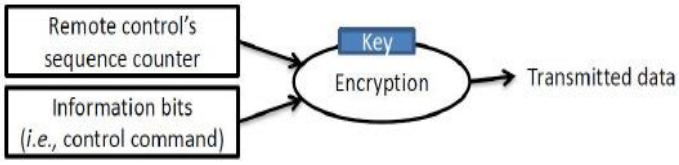


Figure 2.5a: Proposed rolling code encoder in the remote control (Li et al., 2011, p. 154)

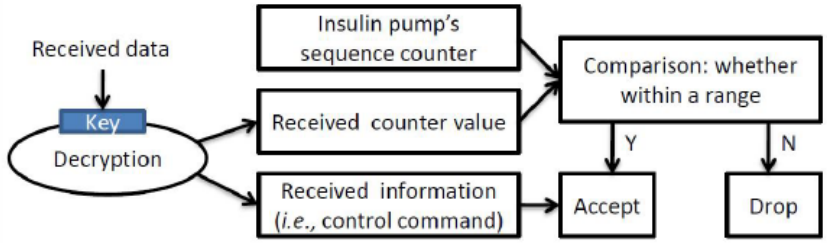


Figure 2.5b: Proposed rolling code decoder in the insulin pump (Li et al., 2011, p. 154)

The second proposed countermeasure (Li et al., 2011, p. 155) against the previously demonstrated attacks is the use of "*human body as the transmission medium to enable wireless communication, referred to as body-coupled communication (BCC)*" in CGMIDS. BCC can prevent interference and consume less power due to the data communications happening within a close vicinity of the patient's body when the insulin pump and the glucose meter are attached directly to the patient for monitoring and insulin injection. The authors (Li et al., 2011, pp. 155-156) conducted BCC experiments by using a *function generator* and *USRP* as a transmitter and a receiver respectively along with the *electrodes* and *mid-wave/short-wave active antenna* to lessen the security attack problems. Further attack experiments are required to be performed on each device to verify whether BCC is possible to enhance the security.

This article and case study identified vulnerabilities and successfully launched security attacks (both passive and active) on a wireless glucose

monitoring and insulin delivery system to demonstrate such attacks could destabilise the operation of a system and jeopardise the patient's life. Furthermore, Li et al. (2011, pp. 154-156) proposed two feasible protection mechanisms, "*the use of rolling code-based encryption*" and "*the concept of BCC*" to mitigate security attacks related to personal health systems.

2.2 CASE 2: Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System

This paper was presented at the *"Black Hat Security Conference in the United States of America"* in 2011. The research was motivated by the author attending a presentation related to the hacking on a smart parking meter at Defcon 2009 conference and "*researching the Stuxnet malwar*e" in his professional job (Radcliffe, 2011, p.2).

The author (Radcliffe, 2011, p. 1) stated that more flexibility, "*better control over insulin delivery*" and "*more data can be captured to help make better decisions for treatment*", were the main advantages of using the wireless-enabled insulin pump, and the continuous glucose monitor (GCM). Furthermore, Radcliffe (2011, p. 2) observed the way in which "*regulating blood sugar to insulin ration*" is similar to the *Supervisory Control and Data Acquisition* (*SCADA* temperature control) system in a chemical plant that "*has a tank of liquid or gas that needs to keep at a stable elevated temperature*". Patients with diabetes need to maintain blood sugar (glucose) within a specified range of 90-120 milligram/decilitre. Otherwise, the excessive amount or dangerously low level of glucose can initiate hyperglycaemia and hypoglycaemia, correspondingly. The author subsequently explained a *Stuxnet* problem that was speculated in such a way that "*malware payload manipulated how fast a centrifuge would spin, ultimately causing them to spin faster than they were designed to go and destroying them*" (Radcliffe, 2011, p. 2). Analogous to *Stuxnet*, the incorrectly reported glucose level manipulated by a malicious programme or attacker could potentially lead to hypoglycaemia. Hence, the hypoglycaemia is a serious problem with a low glucose level if the insulin dosage is high or too low, and it can possibly lead patients to "*coma and death if left untreated*" (Radcliffe, 2011, p. 2).

In this descriptive research, Radcliffe (2011, p. 3) firstly initiated the experiment as a *penetration test* by conducting *reconnaissance* to gather data

relating to an "*insulin pump and CGM devices*" from user manuals. After examining the user manuals, the researcher (Radcliffe, 2011, p. 3) obtained the precise frequencies and modulation methods used by "*insulin pump (916MHZ On-Off Keying, i.e. referred to as OOK)*" and "*CGM (402.142 MHz On-Off Keying)*". Similarly, the researcher performed data gathering from the FCC website by using the medical device's unique identification (ID) number and the patent office's website by using the name of the medical device manufacturer. Hence, FCC information provided the researcher (Radcliffe, 2011, p. 3) the transmission analysis of wireless devices in detail "*including screen captures from spectrum analysers and oscilloscopes*". Likewise, the information from patent documents using the devices, presented the researcher with how the devices were built and functioned (Radcliffe, 2011, p. 3). Therefore, the information gathered from different available sources facilitated finding suitable equipment operating in the same frequencies as the insulin pump and CGM devices for the research experiment.

Secondly, the radio frequency (RF)/wireless module was compromised by an Arduino. One of the reasons why the Arduino RF module was selected for this research was that it utilised the "*CC1101 wireless chip that operates on the 315/433/868/915 MHz Industrial, Scientific and Medical (ISM)/Short Range Device (SRD) bands*" (Radcliffe, 2011, p. 4). Hence, the operating frequencies of the RF module were closely matched with the medical devices under testing. Thirdly, the author stated the configuration of the CC1101 module operated in the same frequency with the OOK modulation method as those of the medical devices targeted, but it is challenging to get the required information from the CC1101 manual. However, the OOK is very close to "*ham radio communication format, Morse code or continuous wave modulation*" and it can easily be analysed by using "*an oscilloscope or logic analyser*" to record the signal into a binary stream (Radcliffe, 2011, p. 4). Afterwards, the problem with understanding of *Preamble* and *Sync Word* parameters settings used in the CC1101 was acknowledged as there was no information related to those two parameter settings in the documentation. *Preamble* is in the length of "*2 to 32 bytes*", and *Sync Word* is ranging from "*8 to 32 bytes*" of predetermined high and low words in hexadecimal format (Radcliffe, 2011). The purpose of *Preamble* is to let the receiving device

acknowledge that a transmission can be easily distinguished. Similarly, the purpose of *Sync Word* is to verify that the transmission from CC1101 is in a standard format and to inform the receiving end that "*the transmission is from a known transmitter*" (Radcliffe, 2011, p. 4). Hence, the author solved the problem with an understanding of *Preamble* and *Sync Word* after finding out the data sheet of RF chip used by the receiver unit of the CGM system.

Furthermore, configuring the CC1101 RF module into "*Direct Mode or Serial Mode*" by using two pins (one for data and the other for clock signal) allowed Radcliffe (2011, p. 5) to manually decipher the transmitted data. With regard to the CGM, some of the known features such as the small packet size of 76 bits, the data transmission rate ("*once every five minutes*") and a unique identifier ("*5 characters*") of the transmitter were discussed (Radcliffe, 2011, p. 6). Then, the author explained that the unique identifier could be extracted from the consistent portion of each data stream. However, the insulin pump under experiment required logging of the data set to "HIGH" instead of "NONE" to get detail "*message information and responses with the device*" (Radcliffe, 2011, p. 7). Information regarding how the transmitted data was encoded, what the format of the message was, and the insulin pump's command codes were obtained from the Java library files (Radcliffe, 2011).

In addition, the security concerned with the CGM and the insulin pump was defined. For instance, a traditional computer attack, such as replay attack are feasible against the medical devices. Similarly, eavesdropping or spoofing of the transmitted signal between devices to find out the serial number or unique identifier of a CGM could easily be performed by malicious attackers if the format of the message and method of encoding were known (Radcliffe, 2011). On the other hand, the serial number of the insulin pump could also be obtained by using a social engineering attack even though the pump has little problem with passive eavesdropping attacks. Likewise, falsifying or manipulating the glucose level is possible by using replay attacks when the transmitted data format was unknown. However, there are some factors that make the replay attack against CGM difficult. The factors (Radcliffe, 2011, p. 8) such as the transmission range ("*within 100 to 200 feet from the CGM device*"), calibration measurement prompt to the patient or device user ("*normally done with a blood glucose meter*"), and

taking a longer time or hours to manipulate the sensor data, could actually mitigate the possibility of a successful attack against a CGM device.

With the insulin pump attack, Radcliffe (2011, p. 8) stated that the "*unknown manipulation of configuration settings*" on the insulin pump could threaten patients' lives. Additionally, the theoretically defined attacks can be performed with the use of wireless radio peripherals communicating with the insulin pump. Also, the command codes and message format of the insulin pump can easily be found on the Internet, as such information is published on different websites, although the manufacturer does not release it directly (Radcliffe, 2011). Nevertheless, attack limitations mentioned in this article include "*the range on an insulin pump's wireless ability*" and the way in which "*acquiring the serial number of the insulin pump target*" (Radcliffe, 2011, p. 8). These limitations can limit the possibility of an attack and hence it is feasible to mitigate impacts.

Finally, the author discussed future research direction and challenges. Radcliffe (2011) stated that more research needed to be done in order to protect WMedDs and related data. The purpose of the research was to disclose and verify the vulnerabilities of WMedDs. Even though the data manipulating attack (active) against the author's CGM and insulin pump is not practically demonstrated in this research, the author explains how to gather information and collect necessary hardware devices to initiate successful passive attacks against WMedDs.

2.3 CASE 3: Pacemakers and Implantable Cardiac Defibrillator: Software Radio Attacks and Zero-Power Defenses

Halperin et al. (2008) conducted a research experiment to evaluate the characteristics of security and privacy of an implantable cardioverter defibrillator (ICD) in the article "*Pacemaker and Implantable Cardiac Defibrillator: Software Radio Attacks and Zero-Power Defenses*". According to the study of Food and Drug Administration (FDA) annual reports on *Pacemaker and ICD generator malfunctions* (Maisel et al., 2006, cited in Halperin et al., 2008, p. 1), there were "*over 2.6 million*" patients implanted with pacemakers and ICDs in the United States between 1990 and 2002. These wireless-enabled implantable medical devices (examples: *pacemakers, ICDs, neurostimulators, implantable drug pumps*) are generally used for monitoring and treating patients with chronic diseases by applying automatic therapies (Halperin et al., 2008). Although there are the

benefits, such as improvements in quality and life-saving opportunities for patients' by using such implantable medical devices (IMDs), vulnerabilities to malicious attacks still exist. Hence, the researchers (Halperin et al., 2008, pp. 1-2) performed software radio attacks that "*changes the operation of (and the information contained in) the ICD*" and presented "*prototype defences against the attacks*".

In this descriptive research, the researchers initially found the contributions of the research by evaluating the security and privacy of an ICD and stressed the device by using different types of security attacks to compromise *privacy, integrity and availability* (see Table 2.2). The key distributions (Halperin et al., 2008, p. 1) provided "*a scientific baseline for understanding the potential security and privacy risks of current and future IMDs*". They also introduced "*human-perceptible and zero-power mitigation techniques*". The attack experiments were initiated by using a software radio and *an ICD programmer* to present the ways in which an ICD could be exploited. By applying numerous eavesdropping and reverse engineering techniques to intercept and understand the wireless communication between an ICD and its programmer, the researchers (Halperin et al., 2008, pp. 2-4) successfully extracted "*patient information (such as name and diagnosis) and medical telemetry (information about vital signs)*".

Table 2.2: Results of experimental attacks and a check mark indicates a successful attack (Halperin et al., 2008, p. 3)

	Commercial programmer	Software radio eavesdropper	Software radio programmer	Primary risk
Determine whether patient has an ICD	✔	✔	✔	Privacy
Determine what kind of ICD patient has	✔	✔	✔	Privacy
Determine ID (serial #) of ICD	✔	✔	✔	Privacy
Obtain private telemetry data from ICD	✔	✔	✔	Privacy
Obtain private information about patient history	✔	✔	✔	Privacy
Determine identity (name, etc.) of patient	✔	✔	✔	Privacy
Change device settings	✔		✔	Integrity
Change or disable therapies	✔		✔	Integrity
Deliver command shock	✔		✔	Integrity

2.4 CONCLUSION

These three cases have shown the vulnerability of wireless medical systems from other people's research reports. Their experiments have exposed vulnerabilities and mitigating features in current architectures that impact patient health and safety. These are disturbing cases and motivation for further technical study and

solution development. Chapter 3 will now summarise specific applications that rely on wireless connections in the medical environment in order to assess the technical scope of the problem area.

Chapter Three

WIRELESS MEDICAL DEVICES AND NETWORKS

3.0 INTRODUCTION

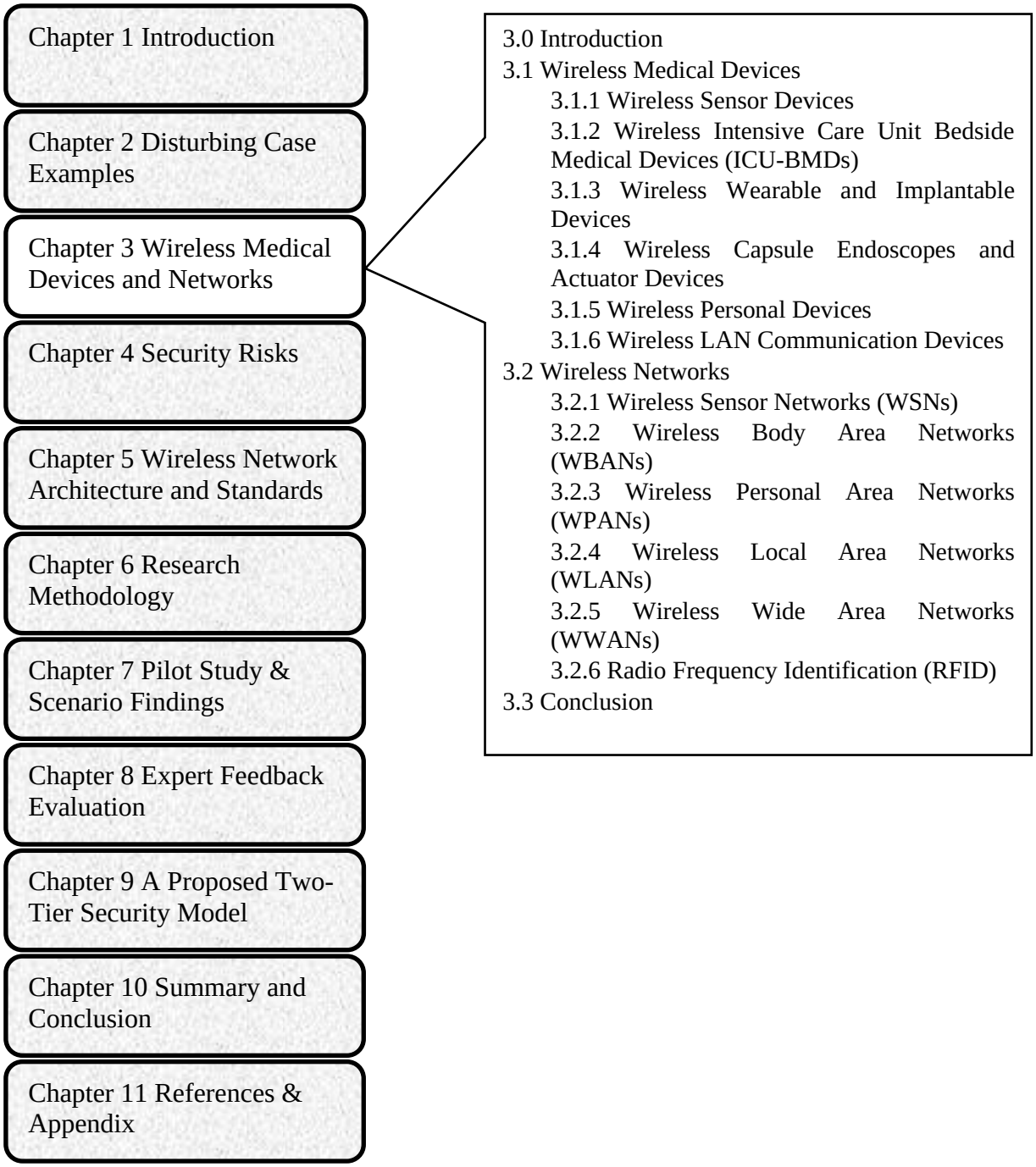


Figure 3.1: Roadmap of Chapter 3

Chapter 2 has elaborated three disturbing cases where the dangers of wireless medical systems were made apparent. Chapter 3 will now focus on specific

medical applications that rely on wireless connections for their services. The chapter is divided into two parts for devices, and network specifications. These map a scope for the problem area and expose technical designs that may be improved for better security.

3.1 WIRELESS MEDICAL DEVICES

Wireless medical networks have been rapidly deployed in the medical healthcare industry due to continuous reduction in the size of wireless electronic devices, and the industry demand. Similarly, the extensive use of wireless technology in various application areas (including healthcare) is due to *the proliferation of wireless devices and wireless networks* in the past decade (Rong & Cayirci, 2009, p. 169). As previously stated in Section 2.2, a wireless medical network (for instance: WBAN) is made up of "*small and intelligent devices attached on or implanted in the body*", which are able to "*provide continuous health monitoring and real-time feedback to the user and medical personnel*" (Latré et al., 2010, p. 1). These devices are generally classified into two types: sensors and actuators. Hence, the different type of wireless devices used in a WMedSys are reviewed in the following sub-sections.

3.1.1 Wireless Sensor Devices

A wireless sensor node is an electronic device that can be employed for monitoring or measuring particular physiological activities of the user. For instance, monitoring the heartbeat or prolonged electrocardiogram (ECG), and measuring body temperature, can be accomplished by using a wireless sensor node (Latré et al., 2010). A wireless sensor node (Figure 3.2) is made up of several components including "*sensor hardware, a power unit, a processor, memory and a transmitter or transceiver*" (Alyildiz et al., 2002, cited in Latré et al., 2010, p. 3). Wireless sensors are developed by many different companies and are enabled to monitor environmental or physical conditions such as pressure, temperature and so on. For instance, the medical research in the United States has been using "*MicroStrain* sensors (also referred to as *StrainLink;* see Figure 3.3) to not only develop better and more durable artificial joints by embedding the sensors within orthopaedic devices, but also monitor stress levels of the joint within patients' bodies" (The National Science Foundation, 2012, p. 1).

Likewise, a low power wireless intelligent sensor (*WISE*) device developed by Jovanov et al. (2001) can be used to monitor physiological signals (heart rate, breathing and movement) of the patient in a healthcare environment. However, these battery powered wireless sensors devices have limited resources in computational power and memory (e.g. 60KB of flash memory and 2 KB of RAM in the *WISE* device).

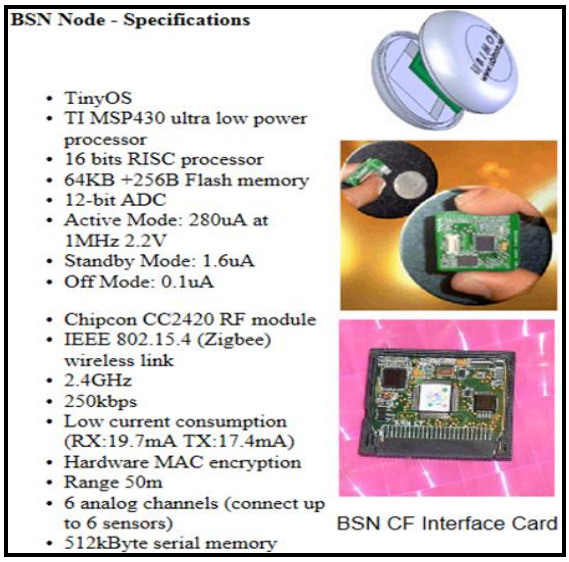


Figure 3.2: BSN node specification (Imperial College London, 2004, p. 1)

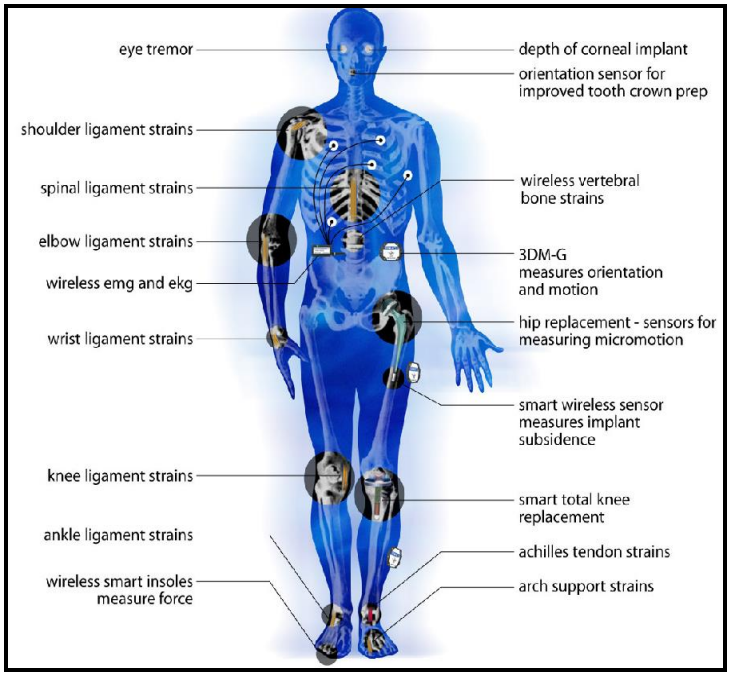


Figure 3.3: Potential uses of sensors in medicine (MicroStrain cited in the National Science Foundation, 2012, p. 1)

According to Eren (2006, p. 181), all of these wireless sensor devices such as "*integrated circuit (IC) sensors, web sensors, intelligent sensors, wireless sensors* typically operate either in licensed or unlicensed industrial, scientific and medical (ISM) bands.

3.1.2 Wireless Intensive Care Unit Bedside Medical Devices (ICU-BMDs)

Friedman, Halpern and Fackler (2007) mention that diverse medical bedside devices such as ventilators, physiological monitors, RFID tags and infusion pumps (Figure 3.4) in hospital intensive care units can now be connected to the patient, network servers and eventually to the electronic medical records (EMR) as a result of development in wireless communications technology.

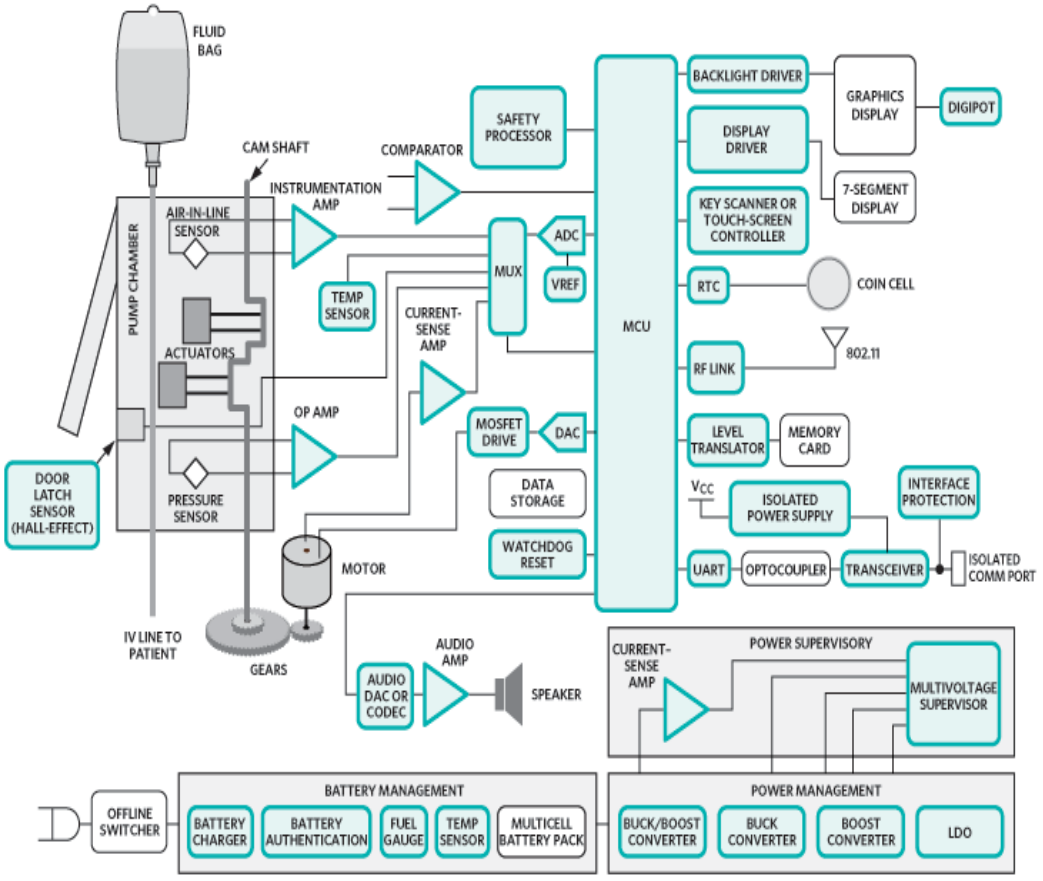


Figure 3.4: Block diagram of Maxim Wireless Infusion Pump (Maxim Integrated, 2013, p. 1)

However, it is significant the wireless coverage and communication must be guaranteed in addition to the deploying of a secure wireless hospital network for effective use. Thus, nurses who use medication computer-on-wheels (COWs) can

record administered doses and doctors or physicians who use tablets or PDAs can enter updated patient information at the bedside (Friedman et al., 2007).

3.1.3 Wireless Wearable and Implantable Devices

Wireless wearable medical devices (WWMDs) are used to monitor physiological parameters of patients with chronic deceases (Table 3.1). Similarly, Denning et al. (2010) states that implantable medical devices (IMDs) are electronic devices used for treating patients with abnormal physiological conditions within the body. Hansen and Hansen (2010, p. 13) describe "*an IMD as permanently or semi-permanently implanted into a patient which treats some underlying medical condition, enhances the function or appearance of some part of the body, or provides a previously unrealised ability*". One of the obvious benefits of using the new generation of IMDs is that doctors or consultants can not only monitor patients, but also provide treatments remotely or autonomously (Hansen & Hansen, 2010). However, there are always risks associated with the benefits of using such WMedDs. For instance, an unauthorised person or a malicious attacker can remotely intercept wireless communications and compromise the medical device. Hence, various IMDs have potential adverse failures that can result in patient heart failure, blindness, and possibly death.

Table 3.1: Some chronic diseases, physiological parameters that are of clinical importance and possible sensors that can be used to observe them (Atallah et al., 2011, p. 4)

Disease	Physiological parameters	Possible sensors
COPD	Respiration, heart rate Oxygen saturation and activity levels	Wearable heart rate/respiration sensors Accelerometers
Parkinson's disease	Gait, muscle tone, activity	Accelerometers, optical/vision sensors Gyroscopes
Hypertension	Blood pressure/activity	Wearable blood pressure sensor Accelerometers
Cancer	Weight loss, activity, behaviour patterns	Accelerometers, gyroscopes Weight sensors
Arthritis	Gait patterns, temperature, stiffness	Accelerometers, optical/vision sensors Gyroscopes
Diabetes	Gait patterns, visual and sensory impairment	Accelerometers, vision, glucose monitors Gyroscopes
Cardiac arrhythmia	Heart rate, ECG	ECG sensors
Heart failure	Blood pressure	Heart rate and blood pressure sensors

3.1.4 Wireless Capsule Endoscopes and Actuator Devices

Olympus Medical Systems Inc developed swallowable wireless video endoscope capsules (Kusuda, 2005). The capsules are very tiny illuminating devices for observing "*the gastrointestinal tract images and transmitting them through wirelessly to the external image receiving device*" (Kusuda, 2005, p. 259).

Wireless actuators are used for taking some precise actions with respect to the data received through interaction with the user or the sensors. For example, a continuous glucose monitoring system that includes "*an actuator equipped with a built-in reservoir and pump*" can give an accurate dosage of insulin to a patient who has diabetes according to the glucose level measurements (Latré et al., 2010, p. 2). The components of an actuator are the same as that of a sensor node, except the actuator hardware has a reservoir to hold medicine for administering medicine.

3.1.5 Wireless Personal Devices

A wireless personal device or a sink node is an electronic device that can collect all the data acquired by the sensors and actuators (Latré et al., 2010). Hence, these sensors and actuator devices communicate with other persons or medical doctors and nurses via sink nodes (e.g. a smartphones or PDAs). The adoption of handheld computers or PDAs in healthcare has been reviewed in previous literature (Lu et al., 2005, p. 409). Most of the healthcare providers use wireless personal devices like PDAs or smartphones "*to be functional and useful in areas of documentation, medical reference and access to patient data*", even though there are obstacles (such as security concerns) to the adoption of wireless personal devices in healthcare.

3.1.6 Wireless LAN Communication Devices

Wireless modems (MOdulators-DEModulators) or radio frequency (RF) transceivers are ubiquitous devices that are capable of transmitting and receiving data through electromagnetic waves (Eren, 2006). In order to enable wireless network connectivity, these modem devices are generally connected to wireless access points (WAPs) as shown in Figure 3.5. Wireless modems can be classified by the use of frequency bands (for example: 900 MHz, 2.4 GHz, 5 GHz, VHF, UHF and so on) and radio communication techniques such as direct sequence

spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). Likewise, the form factors of these devices can be categorised into internal and external modems. The former devices are usually attached in motherboards' slots and the latter devices are connected to communication ports of computers (Eren, 2006).

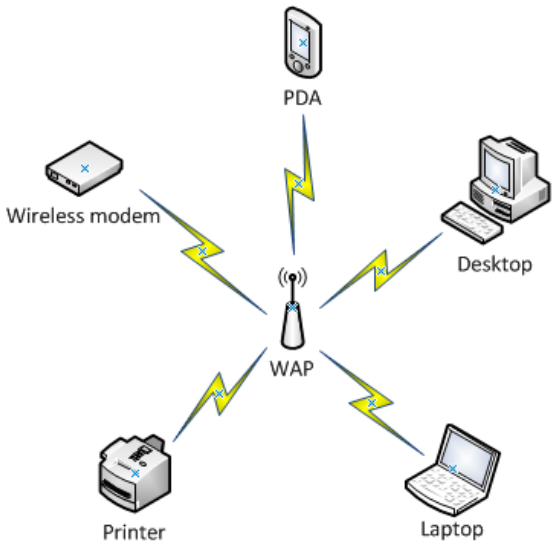


Figure 3.5: Wireless devices associated with a wireless access point

3.2 WIRELESS NETWORKS

Wireless technologies enable the electronic devices to interconnect and communicate without having the need of physical wired cabling by using radio frequency transmissions (Karygiannis & Owens, 2002). As a result of advancement in wireless technologies, the prevalent adoptions of wireless networks offer numerous benefits to users and organisations (Turab et al., 2010). For instance, the deployments of wireless sensor networks (WSNs), wireless personal area networks (WPANs), wireless local area networks (WLANs), wireless body area networks (WBANs) in the industries of healthcare, retail, education and entertainment have not only offered the significant enrichment in quality of life, but also allowed the improvement in mobility and productivity (Yuce & Khan, 2012; Darwish & Hassanien, 2011; Turab et al., 2010). However, the nature of wireless network also exposes the users to potential threats and

attacks (Ngobeni et al., 2010). The following sub-sections will now focus onto different types of wireless medical networks.

There are many different types of wireless networks being deployed in residential, commercial and healthcare areas. According to the Cellular Telecommunications Industry Association (CTIA), *"the wireless health market is expected to grow 4.4 billion in 2013"* (MobiHealthNews, 2009, p.2).

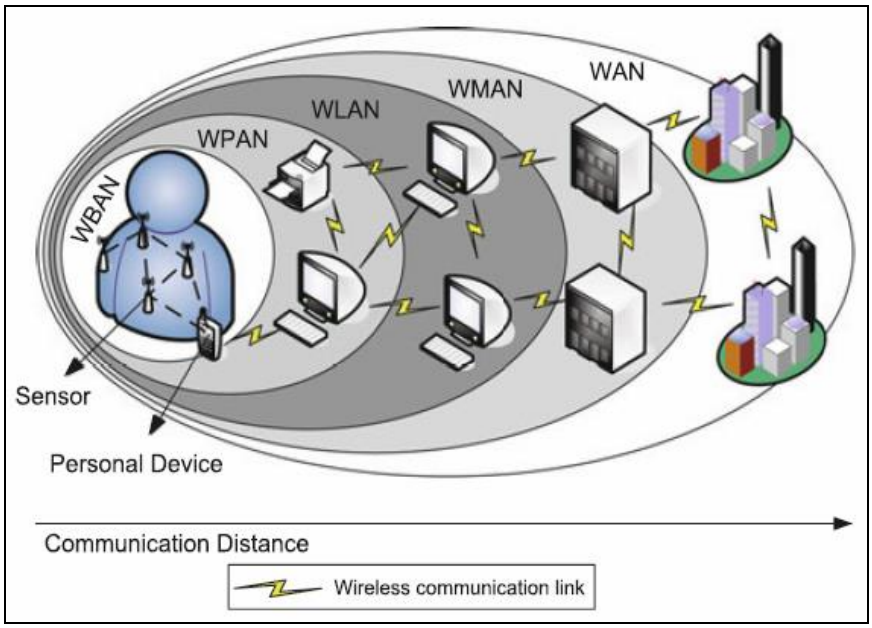


Figure 3.6: Positioning of a WBAN in the the realm of wireless networks (Latré et al., 2011, p. 6)

Likewise, the revenue from worldwide sales of Wi-Fi (Wireless Fidelity) enabled health products including WMedDs are estimated to reach approximately *"$5 billion in 2014"* (ABI Research, 2009, cited in MobiHealthNews, 2009, p.2). Apparently, the wireless health market is rapidly growing. Even though different types of wireless networks (see Figure 3.6) based technologies are being used in the medical or healthcare industry, the following sub-sections explain a brief explanation of Wireless Sensor Network (WSN), Wireless Body Area Network (WBAN), Wireless Personal Areal Network (WPAN), Wireless Local Area Network (WLAN) Wireless Wide Area Network (WWAN), General packet radio service (GPRS), Universal Mobile Telecommunications System (UMTS), and Radio Frequency Identification (RFID).

3.2.1 Wireless Sensor Networks (WSNs)

Wireless sensor networks (WSNs) are gaining popularity in the deployment of healthcare applications as a result of patients' tracking and real-time monitoring can be performed by using low-cost, low-power sensor nodes *deployed either inside the phenomenon or very close to it* (Al Ameen et al., 2010; Yick et al., 2008; Sohraby et al., 2007; Ng et al., 2006; Akyildiz et al., 2002, p. 102).

Table 3.2: Categories of wireless sensor networks (adapted and simplified from Sohraby et al., 2007, pp. 7-11; Darwish & Hassanien, 2011, pp. 5567-5568)

	C1WSNs	***C2WSNs***	***Applications*** **[examples]**
Topology	Multi-point-to-point (Mesh-based)	Point-to-point, (star-based)	**Military** [monitoring forces, targeting, enemy tracking, biological attack detection, etc.,] **Environmental** [forest fire detection, flood detection, etc.,] **Health** [drug administration, monitoring of patients (remote or inside a hospital), etc.,] **Home / Residential** [home automation, automated meter reading, etc.,] **Commercial** [inventory control, vehicle tracking and detection, traffic flow surveillance, etc.,]
Radio connectivity between wireless networks	Multi-hop	Single-hop	
Routing over the wireless network	Dynamic	Static	
Example	Military theatre systems	Residential control systems	
Supported Applications	Highly distributed high-node-count applications like environmental monitoring and national security systems	Confined short-range spaces such as a home, a factory, a building or human body	
Type of data flow	High-data-rate	Low-data-rate	
Standard	ZigBee/IEEE 802.15.4	ZigBee/IEEE 802.15.4	
Frequency	2.4 GHz; Industrial, scientific and medical (ISM) radio band	2.4 GHz; Industrial, scientific and medical (ISM) radio band	
Data transmission rate	Up to 250 kbps	Up to 250 kbps	
Distance	30 – 200 ft	30 – 200 feet	

Darwish and Hasaean (2011) state that a WSN typically consists of a large number of sensor nodes which are equipped with on-board processors, communication and storage capabilities to collect and process significant

information from the environment or the phenomenon being monitored. For instance, a sensor node can use its processing ability to perform *"simple computations and transmit only the required and partially processed data"* (Darwish & Hassanien, 2011, p. 5566). However, sensor nodes in a WSN may have not only different sensing and storage capabilities (e.g., optical or magnetic), but also different communication technologies used (e.g., infrared or radio frequency) and data transfer rates (Dargie & Poellabauer, 2010).

Similarly, Sohraby et al. (2007, p. 1) states that *"a distributed or localised sensor, an interconnecting network, a central point of information clustering and a set of computing resources at the central point or beyond"* are four fundamental elements of a sensor network (SN). Furthermore, the commercial WSNs can also be classified into two categories such as *Category 1 WSNs (C1WSNs)* and *Category 2 WSNs (C2WSNs)* (Sohraby et al., 2007, p. 7).

3.2.2 Wireless Body Area Networks (WBANs)

The emergent use of WBANs in the healthcare industry, especially in the fields of patient monitoring systems, is growing not only due to the advancement in wireless communication technologies, but also due to the development in wearable and implementable devices or sensors (Khan et al., 2012; Jain, 2011; Latré et al., 2011; Liolios et al., 2010; Lim et al., 2010). WBANs are typically deployed within a range of 1 to 2 meters. By deploying WBANs, an extensive group of novel applications such as "*ubiquitous health monitoring (UHM), computer-assisted rehabilitation an emergency medical response system (EMRS)"* are enabled to improve the quality of life (Latré et al., 2011; Li et al., 2010, p. 51). For instance, the real-time monitoring of patients who suffer from diseases such as diabetes, cardiovascular diseases (CVDs) and so on can be performed remotely and continuously whether or not the patients are in the hospital or at home (Khan et al., 2012; Latré et al., 2011; Li et al., 2011; Li et al., 2010).

In general, a WBAN (see Figures 3.6 and 3.7) is made up of a large number of intelligent devices that are tiny and normally implanted in or placed on the body and are capable of continuous monitoring of the patient's physiological activities (Yuce & Khan, 2012; Chen et al., 2011; Latré et al., 2011; Li et al., 2010).

Latré et al. (2011, p. 2) states that *sensors* and *actuators (or actors)* are two types of devices used in BANs in order *"to measure certain parameters of human body either externally or internally"* and *"to take some specific actions according to the data received from the sensors or through interaction with the user"*, respectively. For example, the measurement of the heartbeat or temperature of the body can be done by a sensor device. Likewise, a handheld device such as personal digital assistant (PDA) or a laptop or a smart phone can be operated as a sink to perform interaction between the wireless sensor device and the patient or doctor (Latré et al., 2010). A sink node can either be mobile or fixed and thought of as a gateway between a WBAN and external network (Muhammad et al., 2005). Hence, the patient related data collected from a body-attached or implanted sensors can then be transferred from a sink to a centralised medical database (Li et al., 2010).

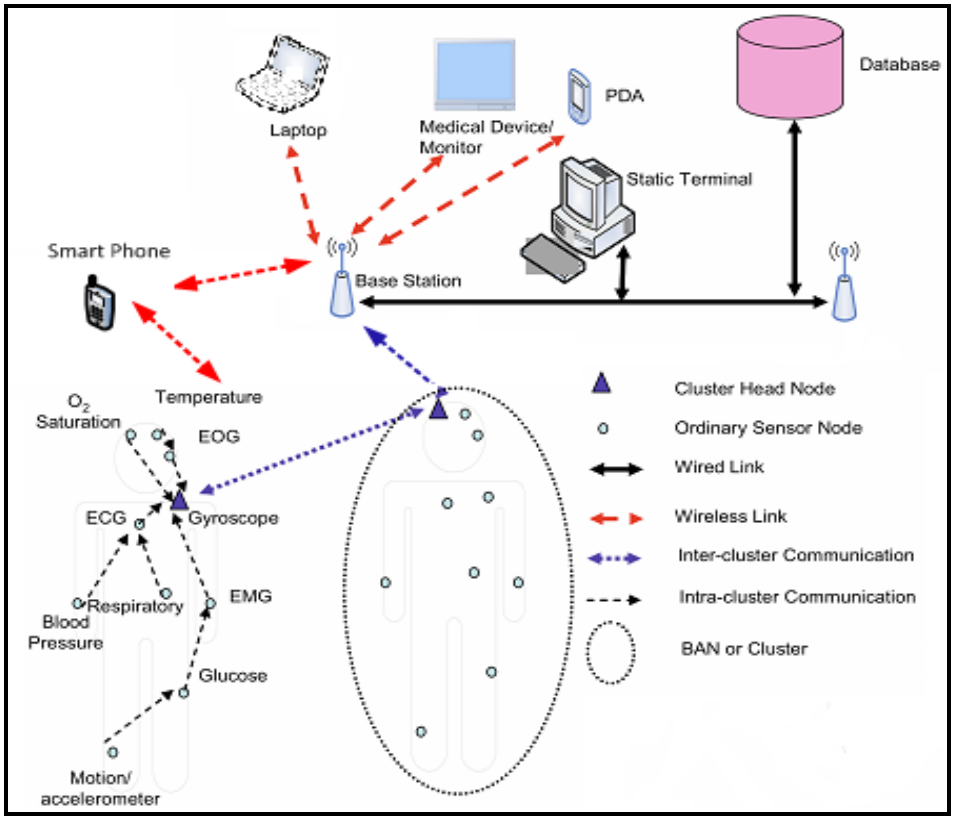


Figure 3.7: A simple continuous monitoring of patient's physiological activities by using BAN and WLAN (adapted from Chen et al., 2010, p.1)

3.2.3 Wireless Personal Area Networks (WPANs)

According to Noorzaie (2006), short range networks like WPANs using IEEE 802.15.4 or Bluetooth can be potentially deployed in the medical or healthcare industry (Chevrollier & Golmie, 2005; Golmie et al., 2003). For instance, WPANs can be used by nurses or doctors in hospitals in order to monitor patients in real-time instead of visiting patients' rooms frequently. Hence, nurses and doctors can have more opportunity to look after patients by saving time. WPANs can also be used to interconnect multiple devices within the hospital as the data collected from the patients can be transferred from one wireless device to another without performing data transfer manually (Noorzaie, 2006).

3.2.4 Wireless Local Area Networks (WLANs)

The Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802) designed the original WLAN 802.11 standard in 1997 for 1 Mbps to 2 Mbps wireless communication in the public frequency band of 5GHz and 2.4GHz (Hoglund, 2007; Karygiannis & Owens, 2002). As a result of flexibility, low cost, mobility and simplicity in operation, the deployments of WLANs have been rapidly growing and widely utilised in enterprises, homes, universities, cafés, airports and hospitals over many decades (Witters, 2011; Ngobeni et al., 2010; Heslop et al., 2010; Achi et al., 2009; Cypher et al., 2006; Banitsas et al., 2002).

Unlike a traditional wired LAN, a WLAN or *wireless Ethernet* provides two or more end-user devices that can communicate with each other without requiring physical cabling, but by using Radio Frequency or Infra-Red technologies (Achi et al., 2009; Karygiannis & Owens, 2002). A WLAN mainly consists of two types of wireless devices such as a wireless station (e.g., laptop or PDA) and a wireless access point (WAP), and it is usually implemented as an extension to wired LAN (Scarfone et al., 2008, Varshney, 2003; Karygiannis & Owens, 2002). However, the typical indoors-connectivity range of IEEE 802.11 devices is up to 50 to 100 meters even though a greater connectivity range can be achieved outdoors (Scarfone et al., 2008). Similarly, Chen et al. (2004, p.1) state that WLANs are considered to be *"the next generation of clinical data network"* due to the prospect of capturing patients' clinical data that can be sent to a doctor

or centralised patient database of the hospital by using different wireless devices like laptops, tablet computers, smart phones, PDAs or pagers (Garrett & Jackson, 2006; Newbold, 2004). For instance, 802.11 WLANs are being deployed to perform continuous monitoring of patients at home or in a hospital (Vassis et al., 2010; Lin et al., 2008; Varshney, 2003). In other words, the *"pervasive health monitoring, intelligent emergency management system, pervasive healthcare data access and ubiquitous mobile telemedicine"* can be carried out by deploying WLANs to fulfil the vision of *"Pervasive Healthcare"* (Malasri et al., 2009; Varshney, 2007, p. 113).

3.2.5 Wireless Wide Area Networks (WWANs) / GPRS / UMTS

The deployment of pervasive wireless technologies such as Wireless Wide Area Networks (WWANs), General Packet Radio Services (GPRS) and Universal Mobile Telecommunications Systems (UMTS) make possible monitoring or transferring of vital data on patients. For instance, the *MobiHealth* project was initiated in Europe in order to establish *"a generic platform for home healthcare using BAN-based sensors and GPRS or UMTS"* (for WWANs connectivity) wireless communication technology (Noorzaie, 2006, p. 8). Consequently, healthcare professionals have benefits of monitoring outpatients remotely. On the other hand, outpatients who wear wireless body sensor devices can also take advantage of improving mobility and reduce the disruption to daily life.

3.2.6 Radio Frequency Identification (RFID)

RFID (radio frequency identification) technology can identify objects or people, and also provide healthcare professionals with precise access to the patient's physiological data by using wireless radio communication (Liu et al., 2011; Yao et al., 2011; Hunt et al., 2007). As every system has its own essential components in order to operate successfully, a typical RFID system consists of three main components such as an RFID tag (active or passive) device, which is sometimes referred to as a transponder, RFID reader (or transceiver) and a host or controller which is connecting to an enterprise system (Roberts, 2006; Xiao et al., 2007; Hunt et al., 2007). RFID tag devices can be used to track patients and medical equipment in a hospital (Parlak et al., 2012; Noorzaie, 2006).

The successful deployment of RFID systems in hospitals or the healthcare industry (see Table 3.3) was reported in the "*Evaluating the business value of RFID: Evidence from five case studies"* (Tzeng et al., 2008, p. 601). For instance, a RFID system was used for an emergency room by tagging patients with passive tags that stored patients' identification numbers (IDs) to track them and to monitor patients' physiological signals. Likewise, a *"RFID smart medical platform"* was used in one of the hospitals in Taiwan to identify new-born babies with active RFID tags (Tzeng et al., 2008, p. 607). Hence, the nurses or doctors can access medical information related to patients by using wireless devices like PDAs or smartphones after the RFID reader has validated patients' IDs.

Table 3.3: Deployments of RFID systems in hospitals (Tzeng et al., 2008, p. 605)

	Taipei Medical University Hospital (TMUH)	Taipei Minicipal WanFang Hospital (WFH)	En Chu Kong Hospital (ECKH)	Show Chawn Memorial Hosptial (SCH)	Koo Foundation Sun Yat-Sen Cancer Center (KCC)
Project	Location-based medicare service RFID-based blood bag and resource management system	Wireless PDA & RFID system for emergency room observation Healthcare industry RFID application system	RFID intelligent healthcare platform Inpatient management system	Intelligent digital health network	Specialized healthcare system
Goal	SARS prevention	Patient safety	Sickroom safety	SARS prevention	SARS prevention
Application	SARS prevention and isolation	Emergency system medicine inspection and audit	Inpatient Management Waste Management	SARS Prevention and Isolation Healthcare Institute	Entry and Exit Control Exhibiting SOP Management
Start date	2003/10	2004/01	2004/01	2003/10	2003/10
Sponsor	Ministry of Economic Affairs	Department of Health	MOEA	MOEA	MOEA
Implement	Corporate with NTU, III and PK technology Establish IT consulting company	In house	Corporate with HP	Outsourcing	Outsourcing
Outcome	Success	Partial success low usage in emergency room	Partial success wireless technology cannot use in surgery room	Success	Success

Similarly, common wireless technologies were also implemented for the *real-time location systems (RTLS)* in 23 hospitals in United States (see Table 3.4) for tracking hospital assets, patients and temperature monitoring (Fisher & Monahan, 2012). Although *RTLS* can be applied for different purposes in *"clinics, emergency departments, operating rooms or throughout the entire hospital"*, Majchrowski (2010, p. 18) states that the most widely implementation of *RTLS* is hospital-wide location tracking of medical equipment (e.g. infusion pumps).

Freudenthal et al. (2007) stated that RFID technology, using passive RFID devices for human implants, allowed monitoring of the patient's biological functions within a short range (maximum 10 cm). Likewise, the implanted RFIDs are not useful for communicating with wireless global positioning systems (GPS). Therefore, the remote monitoring of the patient's biological functions is more appropriate and sensible than patient tracking in real-time with RTLS that uses RFID technologies (Aubert, 2011, Majchrowski, 2010).

Table 3.4: Wireless technologies used for RTLS in hospitals (simplified from Fisher & Monahan, 2012, p. 708)

Hospital ID	Year of assess-ment	Primary technology in RTLS	Purpose of RTLS
01	2007	RFID	Patient ID in surgery
02	2007	A. RFID	A. Asset tracking
		B. Ultrasound	B. Patient tracking
03	2007	RFID	Asset tracking
04	2007	RFID	A. Asset tracking
			B. Personnel tracking
06	2007	RFID	Patient ID in ED
07	2007	ZigBee	Asset tracking
08	2007	RFID	Patient ID for delivering medicine
09	2007	RFID	Patient tracking
10	2007	RFID	Asset tracking
15	2007	Ultrasound	Asset tracking
16	2007	Ultrasound	A. Patient tracking
			B. Personnel tracking
11	2008	IR	A. Asset tracking
			B. Patient tracking
			C. Personnel tracking
05	2009	RFID	A. Asset tracking
			B. Temperature monitoring
12	2009	RFID	Asset tracking
13	2009	RFID	Patient ID in surgery
14	2009	UWB	A. Asset tracking
			B. Patient tracking
			C. Personnel tracking
17	2009	RFID	Personnel tracking
18	2009	RFID	Asset tracking
19	2009	RFID	A. Asset tracking
			B. Patient tracking
20	2009	RFID	A. Asset tracking
			B. Temperature monitoring
21	2009	RFID	Asset tracking
22	2009	ZigBee	Asset tracking
23	2009	RFID	Asset tracking

3.3 CONCLUSION

Chapter 3 has defined and focused on specific medical applications that use wireless connections for their services. These have included devices and network specifications. Specific attention has been paid to the limitations and the designs for implementation. Although wireless connection is an ideal solution in the medical environment it is not a perfect solution. There are physical and logical limitations that must be factored into the use. Chapter 4 now explores the security implications for these limitations. This includes provisions and threats.

Chapter Four

SECURITY RISKS

4.0 INTRODUCTION

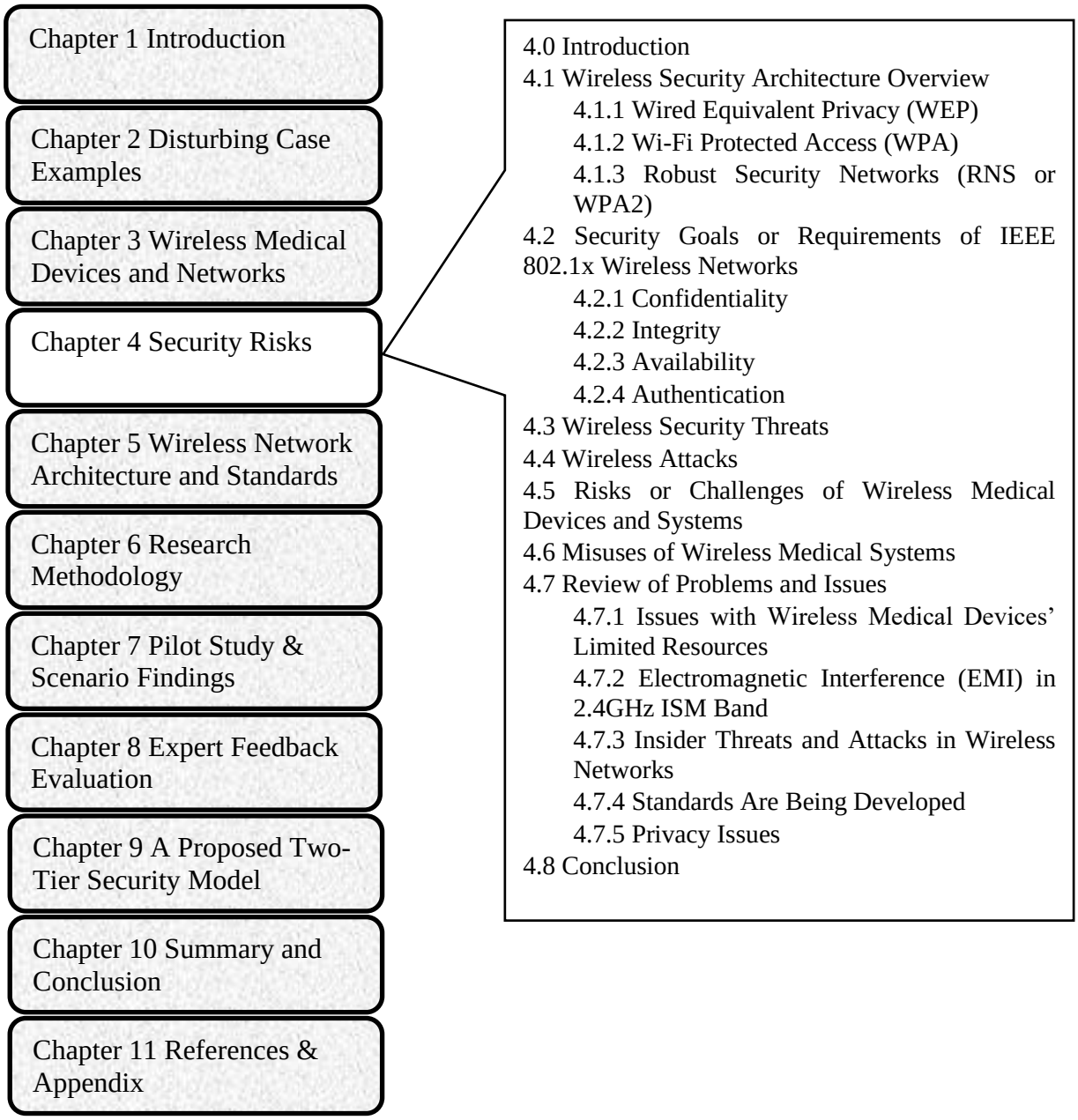


Figure 4.1: Roadmap of Chapter 4

Chapter 4 documents the security vulnerabilities of wireless connectivity. Security is an essential component of any IT systems, either wired or wireless. Wireless networks are ubiquitous and are being deployed in homes, organisations, healthcare industry, and in many contexts the security provisions are yet to be adequate. However, the main difference between wired and wireless network is

the vulnerability at the physical layer (Clonts, 2010). Unlike a wired network, the wireless data transmitted in the wireless network is easily captured or eavesdropped by passive attackers. As a consequence, the aspects and limitations of wireless networks are important to document and evaluate. Therefore, in this chapter, an overview of built-in wireless security architecture for wireless networks, especially IEEE 802.11 WLAN standards, and their limitations (Section 4.1) will be made. Then, the security goals or requirements of wireless networks will be discussed in Section 4.2. Consequently, the security issues related to wireless networks will be described in Section 4.3 and known wireless attacks in Section 4.4. Afterwards, risks or challenges of WMedDs and WMedSys will be highlighted in Section 4.5, which is followed by misuses of WMedSys (Section 4.6). Subsequently, a review of problems and issues will be summarised in Section 4.7 and the conclusion will be drawn in Section 4.8.

4.1 WIRELESS SECURITY ARCHITECTURE OVERVIEW

There are different security requirements for wireless networks that require adoption. In order to address these security requirements, it is essential to understand the existing built-in security features of IEEE 802.11 standards for WLANs. Hence, the existing security features of WLANs such as wired equivalent privacy (WEP), Wi-Fi protected access (WPA) and robust security network (RSN) or WPA2 is reviewed in the following sub-sections.

4.1.1 Wired Equivalent Privacy (WEP)

WEP is proposed to offer a security mechanism to users of wireless network "*that is equivalent to being on a wired network*" (Bulbul et al., 2008, p. 1). The main purpose of the WEP is not only to protect the wireless data transmission between wireless stations (STAs) and APs (Karygiannis & Owens, 2002, p. 29; Scarfone et al., 2008), but also to provide a security equivalent to or higher than that of wired network (Bulbul et al., 2008, p. 1).

However, the end-to-end security between the source and destination devices is not provided by the legacy WEP even though it is designed to provide confidentiality and authentication services (Karygiannis & Owens, 2002). In fact, data encryption is only applied between STAs and APs. When WEP is applied, every 802.11 wireless packet is separately encrypted with 64-bit Rivest Cipher

(RC4) key that consists of a 24-bit Initialisation Vector (IV) and a 40-bit WEP key (Scarfone et al., 2008; Bulbul et al., 2008; Lashkari et al., 2009). A bitwise exclusive OR (XOR) of the original packet and RC4 stream is used to generate an encrypted packet. Likewise, the IV is chosen periodically by the sender and transmitted in clear text with each wireless data packet. Furthermore, an integrity check value (ICV) of 4-byte is calculated on the original packet and appended after encrypting with RC4 cypher (Bulbul et al., 2008). WEP also uses the key size of 128 and 256 bits in the later implementations. Nonetheless, one of the weaknesses of WEP is the 24-bit IV being transmitted in plain text with every packet that allows a passive eavesdropper to know 24-bit of every wirelessly transmitted packet (Scarfone et al., 2008; Clonts, 2010) (see Figure 4.2).

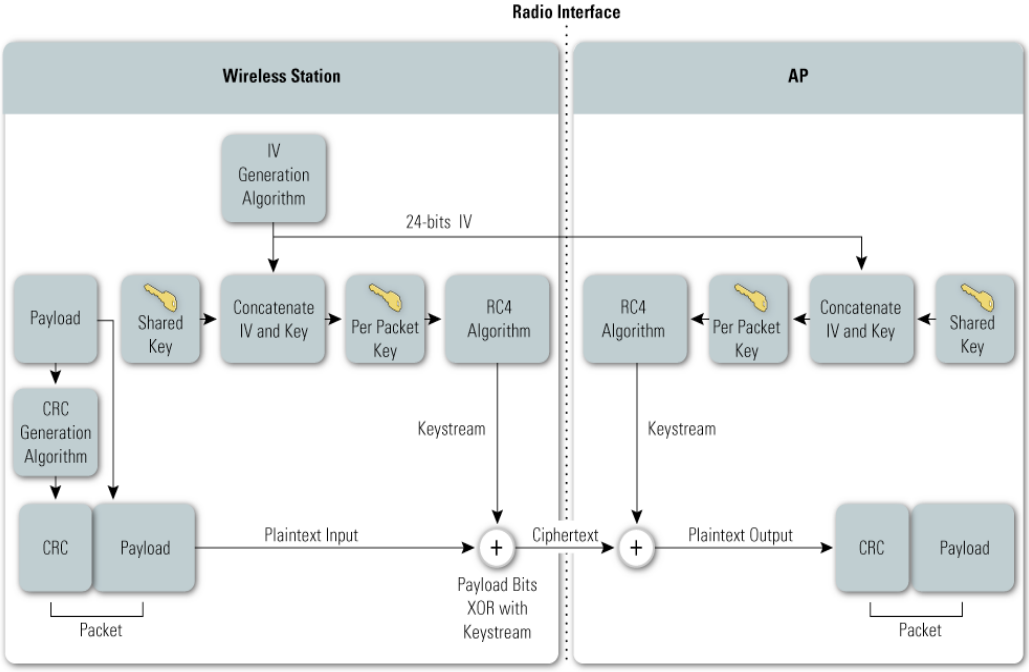


Figure 4.2: WEP encryption using RC4 algorithm (Scarfone et al., 2008, p. 24)

Other vulnerable aspects of the WEP encryption comprise "a lack of key management policy" and "a lack of cryptographic integrity protection" (Bulbul et al., 2008, p. 2; Clonts, 2010, p. 1; Katz, 2010). With respect to the key management, a WEP key often tends to be static and long-lived, and then shared among every node on the network as a result of no requirement for changing the WEP key. Moreover, wireless APs and STAs have to be programmed and then work with the same key. Hence, changing a WEP key is rarely done as it is always left as a task for the system administrators (Bulbul et al., 2008). It results in a large amount of cypher-text data using the same WEP key. This allows malicious

eavesdroppers to crack the key easily. With regard to the integrity risks, the use of a Cyclic Redundancy Check (CRC-32) algorithm to create a checksum (4 Bytes) for each wireless data packet is another problem with WEP. The CRC checksum is not encrypted and thus exposes the media access control (MAC) protocol to "an active attack where a malicious hacker can modify the checksum one byte at a time and send packets to see when it will be correctly acknowledged" (Clonts, 2010, p. 2). Furthermore, one of the weaknesses of WEP is the authentication method. IEEE 802.11 standards has two authentication methods the "Open System" and "Shared Key" authentication (Bulbul et al., 2008). In terms of authentication, WEP supports a shared key authentication sequence in which "the wireless AP sends a clear text challenge to the client, the client encrypts the text using the same WEP key used for normal communication, and then the AP validating the key" (Clonts, 2010, p. 2). The problem is the transmitted clear text and encrypted text during successful authentication can be monitored by a malicious attacker. Therefore, the WEP encryption key can easily be recovered by using both clear and cypher texts. Additionally, the use of a small key size (40 bits) in WEP is not long enough to resist the brute-force attacks initiated by malicious hackers (Bulbul et al., 2008). Likewise, WEP does not prevent replay attacks as the protocol does not maintain sequence counters in packets (Clonts, 2010).

4.1.2 Wi-Fi Protected Access (WPA)

Due to so many vulnerabilities and limitations, WEP is not an accepted wireless security solution. As a result, Wi-Fi (Wireless Fidelity) Alliance and IEEE 802.11 Working Group created the Wi-Fi Protected Access (WPA) standard to temporarily solve the vulnerabilities in WEP, in 2003 (Bulbul et al., 2008; Scarfone et al., 2008; Clonts, 2010). Lashkari et al. (2009) states that WPA operations can be classified into two operation modes with personal WPA or WPA-PSK (pre-shared key of maximum 256 bits) and commercial or enterprise WPA. The former operation mode is used specifically in small offices and residential homes without deploying a centralised authentication server. Due to the encryption key being pre-shared between the wireless AP and client, the mutual authentication is provided by WPA and the key is never broadcast in the medium (Lashkari et al., 2009). However, the latter operation mode utilises

"*authentication server 802.1X that provides an excellent control and security in the users' traffic of the wireless network*" (Lashkari et al., 2009, p. 50). So *this type of WPA uses 802.1X+EAP for authentication,* and replaces WEP with more advanced encryption, using *Temporal Key Integrity Protocol (TKIP)*. Instead of a pre-shared key, enterprise WPA utilises a centralised authentication server that is referred to as *Remote Authentication Dial In User Service* (*RADIUS*). Unlike WEP, combining the secret key with the IV before executing, RC4 encryption in *TKIP* can avoid eavesdroppers getting the IV in plain text and "*adding a sequence counter to messages that ensure out of order messages are not accepted; this prevents attacks where legitimate messages are replayed at a later time*" (Clonts, 2010, p. 2). Moreover, with regard to the integrity, WPA utilises 64-bit *Message Integrity Check* (*MIC*) for *TKIP* in order to check errors in the contents of the transmitted data. Hence, Bulbul et al. (2008, p. 1) observes that "*the ICV is CRC of data and MIC*". However, there are some limitations in WPA from the IEEE 802.11i standard point of view. For instance, WPA is susceptible to a brute force or dictionary attack if the WPA key is produced from a weak passphrase which is less than twenty characters (Clonts, 2010; Bulbul et al., 2008). Nevertheless, *TKIP* addresses "*four main improvements in encryption algorithms of WPA over WEP*" such as "*a cryptographic MIC to defeat forgeries*", "a new IV sequencing to remove replay attacks", "*a per-packet key mixing function to de-correlate the public IVs from weak keys*", and "a *rekeying mechanism, to provide fresh encryption and integrity keys*" to prevent key reuse attacks (Lashkari et al., 2009, p. 50).

4.1.3 Robust Security Networks (RSNs or WPA2)

In 2004, the IEEE published 802.11i amendment in which the enhanced security features were introduced with the perception of a more robust security that is referred to as RSN (also commonly known as WPA2). In contrast to WEP and WPA that employ fixed encryption methods, RNS utilises the Advanced Encryption Standard (AES) and IEEE 802.1X standard (which is an IEEE standard for port-based network access control) for dynamic negotiation of encryption and access control, respectively, between a wireless AP and a wireless client (Clonts, 2010; Bulbul et al., 2008).

Table 4.1: Comparison of IEEE 802.11 security protocols (adapted from Vanhoef & Ronen, 2019; Clonts, 2010, p. 3; Katz, 2010; Scarfone et al., 2008, p. 25; Bulbul et al., 2008, Frankel et al., 2007)

Security Features	WEP (pre-RSN)	WPA	WPA2 (RSN)	WPA3
Cryptographic Algorithm	RC4	RC4/TKIP	CCMP/AES	GCMP-256
Encryption Key Length	40-bit or 104-bit	128-bit	128-bit	192-bit
Encryption Key per Packet	Created through concatenation of WEP key and 24-bit IV	Created through TKIP mixing function	Not needed as temporal key is sufficiently secure	
Encryption Key Change	None	For each packet	Not needed	384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (SHA)
Encryption Key Management	None	IEEE 802.1X	IEEE 802.1X	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)
Initialisation Vector (IV) Length	24-bit	48-bit	48-bit	
Data Integrity Mechanism	Enciphered CRC-32	Michael Message Integrity Check (MIC)	Counter Cipher Mode with Block Chaining Message Authentication Code (CCM) Protocol	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Header Protection/Integrity	None	Source and destination addresses are protected by MIC	Source and destination addresses are protected by CCM	
Replay Attack Detection	None	Enforce IV sequencing	Enforce IV sequencing	Dragonfly protocol
Authentication	Open system or shared key (weak authentication)	EAP method with IEEE 802.1X or Pre-Shared key (PSK)	EAP method with IEEE 802.1X or Pre-Shared key (PSK)	Simultaneous Authentications of Equals (SAE) or the Dragonfly Key Exchange
Key Distribution	Manual	Dynamic IEEE 802.1X or manual	Dynamic IEEE 802.1X or manual	
Standard Mapping	802.11a & 802.11b	802.11g	802.11n	802.11n or 802.11ac

Hence, RSNs does not only offer the technique of extended key management and port-based access control to provide authentication, but also uses *Counter Cipher Mode with Block Chaining Message Authentication Code Protocol* (CCMP) and *TKIP* to ensure data confidentiality and integrity (Frankel et al., 2007).

However, similar to WPA, RNS provides security in two different modes (Lashkari et al., 2009) with the personal WPA2 for home users (that uses a symmetric key block cypher for encryption which is a pre-shared key of maximum 256 bits); and, the enterprise WPA2 for corporate (based on IEEE 802.1X). Even though AES utilises a 128-bit key to provide stronger security, RNS runs weakly on legacy devices (Bulbul et al., 2008). On the other hand, some researchers (Lashkari et al., 2009, p. 52) mentioned that the EAP framework including the *RADIUS* server should be used in order to offer "*the optimal balance between cost, manageability and risk mitigation*" when using 802.1X with 802.11i. To sum up, there has been a number of built-in wireless security features in 802.11 that is standardised by the IEEE since 1997 (see Figure 4.3).

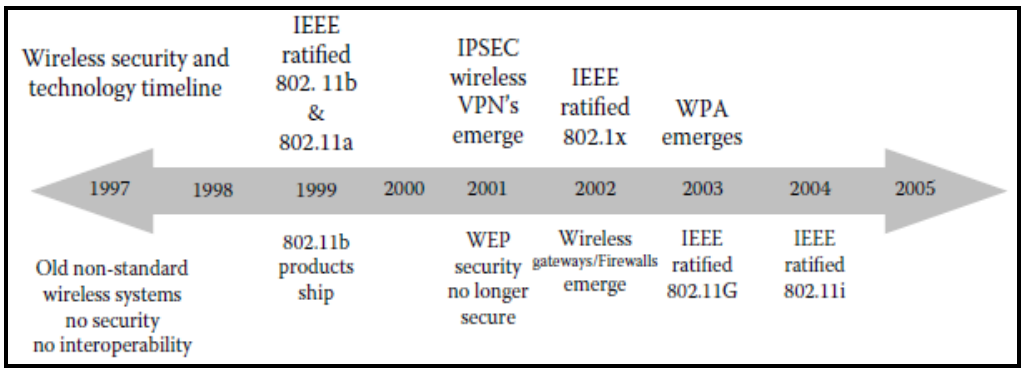


Figure 4.3: Wireless security architecture timeline (Earle, 2005, p. 270)

WPA2 has replaced the legacy 802.11 security (WEP) to address security issues. Table 4.1 summarises the comparison of IEEE 802.11 security protocols. However, WPA2 was cracked in 2017 and replaced by WPA3 in 2018 (Vanhoef & Piessens, 2019).

4.2 SECURITY GOALS OR REQUIREMENTS OF IEEE 802.1X WIRELESS NETWORKS

In order to evaluate the security risks and threats of WMedSys and WMedDs, it is essential to establish the goals of security. Hence, the essential goals or four principles of information security are critical as anchor points for benchmarking performances and expectations. The following sub-sections will briefly explain the critical security components of information security in terms of confidentiality, integrity, availability and authentication (CIAA).

4.2.1 Confidentiality

Confidentiality is an important security component of any organisation, either business enterprises or healthcare providers. Karygiannis and Owens (2002) states that the objective of confidentiality is to avoid critical confidential information being leaked or compromised from passive attacks (for example, eavesdropping attacks) initiated by people with malicious intent. Likewise, Frankel et al. (2007) points out that most wireless threats include, at least, an attacker with access to the radio link between a wireless STA and an AP (in wireless infrastructure mode) or between two STAs (in wireless ad-hoc mode). Furthermore, Al and Yoshigoe (2011) mention that the data or messages in wireless communications can be captured by eavesdropping attacks. The reality is that "*wireless networks propagate signals into space, making traditional physical security countermeasures less effective and access to the network much easier*" (Scarfone et al., 2008, p. 27). Hence, the confidential or sensitive data from a sensor or a WMedD (either on or in the body) should not be leaked or intercepted and should only be transmitted to authorised and intended receivers via a secure channel (Al & Yoshigoe, 2011). Even though the confidentiality of wireless data can be achieved by one of the many encryption mechanisms, it has to be strong enough to stop an unauthorised user accessing information (Al & Yoshigoe, 2011). Previous researchers (Halperin et al., 2008; Li et al., 2011; Gollakota et al., 2011) demonstrated how WMedSys and WMedDs could be compromised by eavesdropping. Moreover, the consequence after confidentiality is compromised (e.g. patient's confidential data including the medical conditions and device PIN is intercepted) will be life threatening for patients with WMedDs such as insulin pumps and implantable medical devices (Halperin et al., 2008; Li et al., 2011,

Radclieffe, 2011). Therefore, confidentiality is one of the critical security objectives to ensure that any unauthorised person will not have access to sensitive information by sniffing the communication link between wireless devices.

4.2.2 Integrity

Integrity of data generally addresses whether or not the original data is modified by unauthorised parties. In other words, the modification of data (editing, changing or deleting, etc.,) should only be performed by authorised parties (Goyal et al., 2010). Hence, the message or data being transferred from a source to the destination within either wired or wireless network should never be modified or corrupted in order to maintain the integrity (Al & Yoshigoe, 2011). However, the researchers (Scarfone et al., 2008; Karygiannis & Owens, 2002) state that the issues related to the integrity of data in wireless networks are comparable to those in wired networks. In fact, integrity could be very hard to achieve if organisations deployed either wireless or wired communications with inadequate cryptographic safeguards for transmitted data (Scarfone et al., 2008; Karygiannis & Owens, 2002). For example, wirelessly transmitted medical data of a patient with implanted (such as ICD or IID) or wearable medical device (such as insulin pump) can be illegitimately obtained and modified by a malicious person or an attacker if there is no encryption of the transmitted data (Malasri & Wang, 2009; Halperin et al., 2008; Li et al., 2011; Gollakota et al., 2011). On the other hand, Scarfone et al (2008, p. 28) claim that "*active attacks that compromise system integrity are possible*" as a result of "*the existing security features of the 802.11 standard do not provide for strong message integrity*". Nevertheless, in order to prevent and detect the modification of data by unauthorised parties, "*cryptographic checking mechanisms such as message authentication codes and hashes*" should be used (Karygiannis & Owens, 2002, p. 38).

4.2.3 Availability

Availability ensures that network assets, both data and services, are available to authorised parties in a reliable and timely manner (Goyal et al., 2010; Veltsos, 2011). Thus, availability is also one of the critical security requirements of every organisation or healthcare provider. For instance, the patient physiological or

medical data should be available despite under denial of service (DoS) attacks in a WBAN or WLAN.

4.2.4 Authentication

Authentication can be generally referred to as a security mechanism that enables "*to verify the identity of communicating client stations*" (Scarfone et al., 2008, p. 21) and controls access to the network resources by either granting or denying with respect to the legitimacy of communicating clients. Likewise, authentication assures that communication parties or clients are "*authenticated and not impersonators*" as only an authorised sender can originate a message or information transfer (Goyal et al., 2010, p. 12).

Similarly, the sending and receiving clients participating in a communication must be able to identify each other or a third-party entity. For instance, the legacy "*IEEE 802.11 specification defines two means to validate wireless users attempting to gain access to a wired network*" such as *open-system* and *shared-key* authentications (Karygiannis & Owens, 2002, p. 30). The former authentication method is not actual authentication and the latter deploys a simple challenge-response cryptographic technique (Karygiannis & Owens, 2002). The wireless AP authenticate a mobile STA to access resources without verifying the STA's true identity in *open-system authentication* even though the identity of the mobile STA is authenticated in *shared-key authentication* (see Figure 4.4).

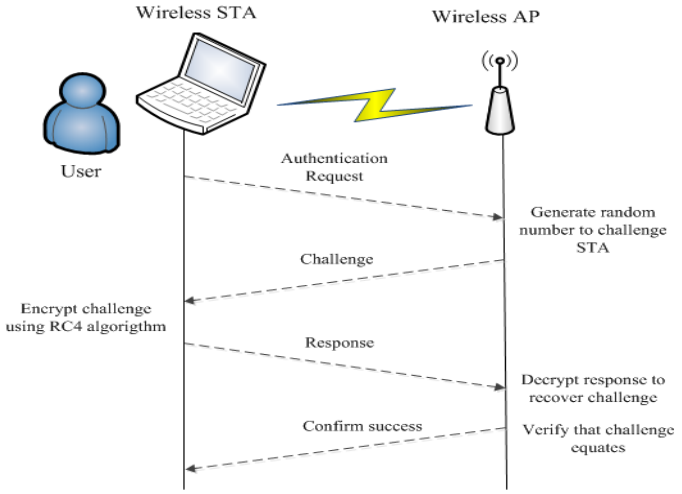


Figure 4.4: Shared-key authentication message flow between wireless AP and STA (adapted from Scarfone et al., 2008, p. 23)

According to the shared-key authentication, AP generates a random challenge and sends it to the associating client in a plaintext format (Scarfone et al., 2008; Karygiannis & Owens, 2002). Then, the client STA responds with a RC4 encrypted (stream cipher) message. Afterwards, the wireless "*AP decrypts the result computed by the client and allows access only if the decrypted value is the same as the random challenge transmitted*" (Scarfone et al., 2008, p. 22). However, in such a shared-key authentication method in legacy wireless networks, mutual authentication is not essential as only the AP authenticates the STA (not vice visa). Hence, the legacy wireless networks are vulnerable and suffer from different attacks including eavesdropping and man-in-the-middle attacks. This is the result of the initial exchange between the AP and the client STA by using the plaintext challenge and encrypted response (Scarfone et al., 2008).

4.3 WIRELESS SECURITY THREATS

Wireless networks and devices have ubiquitously deployed to change the way people live, communicate and work. However, these networks and devices do not only bring the benefits, but also convey new threats and vulnerabilities to users. Even though, there are built-in security mechanisms in of IEEE 802.11 WLANs (as stated in Section 4.1), there exists the risk in which a wireless network or device may be compromised or misused by a malicious person. Vulnerabilities are intentionally (e.g. insider threat) or unintentionally (e.g. through mistake or inexperience) originated with wireless technology and can be compromised by malicious attackers (D'Amico et al., 2010). For instance, an employee with malicious intent may implement an unauthorised AP in a secure company's network to perform either passive or active attacks.

A malicious outsider can attack the system through unintentional misconfigured wireless devices. Furthermore, Frankel et al. (2007, p. 27) mentions that most of the wireless threats entail "*an attacker with access to the radio link between a STA and an AP or between two STAs*", as stated in Section 4.2.1. Similarly, Diksha and Shubham (2006) classified wireless security threats into two categories: common, and malicious wireless threats. Common wireless threats include "*rogue APs, mis-configured APs, client mis-associations and ad hoc connections*" whereas malicious wireless threats comprise "*evil twin/honeypot*

APs, rogue clients and denial of service attacks" (Diksha & Shubham, 2006, pp. 2-3). The major threats related to commonly known wireless networks and devices are summarised in Table 4.2.

Table 4.2: Types of major threats against wireless networks and devices (adapted from Diksha & Shubham, 2006, pp. 2-3; Frankel et al ., 2007, p. 28)

THREAT TYPE	DESCRIPTION
Ad hoc or Peer-to-Peer Connection	Attacker can exploit a wireless client or device after establishing ad hoc connection (unauthorised client attempts to form ad hoc network with legitimate client). After establishing the ad hoc connection, the attacker can perform port scanning to explore and exploit client vulnerabilities.
Client Mis-association	Attacker can compromise a corporate wireless client after the client within business premises mis-associates or connects to an unauthorised external Wi-Fi network (which is set up by an attacker by using a *rogue AP*).
Denial of Service (DoS)	Attacker prevents or prohibits the normal use or management of networks or network devices.
Eavesdropping	Attacker passively monitors network communications for data, including authentication credentials.
Evil Twin/Honeypot AP	Attacker sets up Honeypot AP with a default service set identifier (SSID, network name) hotspot SSID, or corporate SSID and observes many wireless clients connect to it and can then be initiate attacks on connected clients (e.g. stealing passwords by presenting a fake Facebook login page to clients over the mis-associated wireless connection.
Man-in-the-Middle	Attacker actively intercepts the path of communications between two legitimate parties, thereby obtaining authentication credentials and data. Attacker can then masquerade as a legitimate party. In the context of a WLAN, a man-in-the-middle attack can be achieved through a *bogus* or *rogue AP*, which looks like an authorised AP to legitimate parties.
Masquerading	Attacker impersonates an authorised user and gains certain authorised privileges.
Message Modification	Attacker alters a legitimate message by deleting, adding to, changing or recording it.
Message Replay	Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.
Mis-configured AP	Attacker can take advantage of a potential security hole (open door) created by a mis-configured AP to launch an attack on the corporate network.
Rouge AP	Attacker can either plugged an unauthorised AP into the corporate network or use a computer (e.g. laptop) running software *Fake AP* to provide wireless access to Wi-Fi clients within the range.
Rogue Clients	Attacker actively access an authorised cooperate wireless network via mis-configured AP (e.g. encryption turned off) or through an AP after compromising encryption/authentication.
Traffic Analysis	Attacker passively monitors transmissions to identify communication patterns and participants.

4.4 WIRELESS ATTACKS

The security requirements of IEEE 802.x wireless networks and wireless security threats have been stated in the previous sections (Section 4.2 and Section 4.3). Ashraf et al. (2009, p. 2) stated "*the vulnerability is a weak-point in the system or network that may be exploited, whereas a threat is considered as an external or internal influence that may exploit the vulnerability (weak-point)*". Moreover, an attack is defined as "*the consequence of a threat that causes an unwanted event to be occurred in a system such as data steal, denial-of-service, sniffing, spoofing, etc.*," (Kim et al., 2006; Barnum & Gegick, 2005; cited in Ashraf et al., 2009, p. 2). Like all other wired networks, wireless networks and devices are susceptible to malicious attacks. However, wireless networks and devices are more vulnerable to different attacks than its counterpart (wired networks). There are numerous published articles that emphasize the point and list the significant security attacks on wireless networks and devices. For instance, Chanzigiannakis (2007, p. 1408) lists the major security threats for wireless sensor networks (WSNs) and proposed "*a decentralised intrusion detection system*" to improve security in order to prevent attacks "from both external and internal adversaries". Likewise, Gill and Yang (2009, pp. 2063-2065) reviewed three most common denial-of-service (DoS) attacks on WSNs such as "*UDP flooding*", "*TCP SYN*" and "*Smurf*" attacks and proposed "*Virtual Home – DDoS attack detection mechanism*".

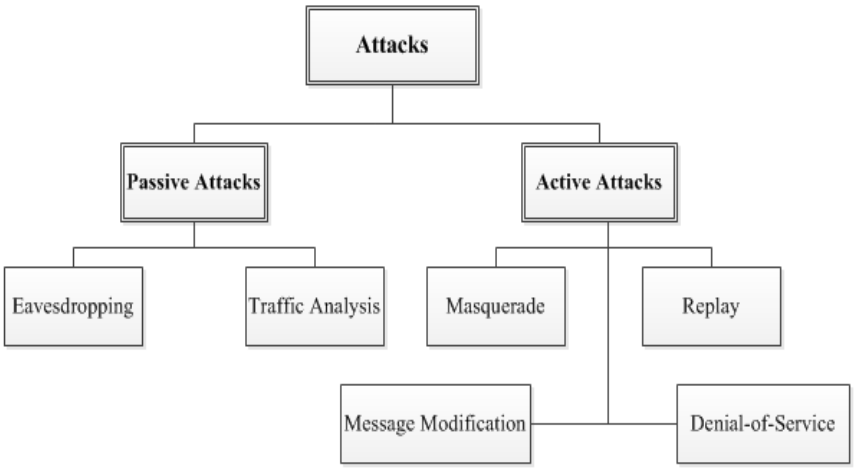


Figure 4.5: Taxonomy of WLAN security attacks (Karygiannis & Owens, 2002, pp. 35)

Similarly, other researchers mentioned different types of vulnerabilities and security attacks in WSNs (Mahmoud & Shen, 2012; Hua & Li, 2012; Lee et al., 2012; Jain et al., 2012; Srivastava & Goel, 2011; Li et al., 2010; Alcaraz & Lopez,

2010; Dargie & Poellabauer, 2010; Al Ameen et al., 2010; Mpitziopoulos et al., 2009; Healy et al., 2009; Ramond & Midkiff, 2009; Chen et al., 2009; 2008; Bojkovic et al., 2008; Tahir & Shah, 2008; Kumar et al., 2008; Habib, 2008; Zia & Zomaya, 2006; Pathan et al., 2006; Ng et al., 2006; Newsome et al., 2004).

Table 4.3: Classifications and association of security VTAs with discrete security assessment framework (Ashraf et al., 2009, pp. 2-3)

NETWORK	***Vulnerability:*** Average energy exhaustion (network), low computational capacity, limited network storage time, self-organisation, fault-tolerance level, distributed storage, task details, simple ciphering, and node deployment ***Threat:*** Topology change, change of frequency, large messaging overhead, non-scalability, recursive routing, system failure ***Attack:*** Complete DoS or DDoS
LINK	***Vulnerability:*** Radio link, Signal transmission range (916MHz, 2.4GHz), Broadcasting, Topology-less infrastructure, Ad hoc Topology information ***Threat:*** Non-reachable, Link-failure, High-density of nodes, Indefinite jamming of signals, Data tampering, High noise, unmanaged mobility, Higher delays (link-setup) ***Attack:*** Collision or checksum mismatch, Unfairness, Spoofing, Sybil, Wormholes, Hello-flood, ACK-spoofing
SINK	***Vulnerability:*** Energy exhaustion @ Sink, Task details ***Threat:*** Unauthorised access ***Attack:*** Sinkhole, De-synchronisation
NODE	***Vulnerability:*** Energy exhaustion @ Node, Resilience to physical security, Limited memory, Short-storage time ***Threat:*** Node failure, Recursive location, Indefinite flooding ***Attack:*** Selective forwarding
OTHER	***Vulnerability:*** --- ***Threat:*** Natural hazards, Environmental interference, Human Interaction (to damage network), Catastrophic (man-made) ***Attack:*** Nil

On the other hand, Karygiannis and Owens (2002, pp. 35-36) classified the common security attacks in WLANs into passive ("*eavesdropping*", "*traffic analysis*") and active ("*masquerading, replay, message modification and denial-of-service*") attacks (see Figure 4.5), whereas other researchers (Watfa and Safa;

2008) generally stated different attacks on WLANs (such as jamming, insertion, misconfiguration, interception and monitoring attacks).

With regard to radio frequency identification (RFID) technology, Karygiannis et al. (2006; cited in Ding et al., 2008) categorises a RFID risk model into three classes: *"network-based risks, business process risks, and business intelligence risks"*. Ding et al., (2008) proposes the taxonomy model of RFID security threats in three layers: *physical layer threats* (eavesdropping, jamming and tag cloning), *communication layer threats* (collision), and *application layer threats* (spoofing and virus attacks). Mitrokotsa et al. (2010) classify RFID attacks into layers where the attack could take place. Ashraf et al. (2009, p. 2) classified WSNs' security issues in association with vulnerabilities, threats and attacks (VTAs) by using a "*discrete security assessment framework*" to completely identify any layer of WSNs under attack (see Table 4.3).

Table 4.4: Potential adverse events in various implantable medical devices (Hansen & Hansen, 2010, p. 15)

DEVICE	ADVERSE EVENTS
Pacemaker, Implanted Cardiac Defibrillator (Mirowski et al., 1970); Ventricular Assist Device (Glenville & Ross, 1986)	Heart failure, Tachycardia, Bradycardia, Arrhythmia
Cochlear Implant	Deafness, Phantom sounds, Distraction/Confusion
Prosthetic Limb Control System (Velliste et al., 2008)	Injury, Damage to prosthetic limb, Inadvertent movement
Spinal Cord Simulator (Brindley et al., 1982)	Loss of pain relief, Inappropriate stimulation
Sacral Anterior Root Simulator (Brindley et al., 1982)	Infection from inability to void, Inappropriate stimulation
Retinal Prosthesis (Chow et al., 2004), Implanted Contact Lens, Intraocular Lens	Blindness, Phantom images, Distraction/Confusion
Implanted Infusion Pump	Inappropriate dosage/timing
Brain-Machine Interface and Other Neuroprosthesis (Santhanam et al., 2006; Song et al., 2009)	Loss of consciousness, Neural effects (Denning et al., 2009)
Responsive Neurostimulator and Other Deep Brain Simulator (Sun et al., 2008)	Inappropriate stimulation, Failure to stimulate
Implanted Monitor or Sensor	Incorrect readings
Implanted RFID Tag (Halima et al., 2006)	Loss of privacy, Data leakage
Implanted Dynamic LED Tatto	Inappropriate display

Hansen and Hansen (2010) described different types of potential adverse events that could happen to different IMDs (Table 4.4), and Ng et al. (2006) defined different wireless security threats and countermeasures on WSNs (Table 4.5).

Table 4.5: Wireless sensor networks security threats, security requirements and possible solutions (Ng et al., 2006, p. 141)

Security Threats	Security Requirements	Possible Security Solutions
Unauthenticated or unauthorised access	Key establishment and trust setup	• Random key distribution • Public key cryptography
Message disclosure	Confidentiality and privacy	• Link/network layer encryption • Access control
Message modification	Integrity and authenticity	• Keyed secure hash function • Digital signature
Denial-of-service (DoS)	Availability	• Intrusion detection • Redundancy
Node capture and compromised node	Resilience to node compromise	• Inconsistency detection and node revocation • Tamper-proofing
Routing attacks	Secure routing	• Secure routing protocols
Intrusion and high-level security attacks	Secure group management, intrusion detection, secure data aggregation	• Secure group communication • Intrusion detection

4.5 RISKS OR CHALLENGES OF WIRELESS MEDICAL DEVICES AND SYSTEMS

"*Christopher Nowak of Universal Healthcare Services Inc. describes everything we do is for the benefits of the patients and impacts the outcome of their care*" (Loughlin & Williams, 2011, p. 98). Medical devices are being integrated into hospital information systems. However, medical devices create an exclusive exposure to threats and attacks (Sections 4.3 & 4.5) as a result of difficulties in not only protecting against viruses and other malicious attacks, but also difficulties in software upgrades and updates (Loughlin & Williams, 2011). For instance, a medical device will not be working effectively when an anti-virus program slows down the operations in the medical device and uses the limited resources. Witters (2011) argued that the risks related to WMedDs and WMedSys

(see Table 4.2) should be effectively identified and attended to, although the advantages of employing wireless technologies (Section 3.2) in the medical or healthcare industry can prevail over the risks. The way in which the risks associated with WMedDs can be addressed is by the detailed description of wireless technology and the associated wireless devices (Witters, 2011). Furthermore, Loughlin and Williams (2011, p. 99) say that "*the trend for clinical engineering has been to come increasingly intertwined with information technology … this trend will continue and today's successful biomed needs to have some grounding in IT training*". The previous researchers (Loughlin & Williams, 2011) explained the top ten challenges faced by biomedical and clinical engineering departments related to medical devices after surveying "*2,522 biomed technicians and clinical engineers by asking them to rank 22 medical device-related challenges*" (p. 99). Hence the top ten medical device challenges and possible solution are summarised in Table 4.6.

Table 4.6: Summarised top ten medical device challenges and possible solutions (Loughlin & Williams, 2011, pp. 99-103)

Challenge	Possible Solution/Best Practice
1. Interfacing between devices and information systems	"*Provide appropriate education and training*" to biomeds or technicians (Loughlin & Williams, 2011, p. 99).
2. Maintaining computerised equipment and systems	Kenneth Maddock of Baylor Health Care System suggested medical device manufacturers should validate "*their equipment with the most popular anti-virus and should provide clear instructions on how to install anti-virus program on particular devices*" (Loughlin & Williams, 2011, p. 100).
3. Managing alarms	Clinical staff from clinical engineering (CE) departments should be given education and training about the "*alarm setup, default settings and proper use of alarms*" in order to avoid the life and death of patients when "*alarms could not either be heard or ignored*" " (Loughlin & Williams, 2011, p. 100).
4. Maintaining and processing endoscopes	Biomeds from CE departments should be given proper education and training on how to clean, sterilise and maintain endoscopes as such devices are very sensitive and can be broken easily.
5. Broken connectors	Kenneth Maddock of Baylor Healthcare System mentioned that "*virtually all medical devices have some sort of connector… they can be difficult to replace*" (Loughlin & Williams, p. 104). Furthermore, "*Jim Welch of Masimo Corp., a global medical technology company, mentions that broken connectors are the most common cause of no*

	problems founds (NPFs) when a clinician raises a concern about a device and then a technician checks it out" (Loughlin & Williams, 2011, p. 101). To prevent the issues related to broken connectors, setting a timer in connectors to remind if replacements are needed after a number of predefined connections has been reached (Loughlin & Williams, 2011).
6. Wireless management	The demand in wireless enabled medical devices for flexibility is raising one of the challenges in hospital/healthcare industry. Proper education and training should be given to biomeds and IT personnel in order to maintain the devices (Loughlin & Williams, 2011).
7. Battery management	Healthcare facilities and patients/users of the medical devices should have efficient "*battery maintenance and replacement in their budgets as part of the preventive maintenance (PM) program*" (Loughlin & Williams, 2011, p. 102). It is important to give proper training biomeds and patients/users of the medical devices. Likewise, additional replacement battery packs and chargers should be given to mobile users of physiological monitors and defibrillators as batteries can easily be failed due to no power outlets available (Loughlin & Williams, 2011).
8. Problems with patient monitors (in-hospitals or at home, at work and around the community)	CE has to work with appropriate stakeholders, IT and clinicians to establish "*a risk management process that identifies vulnerabilities*" associated with patient monitoring systems and devices in order to mitigate all substantial risks (Loughlin & Williams, 2011, p. 103).
9. Problems with dialysis equipment	It is essential to "review the service schedule with clinicians and nurse managers responsible for dialysis service in advance of scheduled maintenance" (McCarthy, 2011, cited in Loughlin & Williams, 2011, p. 101).
10. Managing the radiation dose from Computed Tomography (CT)	According to the **Emergency Care Research Institute** (ECRI), "radiation overdose and other dose errors as its top health technology hazard for 2011" as a result of human (wrongly administered radiation) or software-related errors (Loughlin & Williams, 2011, p. 103). CE has to work with appropriate stakeholders, IT and clinicians to keep up the performance of such therapy systems and devices by regular maintenance.

4.6 MISUSE OF WIRELESS MEDICAL SYSTEMS

A misuse can be defined as a negative *"behaviour that is not allowed in the proposed system"* (Sindre & Opdahl, 2005; cited in Smith et al., 2010, p. 3). For instance, a misuse can be referred when a malicious hacker attacks a wireless medical system like an insulin pump system, to compromise patient safety by stopping or changing the dosage of the drug-administration. Likewise, RFID enabled wireless medical systems used for patients' monitoring or tracking in

hospitals can be exploited by malicious hackers using any one of the potential attacks on implantable identification devices (IIDs), such as the cloning attack (Malasri & Wang, 2009). The IIDs are commonly implantable RFID tags with no power and vulnerable to threats. Hence, the attacker can compromise the privacy of the patients when the patient unique IDs are obtained by using an external RFID scanner.

Table 4.7: Classifications of WLAN misuse (adapted from Ngobeni et al., 2010, p. 108; Slay & Turnbull, 2006, p. 127)

Class	Description	Misuse Example
Wireless Detection and Connection	Misuse involves an intruder using the wireless medium as a tool to commit other criminal activities.	Unauthorised use of WLAN or use of the WLAN as a launch pad for other criminal activities
Concealment of Digital Evidence	Misuse involves hidden wireless devices or hidden wireless networks.	Fake access point
WLAN as an Attack Vector)	Misuse involves attacks against the devices originated from the wireless network and then attacks against the WLAN medium itself.	Rogue access point, Man-in-the-Middle attacks

The illegitimate misuse of WLANs deployed for the pervasive continuous health monitoring of patients in a hospital can be classified into three groups (see Table 4.7). For instance, "*the misuse of Wake Internal Medicine was where the wireless medium was merely a vector susceptible to attack"* (Niemann, 2004; cited in Slay & Turnbull, 2006, p. 127). The case was concluded as the attack was long term and well planned. Similarly, the misuse of wireless medical systems can also be caused by the deployment of new wireless devices within the existing IT system. Hence, Witters (2011) discusses some of the case studies concerned with the problems related to the deployment of wireless devices in hospitals (see Table 4.8).

Malasri and Wang (2009, p. 75) also stated that *the VeriChip Corp.'s RFID tag* allows doctors, nurses or healthcare professionals to promptly access patients' medical related data in the backend database called *VeriMed* (Malasri & Wang, 2009). However, Halamka, Juels, Stubblefield, and Westhues (2006, p. 601) argued that "*the VeriChip (a commercially produced, human-implantable RFID tag) should serve exclusively for identification, and not authentication or access*

control" as it was susceptible to an easy "*over-the-air spoofing attacks*". In 2012, VeriTeQ Acquisition Corporation or VeriTeQ acquired the "*VeryChip implantable microchip and related technologies, and Health Link personal health record (PHR) from Positive ID Corporation*" to focus in identification of patients, identification of implanted medical devices, identification and sensor applications for animals (Business Wire, 2012, p. 1). Then, the chip from PositiveID was acquired by JAMM Technologies in 2016 and secure version of RFID tags were started to use to identify and monitor the medical device and patients (PositiveID, 2019).

Table 4.8: Problems related to the deployment of wireless devices in hospitals (adapted from Witters, 2011, pp. 49-52)

Project	Purpose	Problem	Cause	Recommended
Active RFID Tags	Deployed 802.11 based active RFID tags for locating and tracking equipment in a hospital	Loss of data on 802.11 based patient monitoring system	APs are not acknowledging data due to not implementing off-channel scanning on APs	The true cost of the installation must me learnt before the deployment
Microwave Oven	Replacing one of two industrial microwave ovens in a hospital	Radio Frequency Interface / Electromagnetic Interference (RFI/EMI)	After the replacement the microwave ovens did not run in phase	Adding more Aps at larger distance from the interring microwave ovens Hospital should document all RF sources and perform periodic reviews
Wireless Medical Devices (WMedDs)	Installed more wireless devices on its existing IEEE 802.11 b/g wireless network	War driver hacks into the hospital wireless network and access sensitive medical data after compromising the security of servers	WEP encryption is only supported by the new wireless devices and it is very easy to be deciphered	To mitigate the risk, hospital would install a firewall, or a separate wireless network dedicated to the medical device

The real-world cloning attack or misuse case was carried out efficiently on the *VeriChip* (Halamka et al., 2006; cited in Malasri & Wang, 2009). Even though the

deployment of wireless technologies in the healthcare setting can not only offer benefits to the healthcare professionals but also to patients, the pervasiveness of WMedDs and applications may possibly lead to potential misuse cases (Pyrek, 2011). Hence, Hansen and Hansen (2010) described the potential adverse events can occur by using various implantable medical devices. For instance, the use of a pacemaker or implanted cardiac defibrillator or ventricular assist device could lead to heart failure, arrhythmia, tachycardia and bradycardia. In the medical healthcare industry, the electronic medical records of patients are at high risk as these records tend to be stored in a centralised location. The patients' data could be lost due to a virus infection into the hospital or clinical information systems, and malicious hackers can break into the systems in order to access and change the patients' information (Kierkegaard, 2011). For instance, McBride (2011; cited in Kierkegaard, 2011, p. 510) stated that a *California-based Kern Medical Centre* was attacked by hackers in 2010. As a result, the hospital's computers were crammed with porn and the printers were forced to print until the paper ran out. Eventually, the system of *Kern Medical Centre* was shut down for 16 days (Kierkegaard, 2011). In addition to malicious hackers accessing the hospital information systems, the medical devices including implanted and monitoring devices (such as PDAs, iPads, and smartphones used by nurses and doctors) could be infected by viruses. Hence, the security and privacy of the patients can be compromised. Similarly, there were cases of malicious attacks in which the hackers or extortionists demanded ransoms worth of million dollars. For instance, hackers demanded $10 million after stealing 8 million patients' medical records from a *Virginia state website used by pharmacists* in 2009 (Kierkegaard, 2011, p. 510). Likewise, the extortionists threatened *"to disclose personal and medical information on millions of Americans in October 2008 if Express Scripts, which is the largest pharmacy prescriptions processor in America, failed to meet the payment demands"* (Krebs, 2008; cited in Kierkegaard, 2011, p. 510). Moreover, the insider threat and human error, such as errors caused by healthcare professionals, are one of the serious data vulnerabilities encountered in the medical healthcare industry. Kierkegaard (2011, p. 511) described that *"researchers for London Health Programmes revealed that they had lost unencrypted records of 8.63 million National Health System patients"*.

4.7 REVIEW OF PROBLEMS AND ISSUSES

According to the previous literature reviewed, there have been a number of issues and challenges related to the deployment of wireless communications and WMedDs in the healthcare industry that have potential to balance the benefits such as greater physical mobility and interoperability (Cypher et al., 2006). The numerous issues involve "*a lack of comprehensive coverage of wireless and mobile networks, reliability of wireless infrastructure, general limitations of handheld devices, medical usability of sensors and mobile devices, interference with other medical devices, privacy and security, payment and many management issues*" (Varshney, 2007, p. 124). The issues and challenges are summarised in this section in order to identify researchable areas and the relevant gaps in the literature.

4.7.1 Issues with WMedDs' limited resources

Generally, WMedDs have limited resources (e.g. computational power, memory, and battery power). The resource constraints are one of the factors that can lead to compromised security and privacy of patients or device users. However, to ensure the security and privacy of patient's physiological data in Wireless Medical Networks (WMNs), Yao et al. (2011) state that cryptographic algorithms can be used. Asymmetric key cryptography is not feasible to implement in WBAN due to limited resources of the wireless medical sensors. In fact, asymmetric key algorithm demands more resources such as computational power and storage capacities. Hence, in order to safeguard the problem with security and privacy in BANs, some researchers (Yao et al., 2011, p. 8) proposed an electrocardiogram (ECG)-signal-based biometric symmetric key establishment scheme that could "*protect the confidentiality and integrity of sensitive health information*". Also see: Karie and Venter (2015); Karie, Kebande, and Venter (2017); Kebande and Venter (2014); Kebande and Venter. (2015); and, Kebande and Venter (2016).

4.7.2 Electromagnetic Interference (EMI) in 2.4 GHz ISM Band

It is important to ensure that wireless devices used in hospitals or healthcare environment must meet safety and the *Electromagnetic Compatibility* (EMC) requirement (Turab et al., 2010). The nature of wireless devices does allow the

users of those devices to go anywhere at any time. As a result, there exists a potential issue related to the *Electromagnetic Interference* (EMI) among WMedDs employing the same ISM frequency band of 2.4 GHz. These wireless devices are not only sharing wireless channels in the 2.4 GHz band (see Figure 4.6), but also are capable of operating in very close proximity to each other (Cypher et al., 2006, Boyle, 2006, cited in Turab et al., 2010). For example, research has shown that a Bluetooth enabled device can cause delay in transferring patient data or "*the packet loss up to 60 percent at MAC sublayer of the low-rate WPAN Electrocardiogram (ECG) monitor at very close range*" (Cypher et al., 2006, p. 60).

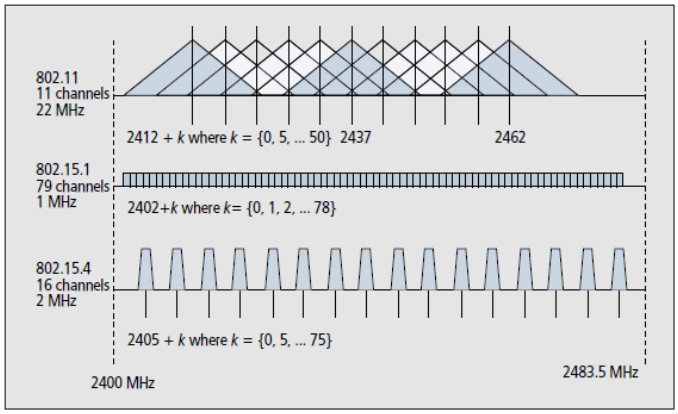


Figure 4.6: Frequency map for selected IEEE 802 specifications in the 2.4 GHz (Cypher et al., 2006, p. 59)

The techniques (collaborative and non-collaborative) to mitigate the interference issues caused by the coexistence of WLAN and Bluetooth-enabled devices have been discussed by Lansford et al. (2001, cited in Cypher et al., 2006). Nevertheless, the problem with interference is still unavoidable. Thus, there is a need for "*a strict monitoring and control of spectrum usage is put in place in order to constantly detect spectrum usage and direct the choice of which technology to use*" in the medical healthcare environment (Cypher et al., 2006, p. 61).

4.7.3 Insider Threats and Attacks in Wireless Networks

The threats associated with insiders are one of the critical security issues in either wired or wireless networks (e.g. WSNs). Although, most of the wireless networks are deployed with cryptography-based authentication and authorisation to protect malicious attacks from outsiders, "*the traditional security mechanisms such as*

authentication and authorisation cannot catch inside attackers" who are authorised and legitimate users of the network (Cho et al., 2012, p. 134).

Table 4.9: Different types of insider attacks in WSNs (adapted from Ren et al., 2006, pp. 3-4)

Insider Attack Types			Cryptography-based solution*	Detection
1.	***Data forwarding related***	Message delay attack Selective forwarding attack Message alteration attack Message replay attack Sinkhole attack Message collision attack	No No Yes Yes No No	Such attacks can be detected if end-to-end acknowledgment is explicitly compulsory for every message transmitted, as a compromised node may drop one packet per message to maximise the attack (Ren et al., 2006).
2.	***Data generation related***	Bogus data attack Bogus query attack Report disruption attack	No No Yes	Such attacks can be detected if there are nodes with significantly sensing results as compromised nodes always either comes up with incorrect sensing result to deceive its neighbours during the process of sensing/aggregation or irregularly initialise bogus queries (Ren et al., 2006).
3.	***Routing related***	Hello attack Wormhole attack Bogus routing info attack Sybil attack	Yes Yes Yes Yes	Routing related attacks (Ren et al., 2006) are generally hard to detect (for instance a compromised node launching message collision attacks).
4.	***Physical related***	Byzantine attack Node replication attack Node relocation attack	No Yes Yes	Attacker runs malicious code to compromise the software platform of a sensor node in a Byzantine attack (Shi et al., 2005, cited in Ren et al., 2006, p. 4). By applying code attestation techniques on the sensor node itself, Byzantine attacks can be identified.
*******The judgements are obtained in the context of static and location-aware WSNs with cryptographic mechanisms in place.*				

Insider attacks can affect the network and cause disruption as a result of the wireless transmitted data being dropped, modified, or misrouted by attackers (Cho et al., 2012). Also see: Kebande, Karie and Omeleze (2016); and, Kebande, Karie, and Venter (2016).

Different types of attacks such as active (data modification, packet dropping) and passive (eavesdropping) attacks can easily be launched by insiders with malicious intents. According to Ren et al. (2006, p. 3), insider attacks in WSNs are classified into four categories: attacks related to "*data forwarding*", "*data generation*", "*routing*" and "*physical*". Hence, the different types of insider attacks in WSNs are summarised in Table 4.9. Also see: Mahncke and Williams (2014).

Similarly, Beyah and Venkataraman (2011) state that wireless rogue devices or access points are an increasing problem domain for the insider threats. Even though many organisations mainly focus on the security of wireless networks by using wireless intrusion detection systems (*WIDS*) in order to protect from attacks initiated by outsiders. However, such systems always overlook the threat of insiders or individuals who have authorised credentials within the organisation (Beyah & Venkataraman, 2011). Thus, most of the problems relating to insertion of rogue APs into the enterprise networks are often due to insiders. Moreover, Beyah and Venkataraman (2011, p. 56) describe the existence of these rogue APs is "*approximately 20 percent of all enterprise networks*" and network security can be compromised as a consequence. Similar to malicious insiders, it is essential to understand that, malicious outsiders can also place Fake APs to deceive a wireless STA into accessing the network though it, instead of the legitimate one. Subsequent attacks on the wireless node can later be initiated. Therefore, the healthcare industry, government and other organisations should be aware of insider threats and promote the methods to detect such rogue APs (Figure 4.7, which was the state-of-play ten years ago from 2001-2009) within the network (Beyah & Venkataraman, 2011).

Blackwell (2009, pp. 3-4) classified insider attacks according to the attacker's "*actions of sabotage (loss of availability and integrity), fraud (financial losses to the organisation or their customers by unauthorised transactions) and theft (disclosure of sensitive information or the loss of physical assets)*", according

the second Computer Emergency Readiness Team (CERT) guide to insider threats.

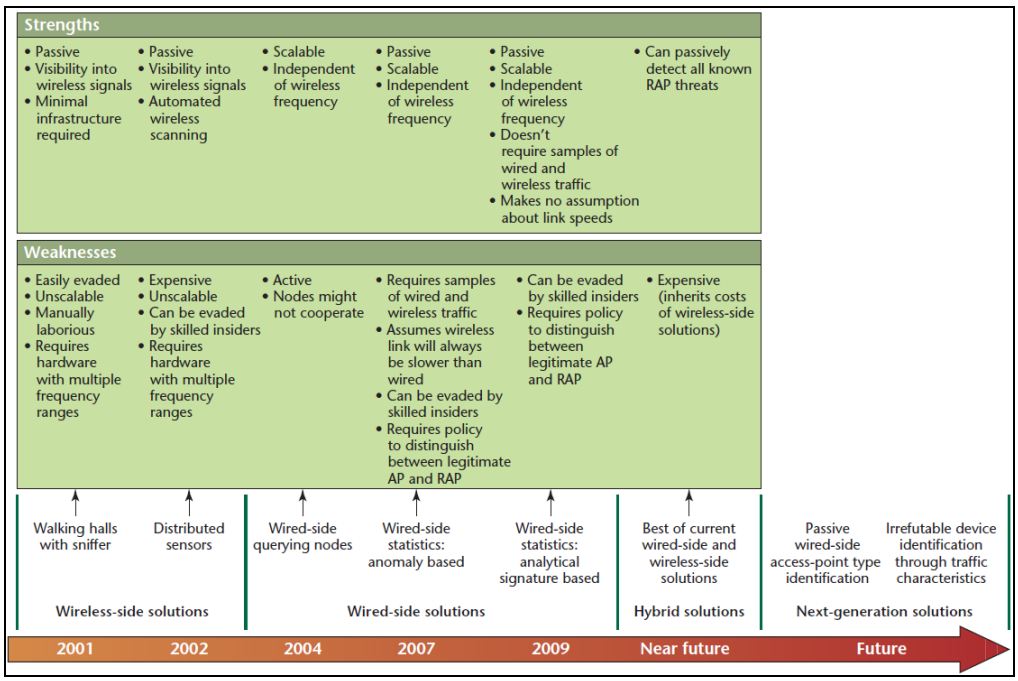


Figure 4.7: A rogue-access-point (RAP) detection road map including past decade of solutions from 2001-2009 (Beyah & Venkataraman, 2011, p. 60)

The insider attacks can be defined as the attacks initiated by insiders or malicious employees and such attacks are very difficult to encounter and diagnose. Accessing an IT system, information and the available resources by a malicious employee is authorised by their credentials (Blackwell, 2009). Furthermore, the security protection mechanisms such as firewalls or intrusion prevention systems (IPS/IDS) to protect IT systems, and entrance to the physical location of the hospitals or healthcare organisation, do not hinder the actions of malicious employees. Hence, a comprehensive systematic defence is essential to wireless medical systems and devices as there is not a single protection or security mechanism to prevent attacks initiated by an insider or the internal employee.

4.7.4 Standards Are Being Developed

There is one substantial limitation with regard to the applications of wireless technologies in healthcare systems (Delmastro, 2012). The problem is the "*the lack of interoperability among devices belonging to different vendors, even if they physically use the same wireless technology*" (Delmastro, 2012, p. 1292). Delmastro (2012) states that there is also a need for a common data format to

store patient's data in a centralised database, however, the problems related to interoperability could be solved by referring to the problems at different layers of ISO/OSI model (Figure 4.8). For instance, the problem at the upper application layer can be solved by "*defining data models and formats for devices' communication*" (Delmastro, 2012, p. 1293). Hence, the international organisations such as Digital Imaging and Communications in Medicine (DICOM), Health Level Seven International (HL7) and ISO/IEEE 11073 (also referred to as X73) are developing standards for interoperability in health information technology.

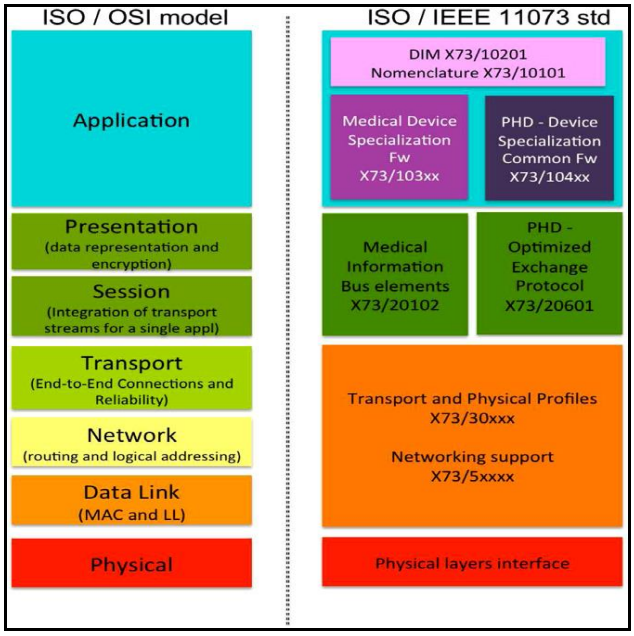


Figure 4.8: Correspondence between ISO/OSI model and IEEE 10073 standards (Delmastro, 2012, p. 1293)

4.7.5 Privacy Issues

As stated in Section 3.6, sensitive patient information can be misused by malicious people. For instance, malicious attackers could access the hospital information systems, the medical devices including implanted ones, and monitoring devices (such as PDAs, iPads, and smartphones used by nurses and doctors) could be infected by viruses. Hence, the security and privacy of the patients can be compromised.

Westin (1967, p. 7, cited in Parks et al., 2011, p. 3) defined information privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is

communicated to others". However, in healthcare informatics, Ishikawa (2000, cited in Parks et al., 2011, p. 4) stated the definition of patient information privacy should be based on "confidentiality, integrity, availability and accountability". There are consequences such as "patients might be subject to harassment, discrimination, economic harm or denied service from insurance or employers" if privacy of patient data is breached (Parks et al., 2011, p. 1).

Other researchers (Garfinkel et al., 2002; Thatcher et al., 2000, cited in Parks et al., 2011) argue that it would be difficult to examine issues related to patient information privacy in a healthcare environment due to changeable and complex variables, and stricter policies and regulations. Nonetheless, Parks et al. (2011, p. 5) summarised healthcare information "privacy issues and threats" from the perspective of a management information system (MIS) and health informatics (Table 4.10).

Table 4.10: Summary of privacy issues, threats and countermeasures (adapted from Parks et al., 2011, pp. 5-7)

Privacy Issues and Threats	**MIS References**	**Medical References**	**Technical Countermeasures**	**MIS and Media References**
Data Collection	(Culnan et al., 2009; Malhotra et al., 2004; Smith, 1993; Smith et al., 1996b; Solove, 2006; Stewart et al., 2002)	(Croll, 2010)	Anonymisation	(Claerhout et al., 2005)
Data Use & Disclosure	(Dinev et al., 2006; Li et al., 2010a; Malhotra et al., 2004; Solove, 2006)	(Agrawal et al., 2007; Boyd et al., 2010; Ishikawa, 2000; Mohan et al., 2004; Hno-Machado et al., 2004; Patel et al., 2000; Quantimet et al., 2000)	Anonymisation	(Boyd et al., 2007; Chiang et al., 2010b; Mohan et al., 2004; Neubauer et al., 2004; Quantin et al., 2000)
			Cryptographic	(Quantin et al., 2000)
			Access control	(Chen et al., 2010; Haas et al., 2011)
Unauthorised Access	(Cuhan et al., 2009; Smith et al., 1996a; Solove, 2006; Stewart et al.,	(Chen et al., 2010; Croll, 2010; Kluge, 2007; Mohan et al., 2004;	Access Control Mechanism	(Blobel et al., 2006; Chen et al., 2010; Lovis et al., 2007; Mohan

	2002)	Neubauer et al., 2001; Patel et al., 2000; Reni et al., 2004; Sujansky et al., 2010; Van der Lin et al., 2009)		et al., 2004; Peleg et al., 2008; Reni et al., 2004; Sujansky et al., 2010; Van der Linden et al., 2009)
			Encryption	(Kluge, 2007)
			Anonymisation	(Boyd et al., 2007; Neubauer et al., 2011)
Secondary Use	(Culnan et al., 2009; Culnan, 1993; Smith et al., 1996a; Solove, 2006; Stewart et al., 2002)	(Aberdeen et al., 2010; Chiang et al., 2003; Croll, 2010; Ishikawa, 2000; Neubauer et al., 2011; Quantin et al., 2000)	Anonymisation	(Aberdeen et al., 2010; Neubauer et al., 2011)
Errors		(Sadan, 2001; Van der linden et al., 2009)		
Balance between privacy policies, Clinical Users and Patient Expectation		(Croll, 2010; Mohan et al., 2004)		
Awareness of privacy practices	(Malhotra et al., 2004)	(Croll, 2010)		
EHRs design and lack of standards		(Kluge, 2007)		

4.8 CONCLUSION

Chapter 4 documented and detailed wireless security architectures, goals, threats, attacks, and the challenges faced in the medical environment. Importantly, significant issues and problems were identified that warrant further investigation. Chapter 5 now reviews and documents the higher level security provisions that impact the matters raised in Chapter 4. These include standards, protocols, legislation, and management models that are implemented to mitigate risk.

Chapter Five

WIRELESS NETWORK ARCHITECTURE AND STANDARDS

5.0 INTRODUCTION

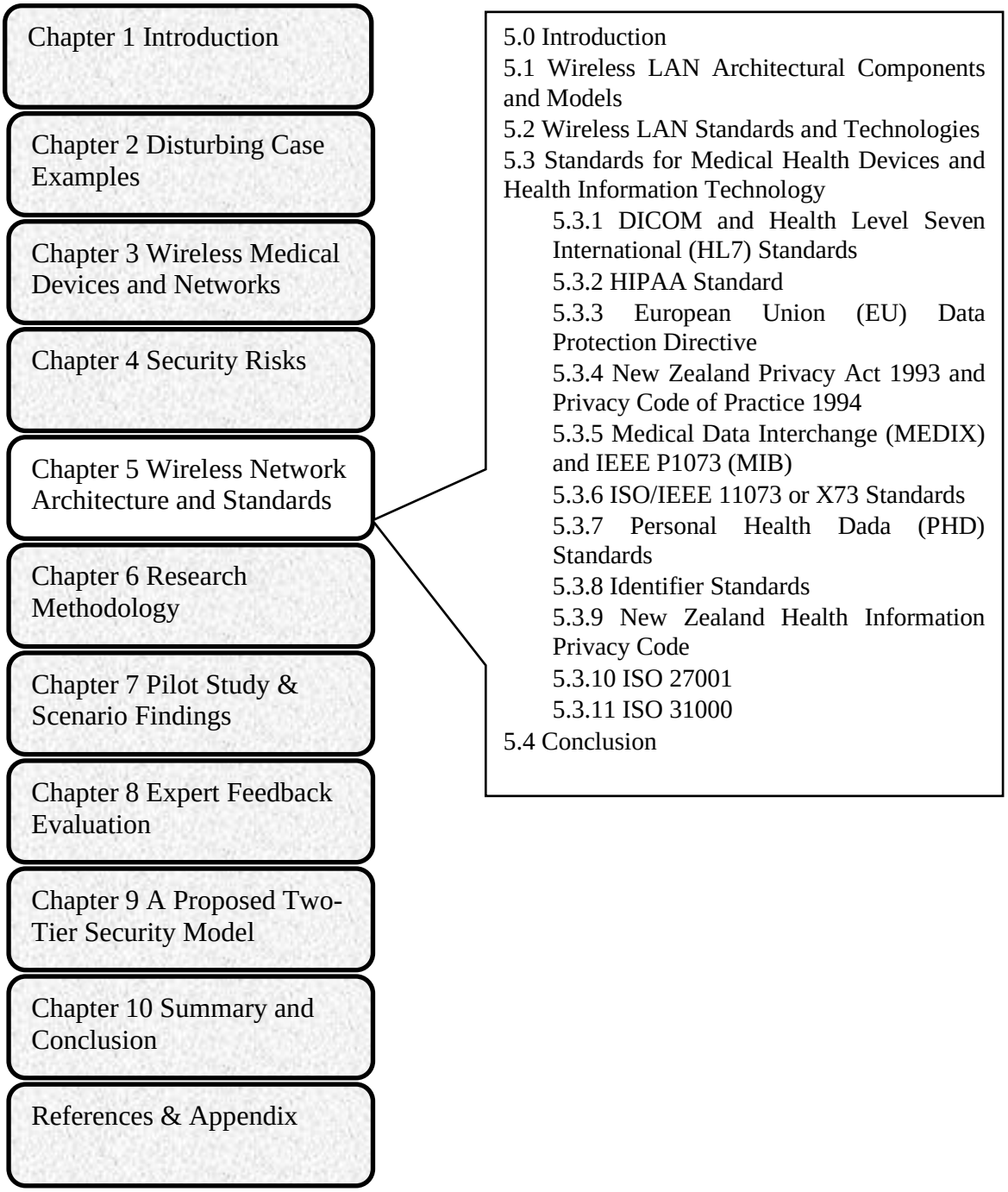


Figure 5.1: Roadmap of Chapter 5

Different types of wireless networks are being deployed in the medical healthcare industry (previously mentioned in Section 2.2.1). The main purpose of the

wireless network is to provide two or more devices to communicate without physical cabling. However, different wireless networks have different operating frequencies, coverage areas and data rates. For instance, Karygiannis and Owens (2002, pp. 17-19) stated that IEEE 802.11 WLAN was designed "*to support medium-range, high data rate applications*" with "*greater flexibility and portability than do traditional wired local area networks (LANs)*" by employing mobile and portable stations connecting to the network. The following sections will document and review typical wireless architectural components and models, WLAN standards, and standards for medical health devices and health information technology.

5.1 WIRELESS LAN ARCHITECTURAL COMPONENTS AND MODELS

The WLAN architecture is made up of physical and logical components. Scarfone et al. (2008, p. 14) state that there are two basic physical components of IEEE 802.11 WLAN, namely a "*Station (STA)*" and an "*Access Point (AP)*". In general, wireless end-user devices such as laptops, personal digital assistants (PDAs), and smartphones are referred to as STAs, whereas any devices or entities that have STA functionality and can provide distributed services via the wireless medium for associated STAs and are known as APs (Scarfone et al., 2008; IEEE Std. 802.11, 2007) (see Figure 5.2).

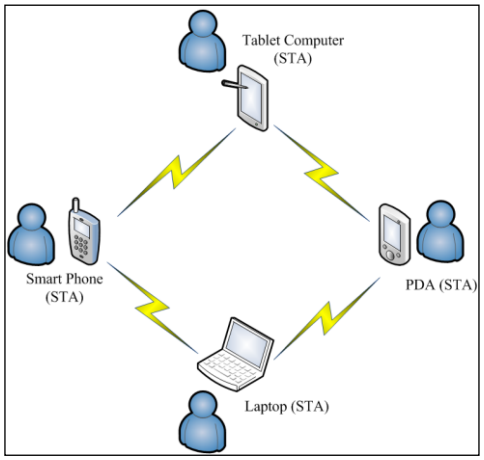


Figure 5.2: Ad hoc mode or independent basic service set (IBSS) model (adapted from Scarfone et al., 2008, p. 15; Earle, 2006, p. 77)

Scarfone et al. (2008, p. 14) add that an AP can logically not only connect "*STAs with a distribution system (DS), which is typically an organisation's wired infrastructure*", but also "*connect wireless STAs with each other without*

accessing a DS". Similarly, the logical component of WLAN can be referred to as the basic service set (BSS) that provides the function to manage a group of wireless nodes (Laet & Schauwers, 2005; Housley & Arbaugh, 2003).

To configure BSS, the IEEE 802.11 WLAN architectural model can be classified into two basic models: ad hoc or peer-to-peer (P2P), or infrastructure modes (Scarfone et al., 2008; Laet & Schauwers, 2005). The former does not utilise APs in data communications between two or more wireless STAs (see Figure 5.2), while the latter has deployed at least an AP to provide communications between the wireless STAs and a DS (see Figure 5.3). Hence, the ad hoc mode or peer-to-peer (P2P) mode of operation is possible "*when two or more wireless STAs are able to communicate directly to one another*" (Scarfone et al., 2008, p. 14) and "*a set of STAs configured in this ad hoc manner is known as an independent basic service set (IBSS)*".

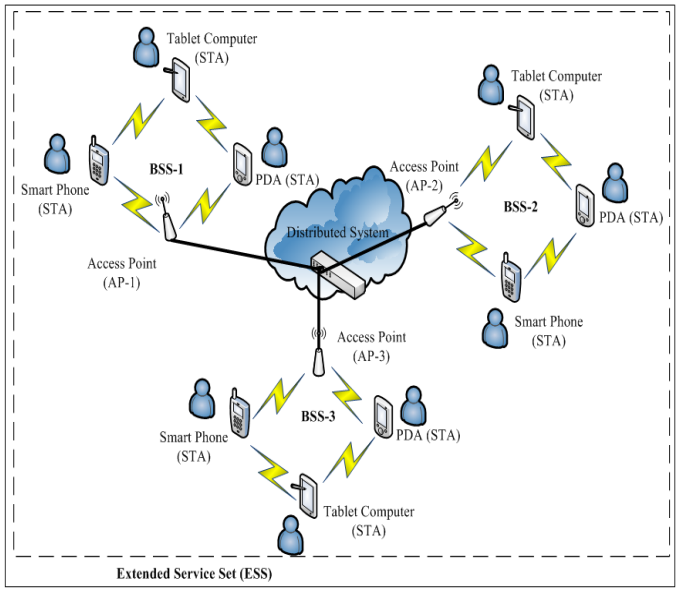


Figure 5.3: Infrastructure mode or extended service set (ESS) model (adapted from Scarfone et al., 2008, p. 15; Earle, 2006, p. 77)

In contrast, the IEEE 802.11 WLAN infrastructure mode consists of one or more AP that controls all wireless traffic (Earle, 2006). The infrastructure mode is composed of a BSS that includes an AP and one or more STAs (Scarfone et al., 2008). The infrastructure mode is commonly an adopted wireless network architecture and it is also referred to as an extended basic service set (EBSS) if multiple BSS networks are connected to a single DS (Scarfone et al., 2008).

Hence, the IEEE 802.11 WLAN infrastructure mode is illustrated in Figure 5.3 by using three BSSs connected to a DS.

5.2 WIRELESS LAN STANDARDS AND TECHNOLOGIES

WLANs and devices were originally specific to the manufacturers (Earle, 2006). As a result, the IEEE standardised 802.11 wireless standards introduced since 1997 allow different wireless devices from different vendors to interoperate together. Even though IEEE 802.11 is the most ubiquitous wireless technology nowadays, there are other wireless technologies (see Table 4.1) such as IEEE 802.15.1 (Bluetooth), IEEE 802.15.3 and IEEE 802.15.4 (high data rate PAN, and low data rate PAN or Zigbee, respectively) and cellular 3, 4, 5G do exist. Paquette et al. (2011, p. 244) state that Bluetooth and Zigbee are preferably suited for BANs, and PANs, and hence "emerging technologies such as body worn smart sensors will use these standards to communicate with each other and a personal server wirelessly". However, it is essential to note that different wireless technologies have different operating frequencies, coverage area, throughput or data rate, and candidate system. Therefore, several different wireless technologies are classified as shown in the Table 5.1.

Table 5.1: Classification of Wireless technologies (adapted from Liolios et al., 2010; Banitsas et al., 2002; Sendra, 2010, Brown, 2003; Elliot, 2007; Haskin, 2007; Jacobs, 2007; Laet & Schauwers, 2005; Stallings, 2004; Stanley, 2002; Varshney, 2003)

Technology	Data Rate	Coverage Area	Frequency Band	Candidate Subsystem
ANT (Wireless Personal Network protocol)	1Mbps	Local area	800 MHz, 1900 MHz, 2100 MHz	WPAN
Bluetooth (IEEE 802.15.1)	721 Kbps	10m – 150m	2.4 GHz ISM	WBAN
Bluetooth Low Energy	1 Mbps	10m	2.4 GHz ISM	WBAN
Bluetooth 3.0 + High Speed	3 – 24 Mbps	10m	2.4 GHz ISM	WBAN
Cellular 3G	14.4 Mbps/5.8 Mbps	m - km	800 MHz, 1900 MHz, 2100 MHz	
Cellular 4G	100 Mbps/ 50 Mbps	m -km	700 MHz, 850 MHz, 900 MHz, 1800 MHz, 2100 MHz,2300 MHz, 2600 MHz	
Cellular 4G+	300 Mbps/	m -km	700 MHz, 850	

	150 Mbps		MHz, 900 MHz, 1800 MHz, 2100 MHz,2300 MHz, 2600 MHz	
Cellular 5G	1,000-10,000 Mbps	m -km	3.5 GHz	
Digital Enhanced Cordless Telecommunications (DECT)	32 Kbps	100m	1880 – 1900 MHz	
IEEE 802.11a	54 Mbps	150m	5 GHz ISM	BAN/PAN
IEEE 802.11b	11 Mbps	150m	2.4 GHz ISM	BAN/PAN
IEEE 802.11g (Wi-Fi)	54 Mbps	300m	2.4 GHz ISM	BAN/PAN
IEEE 802.11n (Wi-Fi)	540 Mbps	300m	2.4 GHz ISM	BAN/PAN
IEEE 802.11ac (Wi-Fi)	3400 Mbps	3 m	5 GHz ISM	BAN/PAN
IEEE 802.15.3 (High data rate wireless personal area network)	11 – 55 Mbps	1m – 50m	2.4 GHz ISM	PAN
IEEE 802.15.4 (Low data rate wireless personal area network such as Zigbee)	250 Kbps	100m – 300m	2.4 GHz ISM 868 MHz, 915 MHz ISM	
Insteon (connecting lights and Switch)	13 Kbps	Home Area	131.65 KHz (power line) 902 -924 MHz	
Infrared Data Association (IrDA)	4 Mbps (IrDA – 1.1)	2m	IR (0.90 micro - meter)	
Radio – frequency Identification (RFID)	10 – 100 Kbps	1- 100m	860 – 960 MHZ	
RuBee (IEEE 1902.1)	9.6 Kbps	30m	131 KHz	
Ultra-wideband (Standard ECMA-368)	480 Mbps	<10m	3.1 – 10.6 GHz	
Z-Wave (Home automation)	9.6 Kbps	30m	900 MHz ISM	

5.3 STANDARDS FOR MEDICAL HEALTH DEVICES AND HEALTH INFORMATION TECHNOLOGY

There are numerous guidelines and standards related to medical healthcare technology. These guidelines and standards are created and embraced by international organisations, government agencies and professional or specialised organisations and societies (David & Judd, 2006). According to the healthcare standards directory of Emergency Care Research Institute (ECRI), which is a non-profit international organisation that promotes the standards to improve patient safety and cost-effectiveness of patient care, there are more than "*20,000 individual standards and guidelines produced by 600 organisations and agencies from North America alone*" (David & Judd, 2006, p. 75-14). Some of the standards address design and manufacturing practices for medical devices and

related software although others apply to the safety and performance requirements for particular technologies (for instance, electrical and radiation safety standards). Likewise, standards are also required for the "*coding and structure of clinical patient care data; the content of data sets for specific purposes; and electronic transmission of such data to integrate data efficiently across departmental systems within a hospital and data from the systems of other hospitals and healthcare providers*" (Fitzmaurice, 2006, p. 41-12). Hence, this section will selectively cover specific standards such as Digital Imaging and Communications (DICOM), Health Level Seven International (HL7), Health Insurance Portability and Accountability Act of 1996 (HIPAA), European Union Data Protection Directive (1998), Medical Data Interchange (MEDIX) Standard, IEEE P1073 Medical Information Bus (MIB), International Standard Organisation/Institute of Electrical and Electronics Engineers (ISO/IEEE 11073 or X73), and Personal Health Data (PHD).

5.3.1 DICOM and Health Level Seven International (HL7) Standards

DICOM is standardised by the American College of Radiology – National Electronic Manufacturers' Association (ACR-NEMA) for medical imaging. It outlines the communication standards and data formats for radiologic images and "*is supported by most radiology picture archiving and communication systems (PACS) vendors*" (Blair, 2006, p. 42-4). On the other hand, HL7 is used for "*the communication of medical information systems residing in different facilities*" (Delmastro, 2012, p. 1293), "*clinical observations and clinical data including test results; admission, transfer, and discharges records; and charge and billing information*" (Blair, 2006, p. 42-4). For instance, Turab et al. (2010) discussed the wireless network architecture that supports HL7 requirements (this is a standard that supports clinical patient care), in which the restriction of different users' rights was explained. To sum up, both DICOM and HL7 standards mainly focus on the data exchange at application layer (Delmastro, 2012).

5.3.2 HIPAA Standard

Health Insurance Policy and Accountability Act (HIPAA) is United States legislation that governs the privacy of medical health data and envisioned to permit entities or individuals to control access to or disclose personal medical

health information. HIPAA details the way in which medical health data has to be protected and who has to protect it. Hence, Fitzmaurice (2006) stated that HIPAA mandate how personal health information should be protected and shared within the United States or any supplier trading with the United States. In fact, it is crucial to protect privacy and confidentiality of patient data as the exchange of patient data is increasingly happening among health service providers' networks.

According to HIPAA, the participants from the health industry have to ensure that patient data can only be disclosed if consent is given by the patient. Otherwise, the consequences of infringing the Privacy Rule (effective in April 2003) can be very costly (Fitzmaurice, 2006). Likewise, HIPAA enforces the Security Rule (effective in April 2005) that addresses guidelines for the minimum-security requirements to ensure the security, confidentiality and integrity of electronically stored or transmitted personal medical health information (Fitzmaurice, 2006). Moreover, the patients' privacy protection mandates HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH) (Parks et al., 2011). Similarly, the requirements of HIPAA including the ways in which to protect medical "*data confidentiality, privacy of patients' personal information, proper access to patients' medical records, the privileged limitation of clinicians and exceptional emergency treatment*" were defined in the published paper written by Ren et al. (2010, p. 60). However, such patient's privacy protection mandates, such as HIPAA, does not specify certain procedures on how healthcare providers should protect personal health information even though security requirements, such as encryption, authentication and authorisation, are noted (Fitzmaurice, 2006).

5.3.3 European Union (EU) Data Protection Directive

The European Union (EU) Data Protection Directive (1998) is an integral element of EU privacy law that enforces the process of individual's personal data protection and its movement within the European Union (European Data Protection Supervisor, 2019, p. 1). The EU directive is also applied to other companies from overseas (e.g. companies from United States, Canada) that do business with the EU. However, such a directive for data protection is superseded

by a new regulation, referred to as "EU General Data Protection Regulation" released on 25 May 2018 (European Data Protection Supervisor, 2019, p. 1).

5.3.4 New Zealand Privacy Act 1993 and Privacy Code of Practice 1994

The deployment of wireless technologies in medical or clinical environments can provide benefits to the existing healthcare services. On the other hand, there are several challenges related to deployment of such technologies due to the inherent nature of wireless. For instance, most of the WMedDs are battery operated, and have low processing power and memory. Hence, the battery power could be exhausted very easily due to the malicious attack and the application of a strong cryptographic algorithm is somewhat impossible to secure transmitted data. However, the information of patients or device users must be secure, private and accessible by authorised people such as physicians or nurses. Similar to other countries, the New Zealand Privacy Act 1993 (Department of Labour, 2005, p. 16) is "*intended to promote and protect personal privacy by imposing rules on the ways that agencies collect, store, use, and disclose personal information. It also gives people a legal right to have access to information about themselves, and a right to request correction of any incorrect or misleading personal information.*" There are twelve privacy principles in the Privacy Act and those principles are summarised in Table 5.2.

Table 5.2: Summary of the New Zealand privacy principles and their coverage areas (adapted from Office of the Privacy Commissioner, 2013a, p. 1)

Privacy Principles	**Related Coverage**
Principles 1-4	*Collection* of personal information
Principle 5	*Storage and security* of personal information
Principles 6 and 7, plus parts 4 and 5 of the Act	Requests for *access* to and *correction* of personal information
Principle 8	*Accuracy* of personal information
Principle 9	*Retention* of personal information
Principles 10 and 11	*Use and disclosure* of personal information
Principle 12	Using *unique identifiers*

Similarly, "*the Privacy Act 1993 gives the Privacy Commissioner the power to issue codes of practice that become part of the law*" (Office of the Privacy

Commissioner, 2013b, p. 1). However, the privacy *Codes of Practices* only applies to specific areas such as "*health, telecommunications and credit reporting*" (Office of the Privacy Commissioner, 2013a, p.1). For instance, the "*Health Information Privacy Code (HIPC) 1994 and a commentary (2008 edition)*" apply to "*the health information relating to identifiable*", "*agencies that provides personal or public health or disability services*" and "agencies that do not provide health services to individuals but which are part of health sector such as the Accident Compensation Corporation (ACC), the Ministry of Health, etc.," (Office of the Privacy Commissioner, 2013c, p. 1). More detailed information about HIPC 1994 and its revised edition 2008 can be found in the documents released on the website of Office of the Privacy Commissioner (2013c, p. 1). These legislations are under regular review and a new round of updates began again in 2018.

5.3.5 Medical Data Interchange (MEDIX) and IEEE P1073 (MIB) Standards

Blair (2006) states that the exchange of medical data between hospital and clinical IT systems (MEDIX) is developed by the Engineering in Medicine and Biology Society (EMB) of the Institute of Electrical and Electronics Engineers (IEEE). Likewise, the IEEE P1073 Medical Information Bus (MIB) standard addresses the connections of medical devices to "*point-of-care information systems*" (Blair, 2006, p. 42-4).

5.3.6 ISO/IEEE 11073 or X73 Standards

Since 1980, there are standards for the medical health devices such as the International Organisation for Standardisation/Technical Committee 215 (ISO/TC215 – the standardisation of Health Information and Communications Technology), European Committee for Standardisation/Technical Committee 251 (CEN/TC 251 - the standardisation of Health Information and Communications Technology in the European Union), IEEE 1073 (Lim et al., 2010). However, these different standards have now converged to establish ISO/IEEE 11073 health informatics (medical device communications) standards (Lim et al., 2010).

These ISO/IEEE 11073 or X73 standards are primarily aimed to provide "*real-time plug-and-play interoperability of medical and healthcare devices*" and "*efficient exchange of care device data, acquired at the point-of-care, in all care*

environments" (ISO/IEEE 11073-20101:2004, 2013; Martinez et al., 2010; Martinez-Espronceda et al., 2008), and hence ISO/IEEE 11073 or X73PoC standards are especially to address medical device communications in *the Point-of-Care* (PoC) of the patients in the *Intensive Care Units* (ICUs). All standards are under regular review and these documents were current at the time of writing.

5.3.7 Personal Health Data (PHD) Standards

According to researchers (Nam et al., 2011; Lim et al., 2010, p. 217), ISO/IEEE 11073 PoC standards are not suitable for healthcare devices at "*home and mobile environments*". In fact, the communication of medical devices (e.g. blood pressure, electrocardiogram, glucose monitoring devices) from different vendors is not feasible as the protocols are mostly developed in-house (Nam et al., 2011). As a result of the development in wearable wireless devices and emergence in communication technologies; the ISO/IEEE 11073 or X73 Personal Health Data (X73PHD) standards have been developed for PHDs with limited resources such as processors, memory and power (Nam et al., 2011; Martinez et al., 2010; Lim et al., 2010; Clarke et al., 2007). Hence, the ISO/IEEE 11073 PHD standards are essentially developed for "*disease management, elderly living alone, and health and wellness*" (Lim et al., 2010, p. 217) by describing "*the protocol for information delivery between individual medical devices*" (e.g. glucose, blood pressure monitors) "*and the manager (e.g. smartphone or personal computer) that collects and manages the information from individual medical devices*" (Nam et al., 2011, p. 789).

5.3.8 Identifier Standards

According to Blair (2006), a comprehensive universal identifier standard is needed in order to exclusively identify each patient, provider, site-of-care and product. For instance, the United States of America (U.S.) and New Zealand generally use *social security numbers* (SSNs) and national health index (NHI) numbers as patient identifiers, respectively. However, the infringements of confidentiality of patient data happen because SSNs are also usually used for other purposes (Blair, 2006, p. 42-2); hence the American Society for Testing and Materials (ASTM) E31.12 subcommittee has developed the "*Guide for Properties of Universal Health Care Identifier*". Similarly, the division of the U.S.

department of health and human services, *Health Care Financing Administration* (HCFA), sets the *Universal Physician Identifier Number* (UPIN) standard (Terrell et al., 1991, cited in Blair, 2006, p. 42-2), which is normally designated to physicians whereas the *Standard Prescriber Identification Number* (SPIN) is standardised by National Council of Prescription Drug Programs (NCPDP) for pharmacists in the retail sector. Likewise, HCFA and the *Health Industry Business Communications Council* (HIBCC) define site-of-care identifier systems for Medicare usage in the U.S. But, Blair (2006) states that these identifier standards or systems are only accepted in the U.S and there exists a need for universally accepted uniform identifier standards.

5.3.9 New Zealand Health Information Privacy Code 1994

The New Zealand Health Information Privacy Code (NZHIPC) is a code of practice regarding how to collect and use health information as issued by the Privacy Commissioner (2017). These may be in the form of the patient's medical history, medical test results, and medical services completed. The code covers health agencies such as organisations that provide health care and services, insurers, and the Ministry of Health. The code states that a patient's health information should not be collected unless the information will be used for a lawful purpose (Privacy Commissioner, 2017; Slane, 1994). The health agency should collect the information directly from the concerned individual or the representative.

The agency should inform the person that the information is collected, the purpose of collecting the information, and who are the recipients of the collected information (Privacy Commissioner, 2017; Slane, 1994). If the concerned individual wants to view the information or to make corrections, the health agency must allow the person to do so. The health agency should also ensure that measures are in place in order to protect the privacy of the information. One way of protecting health information privacy is to limit the number of people that the information will be disclosed to (Privacy Commissioner, 2017; Slane, 1994). Disclosure of the information should be authorised by the concerned individual or representative. Once the information is no longer needed, the health agency

should not keep the patient's information to avoid unnecessary breaches in privacy. To summarise, there are twelve rules in NZHIPC as shown in Table 5.3.

Table 5.3: Summary of rules of New Zealand Health Information Privacy Code and their coverage areas (adapted from Privacy Commissioner, 2017)

Privacy Principles	**Related Coverage**
Rule 1, Rule 2, Rule 3 and Rule 4	*Collection* of health information: must only be done for a lawful purpose and it is essential to collect the information for that purpose. When collecting health information from a person, reasonable steps should be taken including "why health information may be collected, where it may be collected from, and how it is collected" (Privacy Commissioner, 2017, pp. 8-13).
Rule 5	*Storage and security* of health information: health agencies must have reasonable security safeguards to protect against unauthorised access, use, modification or disclosure and other misuse of health information (Privacy Commissioner, 2017, p. 14).
Rule 6	*Access* to personal health information gives "individuals to have the right to access their health information" (Privacy Commissioner, 2017, p. 15).
Rule 7	*Correction* of health information allows "individuals to have the right to correct their health information" (Privacy Commissioner, 2017, p. 16).
Rule 8	*Accuracy* of health information is ensuring "information is accurate, up to date, complete, relevant and not misleading" (Privacy Commissioner, 2017, p. 17).
Rule 9	*Retention* of health information is important. In fact, health information must not be kept for longer than is required (Privacy Commissioner, 2017, p. 18).
Rule 10	*Limits on use* of health information in which "any health agency that holds health information obtained in connection with one purpose must not use the information for any other purpose unless the health agency believes on reasonable grounds" (Privacy Commissioner, 2017, p. 19).
Rule 11	*Limits on disclosure* of health information (Privacy Commissioner, 2017, pp. 21-24).
Rule 12	*Unique identifiers* such as "IRD numbers, bank client numbers, driver's licence and passport numbers can be used" (Privacy Commissioner, 2017, pp. 25-26).

5.3.10 ISO 27001

ISO 27001 is a standard for information security which is designed to provide all types of organisations a model for implementing, maintaining, and monitoring an Information Security Management System (ISMS). This is a framework of

different procedures and controls involved in information risk management (Honan, 2014). It provides best practices and standards which organisations can follow to have their ISMS certified. Aside from security policies and access controls, ISO27001 also discusses standards for asset management, physical security, human resources security, communications management, incident management, business continuity management, information systems acquisition, and compliance (Honan, 2014). By following the ISO 27001 standard, organisations can obtain increased reliability of their security systems, as well as ensure compliance with legislation.

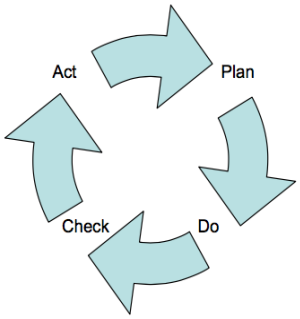


Figure 5.4: PDCA model (Honan, 2014, p. 39)

ISO 27001 follows the Plan, Do, Check, and Act (PDCA) model, as illustrated in Figure 5.4. In the Plan phase, the scope, objectives, and risks of the ISMS are defined. The Do phase is the implementation of the risk treatment plan. The Check phase reviews the procedures of the ISMS, and the Act phase includes the improvements identified in the previous phase of the cycle. The PDCA model ensures that the ISMS is reviewed and improved continuously (Honan, 2014).

5.3.11 ISO 31000

ISO 31000 provides generic guidelines on risk management which can be adapted by any kind of organisation, regardless of the industry (Cherdantseva, Burnap, Blyth, Eden, Jones, Soulsby, & Stoddart, 2016). It provides a common set of terminologies for risk management, as well as performance criteria that organisations can follow. It states that risk management should be systematic and integral to the organisation's processes and should promote the continuous improvement of the organisation (Purdy, 2010). It follows the risk management process as shown in Figure 5.5. The risk management process illustrates that communication and consultation, as well as monitoring and review should be done continuously in parallel with the other phases. The process begins with

identifying the goals of the organisation and the factors that might affect these objectives. The risks are identified analysed by defining the likelihood and consequences of the risks (Purdy, 2010). The risks are then evaluated by prioritising the different risks, then the selected risk treatment is tested and implemented.

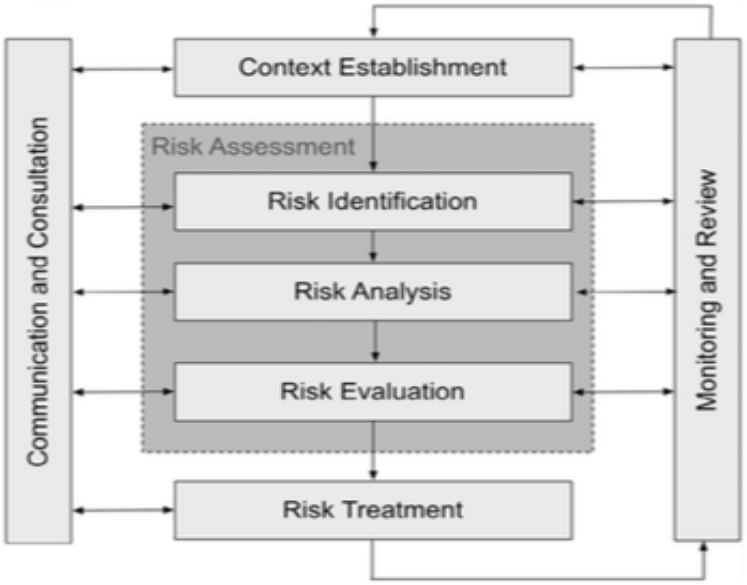


Figure 5.5: Risk Management Process (Cherdantseva et al., 2016, p.19)

5.4 CONCLUSION

Chapter 5 has reviewed the high level security concerns impacting of medical environment IT security. Much of the literature reviewed reflected the data available at the time of reviewing, because legislation and standards are under constant revision. The range and depth of documentation is indicative of the urgency and the concern for risk treatments that protect the patients from unwanted disclosure or harm. Chapter 5 completes the literature review that has from Chapter 2 covered the scope of the research area. Chapter 6 will now define a methodology in which some of the claims from the literature may be tested. The aim of the methodology is to replicate and verify the asserted wireless vulnerabilities identified in the previous chapters, and then to recommend improved technology and information management models.

Chapter Six

RESEARCH METHODOLOGY

6.0 INTRODUCTION

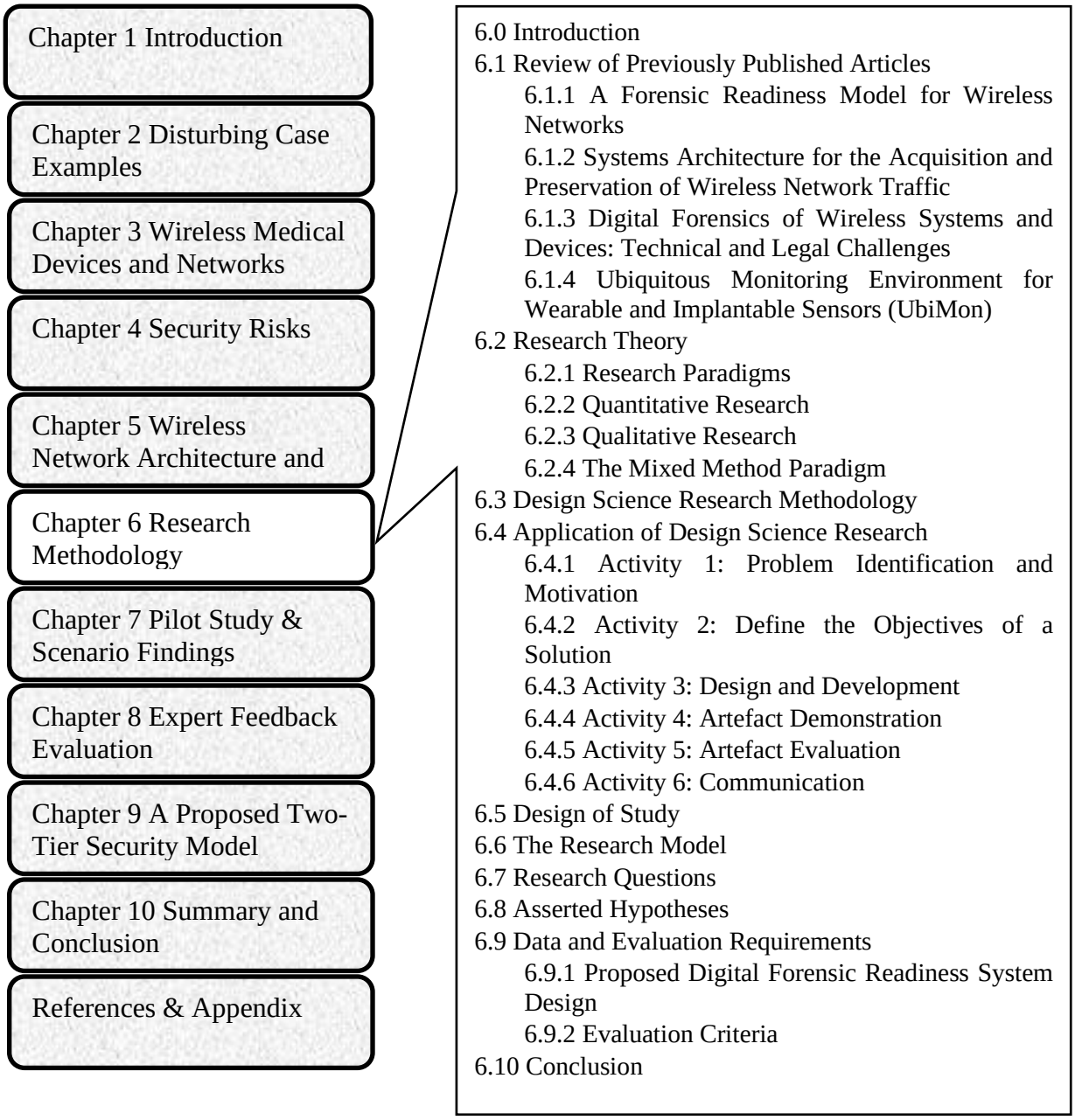


Figure 6.1: Roadmap of Chapter 6

Chapters 2–5 have specified the scope of the problem context, and identified the security problems and vulnerability issues associated with the use of wireless services in medical environments. The problems have both technical and

theoretical (in law and standards) solutions but gaps in knowledge and practice exist. In Chapter 6 a methodology is developed to investigate wireless medical systems for security and forensic readiness. The position that forensic readiness is part of security preparations is adopted from the literature that suggests any security provision has a residual risk of failures. Security comes before an event to protect, and forensic capability allows further risk mitigation after the event to protect the system.

Chapter 6 is structured to review examples of previously published research that identifies how others went about doing research in the target area. In this way, best research practices for the area of study can be targeted and learned from others. Then, a Design Science research methodology is adopted and developed for this project. The objective of the research is to design a forensically ready wireless medical system. Consequently, the literature review has delivered the best design to date (see Figure 6.5) that can be tested for improvements. The pilot study results presented in Chapter 7, provide data and the construction of a new and improved model (see also Appendix E). For the purpose of the design science methodology, the digital forensic readiness models are the artefacts of interest and the artefact that is subjected to evaluation and continuous improvement processes. The second part of Chapter 6 defines the methodology and the data collection requirements.

6.1 REVIEW OF PREVIOUSLY PUBLISHED ARTICLES

Four relevant research reports are reviewed in the following sub-sections to locate guidance on how to investigate security vulnerabilities and how to design a digitally ready system for the wireless medical environment. The first article is an up to date attempt to create a wireless digital readiness model. It reviews the technical challenges and scope. The second addresses the problem of capturing and preserving wireless traffic and delivers working detail for setting up the experiments. The third shows research around standardisation issues and the types of legal risk associated with medical technologies. The fourth is research into the real continuous monitoring of patients. Together these four published papers have comprehensive guidance for guiding a study in the problem area.

6.1.1 A Forensic Readiness Model for Wireless Networks

The article written by Ngobeni, Venter and Burke (2010) proposes a wireless forensic readiness model (*WFRM*) in order to support monitoring, logging and preserving the traffic of wireless local area network (WLAN) for digital forensic investigation (DFI). As a result of advances in wireless technologies, there exists ubiquitous WLANs or wireless "*hotspots*" covering the areas "*such as convention centers, airports, schools, hospitals, railway stations, coffee shops and other locations to provide seamless access to the Internet*" (Velasco et al., 2008, cited in Ngobeni et al., 2010, p. 107). The WLANs users have the advantages of mobility and flexibility due to the nature of wireless, but they also need to be aware that these networks are the main target of malicious cyber-attacks. Hence, the digital forensics of WLAN is valuable for acquiring digital evidence (DE) associated with malicious activities.

Ngobeni et al. (2010, p. 107) firstly states that *WLAN digital forensic* (WLAN-DF) entails "*the application of methodologies and tools to intercept and analyse wireless network events for presentation of digital evidence in a court of law*". The key challenges of performing DFI in WLANs and the techniques required were outlined. Subsequently, the authors identified the possible WLANs' criminal misuses. For instances, the "*WLAN detection and connection*", the "*concealment of digital evidence*" and the "*WLAN as an attack vector*" were classified as WLANs misuses (Ngobeni et al., 2010, p. 108). The sources and acquisition of DE could be determined by the particular wireless device. However, the absence of a physical footprint due to the nature of wireless devices is the critical challenge for identification of the wireless devices (Turnbull & Slay, 2008 cited in Ngobeni et al., 2010). The issues relating to losing DE while identifying and acquiring DE during DFI are often due to huge amount of network traffic and the limitations of different DF tools such as "*Wireshark*, *Kismet* and *AirCapture*" (Ngobeni et al., 2010).

WLAN-DFI investigation requires phases in the DF processes, such as defining "*the scope an goals of the investigation*", determining "*the work and material*", acquiring "*the images of the devices to be examined*", performing "*the digital forensic analysis*" and preparing "*the report*" must be performed (Ngobeni et al., 2010, p. 109). Likewise, the phases for DF process for the renowned and

recognised DF tools used in DFI are elaborated and compared with *WFRM* (as shown in Table 6.1). However, the phases in DF processes for DF tools are not the same due to the lack of standardisation (Ngobeni et al., 2010).

Table 6.1: Digital Forensic phases for EnCase, FTK and WFRM (Ngobeni et al., 2010, p. 110)

Encase	FTK	WFRM
1. Preview	1. Detection	1. Monitoring
2. Imaging	2. Identification	2. Logging
3. Verification	3. Analysis	3. Preservation
4. Recover and Analysis	4. Preservation	4. Analysis
5. Restoration	5. Reporting	5. Reporting
6. Archiving		

The main purpose of DF readiness is to reduce in the cost, and time of incident response and investigation, whereas the credibility of the DE being acquired has to be maintained (Endicott-Popovsky et al., 2007, cited in Ngobeni et al., 2010). The malicious attacks could be promptly and effectively responded by organisations that implement DF readiness (Ngobeni et al., 2010). As a result, the organisation that has implemented WLANs should be "*forensically ready*" in order to collect and store DE prior to the occurrence of malicious attacks.

The researchers (Ngobeni et al., 2010) mentioned that monitoring wireless network traffic at access points is the utmost significant characteristic of the proposed *WFRM* (Figure 6.2). The traffic monitored is stored in a log files and its integrity has to be preserved. DE availability is required that minimises the DFI cost.

Consequently, the phases of DF processes relating to the proposed *WFRM* (such as "*monitoring, logging, preservation, analysis and reporting*") are detailed (Ngobeni et al., 2010, pp. 111-112). In the first phase of *WFRM*, all wireless access points (APs) have to be modified in order to monitor all network traffic created by the connected devices. Filtering "*inbound and outbound wireless traffic*" by using a firewall is also implemented on the devices or components monitored (Ngobeni et al., 2010). In the second phase, each AP being monitored must log the network traffic into its individual "*capture unit (CU)*". Then, the traffic logged should be splited into smaller chunks of data (1MB) and stored in separate areas, such as "*a fixed-size block of data*" (B1, B2 and so on in Figure

6.2). It is transferred to "*permanent storage*" once the *CU*'s buffer is full (Ngobeni et al., 2010, p. 111).

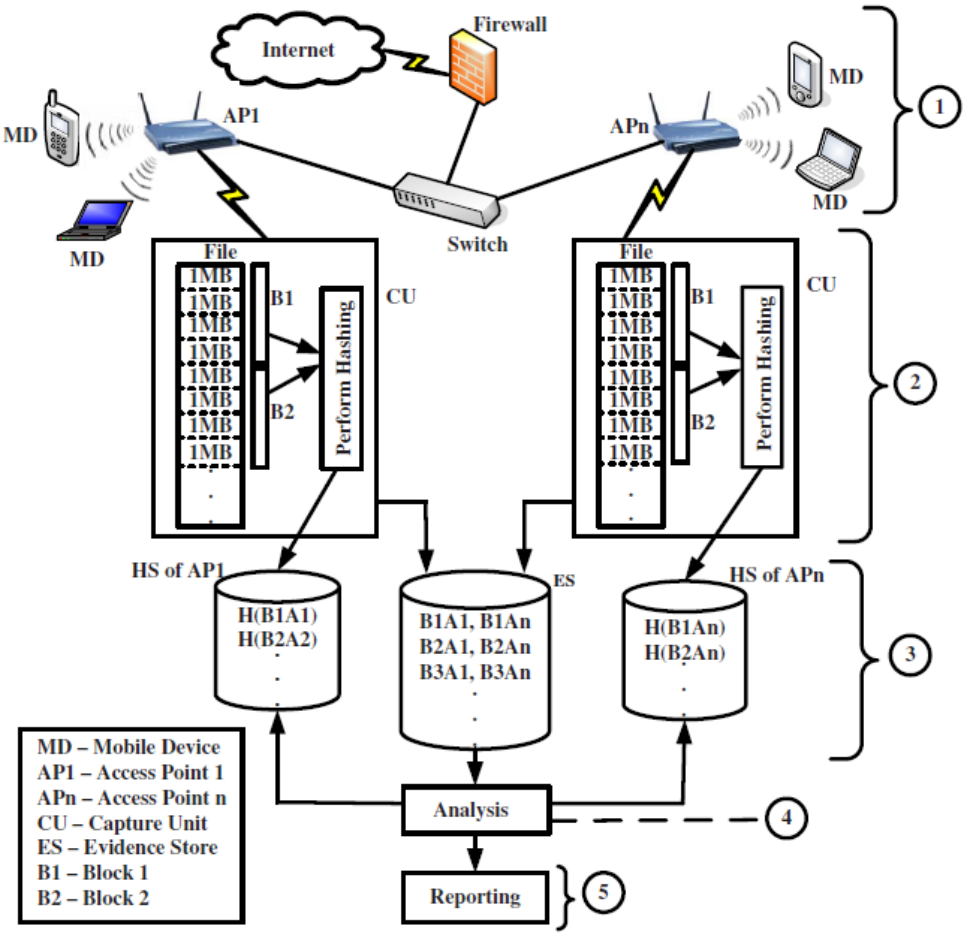


Figure 6.2: Wireless forensic readiness model (Ngobeni et al., 2010, p. 112)

The third phase of *WFRM* is preservation in which each data block accumulated is sent to "*the evidence store (ES)*" and the computed hash value for each data block is also stored in "*the hash store (HS)*" by the *CU* (Ngobeni et al., 2010, pp. 111-112). Hence, the preservation of logged data can be maintained in order to check the integrity of the DE. The last two phases of *WFRM* are analysis of acquired DE and producing a report, respectively. In order to validate the use of the proposed *WFRM*, the researchers used *AnyLogic Professional (version 6.0)* tool for simulation of the prototype (Figure 6.3). *AnyLogic Professional* is "*a Java-based, multi-paradigm, hybrid simulation tool capable of modeling systems as a combination of discrete events, system dynamics and agent*" (Ngobeni et al., 2010, p. 112).

Ngobeni et al. (2010) further elaborates the way in which the integrity of DE is maintained by implementing the mechanism for integrity checking in the

WFRM prototype. Any original block of data stored in the *ES* can be hashed and compared with that of the same block of data from *HS* to verify the data integrity and tampering.

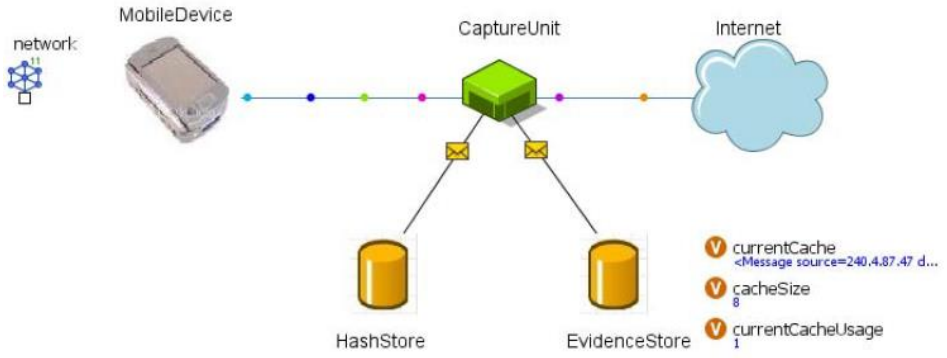


Figure 6.3: WFRM during the simulation (Ngobeni et al., 2010, p. 113)

Hence, the data was logged by *CU* and preserved by "*ES and HS*" during the simulation conducted by the researchers (Ngobeni et al., 2010). However, the monitoring of wireless network traffic by a wireless AP was not applied in the *WFRM* prototype.

In addition, the researchers also discussed how time and money could be saved by having a forensic readiness system in an organisation. If DF investigation needed to be performed in the case of a WLANs compromise, there would be instant availability of DE for investigation and most of the DF processes could be finished quickly by implementing *WFRM* (Ngobeni et al., 2010). On the other hand, one of the drawbacks of deploying *WFRM* is the requriement of large storage areas for preserving the wireless network traffic. However, the cost of buying larger storage is getting cheaper and hence the problem of reqiring large data storage for *WFRM* is no longer an issue. Therefoere, in conclusion, Ngobeni et al. (2010, p. 116) gives details of how to structure DF processes and states that "*further research is needed to address the storage issue*" for *WFRM*.

6.1.2 Systems Architecture for the Acquisition and Preservation of Wireless Network Traffic

The research study conducted by Cusack and Laurenson (2011) was presented at the "*9th Australian Digital Forensics Conference*". Even though IEEE 802.11 wireless local area networks (WLANs) are beneficial to businesses to provide

flexible network connections and extension of wired networks to its users, "*unauthorised application and specific attacks*" can be performed by malicious attackers due to the nature of data transmission happening over in the medium of air (Karygiannis & Owens, 2002; Slay & Turnbull, 2006; Varshney, 2003; cited in Cusack & Laurenson, 2011, p. 48). Hence the criminal misuse of ubiquitous WLANs can occur. As a result of inheriting potential criminal misuse by wireless networks, the researcher proposed a "*Wireless Forensic Model (WFM) system*" to acquire and preserve 802.11 wireless frames by using "*a wireless drone architecture*" (Cusack & Laurenson, 2011, p. 48).

In the first section, the researchers presented an overview of wireless forensics in which the potential locations of digital evidence (DE) from WLANs and two previous network forensic models were discussed based on the literature. The potential DE (Cusack & Laurenson, 2011, p. 49), "*either Live or Post-Mortem sources of evidence*", can be extracted by intercepting or capturing traffic of the wireless network and "*performing traditional computer forensic processes on embedded wireless devices and/or client's wireless devices*" respectively. However, other researchers (Turnbull & Slay, 2008, cited in Cusack & Laurenson, 2011) convey that the ways in which the information related to DE is to be collected and its extraction in WLANs, may depend on the configuration of the operating system and the wireless devices (for instance, wireless-enabled laptops and routers or access points) used. Hence, Casey (2004) stresses that it is challenging to have the network traffic as a source of DE due to losses of potential evidence that will possibly arise from insufficient DE collection systems. The two network forensic models (Cusack & Laurenson, p. 49) are "*a theoretical Wireless Forensic Readiness Model (WFRM)*" and "*a Forensic Profiling System (FPS)*". Ngobeni and Venter (2009) and Yim et al. (2008) correspondingly, provide how to forensically perform DF processes from the captured network traffic (e.g. logs) of different wireless access points (WAPs), and intrusion and detection systems (IDS), if WLANs are compromised by denial of service (DoS) attacks.

In the second section, the researchers explained the system design and components of the proposed *WFM* system in order to passively acquire and preserve the wireless traffic between wireless devices as a source of DE. Two sub-systems: "*the Wireless Drone*" (WD) and "*the Forensic Server*" (FS), are included

in the proposed system architecture (see Figure 6.4) to acquire traffic from a specific WAP by WD, and store the data collected in a centralised FS (Cusack & Laurenson, 2011).

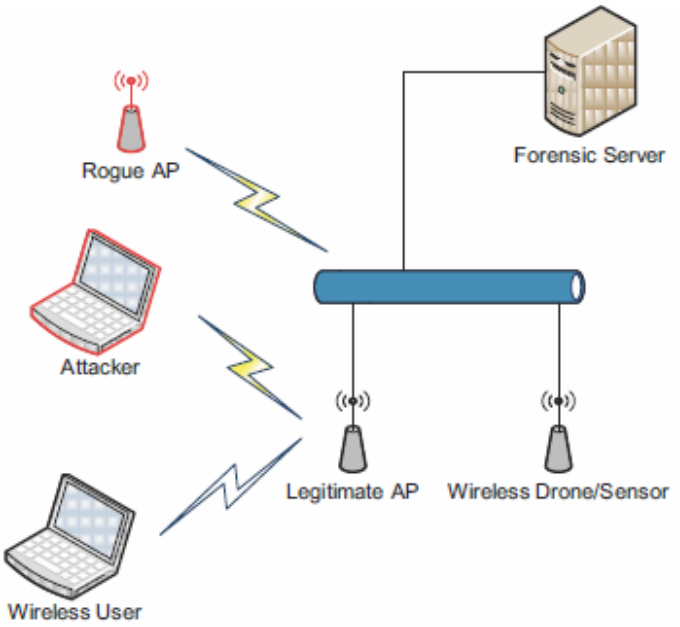


Figure 6.4: WFM system architecture (Cusack & Laurenson, 2011, p. 50)

The detailed information relating to sub-systems of the *WFM* explained in the article is summarised in Table 6.2.

Consequently, the proposed *WFM* model was implemented and tested to evaluate its capabilities after specifying the testing environment. Moreover, the researchers mentioned that the *WFM* was deployed after the "*existing WLAN*" was firstly implemented and benchmarked. The benchmark testing offered the baseline performance of the WLAN, and also specified the capabilities of the WLAN (Cusack & Laurenson, 2011). Hence, a total of five "*bandwidth tests*" (one minute each) between the legitimate AP and STA was performed by using "*the iPerf application*" with "*an average result of 26.54Mbps aligning with real-world 802.11g bandwidth capabilities*" (Cusack & Laurenson, 2011, p. 51). Similarly, the "*Multi-Generator (MGEN) application*" was used for generating network traffic between wireless devices to test "*a packet per second (PPS)*" (Cusack & Laurenson, 2011, p. 51). According to the findings from the five conducted tests, the "*existing WLAN*" was able to support a maximum of almost "*3700PPS*" without delay in transmission.

Table 6.2: Components of the implemented test environment (adapted from Cusack & Laurenson, 2011, pp. 50-51)

Components of the Implemented Test Environment				
	Summarised sub-system components of WFM			
	Sub-System-Component	***Hardware Specification***	***Software Installed***	***Purpose***
	Forensic Server (FS)	A personal computer with a 4GB of RAM, an Intel Dual-Core Central Processing Unit (CPU) and a Gigabyte Ethernet Network Interface Card (NIC).	Ubuntu Desktop Linux Operating System (OS) and the wireless sniffing application (Kismet).	For storing and preserving the collected data forwarded by WD.
	Wireless Drone (WD)	A WAP with a chipset supporting passive wireless monitoring mode, Gigabyte NIC and high power CPU.	OpenWRT embedded Linux OS and Kismet application.	For capturing IEEE 802.11 wireless traffic and forwarding the collected data to the FS.
	Existing WLAN Setup			
	Component	***Hardware Specification***	***Operation Mode***	***Network Encryption***
	Legitimate AP	A "*TP-Link wireless router (model TL-WR1043ND)*".	IEEE 802.11g	Wi-Fi Protected Access version 2 Pre-Shared Key (WPA2-PSK)
	Wireless Client (STA)	An Apple MacBook with a built-in wireless network adapter (*AirPort Xtreme*).		
	Attacker Component			
	Component	***Hardware Specification***	***Operation Mode***	***Purpose***
	Attacker	A laptop computer equipped with an external wireless adapter running the Backtrack 4 OS.	IEEE 802.11g	For conducting attacks such as *DoS* and *FakeAP* against the "*Existing WLAN*".

Then, the proposed *WFM* was integrated into the existing wireless network by using the components mentioned in (Table 6.2). In order to benchmark the *WFM*, the initial testing for the implementation of WD and FS were performed. After testing numerous available wireless routers, the researchers selected "*Ubiquiti RouterStation Pro*" as the hardware platform for the WD. It enabled *OpenWRT* firmware to run and provide Gigabyte Ethernet, and also the operations of several mini-PCI wireless NICs (Cusack & Laurenson, 2011). Hence, the capability of capturing network packets by WD was examined during the testing stage. The WD was eventually implemented by using "*RouterStation Pro with dual Ubiquiti XtremeRange2 (XR2) mini-PCI wireless adapters*" and a customised "*OpenWRT firmware, ath5k wireless drivers and Kismet (version 2010-07-R1)*" in order to

forward collected data to the FS (Cusack & Laurenson, 2011, pp. 51-52). Similarly, the FS was also implemented with hardware and software specified in Table 6.2. In addition, the "*libpcap (version 8.0)*" application was used on FS to support packet capture whereas Kismet was set up in "*server mode to collect and store all network traffic defined by available sources*". "*Network Time Protocol (NTP)*" was implemented for "*synchronisation of time between WFM devices*" (Cusack & Laurenson, 2011, p. 52). However, the researchers have manually preserved the collected DE by applying the "*md5sum*" hashing tool on the "*Kismet's log files*" in order to generate "*unique Message Digest (MD5)*" values. Subsequently, the log files collected were "*stored on two separate partitions and mounted as read-only for data analysis*" (Cusack & Laurenson, 2011, p. 52). The benchmark testing of the proposed *WFM* was performed by using the "*MGEN*", and the benchmarking methodology used the "*existing WLAN*" after the bandwidth testing between the FS and the WD. A five minutes duration for each test was done to verify whether the *WFM* could process the utmost network traffic rates for the extended period (Cusack & Laurenson, 2011).

The analysis of the captured data and the decryption of "*WPA2-PSK encrypted wireless network traffic*" between the WAP and the STA client were performed by using a network protocol analyser, *Wireshark* (Cusack & Laurenson, 2011, p. 52). It was stated that the benchmark acquisition results were calculated according to the number of "frames generated by MGEN" and "frames acquired by the WFM" (Cusack & Laurenson, 2011, p. 52). Even though the acquisition result of the wireless traffic was nearly perfect (approximately 100% at 2200PPS), the results were not based on the acquisition of acknowledgement frames (Cusack & Laurenson, 2011).

The researchers initiated malicious attacks such as denial of service (*DoS*) and "*Fake AP*" five individual times (at five minutes each) on the implemented WLAN, once the benchmarking processes were done. Hence, the two wireless adapters were installed and configured on WD "*to monitor the wireless traffic of AP channel*" and "*to hop between the remaining available channels in the 2.4GHz ISM band*", respectively (Cusack & Laurenson, 2011, pp. 52-53). Likewise, IDS was run on the FS by using built-in intrusion rules of the Kismet application in order to generate alerts during malicious attacks.

According to the acquisition results, the proposed *WFM* was able to collect the frames (over 90%) related to DoS attacks and the useful information for forensic investigation ("*such as source MAC address, timestamp, frame type and sequence number*") could be found in each of the frames collected (Cusak & Laurenson, 2011, p. 53). However, *Fake AP* attacks were unable to accurately acquire (only just over 60%) as because the attack happened on another channel than the AP channel.

In conclusion, the researchers Cusack & Laurenson (2011, p. 54) state that there are numerous potential issues with the implemented WFM such as "attack detection capabilities, data loss and the effect of monitoring a large scale WLAN with multiple APs". For instance, it is impossible to acquire 100 % of potential DE although the loss of data can be reduced from a live evidence source by using the proposed WFM. Likewise, it is also difficult to associate the acquired evidence to the physical, Media Access Control (MAC), address of the malicious attacker's laptop (if MAC spoofing is implemented) even though the proposed WFM is able to acquire and preserve the DE of the attacks performed (Cusack & Laurenson, 2011). Similarly, the wireless attack detection is unable to function due to deficiencies in the IDS during the experiment. Nonetheless, the researchers claim that their proposed WFM is capable of acquiring and preserving "wireless network traffic from a live source of evidence" to later perform the DF investigations (Cusack & Laurenson, 2011, p. 54). For my research this is valuable information regarding how to conduct such experiments and guidance on best practices when managing the experiments.

6.1.3 Digital Forensics of Wireless Systems and Devices: Technical and Legal Challenges

Wireless systems and devices have been deployed and utilised in home and enterprise networks (Achi, Hellany and Nagrial, 2009). However, the growing deployment of such systems and devices has many security vulnerability problems and issues to not only the consumers, but also to the enterprises or organisations. The misuse of such networks and devices can simply be caused by malicious attackers (internal or external) due to the inherent weaknesses in wireless. This research paper discusses the current technical and legal challenges related to the

digital forensic investigation (DFI) of wireless systems and devices, and will provide strong contextual guidance for my research methodology.

In the introductory section, Achi et al. (2009, p. 43) highlights the reasons why forensic investigators (FIs) working for Law Enforcement Agencies (LEA) encountered technical and legal challenges throughout the DFI and "*collection of digital evidence (DE) leading to analysis and presentation at courts of Law*". For instance, the researchers claim that "*there is no one standard which can be followed across one nation not to mention across the world, LEA are using tools at hands during their investigations, and thus making the e-evidence subject to scrutiny by other legal and technical experts and hence subject to rejection by the court*" (Krone, 2004, cited in Achi et al., 2009, p. 43).

The components of a wireless system (see Figure 6.5) such as wireless access devices (Personal Digital Assistants or PDAs), 802.11b wireless LAN and wireless access points are explained in terms of their relational architecture.

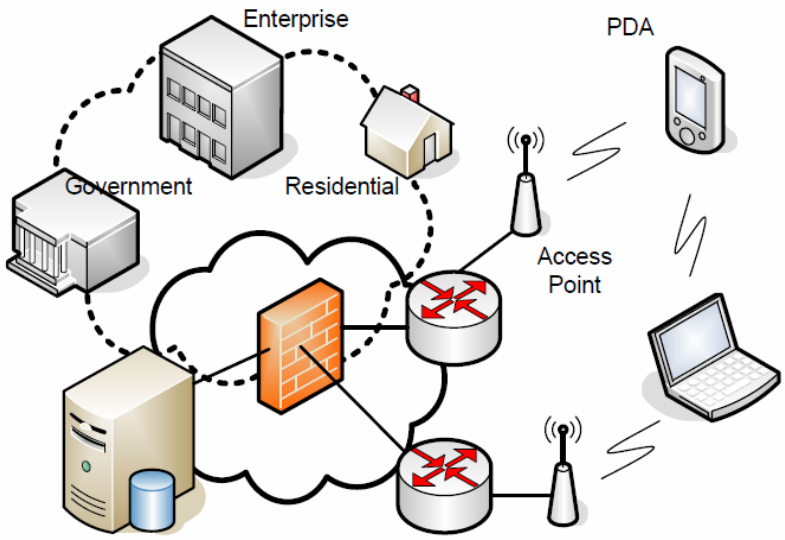


Figure 6.5: Network diagram of Wireless system and devices (Achi et al., 2009, p. 43)

Consequently, technical and legal challenges faced by DF investigators of LEA during the investigation relate to the technology and the vulnerabilities or non-performances. With respect to the technical challenges, the researchers (Achi et al., 2009) stressed that the potential DE or electronic evidence (such as wireless devices that are turned off) could be lost during the DF investigation even though numerous DF tools had been developed to work well with acquiring static evidential data (examples: system logs, hard disks, physical memory). Hence, DF

investigators have to establish correct procedures in which the wireless devices need to be seized (by performing a comprehensive passive scanning of the network), and how and when to acquire the potential DE. The potential DE can be found in different media or locations (e.g. log files, routers, switches, servers, PDAs, laptops, etc.,) and therefore there exists particular challenges in the acquisition of DE from "*magnetic devices or volatile memory*" (Achi et al., 2009, p. 44). Legal challenges come from specific forensic acquisition methods or techniques that are critical to verify the integrity and validity of the evidence acquired. The volatility characteristic of DE raises the problem of admissibility of DE in a court of law (Achi et al., 2009). Thus, DE is not comparable to any forms of traditional evidence when very precise investigation or rigourous examination is essential to be admissible to the court of law. Similarly, the researchers state that the definitions of law and DE in different places could not be the same due to various standards and acceptance levels of DE by "*Courts of Law*" in different "*countries or even states of one country*" (Achi et al., 2009, p. 44). As a result, LEA can encounter barriers when: acquiring DE from systems, prosecuting perpetrators located in "*foreign countries where there are no extradition agreements*", and getting search warrants and "*obtaining open warrants for scanning wireless interfaces without substantial proofs for potential evidence of crime*" (Achi et al., 2009, p. 44).

Subsequently, in the fourth section, the researchers briefly described the current issues related to the DF of PDA devices. The issues originate from the rapid development of PDAs. All PDA family devices provide users with "*a set of basic Personal Information Management (PIM) application*" and "*can communicate wirelessly, review electronic documents, and surf the internet*" (Achi et al., 2009, p. 45). Likewise, PDAs could be synchronised with personal computers (PCs) while other researchers (Jansen & Ayers, 2004, cited in Achi et al., 2009, p. 45) stated that the reconciliation and replication of PIM data between such wireless devices could also be done by "*using synchronisation protocols such as Microsoft's Pocket PC ActiveSync and Palm's HotSync protocols*". Hence, the researchers acknowledge the legal issue with the validity of DE when there exists the risk of obtaining potential DE from a PC to which the PDA had been synchronised (Achi et al., 2009). Moreover, the technical issue of "*the*

development of a new tool with open architecture allowing for a broad range of models" (Achi et al., 2009, p. 45), is pointed out in this article since the newer PDA models have different functions to the previous ones. As a result, DF tools should be updated to keep up with the changes.

In the fifth section, the researchers discuss the problem with tracing back to malicious wireless intruders or hackers as their physical locations could not be precisely detected or identified. The internet service providers (ISP) are mostly the end point of an investigation where DF terminates when intruders cover their digital tracks. To identify intruders, the frequency monitoring or scanning (RFMON) has to be performed to find the initiation of attacks and then existing Internet Service Provider (ISP) information gained to find the gateway used by the intruders to carry out the attacks. Hence, the researchers reviewed two DF methods in order to trace-back the malicious wireless hackers based on the previous literature. To solve the problem with "*tracing and locating wireless hackers*", previously proposed techniques to locate the intruders of WLANs such as "*closet AP*", "*triangulation*" and "*RF finger printing*" were briefly outlined (Velasco & Chen, 2008, cited in Achi et al., 2009, pp. 45-46).

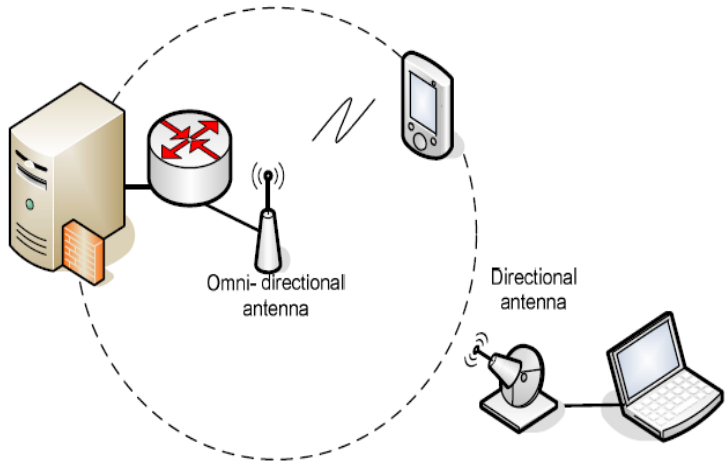


Figure 6.6: WLAN access with Directional antenna into Omni-directional AP (Achi et al., 2009, p. 45)

However, these techniques still prove inadequate or imprecise when the directional antenna with high transmitting power (Figure 6.6) is used by the intruders to connect to WLANs outside the detectable range. The information is useful for this research because it places limitations on scope and limitations for exploring in this area.

6.1.4 Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon)

The research conducted by Ng et al. (2004), "*Ubiquitous monitoring environment for wearable and implantable sensors (UbiMon)*", was presented at the *"6th International Conference on Ubiquitous Computing"* in 2004. As a result of the developments in monitoring and sensing devices, wireless sensor networks (WSNs) are significant in providing the ubiquitous monitoring of patients in the healthcare industry. The perception of ubiquitous health monitoring has been established comprehensively and significantly in clinical applications (Jovanov et al., 2001; Wilson et al., 2000; Koval & Dudzaik, 1999, cited in Ng et al., 2004). However, there are several problems that need to be addressed in relation to employing such wearable and implantable sensors in body sensor networks for ubiquitous health monitoring. Hence, the purpose of this paper is to provide "*continuous management of patients under their natural physiological states so that transient but life-threatening abnormalities can be detected and predicted*" (Ng et al., 2004, p. 1).

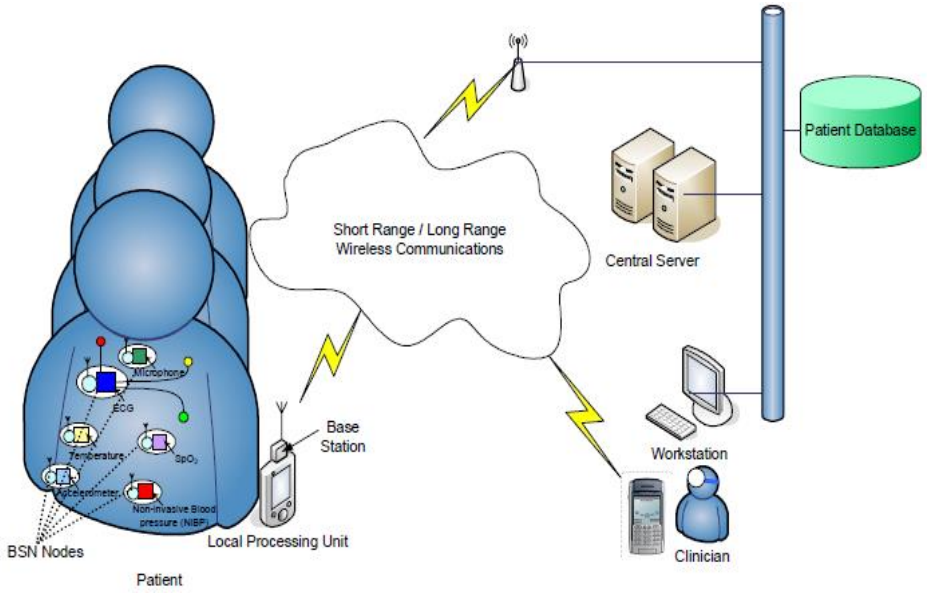


Figure 6.7: UbiMon system design (Ng et al., 2001, p. 1)

Firstly, the researchers presented the UbiMon system architecture (Figure 6.7). The architecture (Ng et al., 2004, p. 1) was composed of "*the body sensor network node (BSN node), the local processing unit (LPU), the central server (CS), the patient database (PD) and the workstation (WS)*".

A wireless *BSN node*, with or without battery, is to monitor a patient's physiological parameters and the node can be integrated with "*a wearable or implantable physiological biosensor such as the electrocardiogram (ECG), blood oxygen saturation (SpO2) or temperature sensors*" (Ng et al., 2004, p. 1). Moreover, the *BSN node* can be equipped with the context aware sensor (e.g. an accelerometer) in order to monitor the movement of the patient. The *LPU* (Ng et al., 2004) is a portable device (either a PDA or a mobile phone) and can be referred to as the base station that collects and processes the data acquired by *BSN nodes* (see Figure 6.8). Furthermore, Ng et al. (2004) stated that the *LPU* was intended to uncover irregularities and deliver instant warnings to the patients. Likewise, the *LPU* is also considered as "*a router between the BSN nodes and CS via short-range wireless communication standards such as Bluetooth/Wi-Fi or another long-range mobile network such as 3G/GPRS*" (Ng et al., 2004, p. 1).

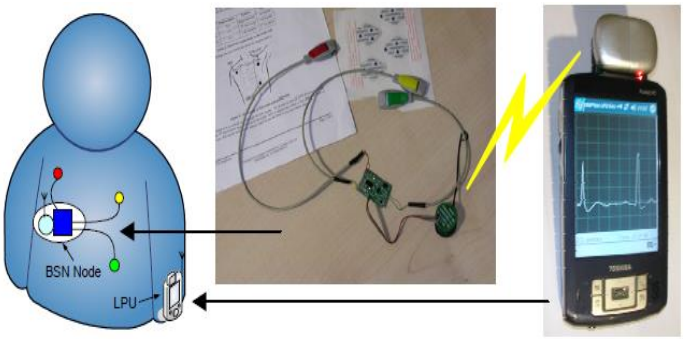


Figure 6.8: An ECG module (BSN node) communicating with the base station en-slotted to the PDA (LPU) (Ng et al., 2001, p. 2)

The *CS* receives the real-time sensor data from the *LPU*, stores the collected data to the *PD*, and performs the long-term trend analysis to predict the condition of a patient (Ng et al., 2004). Hence, any possible life-threatening anomalies or irregularities can be avoided. Likewise, the WS or patient monitoring station is either a portable device or a personal computer for allowing clinicians to examine the patient physiological data. Therefore, the clinicians can see and retrieve either real-time monitoring or the history of patients' data to perform the diagnosis.

Subsequently, the researchers discussed the prototype of *UbiMon* system that was developed for patients with heart diseases. A small-scale *BSN node* was designed based on the Berkeley mote (*Mica2 Dot*) with an ECG sensor to interface with the PDA as the *LPU* (see Figure 6.8). Hence, software for the *BSN node* was written based on TinyOS to collect sensor data and transfer it to the

LPU whereas the base station was designed by "*using the MICA2 Dot with a serial interface connected to the PDA*" (Ng et al., 2004, p. 2). However, a lightweight protocol with a special frequency channel access method, time division multiple access (TDMA), was used when developing the *BNS node* software as a result of the high data rate required by ECG signals (Ng et al., 2004). Furthermore, in order to collect context-aware sensor data, *LPU* software was also developed for displaying the data gathered (e.g. real-time ECG signals) and identifying patient's activities. Afterwards, the data collected by *LPU* was routed to the *CS* via Wi-Fi or GPRS and hence the collected data was then stored in *PD*.

In addition, Ng et al. (2004) developed a specific software (graphical user interface) for *WS*, which could retrieve patients' data from the backend database. Thus, the clinicians could retrieve and examine patients' data by using the developed *WS* software (Figure 6.9).

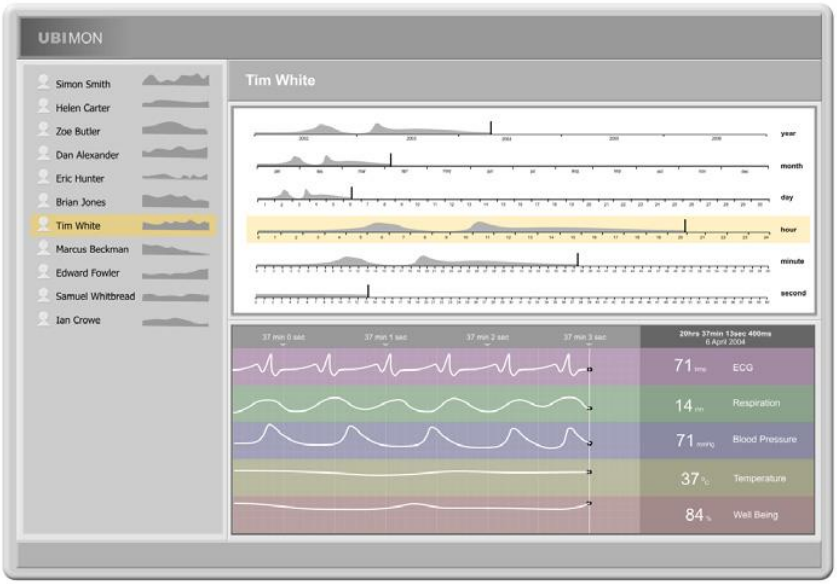


Figure 6.9: Graphical user interface of Workstation software (Ng et al., 2001, p. 2)

To sum up, the *UbiMon* system has delivered not only the basic architecture for wireless biosensor (wearable and implantable) modules; but also provided the system "*architecture for collecting, gathering and analysing data from a number of biosensors*" (Ng et al., 2004, p. 2). Furthermore, *UbiMon* provides the aspect of context awareness in the system to enable acquiring of any relevant clinical event. Therefore, this is useful context-awareness information and also detailed information on how to go about this type of research.

6.2 RESEARCH THEORY

Selecting the appropriate research paradigm is important for achieving any research project objectives. As this research is related to Information Systems (IS), it is essential to consider the available research paradigms and methodologies in the area in order to identify the most suitable one to fulfil the aims of this research. The objective of the research is to design a forensically ready wireless medical system. The previous studies reviewed have delivered guidance from how others have investigated the problem area. The review in Section 6.1 is helpful for identifying approaches and also the tools and techniques used. In particular, Figure 6.5 provides a starting point for this research. The researchers provide a network architecture for forensic readiness. This is the ideal starting point for this research and the first artefact input to a Design Science improvement methodology. For the purpose of the design science methodology, the digital forensic readiness models are the artefacts of interest and the artefact that is subjected to evaluation and continuous improvement processes. The following sections review potential research paradigms and methodologies in IS research.

6.2.1 Research Paradigms

Research is commonly referred to as "*a search for knowledge*" and also defined as "*the art of scientific investigation*" (Kothari, 2004, p. 1). It is essential to select the research paradigm most suited to this research before defining the research methodology and methods. According to Crotty (1998), a methodology is defined as an approach, an action plan, a process or a strategy that comprises a collection of research methods. Similarly, Hewitt (2009, p. 7) states that methodology is matters relating to "*the structure and design of the research study*". Thus, a research methodology is a guide for the way in which a research project is to be done or the way in which the research problems are to be addressed. Moreover, Creswell (2011) states that the researcher will choose a research method either quantitative, qualitative or mixed research methods based on the purpose of the research and research questions. The different nature of quantitative, qualitative and mixed research, including the benefits and deficits will be reviewed in the following sub-sections.

6.2.2 Quantitative Research

In quantitative research, the researcher understands the research problem related to measurable attributes or based on the demand to explain why something happens. Quantitative research begins with understanding the main variables in the research. After identifying the main variables in the research, the researcher tries to understand the relationship between variables in the study such as how one variable relates to another variable or to expose the source of particular events (Flick, 2015). In a quantitative literature review, there will be a correlated amount of literature supporting the research question and measurement tools. That is why the literature review takes the lead role in two different ways in order to explain the necessity for the research problem and to show the potential research questions and intent for the research study (Creswell, 2013). Consequently, the researcher tries to understand and predict the result of the relationship between variables by using questions and hypotheses. Similarly, hypotheses are further refined to obtain observable and measurable data from specific variables that are suitable for the research (Creswell, 2013). For quantitative data collection, the researcher has to use a tool that allows observing, measuring and documenting the data. This type of tool has to include suitable questions and reactivity that the investigator sets up or develops before the research begins. According to Creswell (2013), there are two types of research designs for collecting data in quantitative research: surveys and experiments. In data analysis, statistical studies for examining the data may include breaking data into sections to answer the research questions. For instance, statistical methods such as contrasting relevant values or groups of interest for individuals give data to solve the hypotheses or research questions. Then, the researcher evaluates the findings related to research questions or hypotheses and defines the result as either negative or supports the desirable predictions of the research (Creswell, 2013). Therefore, the structure of the research follows a predictable model including: an introduction, literature review, design methods, search results and discussion.

6.2.3 Qualitative Research

In a qualitative research problem, the researcher does not know which variable should be studied. The previous research or literature may expose information

about the central phenomenon. The idea, key concept or procedures studied in the research may be structured or left open, so the investigator needs to study in an exploratory fashion and get more data from the participants and the context.

The literature review in qualitative research plays a negligible role in the beginning of research compared with the extent in quantitative research (Creswell, 2013). The qualitative research is concerned more with the participants in the research and the literature is used to justify the choice of research methods. The research questions in qualitative research may be specified so the investigator has to collect data from participants in a particular way, such as interviews, or they may arise from the field as the researcher investigates. Also the qualitative purpose statements include the central phenomenon information, the participants, and the research site which is studied in the research. The investigator may differentiate between research questions and concentrate on the practicable data and look for repetition and other verification or explore new appearances that arise in the processes of investigation (Flick, 2015).

In qualitative research, there are two main ways to collect data: questionnaires or interviews. The investigator shapes protocols (or forms) based on the discovered data which were collected from the participants in the research for indicating information as the research proceeds. These forms shape questions which allows an investigator to collect the participants' answers. However, the questions often change and may be replaced during the research data collection. These forms contain an interview protocol which includes several questions or an observation protocol which the investigator collects the data around about the conduct of the participants. In addition, the investigator can collect the information from texts, pictures, audio data, and so on, and generally uses a database with aggregation mining tools for data/thematic analysis. Research analysis proceeds using methods for text segmentation. It is analyses of the text including the separating into groups of sentences and specifying the definition of each sentence. The researcher uses pictures or words to explain the main phenomenon in the report and to show the results of the research which explains specific places, people or themes, for the large categories in the research.

In qualitative research, the researcher can choose different types of structure to suit the data collection and analytical strategies. To show the research

result more attractive, narrative text is the most common form of exhibiting qualitative data. The research report is written in narrative and descriptive forms rather than scientific report format. The report also needs to contain reliable and accurate data to express the difficulty of the processes used and volatility of the phenomenon. In addition, the researcher needs to explain their role in the research that includes their personal discussion, opinions, how they co-operate with participants and their experiences during the research. They must include any relevant matters and relationships that the researcher has contributed to the study.

6.2.4 The Mixed Method Paradigm

There are many approaches that do not fit either quantitative or qualitative requirements or may fit either or both. Such approaches fall into a mixed methods approach to research. Design science (DS) is one such approach that may accommodate both worlds. It is "*for developing scientific knowledge about the problem domain, including artefact, and engineering knowledge about carrying out design*" (Fleming, 2009, p. 134). However, Fleming (2009) claims that the DS paradigm provides the way in which the process of research should progress and what is required to be addressed in the research to assure its quality, instead of giving the direction on how the artefact should be designed. Moreover, Fleming (2009) also argues that the research rigour requirements are commonly in conflict with a major requirement of DS, which is related to real business problems. As a result, a DS paradigm should provide a framework that addresses the problems related to research rigour rather than specifying ridged requirements.

6.3 DESIGN SCIENCE RESEARCH METHODOLOGY

Design science research methodology (DSRM) is proposed by Peffers et al. (2007, p. 1) in order to achieve "*a commonly accepted framework for DSR*" by integrating "*principles, practices, and procedures required to carry out DSR*" in information systems. To provide a proof of concept, the proposed DSRM is evaluated by using four IS case studies. There are six process elements in the proposed DSRM (Figure 6.10), which are based on peer accepted elements and are derived from previously published papers (Nunamaker et al., 1991; Walls et al., 1992; Archer, 1984; Eekels & Roozenburg, 1991; Takeda et al., 1990; Rossi & Sein, 2003; Hevner et al., 2004; Peffers, 2007, p. 52).

The first process of the DSRM is the "*problem identification and motivation*" as it is important to define the particular research problem that will be employed in the development of an artefact and effective solution. The value of such a solution can be achieved by motivating "*the researcher and the audience of the research to pursue the solution and to accept the results and it helps to understand the reasoning associated with the researcher's understanding of the problem* (Peffers et al., 2007, p. 55)". Hence, the knowledge of the state of the problem and the importance of its solution are required resources for the process stage.

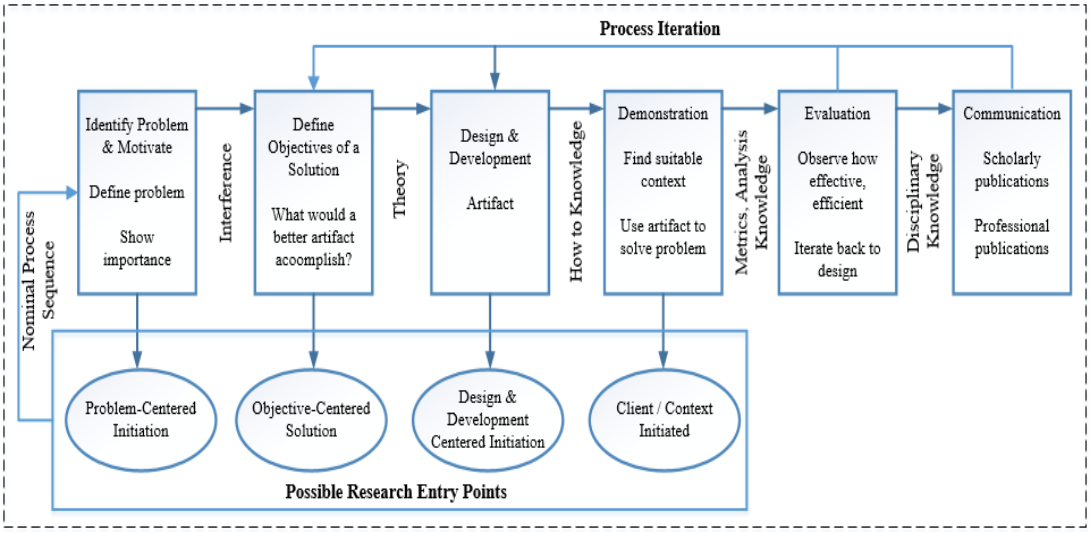


Figure 6.10: Design Science Research Methodology Process Model (Peffers et al., 2007, p. 54)

The second process of DSRM is to "*define the objectives for a solution*" from the definition of the problem and knowledge of feasibility (Hevner, March, Park, & Ram, 2004; Cole, Purao, Rossi, & Sein, 2005). The objectives should be deduced from the problem specification and could be quantitative or qualitative. For instance, the quantitative objective can be "*a desirable solution would be better than current ones* (Peffers et al., 2007, p. 55)". Similar to the first process stage, the knowledge of the state of problems and current solutions, if any, and their efficacy are required as resources in this process stage.

The third process is to "*design and develop*" the artefact, which can be "*constructs, models, methods, or instantiations*" or "*new properties of technical, social or informational resources* (Jarvinen, 2007, p. 49 cited in Peffers et al., 2007, p. 55). According to Peffers et al. (2007), a conceptual DS artefact is an artefact in which a research contribution is embedded in the design. The

architecture and desired or required functionality of the artefact is indispensable for creating the tangible artefact, and therefore theory knowledge is an essential resource in a solution (Hevner & Chatterjee, 2010; Gregor & Hevner, 2013; Drechsler & Hevner, 2016).

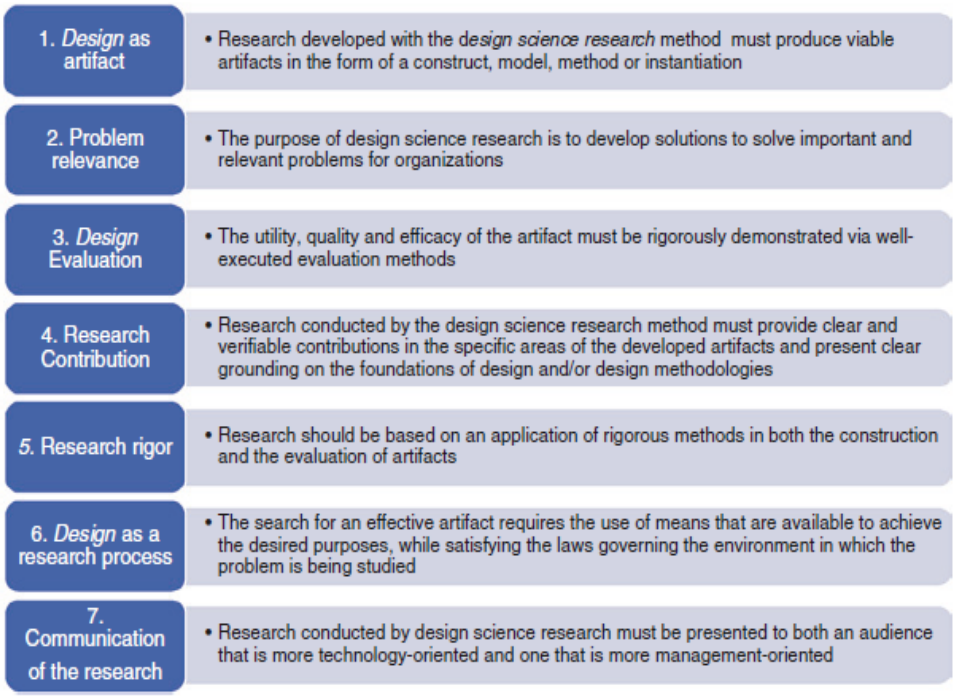


Figure 6.11: Criteria for conducting design science research (Hevner et al., 2004, p. 83 cited in Dresch, Lacerda, & Antunes Jr., 2015, p. 70)

The fourth process is the "*demonstration*" of the artefact application in order to answer one or more cases of the problem by using "*experimentation, simulation, case study, proof or other appropriate methods*" (Peffers et al., 2007, p. 55). Thus, the effective knowledge for utilising the artefact to answer the problem is an important resource in this process stage. The fifth process is the "*evaluation*", in which the artefact is assessed as to how well it provides a solution to the problem. The effectiveness and efficiency can be observed and measured by evaluating "*the objectives of a solution to actual observed results from the use of artefact in the demonstration*" (Peffers et al., 2007, p. 56). As a result, the knowledge of relevant metrics and analysis methods are necessary in this stage. However, the artefact evaluation may be different depending upon the nature of the problem context. For instance, the evaluation may be done by comparing the functionality of the artefact with the solution objectives from the second process of the DSRM process model, in addition to other quantitative evaluation methods such as surveys, client feedback, or simulations (Peffers et al., 2007).

Nevertheless, the evaluation should conceptually consist of any suitable empirical or pragmatic evidence or plausible proof (Kleinschmidt & Peters, 2017). After completing the evaluation process, the researchers can make a decision as to whether to iterate back to the third process phase "*to try to improve the effectiveness of the artefact or to continue on to communication and leave further improvement to subsequent projects*" (Peffers et al., 2007, p. 56). Moreover, the feasibility of iteration will be based on the nature of the research in the problem context.

The final process of the DSRM process model is "*communication*" according to previous researchers (Archer, 1984, and Hevner et al., 2004 cited in Peffers, 2007, p. 56). Thus, the problem, the significance of the problem, the artefact design, the utility and novelty, the rigour of the artefact design and its effectiveness should be communicated "*to researchers and other relevant audiences such as practicing professionals, when appropriate*" (Peffers et al., 2007, p. 56). Similarly, the outcome of DSR can be communicated in scholarly research publications.

To sum up, the DSRM has four research entry points: a problem-centred initiation, an objective-centred solution, a design-and-development-centred initiation and client-/context-initiated solution. However, the researchers can start their research from any entry point although the proposed DSRM process model is planned in a nominally sequential order (Peffers et al., 2007).

6.4 APPLICATION OF DESIGN SCIENCE RESEARCH

DS is an important research paradigm in Information Systems (IS) research that has been used by a large number of researchers (Hevner, March, Park, & Ram, 2004; Cole, Purao, Rossi, & Sein, 2005; Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007; Hevner & Chatterjee, 2010; Gregor & Hevner, 2013; Drechsler & Hevner, 2016; Kleinschmidt & Peters, 2017). For instance, Hevner et al. (2004, p. 77) used the design science framework as a research approach "*that creates and evaluates IT artefacts intended to solve identified organisational problems*". The artefact is designed and modified until the desired solution is achieved to solve the problem (Peffers et al., 2007). Similarly, March and Smith (1995 cited in Iyawa, 2017) point out that such artefacts can be one of different types, such as:

constructs, models, methods and instantiations (Hevner et al., 2004). Moreover, the artefact may involve "*social innovations or new properties of technical, social, or informational resources*" (Peffers et al., 2007, p. 49).

However, the artefact in this research is the digital forensic readiness framework for WMedSys and can be referred to as an instantiation. The framework comprises different components including a Pi-drone, a wireless forensic server, and a centralised Syslog server (see Figures 6.5 and 6.14). In order to achieve the research objectives, the DSRM presented by Peffers et al. (2007) will be applied.

The design of this DSRM process model (Peffers et al., 2007) has originated from common DS process elements from the research work done by different researchers (Archer, 1984; Takeda et al., 1990; Eekels & Roozenburg, 1991; Nunamaker et al., 1991; Walls et al., 1992; Rossi & Sein, 2003; Hevner et al., 2004; Cole et al., 2005). DSRM consists of six nominal activities in sequential order that will be specified for this research project in the following sub-sections.

6.4.1 Activity 1: Problem Identification and Motivation

The main purpose of the first activity of DSRM is to identify the problem and motivation. Johannesson and Perjons (2014, p. 91) define a problem as "*an undesirable state of affairs or a gap between a desirable state and current state*". However, the researcher has to precisely identify the problem, justify the importance of the problem and investigate the underlying causes of the problem. For example, in Chapter 2 the recent hacking or compromising cases of WMedDs and WMedSys were shown to pose risks for users or patient safety. Hence, to improve user or patient safety, the researcher has to find a suitable solution (an artefact) for the identified problem. A well-founded solution cannot only be exclusively based on the investigation of previously published work from literature, but also based on other methods (example: surveying or interviewing stakeholders). Therefore, the researcher can utilise any research method such as surveys, case studies, action research, interviews, questionnaires, observation, documents and so on (Johannesson & Perjons, 2014). With regard to justifying the problem, it is important to describe why such problem is critical and to whom it will affect. In this research, the safety of users or patients is a critical problem if

WMedSys are attacked or compromised. After justifying the problem, the researcher analyses the underlying causes of the identified problem in order to obtain a feasible solution. The analysis of such problems can be based on previous research work from literature or statements from stakeholders. To analyse the underlying problem in this research, the researcher has conducted a literature review of previously published work from books, journals, digital libraries such as IEEE, ACM, and Google Scholar. These findings have been presented in Chapters 2-5, and Section 6.1. Similarly, the researcher has chosen to perform comprehensive studies of wireless LAN security in Auckland City (Kyaw & Agrawal, 2015; Kyaw et al., 2015).

6.4.2 Activity 2: Define the Objectives of a Solution

The analysis of the literature has delivered the problem, the context, and the state of current solutions. The literature in Chapters 2-5 clearly specifies the technical and theoretical risks associated with WMedDs. It also reports security defences that are viable in the technology and related environments. Digital forensic readiness as a security provision has also been reviewed and current research publications reviewed in Section 6.1. Figure 6.5 provides an architecture from the literature for a digital forensic ready WMedSys. Consequently, the objective for this study is re-stated as: “The objective of the research is to design a forensically ready wireless medical system”. The DS methodology is to be used to provide progressively improved solutions to the problem.

6.4.3 Activity 3: Design and Development

This activity of DSRM is to design and develop an artefact that should fulfil the requirements from a previous activity (Johannesson & Perjons, 2014). The design in Figure 6.5 is the result of previous research in the area. This artefact is ready to enter into the DS methodology for an improvement on the design solution. It is proposed to make amendments based on the other research reports in Section 6.1, and then use the improved artefact to guide a technical pilot study that will test the relevancy in a testbed situation. Figure 6.15 takes the core contribution of Figure 6.5 and innovates potential attack scenarios. For the Pilot Study one scenario of a man-in-the-middle (MIMT) attack is tested to investigate the concern of patient records disclosure. The intention is to then to confirm or reject the literature

vulnerability claims for WMedSys, and then in the scenario tests produce an improved design.

6.4.4 Activity 4: Artefact Demonstration

Principally system designs and device designs that relate to WMedSys are the input data. These designs are to be critically analysed and the theoretical data processed. The assessment is to be for security provisions and forensic provisions in the designs. This theoretical data is to be used as the basis of advice on how to improve designs for better user safety; and easier access for forensic and security investigators. Gap analysis will be used on the designs and the ideal situation proposed where the trade-off of costs and benefits is made against risk mitigation. No testing of actual medical devices or systems will occur in the proposed research. The theory is to produce improved artefacts from the Pilot Study and then the artefact is to be demonstrated to experts to gain their feedback. A full implementation runs beyond the scope of this theoretical research.

6.4.5 Activity 5: Artefact Evaluation

Evaluation of the artefacts is to occur progressively. The first improvement of Figure 6.5 is from the researcher's critical reflection on the literature analysis and analysis of similar studies in Section 6.1 that suggests some components are missing from Figure 6.5. The second evaluation is made from data analysis of the scenario testing of Figure 6.15 in the laboratory testbed. This data is evaluated for completeness, functionality, and artefact ease of use. The improved artefact is then submitted to experts as a demonstration for them to advise further improvements. As noted in sub-section 6.4.6 the researcher has continuously submitted the development of ideas and artefact improvements to peer review through publications. This has also included oral presentations to international audiences and feedback sessions.

6.4.6 Activity 6: Communication

The DS approach is populated with continuous processes. One of these processes is that of communication that also acts as a feedback loop on the state and value of the artefact. From day one the University has required proposals and amendments (PGR2), and then a formal written and oral communication to two assessors for

the PGR9. All of these communications have been completed, passed and approved for progression of the study. In addition the researcher has actively published in conferences and Journals to get peer review in oral and written formats (see publications in thesis formalities). The final communication will be this thesis in the electronic library and any arising Journal articles.

6.5 DESIGN OF STUDY

The study has a high level and a lower level design to reflect the planning and the implementation processes respectively. The high level plan in Figure 6.12 shows the phases from the literature analysis through artefact testing and the final Report.

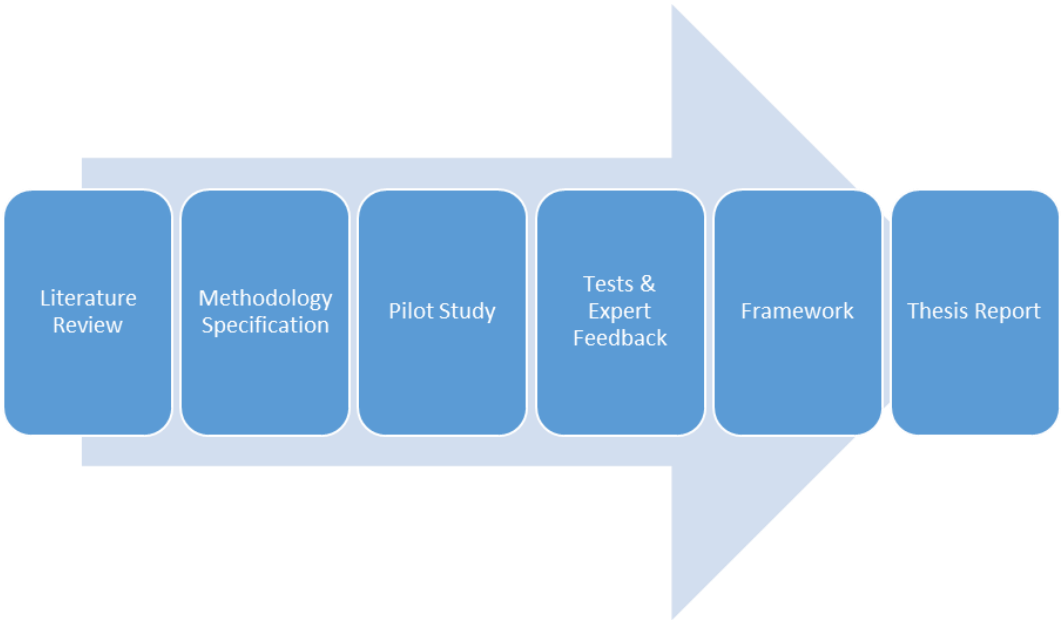


Figure 6.12: High level research Plan

In Figure 6.13 the lower level of research processes is summarised to show how inputs are fed into the testing processes and the resultant output of feedback on the artefacts is achieved. These two plans elaborate the design as an action based plan for investigation and the achievement of the research aim, to improve current wireless medical network security designs by adding forensic readiness capability.

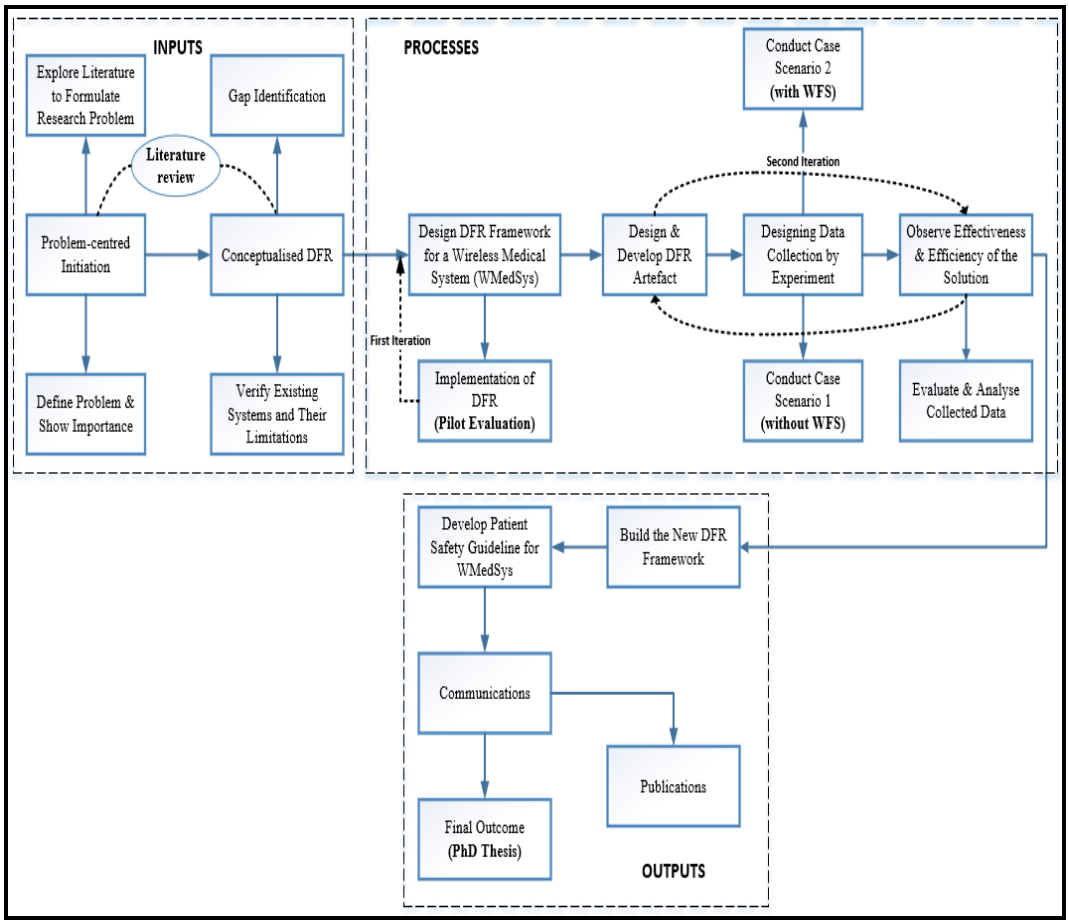


Figure 6.13: Low level research plan

6.6 THE RESEARCH MODEL

Based on the review of related and similar studies published in the literature, a design science methodology is employed to conduct the proposed research. Vaishnavi and Kuechler (2008) states that the design science research methodology initiates with a problem awareness which is followed by suggestions for solutions that are reinforced with existing knowledge in the associated field in order to produce a proposal and a tentative design. Hence, the proposed research model includes seven phases (as shown in Figure 6.14). In the first and second stages of the research, the comprehensive literature review of published papers from different digital libraries and reputable journals from the past decade was conducted to give a cohesive treatment of the chosen research topic. For instance, the publications from different digital libraries such as the Institute of Electrical and Electronics Engineers (IEEE), the Association for Computing Machinery (ACM), *Springer Link, Science Direct, ProQuest Central, Digital Investigation, Google Scholar, The New England Journal of Medicine, Journal of Medical*

Devices: Evidence and Research, PubMed, National Institute of Standards and Technology, Cellular Telecommunications Industry Association (CTIA – The Wireless Association), ECRI Institute, Food and Drug Association – U.S. (FDA), and Federal Communications Commission (FCC), were searched and reviewed.

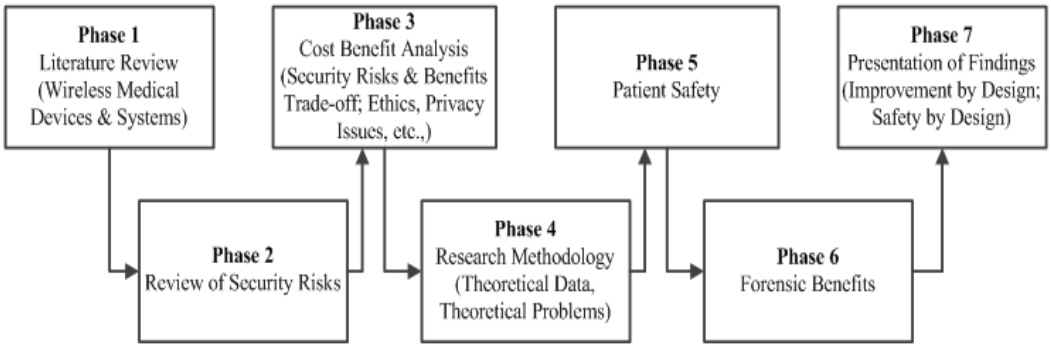


Figure 6.14: Logical content research phases

Likewise, books from AUT library and Amazon website were also searched and reviewed. The searching was done by using keywords such as *WMedDs*, *Wireless Devices*, *Wireless Medical Device Security*, *Misuse Cases*, *Misuse of WMedDs and WMedSys*, *Infusion Pump*, *Pacemaker*, and so on. The literature was analysed, and the learning compounded into actions.

The second phase of the research (Phase 2 in Figure 6.14) is to review security risks related to the WMedDs and WMedSys. Then, in research phase three, the cost benefit analysis (CBA) will be performed by accessing security risks and benefits trade-off based on the issues (for examples: ethics, privacy, and so on)(see appendix C for the result). In the fourth phase of the research each entity, sub-system and service of the WMedSys is theoretically interrogated to identify, acquire or preserve DE remaining after the test security attacks. Subsequently, how patient safety will be improved by the re-design of wireless medical device and systems is done in Phase 5, and what forensic benefits can be achieved are established in Phase 6. This is achieved by improving designs for the current WMedSys architectures. The final phases of the research involve an evaluation of the learning in the form of data analysis and conclusions.

6.7 RESEARCH QUESTIONS

As previously stated, the research question that guides the investigation is:

> "**What can be improved to make digital forensic investigation more effective in a wireless medical system?**"

Subsequently, several related secondary or subordinate (sub) questions are formulated in order to answer the main question.

Sub-Question 1: What are the potential risks (security and privacy) of current WMedDs and WMedSys?

Sub-Question 2: What are current protection mechanisms to mitigate security attacks related to a WMedSys?

Sub-Question 3: What are feasible protection mechanisms to improve the design of WMedDs to mitigate security attacks related to a WMedSys?

Sub-Question 4: What are the hardware and software required for the successful acquisition of Digital Evidence (DE) from a WMedSys?

6.8 ASSERTED HYPOTHESES

The main objective of sub-questions is to investigate both the security and forensic capabilities of a WMedSys so that the scope of both risk mitigation strategies can be considered. The intention is to bring about design improvements that reduce the residual risk to a patient of harm or mis-adventure. Hence, in order to answer the aforementioned secondary questions, asserted hypotheses have been established as follows:

Hypothesis 1 (H_1): There will be potential DE in the memory of medical or end-user devices (examples: PDA or remote control of the insulin pump or server logs) of a compromised WMedSys.

Hypothesis 2 (H_2): There will be potential DE that can be found in intermediary devices (such as wireless access point, switches, and so on) of a compromised WMedSys.

Hypothesis 3 (H_3): There will be improved retention of DE when a Forensic Server (FS) is in the WMedSys.

Hypothesis 4 (H_4): There will be potential DE that can be found in other network locations (examples: IDS, system logs, transaction logs

and database of the backend database server) of a compromise WMedSys.

Hypothesis 5 (H_5): There will be improvement of investigator efficiency when forensically ready designs are implemented.

Hypothesis 6 (H_6): User safety can be improved by adding forensic capability in the security design of WMedDs and WMedSys in order to mitigate risks and to preserve DE for post event analysis.

6.9 DATA AND EVALUATION REQUIREMENTS

The hypotheses are to be tested by collecting two sets of data. One from the pilot study and the second from the scenario test. In addition expert feedback will be obtained to learn improvements for the artefact. The pilot study will be used to confirm or otherwise the validity of the knowledge gap identified in the literature. The scenario tests will validate claims for improvement or otherwise for the state of the artefact. The following sub-sections specify the test bed requirements, the updated artefact, and the expert feedback questions.

6.9.1 Proposed Digital Forensic Readiness System Design

To conduct the research, a model of forensic ready WMedSys will be constructed as drafted in the Figure 6.15. The proposed WMedSys is a combination of the existing WLAN and BAN. Hence, according to the previous literature the BAN is comprised of the WMD (for example: the wireless infusion pump or wireless continuous glucose monitoring system or an ICD) and controller or wireless gateway (such as a PDA or a remote control of CGMIDS). Likewise, it is important to monitor and store the wireless network traffic at access points in a log file and its integrity can be preserved in order to get useful information to assist DFI when the WMedSys is compromised. Thus, with respect to the existing WLAN; the proposed forensic ready system architecture will consist of a wireless drone, a Wireless Forensic Server (WFS), a centralised syslog server, a backend database server, and a patient monitoring station (PMSta) (Figure 6.15). Hence, it is proposed that the WFS and wireless drone within the existing WLAN will be set up based on the previous literature. Figure 6.5 is the core design obtained from

literature and Figure 6.15 has added features. Further design research is required to authenticate, to propose beneficial improvements, and to provide far greater detail than Figure 6.15.

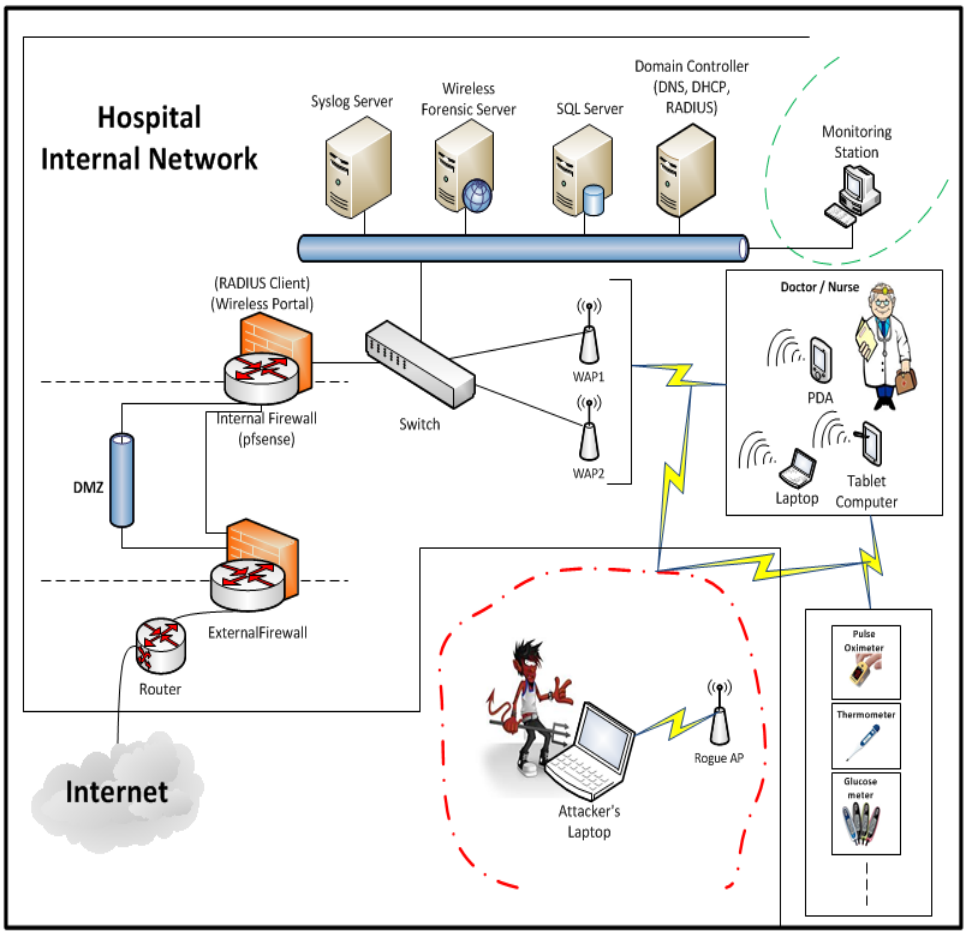


Figure 6.15: Proposed forensic ready wireless medical system

A completed forensically ready system has security for prevention of events and forensic capability to investigate post events. In Figure 6.15, the system architecture is enhanced by adding a forensic server to the hospital information system and also the deployment of drones within the wireless network. These drones within the network are not visible to the wireless network users but they can track, tap and forward packets to the forensic server. In such a proposal the cost of information storage is balanced against the benefit of having the evidence that is readily available. Similarly, the utility cost to the service system is minimal as the forensic element is independent and self-resourcing and can function without visibility. Through this proposed research further improvements and greater detail can be delivered for the understanding of optimal device and WMedSys design.

6.9.2 Evaluation Criteria

According to March and Smith (1995), the main purpose of evaluation in Design Science Research (DSR) is to ensure the goal that an artefact design aligns with the solution of an identified problem and also progress of the design development and deployment of an artefact. To systematically review whether the progress has been accomplished or completed, evaluation criteria should be formulated. Hence, March and Smith suggest a set of evaluation criteria for DSR artefacts.

Nonetheless, researchers not only need to focus on academic interest, but also more importantly need to consider the industry application and adoption of the artefact. For example, on the one hand, industry is more concerned with how easy the artefact can be used, how well it can be adopted and how efficient it can be. On the other hand, a researcher is more interested in how reliable the artefact is and whether or not it is adequate. Therefore, when selecting the evaluation criteria and subsequently formulating evaluation questions, a researcher must satisfy both needs and only ask relevant and appropriated questions to ensure the process will be conducted thoroughly and rigourously.

Table 6.3: Expert evaluation criteria

System dimensions	Evaluation criteria	Sub-criteria	Questions
Goal	Efficacy		Q1: Overall, how effective do you think the proposed DFR Framework artefact would be in the production environment in case of preserving potential digital evidence?
	Validity		Q2: Are the defined components of the proposed DFR Framework artefact clear and relevant to what you observe? Q3: Do you think the provided requirements helpful and adequate in designing DFR Framework artefact for WMedSys?

Environment	Consistency with people	Utility	Q9: Do you think the proposed DFR Framework is effective and efficient in capturing security attacks on a WMedSys? Q10: Do you think the proposed DFR Framework is effective and efficient in determining security attacks on a WMedSys? Q11: Do you think the proposed DFR Framework is effective and efficient in addressing to improve patient/user safety? Q18: How effective do you think the proposed DFR Framework could be if IT managers/security engineers of clinical and hospital networks start using it in their WMedSys?
		Understand-ability	Q6. What was an approximate time for you to follow all components of proposed DFR Framework artefact? Was it easy to understand? Q15. Were the information provided related to the artefact logical and helpful?
		Ease of use	Q5: How easy or difficult do you think it is to implement and integrate the proposed DFR Framework artefact in an existing WMedSys? Q12: Please provide your comments on the usability and ease of operation.
	Consistency with organisation	Utility	Q4: Do you think the proposed artefact is useful and realistic in improving/addressing user/patient safety? Q16: Is the proposed DFR Framework artefact cost effective and efficient? Q17: Is the proposed artefact likely to be widely adopted and implemented in WMedSys?

Structure & Activity (Dynamic, the operations and functionalities of the artefact)	Completeness		Q7: Do you think there is any area of improvement in the proposed artefact? If so, please give your suggestion. Q8: Is there any modification that should be made to any component of the proposed DFR Framework? Q13: Can you list the weaknesses and strengths of the proposed DFR Framework artefact for WMedSys? Q14: Regarding the completeness of the DFR Framework artefact for WMedSys, how do you think?

In addition, another set of evaluation criteria has been developed by Rosemann and Vessey (2009). These criteria focus on whether or not an artefact can be applicable to an industry practitioner. These criteria include importance, suitability and accessibility of an artefact. Further, Prat et al. (2014) have recommended a new set of criteria based on March and Smith (2001) for evaluating information systems (IS) artefacts which is comprised of three major components including system dimensions, evaluation criteria and sub-criteria. The new set of evaluation criteria introduces more categories and further divides March and Smith's criteria into a hierarchical set. Thus, it provides a more precise and comprehensive evaluation for an artefact. Table 6.3 shows artefact evaluation criteria based on a systematic approach derived from Prat et al. (2014).

6.10 CONCLUSION

Chapter 6 has specified a methodology for developing and improving previous wireless medical system forensic designs. The review of previously completed and published research identified tools, techniques and methods that others have used to investigate the wireless vulnerability problems in the medical environment. The result was also the identification of a systems architecture that served as the starting point for artefact improvement (Figure 6.5). The DS methodology was adopted as an appropriate approach and methodology for the study aims. In Chapter 7 the findings from the pilot study and scenario test will now be reported.

Chapter Seven

PILOT STUDY AND SCENARIO FINDINGS

7.0 INTRODUCTION

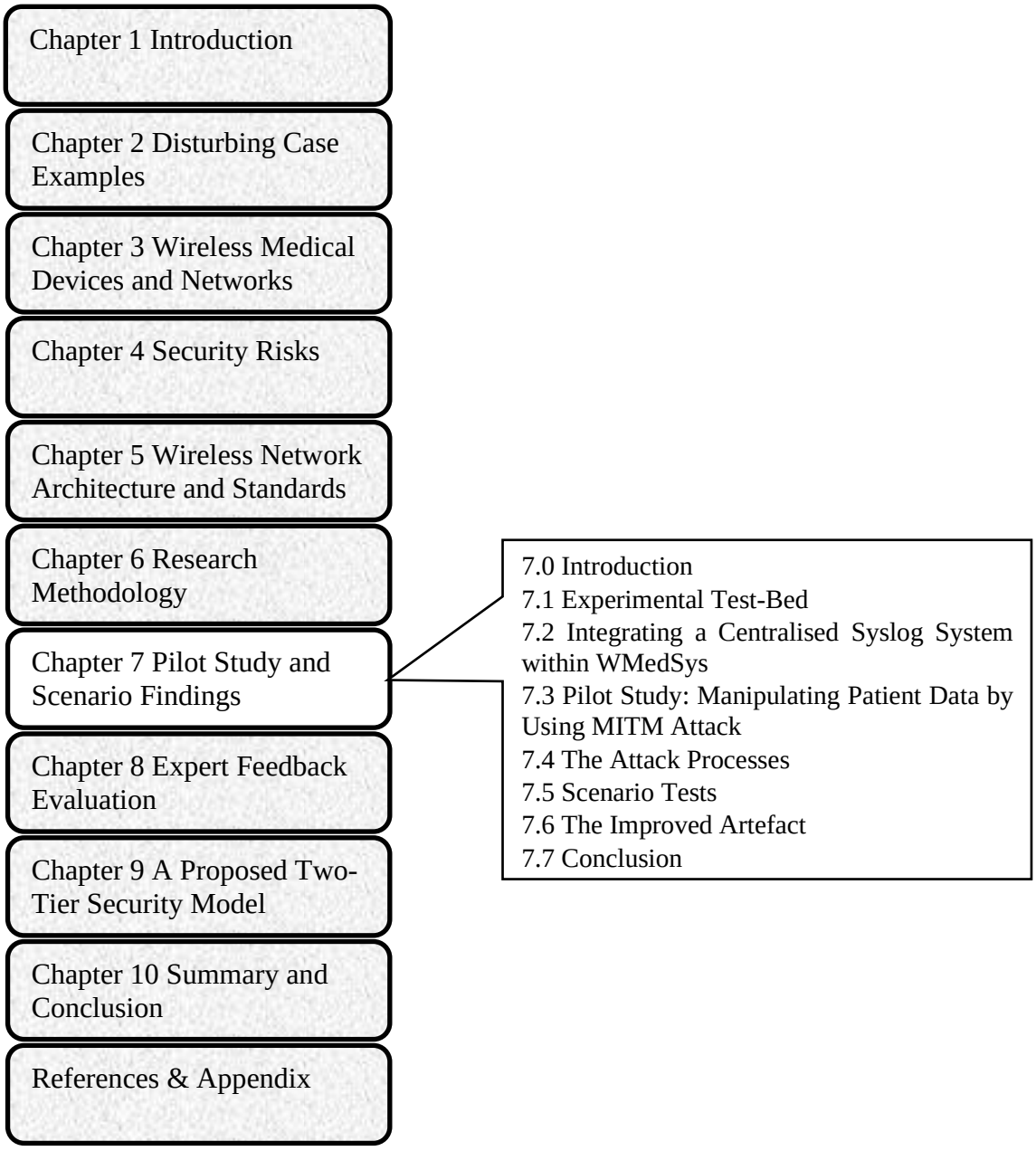


Figure 7.1: Roadmap of Chapter 7

Wireless local area networks (WLANs) are widely deployed in the healthcare industry due to the benefits provided by these networks such as improvement in the quality of delivering medical services, mobility, productivity, efficiency and

the reliability of real-time patient monitoring. However, as was established theoretically in Chapters 2–4, the nature of wireless networks inherently exposes patients and medical staff to security and privacy risks, thus reducing the potential benefits. For example, the design and implementation flaws present in wireless security protocols such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2 make wireless medical systems and devices vulnerable to various attacks. In this Chapter 7, the results of the Pilot Study to confirm or otherwise the literature findings on vulnerabilities are reported. Also the findings from the scenario tests are reported for quality improvement to the artefact in Figure 6.15.

Experiments on a typical wireless medical system that utilises WPA2-PSK and WPA2-Enterprise with various attacks are made by using freely available off-the-shelf tools to successfully compromise it. The experimental results show that tools such as “Aircrack-ng” and “Pyrit” can be used to initiate the Man-in-the-Middle attack on a Wi-Fi Protected Access version 2-Pre-Shared Key (WPA2-PSK) based WLAN that results in capturing the legitimate credentials of medical records. Similarly, “Asleap” and “Mana” tools can be used to successfully obtain login credentials by carrying out dictionary and SSL Stripping attacks on WPA2-Enterprise, respectively. A comparison of exploiting security vulnerabilities in these two protocols is also reported. First the pilot study findings are reported to (in this case) confirm the vulnerabilities identified from the literature. The scenario findings are then reported to identify elements of improvement of the artefact design given in Figure 6.15.

A prototype of a typical WMedSys is set up in a controlled laboratory environment that comprises different servers including a patient database system and networking devices. The initial forensic readiness components were based on Figure 6.15. Two fictitious scenarios are used: the first for the Pilot Study, and the second for the Scenario Test. The experiments demonstrate that MITM attacks performed by using the tools Aircrack-ng and Pyrit can obtain the credentials of authorised medical staff of a WMedSys based on WPA2-PSK. Similarly, attacks on a WMedSys based on WPA2-Enterprise using SSL Stripping and dictionary attacks are successfully carried out by using Asleap and Mana tools. Moreover, the comparison of compromising security vulnerabilities in WPA2-PSK and

WPA2-Enterprise is reported. The contribution of this chapter is to present data that confirms the literature assertions for vulnerabilities in WMedSys, and also provide data for the improvement of the artefact (see Figure 7.36 improvements).

7.1 EXPERIMENTAL TEST-BED

The main purpose of this research was to find the answers to the following questions.

- Question 1: What are the procedures to compromise a WMedSys that utilises WPA2-PSK by using off-the-shelf tools?
- Question 2: What are the procedures to compromise a WMedSys that utilises WPA2-Enterprise by using off-the-shelf tools?

In order to answer the research questions, a test bed of relevant hardware and software was constructed and then artefacts tested. This phase included designing the network topology, identifying the required hardware (HW) and software (SW) tools, and setting up the experimental test-bed to replicate the real-world WMedSys. Then the WMedSys was stressed by performing different attacks (for example Man-in-the-Middle attack to manipulate the information related to a patients' health records). The simulated WMedSys held a centralised Syslog System for patient records and the wireless network access that would be found in a real medical environment. The experimental test-bed (WMedSys) was set up in a controlled environment in the laboratory and based on the previously published research Vassis et al., 2010; Malasri et al., 2009; Varshney, 2007, Lin et al., 2004, Varshney, 2003). The WMedSys network included various components such as servers and networking devices (as shown in Table 7.1 for hardware specifications). WMedSys architecture is based on a type of infrastructure wireless network that is composed of the IEEE 802.3 Ethernet wired network and IEEE 802.11 wireless network. It has wireless clients that emulate doctors or nurses using wireless devices to monitor patients or update clinical data (such as blood pressure, glucose levels) related to patients in a real-world hospital or clinical environment. A widely used open-source electronic medical records system (OpenEMR) was implemented in the WMedSys to store patient related data for this research.

In order to collect the experimental data, the following fictitious case scenarios, based on previously well-cited articles are used (slightly different scenario for each test).

Table 7. 1. Components of WMedSys.

Component	Description	Computer Name	IP Address (x.x.x.x/24)	Software Version
ADDS DNS DHCP RADIUS	Active Directory Domain Services Domain Name System Dynamic Host Control Protocol Remote Authentication Dial-In User Service	dc01 (Domain Controller Server)	172.16.50.1	Windows Server 2008 R2 (Enterprise Edition)
XAMPP Web Host & OpenEMR [38-39]	Electronic Medical Records (Open-source)	logclient01	172.16.50.5	XAMPP (version 3.2.1) & OpenEMR (version 4.1.2), running on Windows 8 Enterprise
BroIDS [40]	Bro-Network Intrusion Detection System (Open-source)	Bro-VM	172.16.50.8	Bro 2.5.4
Splunk [41]	Centralised Syslog Server	logsrv02	172.16.50.12	Splunk (Enterprise version: 6.4.0)
UniFi Controller	Software for Managing UniFi Wireless Networks	fwdsrv	172.16.50.2	Controller version: 3.2.10
Ubiquiti UniFi AP-LR (Long Rang)	UniFi WAP for Wireless LAN	-	172.16.50.25	Firmware version: 3.2.12.2920
Default Gateway	Firewall and Router Software (Open-source)	pfSense	172.16.50.254	pfSense version: 2.2.4
Cisco 2950 Catalyst Switch	24-ports	-	-	Cisco IOS version: 12.1

Scenario 1 (WPA2-PSK) is the compromising of a WMedSys that utilises WPA2-PSK (The Pilot Study). The first case scenario is created to confirm or otherwise the vulnerability of the system to attack. A 50-year-old Chief Executive Officer (CEO), John Lauren, from one of the fortune 500 companies, with underlying poorly controlled diabetes mellitus was on a wireless insulin pump to get better control of his blood glucose level. The insulin pump was wirelessly connected with an automatic glucose monitor. Both the pump and glucose monitor were attached to the body and the pump infuses insulin depending on the glucose level data transmitted by the glucose monitor.

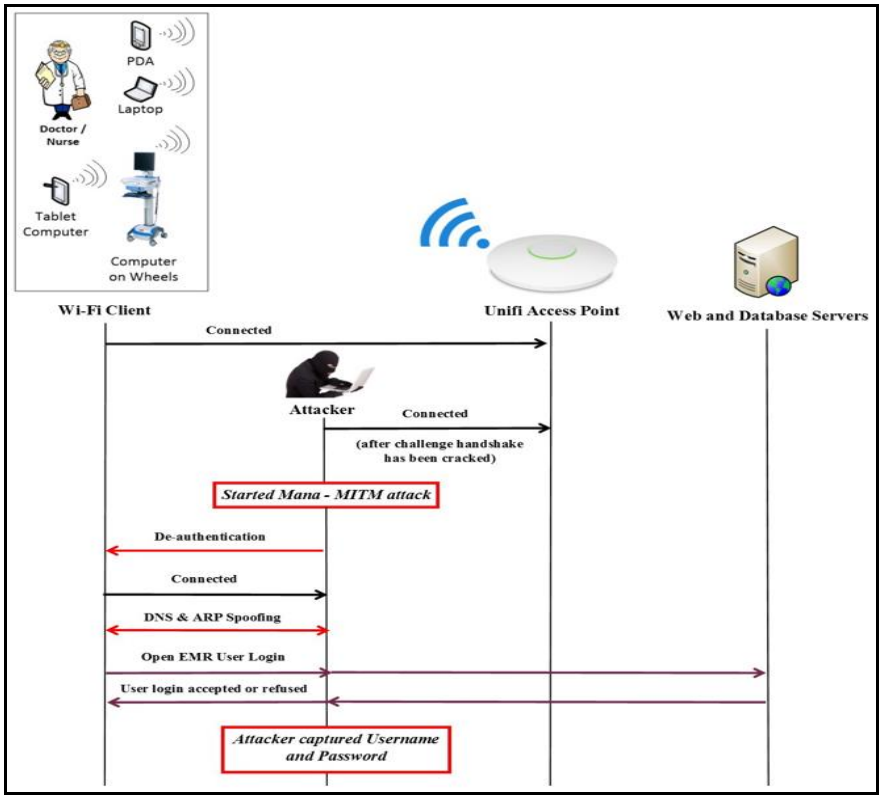


Figure 7.2: Man-in-the-Middle Attack on a WMedSys Using WPA2-PSK.

The pump can store up to 500 units of insulin (250 each for short acting and long acting insulin). The total daily requirement dosage of the insulin is between 0.2-05 units per kilogram based on body weight of the patient. The higher insulin dose can induce hypoglycaemia and without immediate correction of the glucose level, the patient could suffer from permanent brain injury and this could eventually lead to death. John was currently admitted to the emergency department (for seizure followed by loss of consciousness) in order to control his blood glucose level. The blood glucose level was very low. He was immediately treated with glucose bolus

IV infusion and he regained conscious later with permeant neurological deficiency. In this first scenario, the emergency department John was admitted to a private clinic that deploys the wireless network based on WPA2-PSK (SSID of WLAN for WMedSys was MyWiFi-Guest).

Figure 7.2 shows the Man-in-the-Middle (MITM) attack carried out by a malicious attacker deploying the MANA Toolkit in order to manipulate the patient's data, which was saved on the backend server (OpenEMR). The MANA Toolkit is used to create a Fake AP with the same SSID of the legitimate AP used by the clinic. Hence, in this attack scenario, the attacker used a legitimate client login and its password. This legitimate credential was obtained after sniffing the wireless communication (used by a doctor who has a legitimate login username, doc007), and performing the brute force attack to crack the password by using Aircrack-ng suite. Afterwards, the malicious attacker accessed the OpenEMR and changed the patient's physiological data (the blood glucose level). The successful MITM attack included de-authentication, DNS and ARP spoofing and capturing the packets related to authentication.

7.2 INTEGRATING A CENTRALISED SYSLOG SYSTEM WITHIN WIRELESSS MEDICAL SYSTEM (WMedSys)

In the preliminary test environment (Figure 6.15), the OpenEMR system where the electronic medical records of patients were stored, was installed on a local host in the proposed forensic ready WMedSys. The healthcare professionals or authenticated users such as clinicians, doctors or nurses had wirelessly access to OpenEMR by using mobile devices in order to retrieve or update registered patient medical record or data (Figure 7.3).

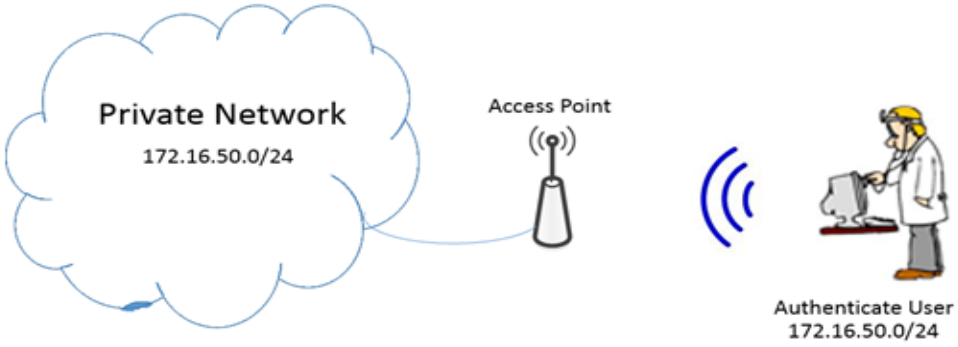


Figure 7.3: Communication path between un authenticated user and WMedSys

In Figure 7.4 the attacking path is identified.

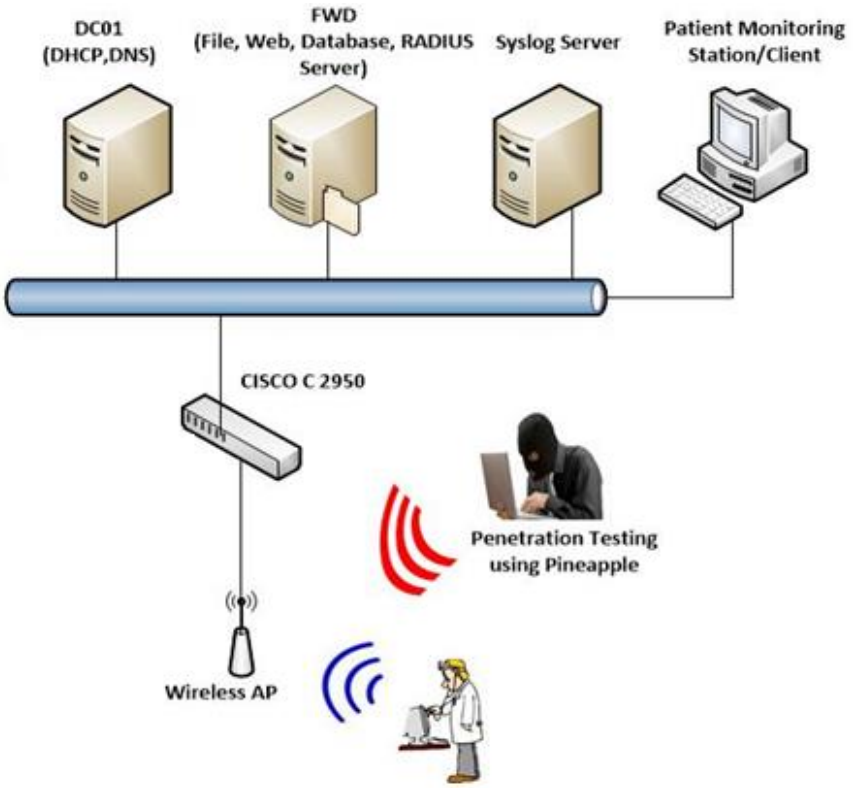


Figure 7.4: Integrating a centralised system system in the proposed WMedSys

During the experiment, three different types of open-source syslog servers (one at a time) were used in order to capture the footprint of patient data manipulation and malicious attacks. Hence, the best open-source syslog server could be chosen for the proposed forensic ready WMedSys.

7.3 PILOT STUDY: MANIPULATING PATIENT DATA BY USING MITM ATTACK

The scenario was an adversary or unauthorised person performing data manipulation attacks (De-authentication, Man-in-the-Middle or SSL stripping) by using a Wi-Fi Pineapple (version. Mark IV) while a doctor or nurse updated a patient data to the backend OpenEMR system (see Figure 7.5). Then, the analysis of the syslog messages on open-source syslog servers (LOGalyze, Snare Backlog and Rsyslog) were performed the digital evidence of the attacks. See Appendix E for the full transcript of the attack communications and device code.

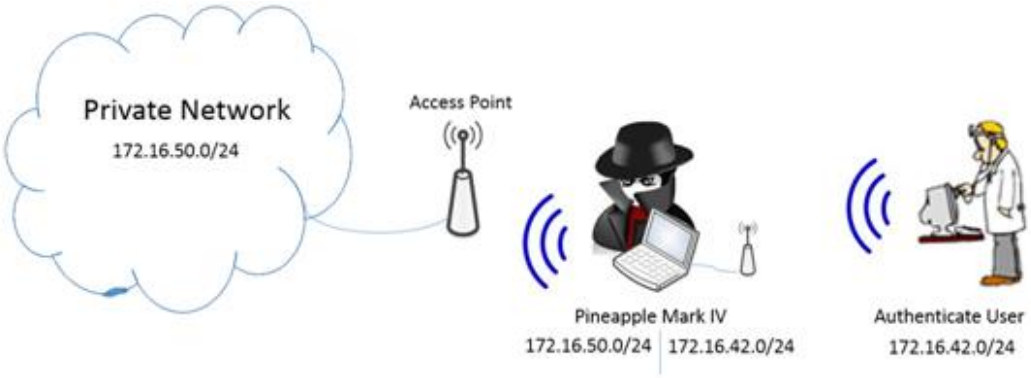


Figure 7.5: Man-in-the-Middle (MIMT) attack by using a Wi-Fi Pineapple

With the combination of de-authentication (De-Auth) and fake access point (Fake AP) attacks, an adversary was able to initiate the MIMT attack after compromising an authenticated user's login credential. MIMT attack was initiated by creating the name of a Fake AP with the same as that of the legitimate one and forcing authenticated users (either doctors or nurses) to get connected with the fake. Hence the Wi-Fi Pineapple mimicked as a legitimate AP within the system and all the data traffic during communication could be traced in order to get an authorised user's login credentials. However, to trace login credentials, a secure socket layer stripping (SSL) plug-in was used with the Wi-Fi Pineapple. The intermediary device (Wi-Fi Pineapple) would not allow any user associated with it to initiate a secured connection with the private network and forced communication with an insecure connection once the SSL stripping was enabled. Thus, the login credentials (username and password) of a doctor or a nurse were captured along with the patient's physiological data. This allowed access to the OpenEMR backend, and an adversary could manipulate/access patient data with the help of the compromised credentials.

7.4 THE ATTACK PROCESSES

The procedures to compromise the WMedSys that utilises WPA2-PSK, was done by using off-the-shelf tools and Kali Linux 2.0. The following steps report the technical actions (see also Appendix B for code).

Step 1: Airmon-ng tool (which is a tool integrated into Aircrack-ng) should be run to discover the available wireless network interface cards (NICs) on the attacker's computer. If there are current processes running in the background, those processes should be stopped by using the command, "airmon-ng check kill". After getting the information about the wireless NIC and terminating any running

process, the wireless NIC should be put to monitoring mode by running the "airmon-ng start wlan0" command (Figure 7.6).

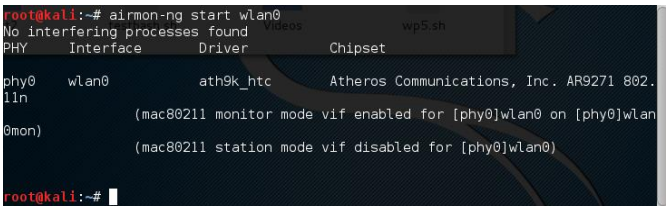


Figure 7.6: Wireless NIC was placed in monitoring mode on attacker's machine running Kali Linux 2.0

Step 2: In this step, the attacker changed the wireless MAC address of the machine used to perform WPA2-PSK attack by using the "macchanger" command. However, the monitoring interface should be turned off by using "ifconfig wlan0mon down" command before changing the MAC address and the monitoring interface should be turned on after changing it (Figure 7.7).

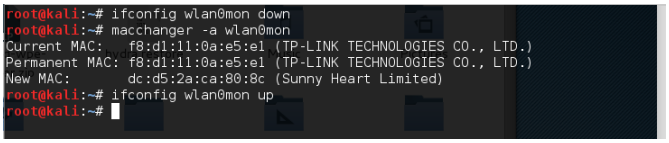


Figure 7.7: Changing wireless MAC address on the attacker's machine

As shown in Figure 7.7, the command option (-a) used after "macchanger" is to set a new random vendor MAC address of the same kind. By doing so, the attacker's machine is difficult to trace back.

Step 3: The "Airodump-ng –M wlan0mon" command was used to capture the wireless traffic. By doing so, the attacker could obtain the sensitive information including the MAC addresses of WAPs (Basic Service Set Identifications or BSSIDs), signal power (PWR) of WAPs, total numbers of beacons (Beacons),

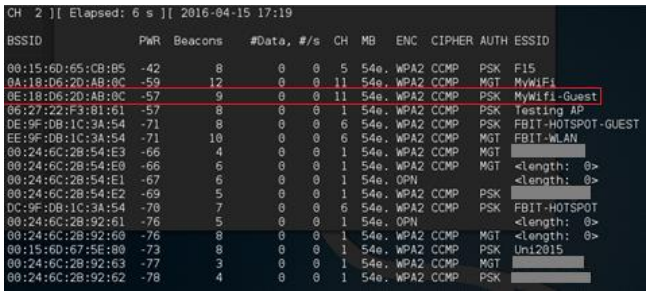


Figure 7.8: Screenshot of the captured wireless traffic

channels used (CH), encryption protocols (ENC) in use, detected cipher (CIPHER), authentication protocols used (AUTH), Extended SSIDs (ESSIDs), manufacturer names and the like (Figure 7.8).

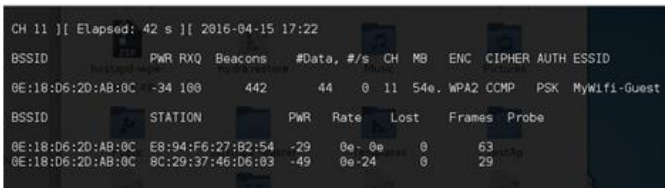


Figure 7.9: Output screenshot of capturing the authentication handshake

Step 4: Then, "Airodump-ng –c 11 –w root/testAp/WPA2capture --bssid 0E:18:D6:2D:AB:0C wlan0mon" command was used on WAP channel to capture the authentication handshake for the WAP when under attack (Figure 7.9).

In this experiment for the Pilot scenario, the SSID of the WLAN for the WMedSys is MyWiFi-Guest and thus the MAC address of WAP under the attack is 0E:18:D6:2D:AB:0C. The command options used are: "-c" and "-w"; which are the channel being used by WAP and the file for saving captured data, which contains the authentication handshake between the supplicant (client) and the authenticator (WAP) respectively. Similarly, "-0 5" options were used for performing de-authentication attack. For cracking the encrypted password, a legitimate client must be associated with the WAP. As shown in Figure 7.9, there are two clients connected to the WAP under attack.

Step 5: However, the time taken to capture a successful handshake create delays. In order to speed up the handshake capture time, the attacker can initiate a de-authentication attack by opening a new terminal while still running the previous one in Step 4 and running the "Aireplay-ng" tool.

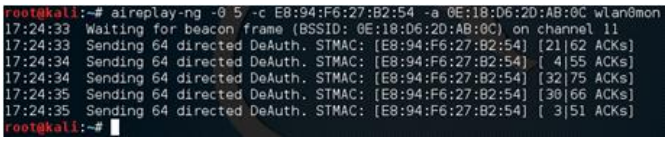


Figure 7.10: De-authentication attack

To be able to perform Fake AP attack, the signal strength of Fake AP running on the attacker's machine should be stronger than that of WAP under the attack. Hence, the de-authentication attack performed by the adversary can be seen in Figure 7.10.

Step 6: The adversary could passively wait for a nurse or doctor who used the wireless client station (Victim's MAC: E8:94:F6:27:B2:54) by reconnecting to the WMedSys with a legitimate username and password. After a while, the WPA2 handshake could be captured (as shown in top right corner of the terminal window in Figure 7.11) and the captured handshake would be saved in the file

(root/testAp/WPA2capture). Once the handshake had been captured, the current process was stopped by using “Ctrl+c” keys (Figure 7.11).

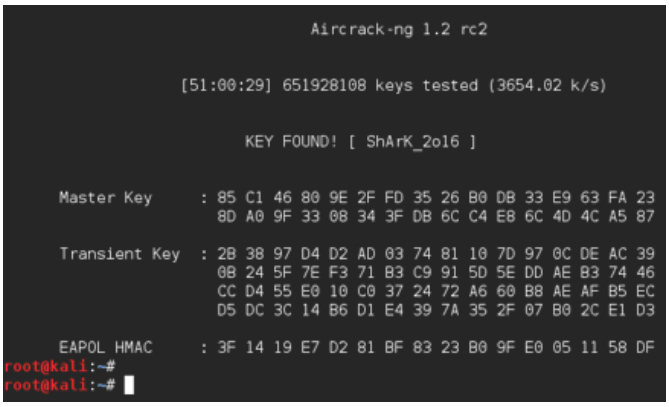


Figure 7.11: The result of cracking WPA2-PSK password with Aircrack-ng

Step 7: This step is to perform the dictionary attack to get the password from the handshake captured. As the offline dictionary attack was carried out by using Aircrack-ng along with a customised wordlist, the Crunch wordlist generator tool was initially used (Figure 7.12).

Figure 7.12: Authentication handshake captured

After creating the customised wordlist and cracking password by using Aircrack-ng, the password (ShArK_2016) was obtained. The result of Aircrack-ng was shown in Figure 7.13.

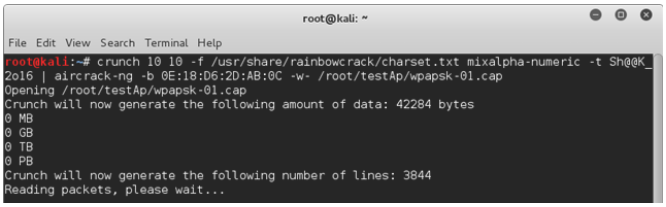


Figure 7.13: Creating password list by using Crunch tool

Step 8: Finally, the adversary changed the patient’s physiological data (the blood glucose level) after logging to the web interface of patient database (OpenEMR) of the WMedSys by using the credentials of a doctor obtained from previous steps (as stated in the Scenario 1 of Section 8.).

Figure 7.14 summarises the steps or procedures used to compromise WPA2-PSK by using different tools such as Airmon-ng, Airodump-ng, Aireplay-ng and Aircrack-ng. Similarly, WMedSys system using WPA2-PSK can also be

compromised by using other tools and techniques. One of the most powerful tools to carry out wireless attacks against widely used security protocols is Pyrit.

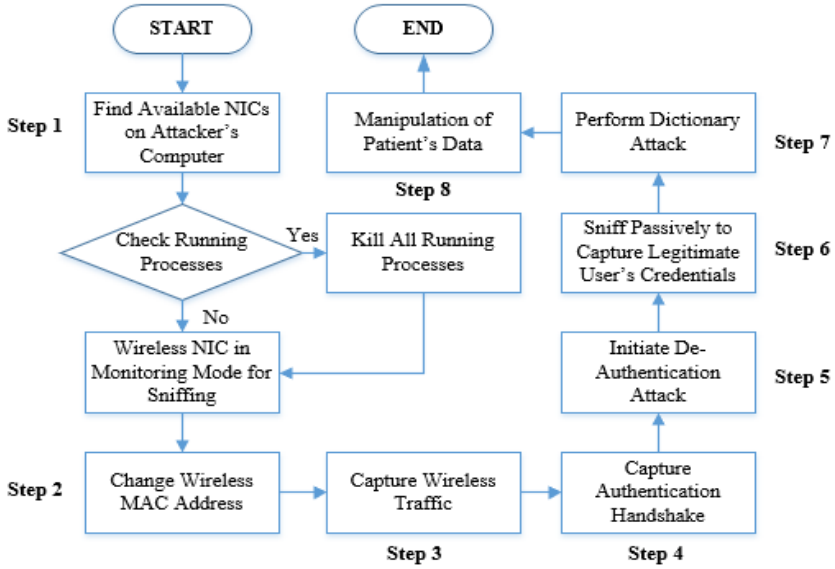


Figure 7.14: Procedures used to compromise WPA2-PSK

In summary the following steps are used to compromise WMedSys by Pyrit from Kali Linux running on the attacker's computer.

Step 1 to Step 4: The initial steps for conducting WPA2-PSK attack by using Pyrit are the same as using aforementioned Aircrack-ng tool.

Step 5: In this step, the Pyrit tool was run by using the following command to capture the wireless traffic (Figure 7.15).

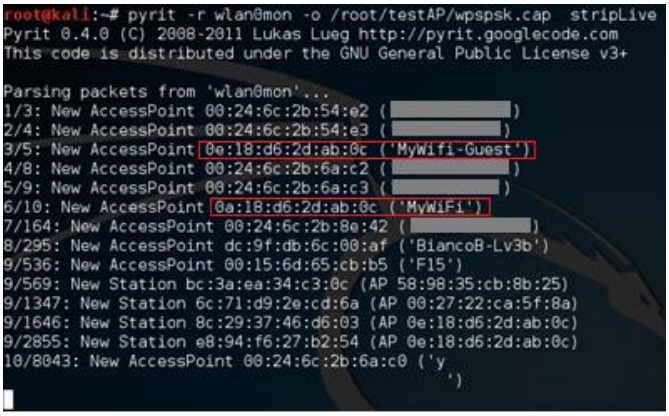


Figure 7.15: Capturing the wireless traffic with Pyrit tool

Step 6: Similar to Steps 5 and 6 in the previous attack by using Aircrack-ng, the de-authentication attack was carried out by using the "Aireplay-ng" tool (Figure 7.16).

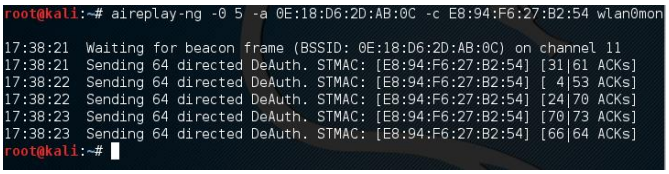


Figure 7.16: De-authentication by using Aireplay-ng tool

Step 7: Finally, the captured packet file "wpspsk.cap" located in the folder, "/root/testAP/" was attacked by using the Pyrit tool without creating the customised password list. As shown in Figure 7.17, the password (ShArK_2016) was obtained. By using the cracked password, the attacker could carry out further attacks in WMedSys. The next sub-section will explain the steps required to crack WPA2-Enterprise in WMedSys.

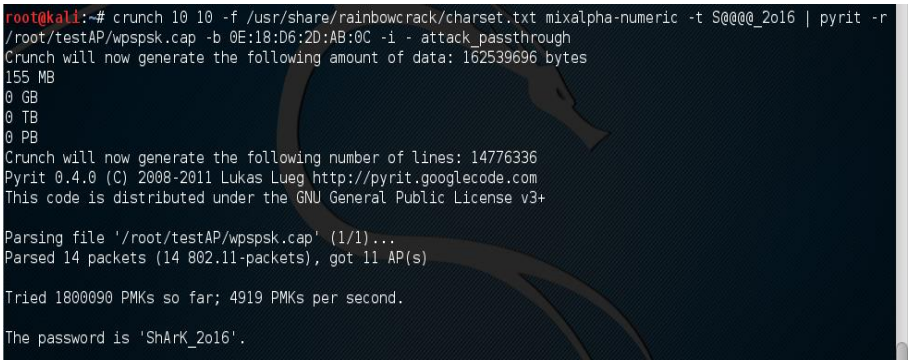


Figure 7.17: Cracking password by using Pyrit Tool

7.6 SCENARIO TESTS

The Pilot study has confirmed some of the security vulnerabilities identified in the literature review. Although not all could be tested in the time available, the results are indicative of serious vulnerabilities inherited by WMedSys from the current state of real wireless technologies. The Scenario tests will now proceed to test the forensic ready framework (Figure 6.15) and to identify any areas for improvement. All testing has learning feedback loops and the information will be collected for analysis. The Scenario 2 is similar to Scenario 1 that is a documented example of the fictitious case of a patient admitted to hospital and who experienced harmful events. It is a Joe Doe case that represents information taken from many reports.

Similar to the first scenario, John Lauren was admitted to a hospital in order to control his blood glucose level. The patient's data is manipulated from the backend server (OpenEMR) by a hacker. However, the WMedSys in this

scenario is based on WPA2-Enterprise (WPA2-EAP), where users are authenticated by using RADIUS and AD database (SSID of WLAN for WMedSys was MyWiFi) (see Figure 7.18). The way in which legitimate users are authenticated against the RADIUS server is stated and described in Chapter 4. After getting the credentials of the WMedSys user (a nurse whose login username is nurse007), the malicious attacker amended the patient's physiological data (the blood glucose level).

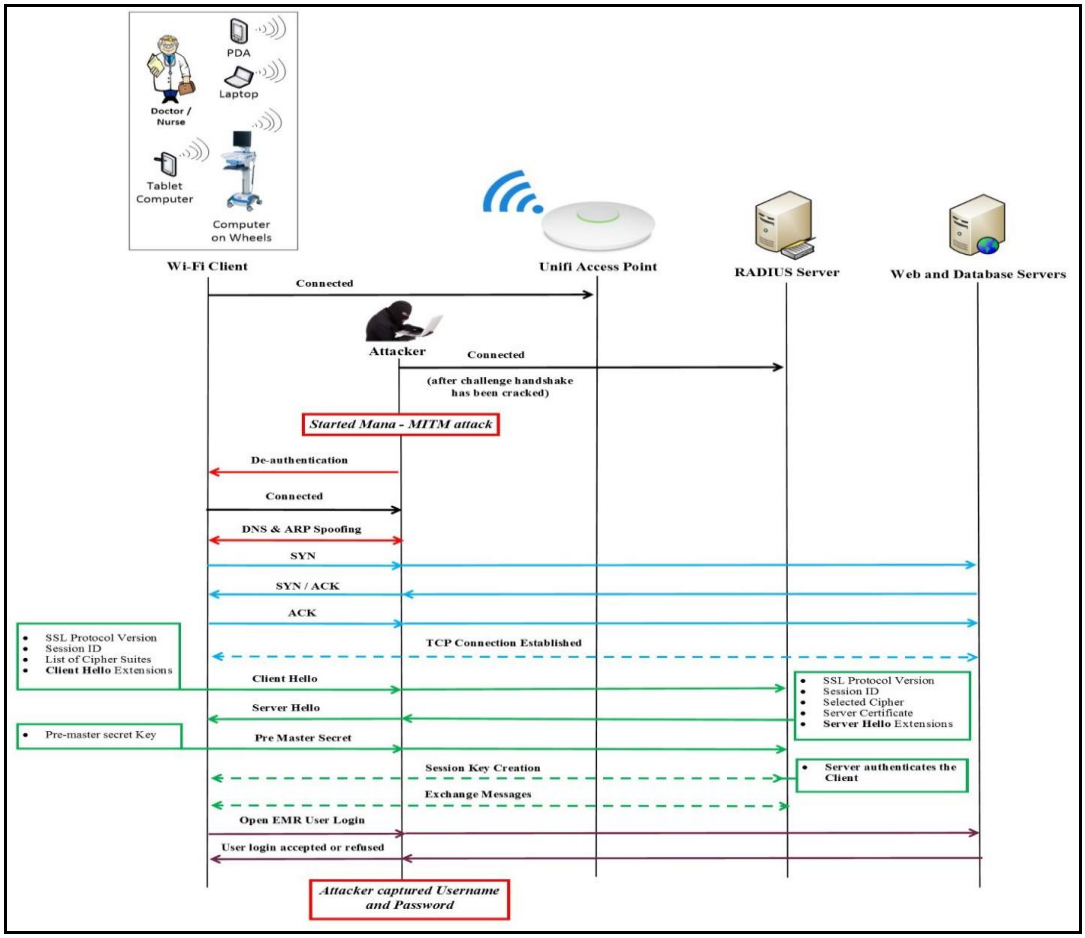


Figure 7.18: Man-in-the-Middle attack on a WMedSys using WPA2-Enterprise

The test was set up to run Kali Linux 2.0 version running with two wireless NICs on the attacker's computer, one NIC was used for monitoring (wlan1) and the other (wlan0) was deployed for running a Fake AP. All the software packages were also installed and updated on the attacker's computer. For instance, packages for OpenSSL and the certificate for authentication were installed in addition to updating all necessary library packages. Similarly, the source list file, located in /etc/apt/sources.list, has to be updated. Figure 7.19 shows the library updates for the "hostapd-wpe" Configuration File.

```
# wlan Interface
interface=wlan1

#SSID, 802.11 mode and Channel information
ssid=TEST_EAP
hw_mode=g
channel=6

# WPA version of WAP under attack should be changed
eap_server=1
eap_fast_a_id=101112131415161718191a1b1c1d1e1f
eap_fast_a_id_info=hostapd-wpe
eap_fast_prov=3
ieee8021x=1
pac_key_lifetime=604800
pac_key_refresh_time=86400
pac_opaque_encr_key=000102030405060708090a0b0c0d0e0f
wpa=1
wpa_key_mgmt=WPA-EAP
wpa_pairwise=TKIP CCMP
```

Figure 7.19: Changes in "hostapd-wpe" configuration file

The procedures to compromise a WMedSys that utilises WPA2-Enterprise by commonly used off-the-shelf tools are summarised in the following steps.

Step 1: The initial step is to download and install "hostapd-wpe" package, which is used to carry out the impersonation attack for getting login credentials of the staff (doctor or nurse). In fact, this toolset allows an attacker to perform impersonation attacks against WPA2-Enterprise.

Step 2: In this step, the attacker runs the "ifconfig" command in order to note down details of the wireless NICs (including the name).

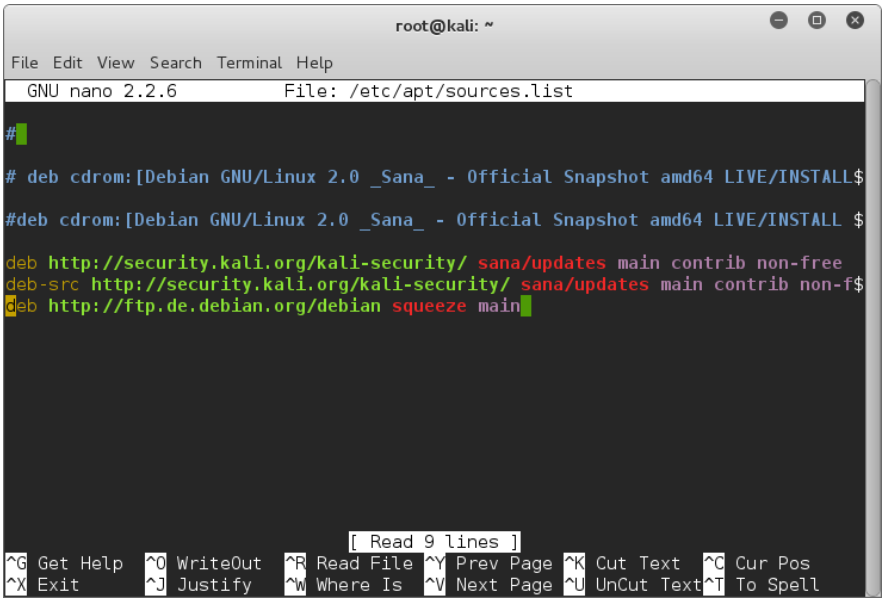


Figure 7.20: Updating source list file

Step 3: Similar to Steps 1 and 2 (in conducting WPA2-PSK attack), Airmon-ng tool is run by using the "airmon-ng start wlan1" command to start the wlan1 NIC interface for sniffing the wireless traffic. Any processes that could cause problems

should be killed. In addition, MAC addresses of wlan0 and wlan1 are changed to set new random vendor MAC addresses of the same kind (Figure 7.20).

Step 4: The "Airodump-ng –M wlan1mon" command was used to capture the wireless traffic in the air to obtain the critical information such as BSSID, ESSID, etc., mentioned in Step 3 of WPA2-PSK attack.

Step 5: After getting the detailed information about BSSID, ESSID, the channel used, the type of WPA and WPA versions; the Airodump-ng tool is used again to capture the authentication handshake. The command used in this step is "Airodump-ng –c 6 -- bssid 00:26:5A:F2:57:2B wlan1mon" (similar to Step 4 of WPA2-PSK attack). After making changes, the configuration file should be saved and the "hostapd-wpe" is run with the modified configuration file.

Step 6: In this step, the configuration file of "hostapd-wpe" should be opened with "nano" text editor and modified with the information gathered in Step 4, which is the information related to the WAP under attack, such as NIC interfaces for monitoring and running the Fake AP.

Step 7: The running terminal of Airodump-ng (Step 5) should be terminated. Then, a new terminal should be opened for running the "Aireplay-ng" tool to perform de-authentication attack. The command used for such attack is as follow in Figure 7.21.

```
root@kali:~# aireplay-ng -0 5 -a 00:26:5A:F2:57:2B -c
C0:C1:C0:4C:F9:B2 wlan1mon
```

Figure 7.21: De-authentication attack using Aireplay-ng tool

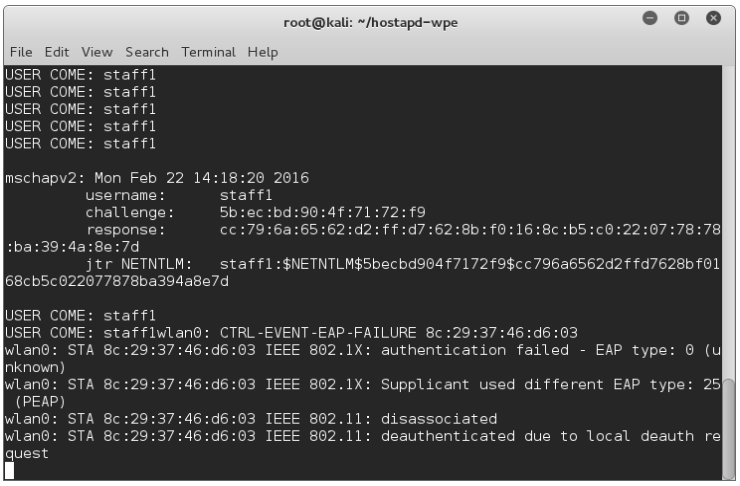


Figure 7.22: Captured sensitive information

In Figure 7.21, the interface used for this attack is wlan1, the victim's MAC address is C0:C1:C0:4C:F9:B2 and BSSID of the WAP is 00:26:5A:F2:57:2B.

Step 8: After waiting for a while, the client will try to reconnect to the WAP. When the reconnection is being established, the authentication request challenge will be transmitted between the legitimate client and WAP.

Once the client under attack accepts the new certificate and connects to the Fake WAP, the sensitive information such as username (staff1 in this attack example), challenge and response hash values are captured (Figure 22).

Step 9: The character set the victim (staff1) is using for a password, is useful for creating a password list to crack any password. In order to find the choice of character sets, the "cat /usr/share/rainbowcrack/charset.txt" command is used.

Step 10: Afterwards, similar to Step 7 (in conducting WPA2-PSK attack), the Crunch wordlist generator tool was used to create the customised password list. The Crunch command options used in Figure 7.23 were minimum and maximum password lengths (9 and 9 respectively), "-t P@@@@@@@@1" for generating the pattern of passwords with 7 unknown characters and "-o /root/testkey5.txt" for saving the generated password list in the dictionary file.

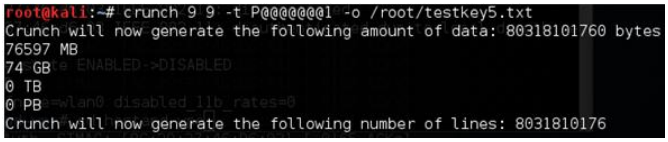


Figure 7.23: Creating password list by using Crunch tool

Step 11: After creating the customised password list, one of the Kali Linux's tools ("asleap") was used for the offline dictionary attack as it could attack the MS-CHAPv2 that was used as an authentication protocol option with a RADIUS server for securing WMedSys using the WPA2-Enterprise protocol. The result of cracking the victim's password with the "asleap" tool is shown in Figure 7.24.

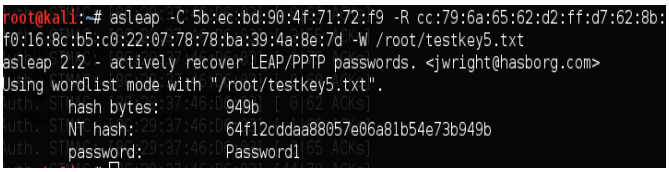


Figure 7.24: Result of cracking WPA2-Enterprise password by Asleap tool

Step 12: Hence, in this case, the victim's password cracked was "Password1". By using such credentials of a legitimate user, the attacker could initiate different attacks such as changing the electronic medical records of patients.

Figure 7.25 summarises the steps or procedures used to compromise WPA2-Enterprise by using different tools such as Airmon-ng, Airodump-ng, Aireplay-ng, Crunch and Asleap tools.

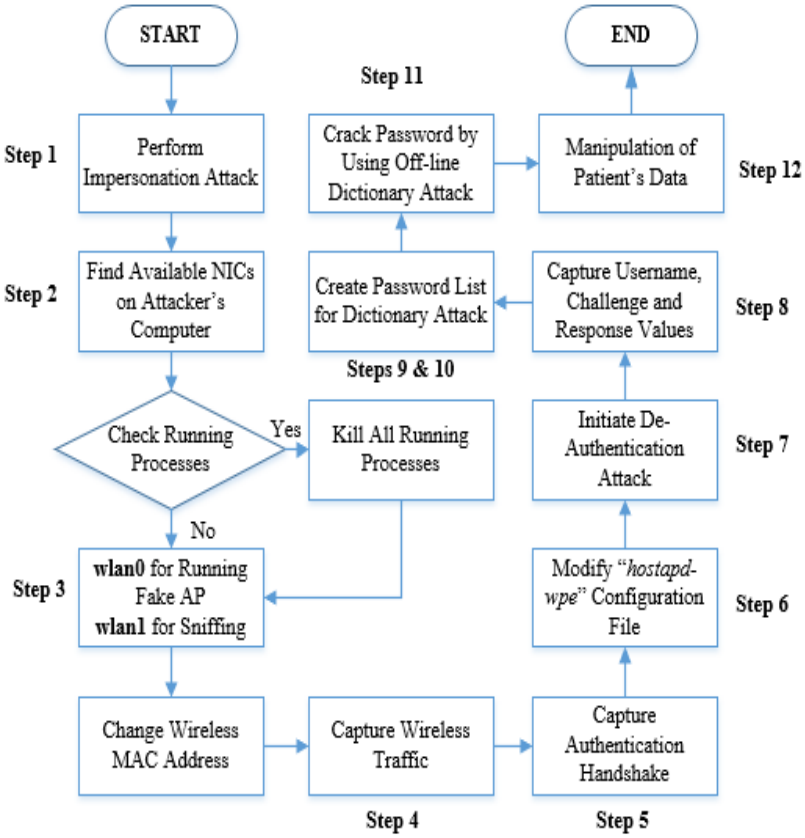


Figure 7.25: Procedures Used to Compromise WPA2-Enterprise

The following steps are used for attacking WMedSys using WPA2-Enterprise with Mana toolkit.

Step 1: Updating source list file required the necessary sources to be added initially to the source file in order to perform a successful MITM attack (Figure 7.26).

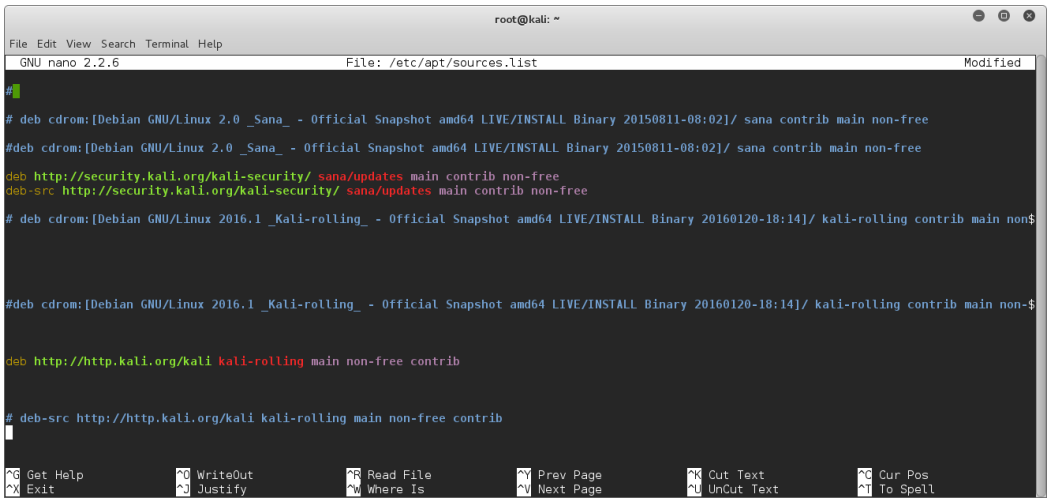


Figure 7.26: Adding sources in source list file

Step 2: Then, the source list database was updated, and all packages were upgraded by using "apt-get update" and "apt-get upgrade" commands.

Step 3: Subsequently, Mana toolkit was installed by using the "apt-get install mana-toolkit" command (Figure 7.27). In fact, Mana toolkit has a set of tools for performing wireless MITM and rogue AP (evilAP) attacks.

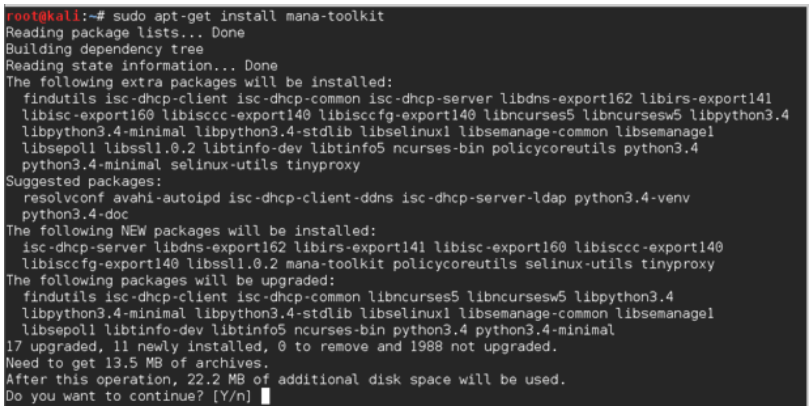


Figure. 7.27: Installing Mana tool

Step 4: In this step, a new database file (namely "dhcpd.leases") was created for temporary IP address leases (Figure 7.28).

```
root@kali:~# nano /var/lib/dhcp/dhcpd.leases
```

Figure 7.28: Creating a new file for IP address leases

However, the newly created file was modified by adding "#" in the file (Figure 7.29).

Figure 7.29: Modifying "dhcpd.leases" file

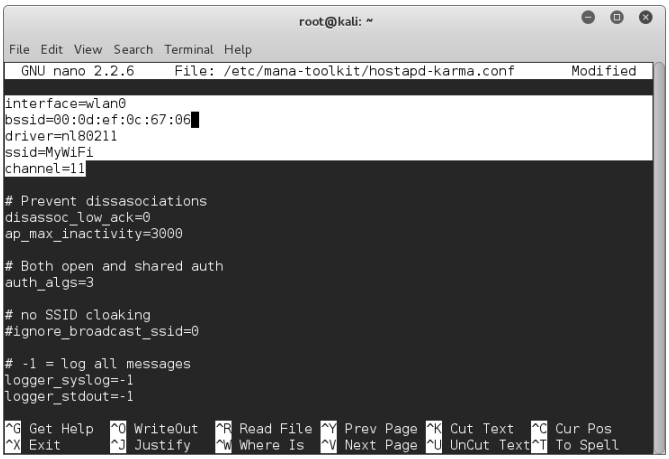


Figure 7.30: Adding sources in source list file

Step 5: Afterwards, the "hostapd-karma.conf" configuration file was modified by using the same SSID and channel used by the WAP of WMedSys under attack (Figure 7.30).

Step 6: For this MITM attack, the Ethernet interface was used for connecting to the Internet, otherwise the attack might not be successful. Hence, it is essential to check the information of NICs on the attacker's computer.

Step 7: In this step, the Mana tool should be configured with the interfaces for connecting the Internet (eth0) and running the evilAP or Fake AP (wlan0). Hence, the shell script file "start-nat-full.sh" was modified as shown in Figure 7.31. In this attack scenario, it should be noted that the network interface connected to the Internet (upstream) was configured to use eth0 and the wireless interface for Fake AP was assigned to use wlan0.

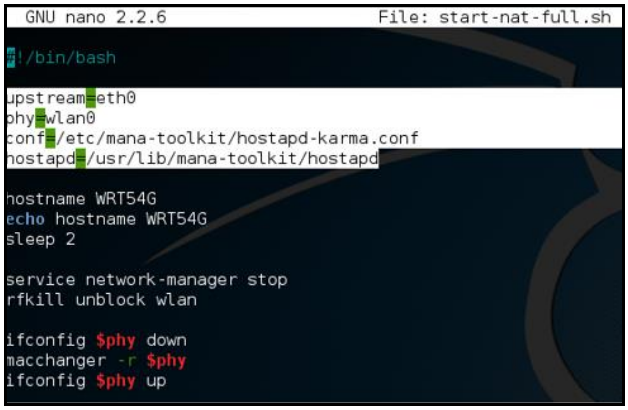


Figure 7.31: Updating "start-nat-full.sh" file

Step 8: The Mana tool was run by using the following command (Figure 7.32).

Figure 7.32: Running "start-nat-full.sh" file

Step 9: After running MITM with Mana tool, the log files related to the victim accessing the OpenEMR was found in the folder "/var/lib/mana-toolkit" (Figure 7.33).

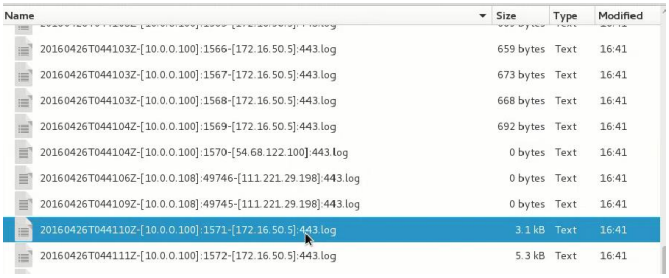


Figure 7.33: Captured log files related to the victim

Step 10: Finally, the log files were analysed in order to get the credentials of the victim. As the Mana tool for running Fake AP is integrated with the SSL

Stripping attack, the credentials of the victim could be found in plain-text (Figure 7.34).

Figure 7.34: Legitimate Credentials Obtained from a Log File

According to the obtained credentials, the victim in this case was a nurse who accessed the OpenEMR by using the login username "nurse007" and the password "Password1". Hence, the attacker could now initiate different attacks such as changing electronic medical records (EMR) of patients by using such credentials.

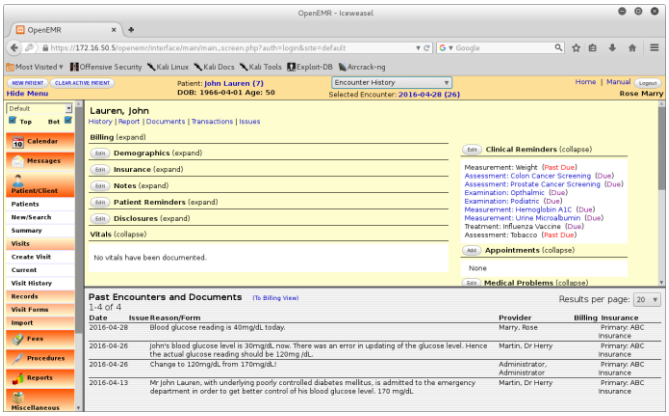


Figure 7.35: Attacker Compromises Patient Data by Using Captured Legitimate Login Credentials of a Nurse

In this fictitious case scenario, the attacker amends the blood glucose level of John Lauren (changed to 120mgl/dL to 40mg/dL) by using the captured legitimate login credentials of a nurse (Name: Rose Mary; login username: nurse007) from a MITM attack on a WMedSys that uses WPA2-Enterprise (Figure 7.35).

7.8 THE IMPROVED ARTEFACT

One of the significant challenges in the healthcare industry is how to maintain the safety of every patient. Patient safety is a fundamental element that drives constant enhancements in delivering the quality healthcare to patients (Hunt, 2002) and can be referred to as "freedom from accidental injury while receiving healthcare services" (Barach, 2002, p. 43). According to the research conducted in

United Kingdom, America and Australia, it is suggested that 10% of patients admitted to hospital experiences an adverse event although “at least half of those adverse events are thought to be preventable” (Hunt, 2012, p. 4). The consequences of those adverse events lead to the patient deaths in 8% of the cases. Hence, it is very important to ensure the safety of patents, especially in the area of healthcare where wireless technologies are deployed. The nature of wireless is more susceptible to threats and malicious attacks than its wired counterpart. Thus, the healthcare information systems like WMedSys should be securely designed to improve the safety of patients.

Similarly, the aim of advancement in patient safety can be accomplished by changing organisational culture of national health systems (Emslie, 2012). Consequently, one of the American healthcare organisations once states that: “We live in a culture that manages error by looking for people to blame; that silences admission of errors; and that focuses on the ‘sharp end’ (i.e. the clinician) instead of working at to improve the systems we have created. We must foster responsible reporting and focus on the ‘blunt end’ (i.e. the system) to build more error-proof systems. Our organisation faces the challenge of permanently changing our culture to embrace the new paradigm” (Kaiser Permanente, 2002 cited in Emslie, 2002, p. 9).

In other words, the frontline healthcare professionals such as clinicians or doctors cannot be blamed if a severe adverse event or incident happens. In fact, the hospital management has responsibility to improve healthcare systems for the safety of patients (Emslie, 2002). Therefore, in order to design a secure WMedSys for the safety of patients, it is critical to understand the capabilities and problems of stakeholders involved in creating trust and eliminating weaknesses within WMedDs, and to prevent locations where breaches of security can feasibly occur within WMedSys (Kobes, 2014). In Figure 7.36, the learning and innovations from the Pilot Study and Scenario tests are implemented to improve the artefact from Figure 6.15. These innovations, reorganisation, and improvements are itemised and reported in Chapter 8.

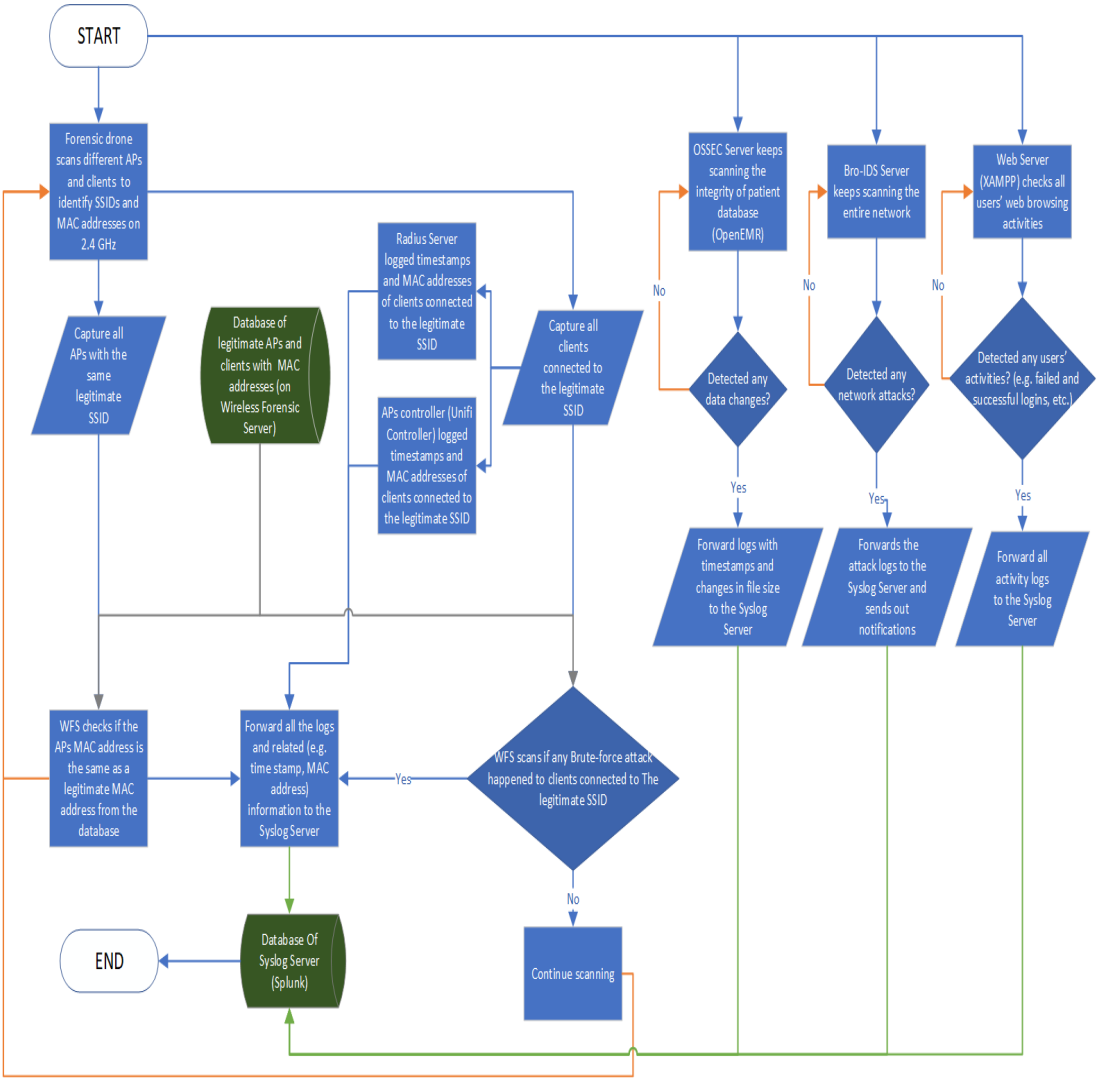


Figure 7.36: Improved Digital forensic readiness framework for WMedSys

7.7 CONCLUSION

Chapter 7 has reported the findings from the Pilot Study to crack a WMedSys and to confirm the vulnerabilities identified in the literature. It has also specified the actual hardware and software used in the testbed and the tools. The scenario test has provided data for improvement of the previous artefact (Figure 6.15) and the result is presented in Figure 7.36. Chapter 8 will now explain the improved artefact, submit it to expert feedback for further improvement, and answer the research questions.

Chapter Eight

EXPERT FEEDBACK EVALUATION, ANALYSIS OF FINDINGS AND ANSWERS TO RESEARCH QUESTIONS

8.0 INTRODUCTION

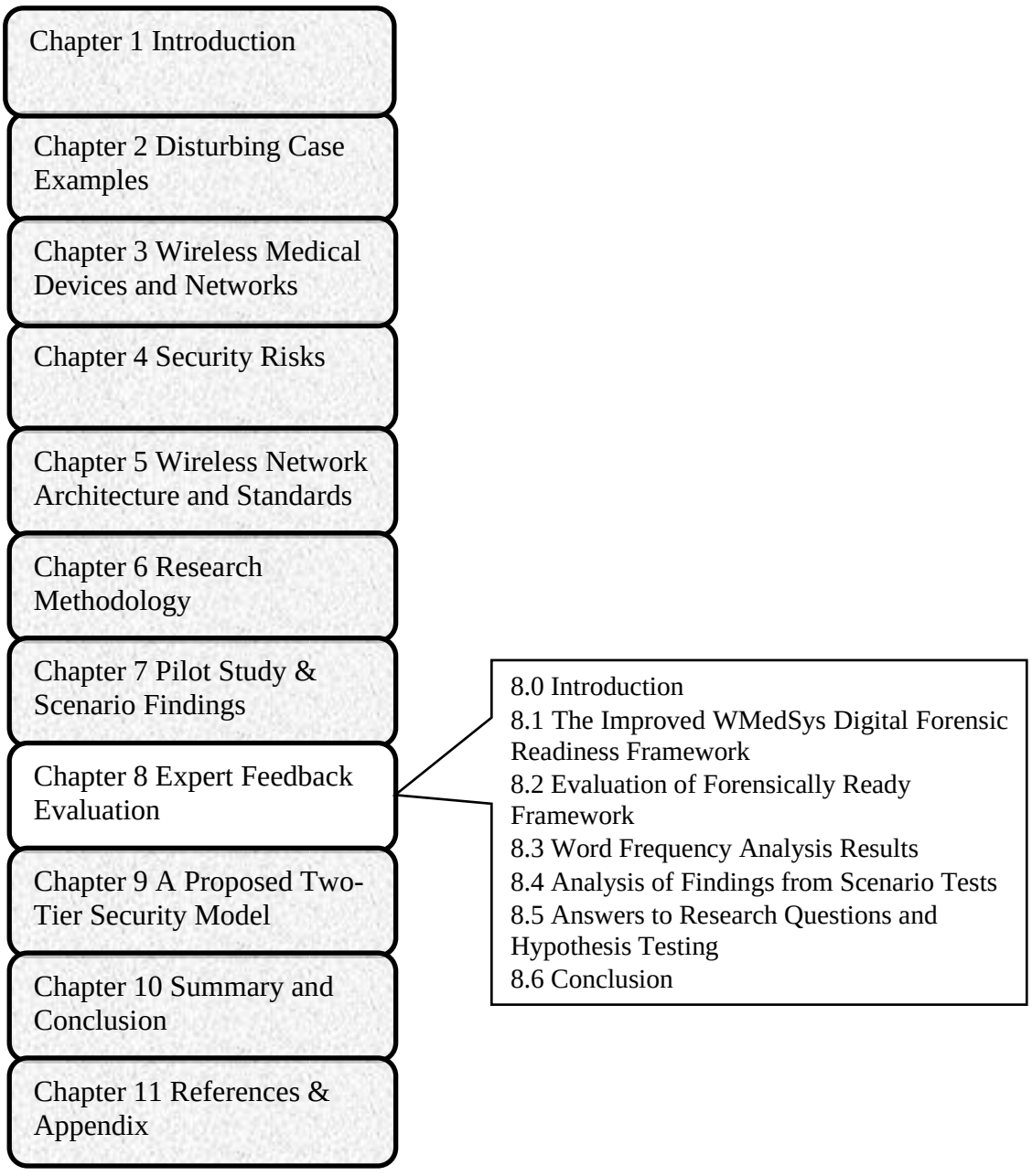


Figure 8.1: Roadmap of Chapter 8

The improved framework for digital forensic readiness for WMedSys shown in Figure 7.36 will now be explained and submitted to experts in industry. The feedback will inform further improvement and also the ability to test the research

hypotheses and questions. Section 8.1 summarises the work to date, and then has eight sub-sections that each provide specification of the improved elements for Figure 6.15. Section 8.2 briefly adds to the information presented in Chapter 6 for doing the expert feedback by providing the reasons the participants are considered expert for this evaluation. Section 8.3 presents the analysis of expert feedback, and Section 8.4 and Section answers the research questions based on the accumulated evidence from each research process. Then, Section 8.5 concludes this chapter.

8.1 THE IMPROVED WMedSys DIGITAL FORENSIC READINESS FRAMEWORK

The improved WMedSys digital forensic readiness Framework (artefact for WMedSys (Figure 8.2) is composed of many co-ordinated components: Pi-drone, Wireless Forensic Server (WFserver), Remote Authentication Dial-In User Service (RADIUS) Server, Wireless Access Point (WAP) Controller, Integrity Checking/Hashing Server (OSSEC), Intrusion Detection/Prevention System (Bro-IDS) Server, Web Server (XAMPP), and a centralised Syslog Server (Splunk).

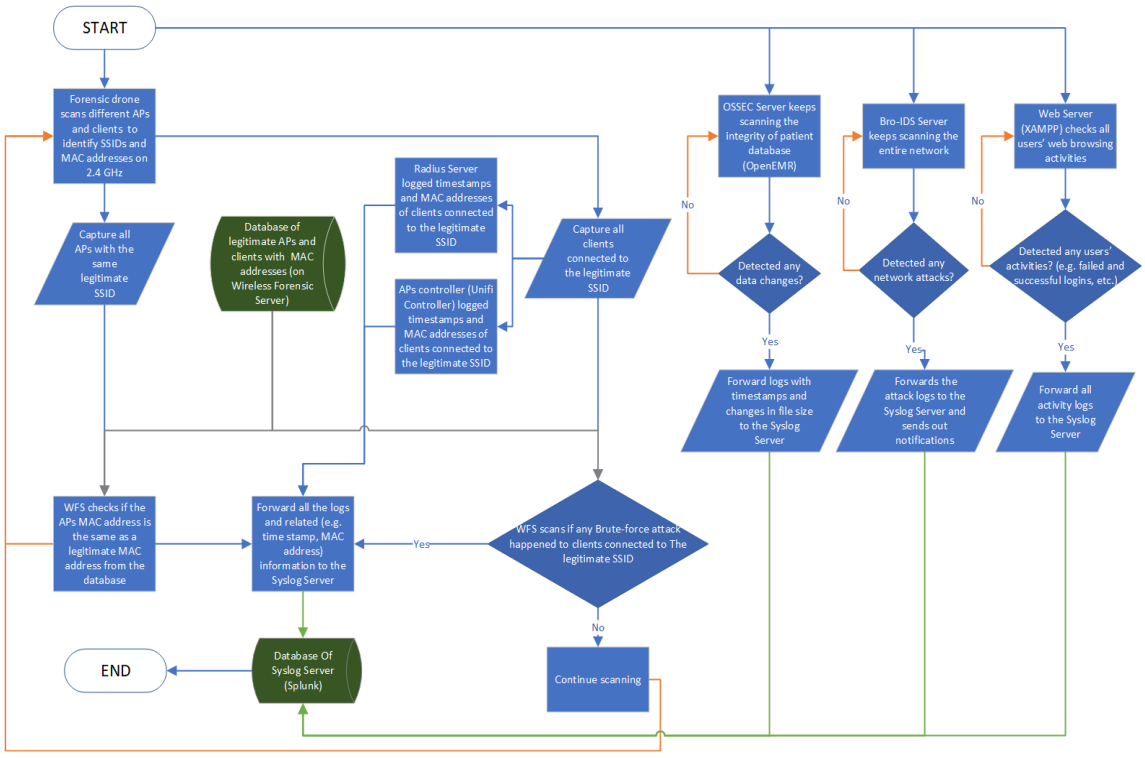


Figure 8.2: Digital forensic readiness framework for WMedSys

The following sub-sections will now explain each of the improved elements.

8.1.1 Pi-drone

The Pi-drone uses the Kali Linux ARM software version to act as a forensic wireless drone. Kali Linux is a Debian-based Linux distribution which contains many tools designed for penetrating testing and security audit (Kali, 2019). A TP-link Wi-Fi USB was connected to the Raspberry Pi to scan the Wi-Fi signal on 2.4GHz. Pi-drone also utilises the Kismet application which can sense any wireless network device detector, sniffer, wardriving tool, and WIDS (wireless intrusion detection) framework (Kismetwireless, 2019). By using Kismet in drone mode, Pi-drone can scan and capture the wireless signals coming from any Wi-Fi devices. Then all the information collected is sent to a Wireless Forensic Server for analysis.

8.1.2 Wireless Forensic Server

The Wireless Forensic Server (WFserver) uses a Kali Linux operating system and runs the Kismet application as a wireless intrusion detection system (WIDS) server. The Kismet server receives, categorises and analyses the information sent by the Pi-drones. The server lists the wireless access points (APs) based on the service set identifiers (SSIDs) and their associated Media Access Control (MAC) addresses. Moreover, it also presents all the client MAC addresses connected to the same SSID (Kismetwireless, 2019). The WFS server hosts a database which stores all the legitimate APs and clients' MAC addresses. The server will then forward all the logs with content information (e.g. timestamps, clients' MAC address, and brute force attack timestamps). WFS can identify different brute force attacks on the wireless client as soon as it detects the attacks. In addition, the source code of Kismet can be modified to add new capabilities to detect different wireless attacks. Then, all the information is forwarded to the Syslog server for further investigation.

8.1.3 Remote Authentication Dial-In User Service

The Remote Authentication Dial-In User Service (RADIUS) Server is central to authentication. The main purpose of the RADIUS server is to provide the authentication service for a user's network connection requests and return

appropriate configuration information, accordingly (Cisco, 2006). By using a Microsoft Windows Server 2008R2 for the RADIUS server, the RADIUS controls devices and user's authentication based on the username and password stored on the Domain Controller server. In this proposed DFR Framework, all the information and logs (including username, timestamp, client MAC address) of the RADIUS server are forwarded to the Syslog server as soon as a wireless client is successfully or unsuccessfully connected to the legitimate AP.

8.1.4 Access point controller

The Access point controller (Unifi controller) controls and monitors all applications. A Microsoft Windows Server 2008R2 hosts the UniFi Controller software. This software controls and monitors all the Unifi APs on the network and decides the SSID on each APs based on different VLANs. It also monitors clients connected to each APs and SSIDs (Unifi, 2018). In the forensically ready Framework, the server forwards all the logs (e.g. the AP MAC address a client connects to, timestamp, and client MAC address) to the Syslog server.

8.1.5 Integrity Checking/Hashing (OSSEC) Server

OSSEC is a widely used as a scalable open-source application for Host-based Intrusion Detection System (HIDS), which can run on different operating system platforms. It provides extensive features such as file integrity checking, Windows registry monitoring, rootkit detection, real-time alerting and active response (OSSEC, 2019). The security requirements can be tailored through configuration options and the customised rules can be added. For example, OSSEC scripts can be written to perform actions responding to security alerts. In addition, the source code of OSSEC can be modified to add new capabilities. In the forensically ready Framework, OSSEC is used to check the integrity of the patient's database (that is specific to where that database is located, e.g. OpenEMR runs on the server with IP address of 172.16.50.5). Any change in patient-related data will be logged. Those logs comprise of timestamps, hash values, and changes in file sizes. Then, all information is configured and forwarded to the Syslog server.

8.1.6 IDS Server (Bro-IDS)

The IDS server (Bro-IDS) runs Bro-IDS on top of Ubuntu OS. Bro-IDS is a passive, open-source network traffic analyser. Its primary function is to provide security monitoring and inspection of all traffic for signs of suspicious activity. Furthermore, it supports various traffic analysis tasks including performance measurements and helping with trouble-shooting (Zeek, 2019). In the forensically ready Framework, the Bro-IDS continually scans the entire network to identify any attacks on the network such as Distributed Denial-of-Service (DDoS) attacks, and a network scanner. All the information collected by the server is forwarded to the Syslog server.

8.1.7 Web Server (XAMPP)

The Web server (XAMPP) is a compilation of free software (comparable to a Linux distribution) (Apachefriends, 2019). XAMPP provides a web server platform which allows the hosting of any website or web services at low cost. This server hosts OpenEMR which provides patient related electronic medical records (OpenEMR, 2018), and provides a platform for users to use a different function from OpenEMR. In the forensically ready Framework, all the users' activities (e.g. user success and failure logins, setting changes, and timestamps) are logged by XAMPP and then forwarded to the Syslog server.

8.1.8 Syslog Server (Splunk)

The Syslog server (Splunk) is a commercial software which is designed to collect and analysed data from different devices, and the software on the network system (Splunk, 2019). The Splunk server runs on a Windows Server 2008R2 and in the forensically ready Framework, this server will collect all the logs and information from different components of the framework. The server allows the forensic investigator to select a specific timestamps and create a report including detailed information from all servers in the network. It also supports search functions to help the forensic investigator to search for specific information.

8.2 EVALUATION OF FORENSICALLY READY FRAMEWORK

Based on the planning of Chapter 6 for expert feedback evaluation criteria, the 18 questions and the improved artefact were submitted to all the experts for a response and advice. In order to thoroughly evaluate the proposed artefact, the following five experts from related fields with exclusive knowledge and work experience were selected and requested to conduct the evaluation of the proposed artefact against the suggested evaluation criteria (see Chapter 6).

- Expert 1 has specialised in the areas of Health Information Technology (HIT), Wireless Networks, Internet of Things (IoT), and Software Defined Networks (SDN) for more than 25 years. He was a researcher and the head of the management section of Ministry of Science and Technology, Iraq. Currently, he is a senior academic staff member of an Institute of Technology in New Zealand as well as being a certified instructor of Cisco Networking Academy for 14 years.
- Expert 2 has been a senior field service engineer for GE Healthcare and Siemens Private Limited (Pte. Ltd) specialising in medical equipment including X-Ray systems, Digital Mammography, Digital Angiography, computed tomography (CT) and Magnetic resonance imaging (MRI) systems for more than 19 years in the Healthcare Industry.
- Expert 3 has extensive knowledge and work experience as a digital forensic investigator and a researcher of more than 7 years. He has also been a lecturer in Information Security, Risk Management, Microsoft Windows Servers based Networks at both graduate and post-graduate level for more than 4 years. Moreover, Expert 3 has published and presented several research papers closely related to the new emerging research areas in Digital Forensics and Network Security at international high rank conferences and journals.
- Expert 4 has more than seven years experience as a Digital Forensic Analyst in the IT Industry. He has worked on hundreds of investigations looking for electronic evidence on a wide range of devices including computers, mobile devices, global positioning system (GPS) units, and other storage devices. For the last two years, Expert 4 has worked as a Penetration Tester, working on a number of security reviews, including

web application reviews, mobile application testing and hardware reviews of embedded devices. He has also written a Master's thesis on forensic data collection of Apple iPhones and recently presented publications on a number of undisclosed vulnerabilities found in modern routers.

- Expert 5 specialises in wireless networks and security, cloud computing, network architectures and protocols and SDN. He is an assistant professor and also a reviewer for many prestige international journals and conferences. Expert 5 used to work as a head of telecommunications and computer networks group for a university.

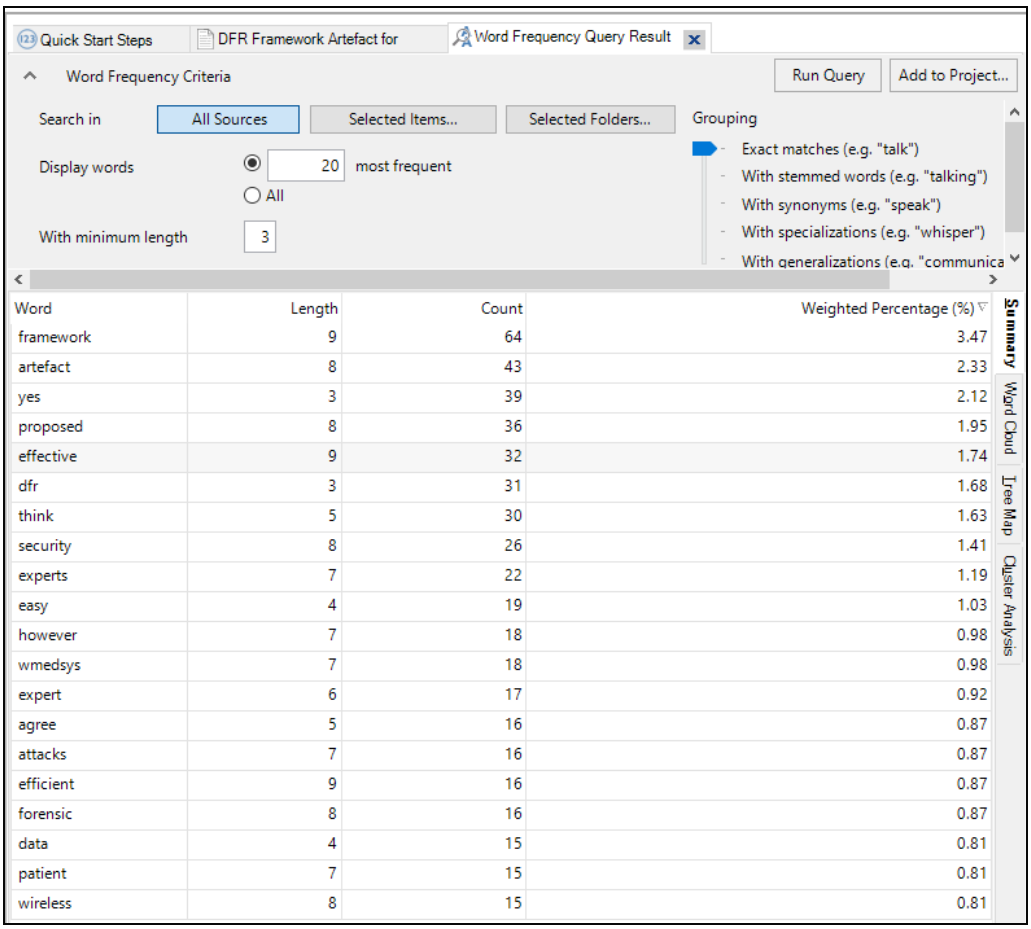
The evaluated artefact is further analysed using a thematic approach with NVIVO software. Thematic analysis is commonly used approach in conducting qualitative data analysis in DS research. Qualitative methodologies aim to explore complex phenomena (Vaismoradi, Turunen, & Bondas, 2013). They accept multiple realities and have a commitment to identifying an approach to in-depth understanding of the phenomena, a commitment to participants' viewpoints, conducting inquiries with the minimum disruption to the natural context of the phenomenon, and reporting findings in a literary style rich in participant commentaries. Thematic analysis is a process for encoding qualitative information (Boyatzis, 1998). This type of analysis looks mainly at "*what and how*" the data has and aims at identifying patterns within the data.

The feedback received from expert evaluations, was analysed for a central theme and word consistencies. The central theme was then categorised into three areas for further analysis against the evaluation criteria in the three system dimensions, which are "Goal", "Environment" and "Structure/Activity". "Goal" is to analyse whether or not the forensically ready framework has achieved its design goal. "Environment" is to analyse whether or not the framework has been consistent with an organisation and its people. "Structure/Activity" is to analyse the artefact's dynamic operations and its functionalities. Each of these three areas is divided into smaller areas of prospect for in-depth analysis. For example, "Goal" is divided into two smaller areas of prospects of "Efficacy" and "Validity". "Environment" is divided into two smaller areas of prospects of "Consistency with organisation" and "Consistency with people". "Consistency with people" is

then classified into “Utility”, “Understandability” and “Ease of use”. “Activity” is divided to “Completeness”.

8.3 WORD FREQUENCY ANALYSIS RESULTS

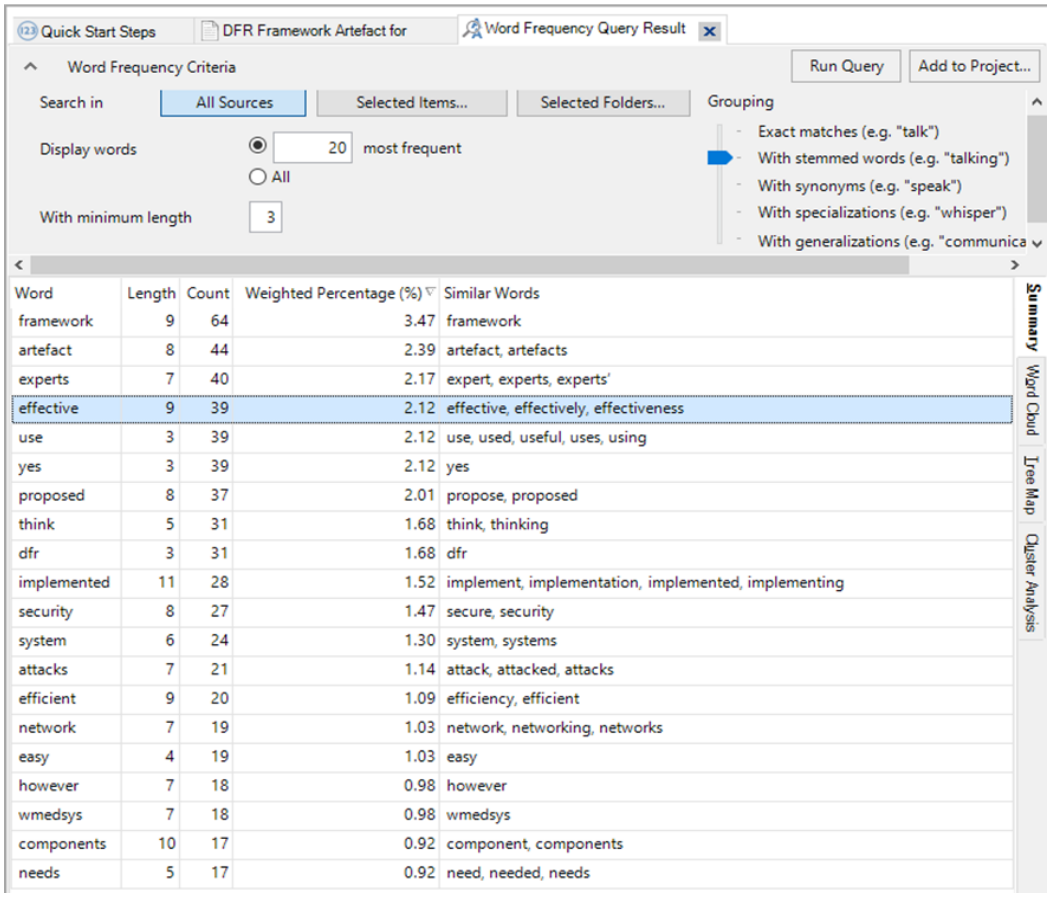
Word frequency queries in NVIVO provides researchers with a list of the most frequently occurring words or concepts of referenced material.



Word	Length	Count	Weighted Percentage (%)
framework	9	64	3.47
artefact	8	43	2.33
yes	3	39	2.12
proposed	8	36	1.95
effective	9	32	1.74
dfr	3	31	1.68
think	5	30	1.63
security	8	26	1.41
experts	7	22	1.19
easy	4	19	1.03
however	7	18	0.98
wmedsys	7	18	0.98
expert	6	17	0.92
agree	5	16	0.87
attacks	7	16	0.87
efficient	9	16	0.87
forensic	8	16	0.87
data	4	15	0.81
patient	7	15	0.81
wireless	8	15	0.81

Figure 8.3: Top 20 most frequent exact word matches

This can help the researcher in not only identifying possible themes, particularly in the early stages of the project; but also finding the most frequent words occurring in a particular referenced material. In qualitative research this repetition is important for identifying key concepts and common understandings. Figures 8.3 and 8.4 show the top 20 most frequent stemmed word matches and exact word matches.



Word	Length	Count	Weighted Percentage (%)	Similar Words
framework	9	64	3.47	framework
artefact	8	44	2.39	artefact, artefacts
experts	7	40	2.17	expert, experts, experts'
effective	9	39	2.12	effective, effectively, effectiveness
use	3	39	2.12	use, used, useful, uses, using
yes	3	39	2.12	yes
proposed	8	37	2.01	propose, proposed
think	5	31	1.68	think, thinking
dfr	3	31	1.68	dfr
implemented	11	28	1.52	implement, implementation, implemented, implementing
security	8	27	1.47	secure, security
system	6	24	1.30	system, systems
attacks	7	21	1.14	attack, attacked, attacks
efficient	9	20	1.09	efficiency, efficient
network	7	19	1.03	network, networking, networks
easy	4	19	1.03	easy
however	7	18	0.98	however
wmedsys	7	18	0.98	wmedsys
components	10	17	0.92	component, components
needs	5	17	0.92	need, needed, needs

Figure 8.4: Top 20 most frequent stemmed word matches

Comparison is made after running both features to provide more in-depth and broad analysis. Noticeably, “effective” is in the fourth place on the stemmed word match table, up from the fifth place on the exact word match table. Also, “implemented” has gone up. This is consistent with overall expert comments that emphasise implementation potential of the artefact. Moreover, “use/useful”, “efficient/efficiency” and “easy” are also on the top of the table. Thus, analysis shows that experts agree that the proposed forensically ready framework is “effective”, “efficient”, “useful” and “easy” to implement and utilise.

After conducting the “word frequency query”, a “text search query” is used to understand the meaning of these most frequently appearing words in the content. This can provide the researcher with better understanding of the implication and interpretation of these words in context and with a more meaningful context for reasoning. Based on the results provided from “word frequency query” and evaluation criteria in Section 3, the following words are used, which are “effective”, “efficient”, “useful”, “strength”, “weakness”, “easy”, “security”, “safety” and “evidence” showed in Figures 8.5 to 8.13.

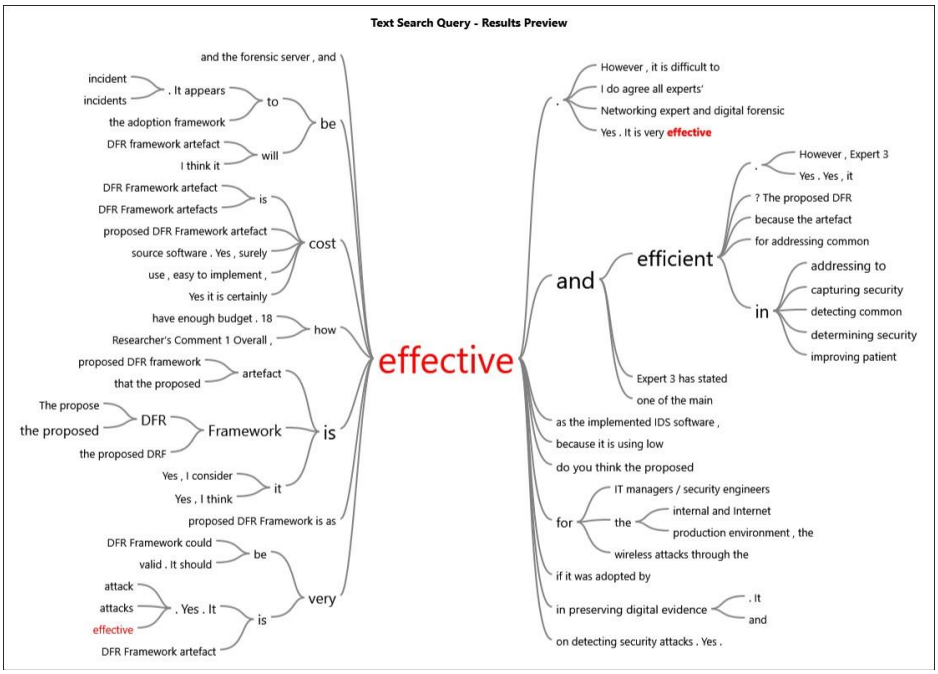


Figure 8.5: Text search query result for "effective"

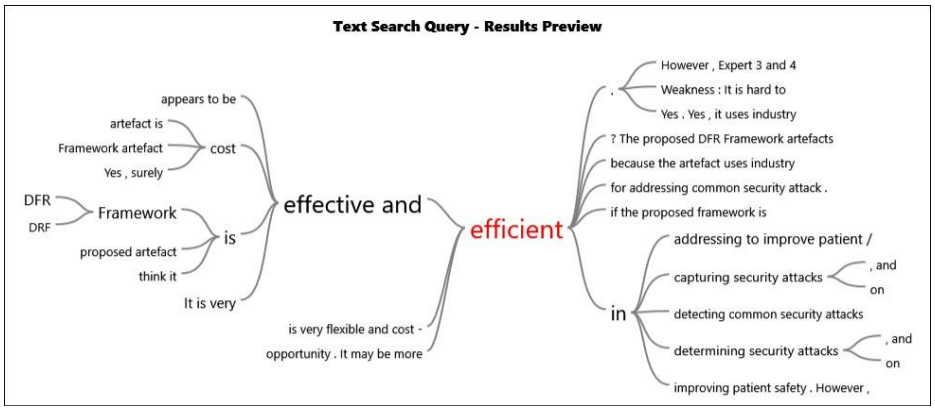


Figure 8.6: Text search query result for "efficient"

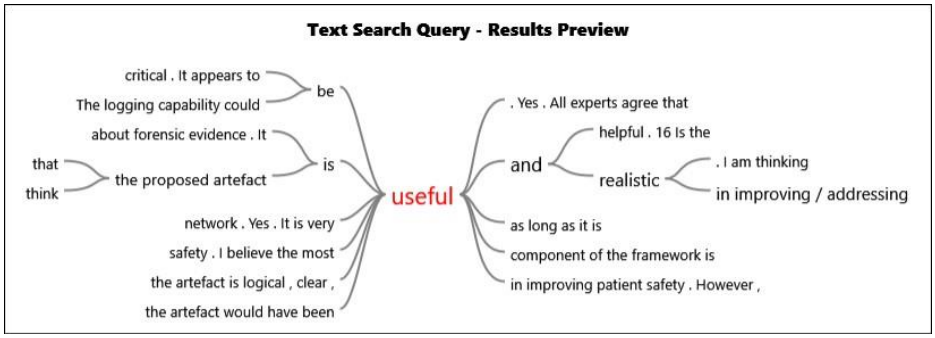


Figure 8.7: Text search query result for "useful"

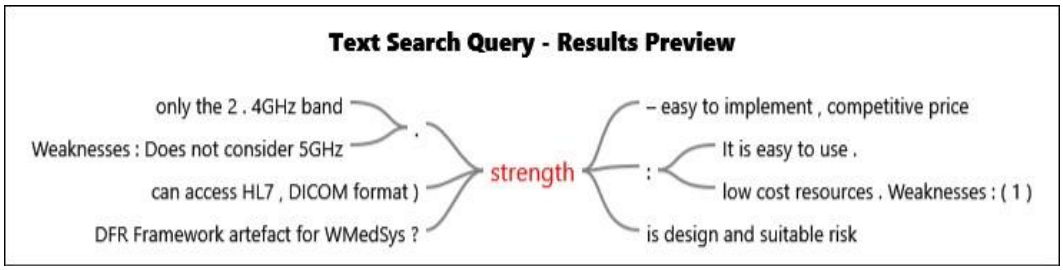


Figure 8.8: Text search query result for "strength"

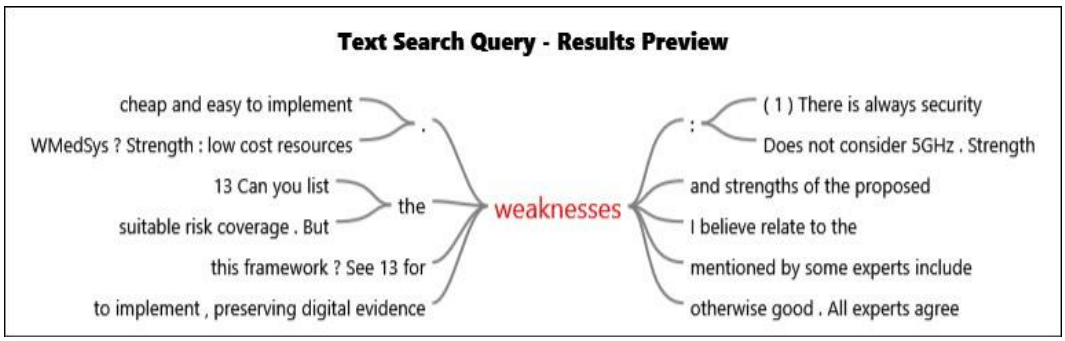


Figure 8.9: Text search query result for "weakness"

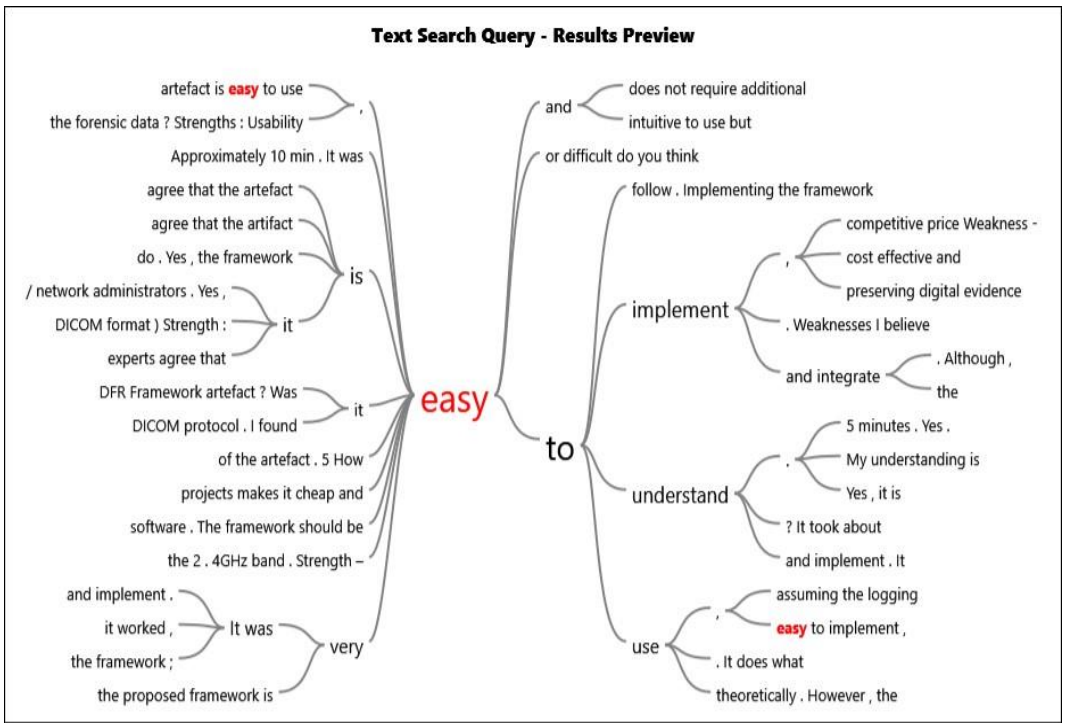


Figure 8.10: Text search query result for "easy"

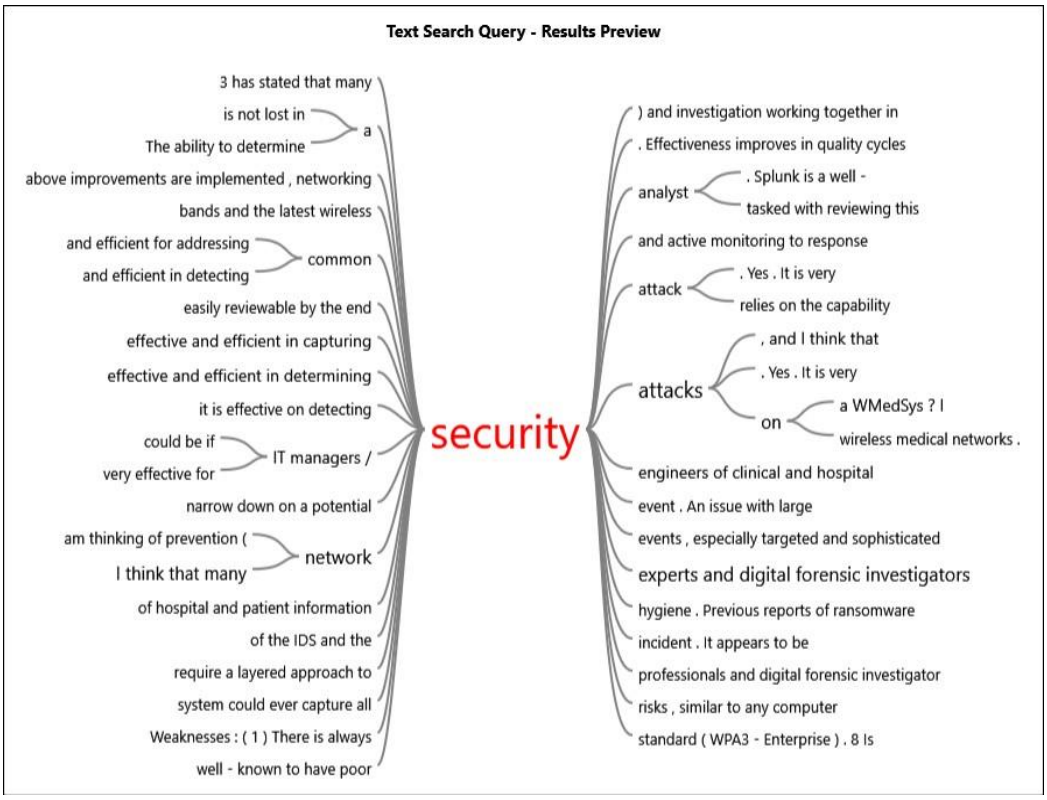


Figure 8.11: Text search query result for "security"

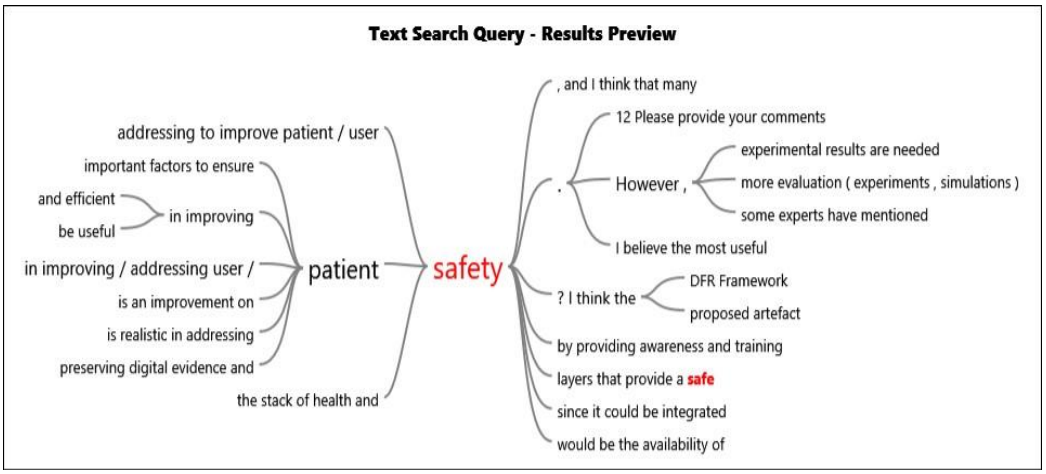


Figure 8.12: Text search query result for "safety"

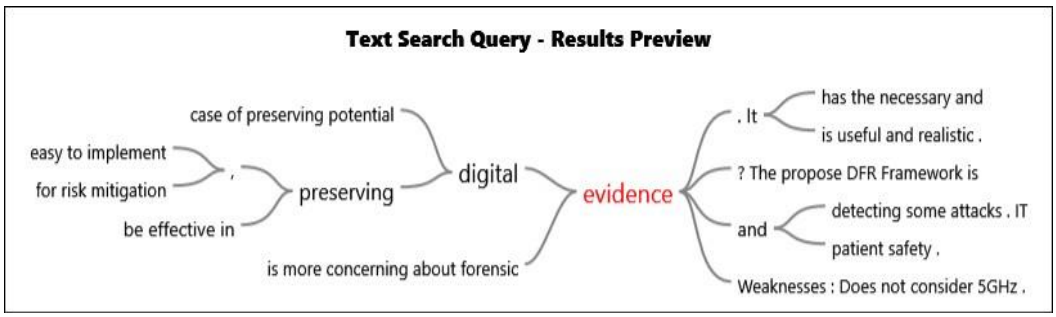


Figure 8.13: Text search query result for "evidence"

Since the goal of this research is to design and develop a cost-effective forensically ready framework for WMedSys, hence “effective” and “efficient” are essential characteristics to evaluate whether or not such a goal has been achieved. The analysis shows that most of the expert feedback provides evidence for adoption of the current state of the design. Thus, the artefact is considered as “effective” and “efficient” in preserving digital “evidence”. Consequently, the goal of the design has been achieved, and is now ready for further iterations of development in adoption. In addition, the artefact is considered as “useful” and realistic in improving and addressing patient “safety” and overall medical system “security” in a clinical or healthcare environment against attacks. Thus, patient safety is protected and assured to a greater level than at present.

However, due to all experts have different levels of expertise, the time taken to follow all components of proposed DFR Framework artefact is different (Expert-3 took 2 to 3 minutes, while Expert-2 took 2 hours) although all experts agree the proposed artefact is believed to be easy to implement, understand and use. Moreover, the “strength” and “weakness” analysis show that the proposed framework is designed and suitable for security risk coverage, has several benefits in “easy” implementation, “easy” to use, low cost resources, competitive price for “easy” implementation and use. It can also access HL7 and DICOM formats. However, the proposed framework does not consider 5GHz and residual risk management. Otherwise, all experts agree the proposed framework is good in preserving digital evidence and better than current provisions. All experts recommend integrating the forensic readiness framework into existing networks to test the proof the concept.

8.4 ANALYSIS OF FINDING FROM SCENARIO TESTS

This sub-section presents the analysis of findings from scenario tests or experiments. To proof the theoretical concept of the proposed Digital Forensic Readiness Framework for WMedSys, the scenario tests on a typical WMedSys as an experimental test-bed that utilises WPA2-PSK and WPA2-Enterprise with various attacks by using freely available off-the-shelf tools were carried out in a controlled laboratory. Then, the fictitious case scenarios which were based on previously well-cited articles (Li et al., 2014; Halperin et al., 2014; Radcliffe,

2012; Li et al., 2011) were used to collect the experimental data. After performing various attacks, all components of the compromised WMedSys were interrogated to find DE related to various attacks.

Hence, during the analysis phase, DE were found were found in the logs of the attacker's personal computer, DHCP server, UniFi Controller, RADIUS, WFserver, OpenEMR, XAMPP, Bro-IDS, OSSEC, Centralised Syslog (Splunk Enterprise) and SolarWinds server. These findings from scenario tests are presented in Appendix F.

8.5 ANSWERS TO RESEARCH QUESTIONS AND HYPOTHESIS TESTING

Based on the evidence presented in Chapter 7 and Chapter 8 (see the relevant Appendix E and Appendix F also) the research hypotheses can be tested, and sub-questions can be answered. The main research question can also be answered based on these findings. The following sub-sections present a summary of results in tabulated form.

8.5.1 Hypothesis Tests

Hypothesis 1 (H_1): There will be potential Digital Evidence (DE) in the memory of medical or end-user devices (examples: PDA or remote control of the insulin pump or server logs) of a compromised WMedSys.	
For	**Against**
In the Pilot Study and Scenario Tests, potential DE were found in all places such as the attacker's personal computer, DHCP server, UniFi Controller, RADIUS, WFserver, OpenEMR, XAMPP, Bro-IDS, OSSEC, Centralised Syslog (Splunk Enterprise) and SolarWinds server. See findings in Appendix E and Appendix F.	There is no evidence.
Conclusion: Accepted	

Hypothesis 2 (H_2): There will be potential DE that can be found in intermediary devices (such as wireless access point, switches, and so on) of a compromised WMedSys.

For	**Against**
Evidence was found UniFi Controller and WFserver (as the Pi-drone forwarded the evidence of illegitimate association to WAP in WMedSys). See the analysis of findings in Appendix E, and Appendix F.	There is no evidence.
Conclusion: Accepted	

Hypothesis 3 (H_3): There will be improved retention of DE when a Forensic Server (FS) is in the WMedSys.

For	**Against**
This was observed during the scenario tests and also commented on in the expert feedback. See Chapter 8 (Section 8.4) and Appendix F.	There is no evidence.
Conclusion: Accepted	

Hypothesis 4 (H_4): There will be potential DE that can be found in other network locations (examples: IDS, system logs, transaction logs and database of the backend database server) of a compromised WMedSys.

For	**Against**
Yes, the potential DE was found in Bro-IDS, server and OpenEMR logs. See Appendix E and Appendix F.	There is no evidence.
Conclusion: Accepted	

Hypothesis 5 (H_5): There will be improvement of investigator efficiency when forensically ready designs are implemented.	
For	**Against**
The industry experts provided feedback. They commented on the efficiency and speed of investigation, which was not possible before (Appendix D). See also Chapter 8 and Appendix E and Appendix F.	There is no evidence.
Conclusion: Accepted	

Hypothesis 6 (H_6): User safety can be improved by adding forensic capability in the security design of WMedDs and WMedSys in order to mitigate risks and to preserve DE for post event analysis.	
For	**Against**
The industry experts commented that all of these benefits are now possible. See Chapter 8, Appendix D, Appendix E and Appendix F.	There is no evidence.
Conclusion: Accepted	

8.5.2 Research Sub-Questions

Sub-Question 1: What are the potential risks (security and privacy) of current WMedDs and WMedSys?	
For	**Against**
All of the evidence from the literature suggests that WMedSys have significant security vulnerabilities. In the pilot study, the vulnerabilities were shown to be real. See Chapter 7, Appendix E and Appendix F.	Several writers suggested countermeasures, but none of the countermeasures were 100 percent effective.
Conclusion: There are many potential risks that have been identified.	

Sub-Question 2: What are current protection mechanisms to mitigate security attacks related to a WMedSys?	
For	**Against**
Currently, they have IDS and firewall as main line of defences. They also use usernames and passwords for domain logins, and they also use RADIUS server for authentication.	None of these security mechanisms are 100 percent assured because of limited bandwidth and weak encryption in WMedSys.
Conclusion: These security mechanisms are listed in Chapters 2, 3 and 4.	

Sub-Question 3: What are feasible protection mechanisms to improve the design of WMedDs to mitigate security attacks related to a WMedSys?	
For	**Against**
More processing power and memory space for these WMedDs will be helpful. Also the addition of forensic capabilities for post-event investigation.	There is only weak encryption that needs to be improved.
Conclusion: Due to the limited resources, only light-weight encryption will be helpful for these WMedDs.	

Sub-Question 4: What are the hardware and software required for the successful acquisition of DE from a WMedSys?	
For	**Against**
See Appendix C, where all of these are itemised and costed. Also see Figure 10.2 where a low-cost solution is provided.	Current systems are too expensive and ineffective.
Conclusion: The provided low-cost solution includes the required hardware and software. The expert feedback also suggests it is ready for real environments.	

8.5.3 The Research Question

"**What can be improved to make digital forensic investigation more effective in a wireless medical system (WMedSys)?**"	
For	**Against**
One of the most important aspects is to get ready. A forensically ready system has to be integrated into the current WMedSys. With the proposed system (see Figure 10.2), evidence can be found in all the different elements of the system (see Appendix E and Appendix F).	If there are no security and forensic preparation, then the whole system is compromised, and the patients are open to harm and adverse events.
Conclusion: A cost effective digital forensically ready system can reduce some of the security risks in current systems. See Figure 10.2.	

8.6 CONCLUSION

The main contribution of this research is to present a novel conceptual design for a forensically ready framework for WMedSys, which can be easily implemented and integrated into the existing wireless networks in the healthcare sector. Thematic expert evaluation analysis shows that the proposed artefact is efficient and effective in providing better security for patient safety. The proposed artefact uses Pi-drones to collect any user's successful and unsuccessful wireless login attempts to WMedSys and forwards them to a centralised logging system in order to preserve digital forensic evidence. In addition, it has low resource requirements, is cost-effective and has customisation benefits by adapting free open-source software (See Appendix C financial analysis). Hence, it is suitable for security risk coverage. Nevertheless, it also has several limitations. Although experts believe that proposed framework is only designed for the WMedSys in 2.4 GHz band, the proposed framework can easily be adopted to both 2.4 GHz and 5GHz by replacing the hardware of the Pi-drone. As future work, experts suggest that the prototype framework be implemented and tested in a real environment to further evaluate the design and the performance. Chapter 9 now critically reflects on these findings in terms of the primary concern of this Thesis – patient safety.

Chapter Nine

A PROPOSED TWO-TIER SECURITY MODEL FOR PATIENT SAFETY

9.0 INTRODUCTION

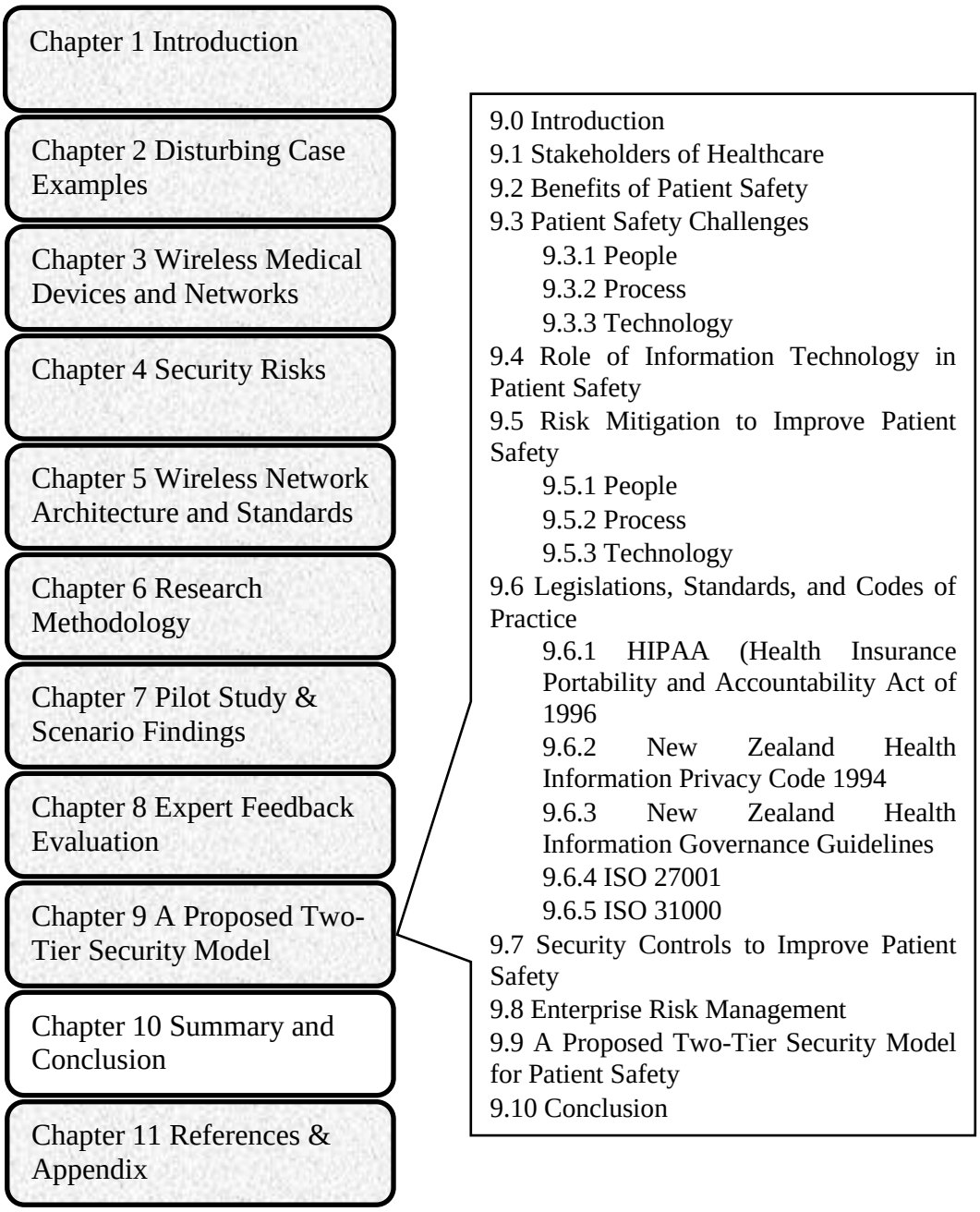


Figure 9.1: Roadmap of Chapter 9

Chapter 9 draws together the purpose and motivation of the research, and the empirical findings, and looks directly at the core issue of Patient safety. This chapter satisfies the requirement to answer the sub-question that concerned patient safety and well-being. Patient safety is a health care principle that aims to enforce

the absence of an accidental injury as a result from a medical error (Fortune, Davis, Hansin, & Phillips, 2013). It consists of the prevention and treatment of unnecessary injuries to patients. The awareness on the concept of patient safety started when the Institute of Medicine (IOM) published their report in 1999 called To Err is Human: Building a Safer Health System (Rozovsky & Woods, 2005). Nowadays, it is becoming one of the highest priorities in the health care industry. This is because statistics show that many patients experience adverse events (AE) which are possibly preventable during their hospitalisation (Tedesco, Hernandez-Boussard, Carretta, Rucci, Rolli, Di Denia, McDonald, & Fantini, 2016). There have been several studies that support this statement. In a Canadian study in 2004, 36.9% of AE were preventable (Popovici, Morita, Doran, Lapinsky, Morra, Shier, Wu, & Cafazzo, 2015). In the United States, 58% of AE were found to be preventable, 14% of which led to the death of the patient (Fortune et al., 2013). Aside from affecting a patient's health, medical errors can also be costly. In 1999, it is estimated that medical errors in the United States cost $38 billion per year, $17 billion of which is related to preventable medical errors (Chenot, 2007). Medical errors can be attributed to many factors, including lack of appropriate technologies and tools, as well as human factors such as long work shifts of medical staff, and a person's medical knowledge and skills. Because of these preventable medical errors, patients who experience adverse events lose their trust in the health care organisation. A study in Europe showed that Europeans over 15 years old are much more inclined to believe that they can be harmed in health care in 2013 that in 2009 (Filippidis, Mian, & Millett, 2016).

The value of the research completed is to heighten awareness of the vulnerabilities in WMedSys that can have serious consequences for Patient safety. An effective mitigation system has also been designed and costed. These contributions add to the discussion of safety issues and the management of prevention strategies. The solutions require a two tier approach. The technologies and the technology risk require full evaluation. Then the people aspects that include policies, standards, guidelines, training, and so on have to be factored into a comprehensive mitigation plan. Together a two tier model has the best chance of minimising points of failure while maximising the opportunities for safe patient care.

Several institutions have been formulating guidelines to improve patient safety. The Canadian Patient Safety Institute introduced six core competencies that health care professionals can incorporate in their tasks and activities: i.) contribute to the patient safety culture, ii.) collaborate with other medical teams, iii.) effective communication, iv.) management of safety risks, v.) optimization of human and environmental factors affecting patient safety, and vi.) identification, response, and disclosure of adverse events (Hwang, 2015). In 2004, Hamilton Health Sciences (HHS) developed the cornerstones of patient safety which include collaboration of different teams and disciplines, continuous education and development, effective communication, and defined measurements of improvement (Zimmerman, Christoffersen, Shaver, & Smith, 2006).

9.1 STAKEHOLDERS OF HEALTHCARE

Healthcare is a huge and complex industry and has several stakeholders. The stakeholders related to healthcare systems may include the clinical staff (such as physician, doctors and nurses), care givers, patients, medical device manufactures, medical device software developers, information technology (IT) department, management of hospitals or healthcare providers and government regulators. The most significant are the patients as they are the ones who receive care services from health care organisations and personnel. Patients also receive the most significant impact of medical errors since their health is at stake.

Medical staff provide the health services to patients. They have the responsibility to make decisions regarding the medication and health of a patient (Rozovsky & Woods, 2005). Aside from doctors and surgeons, nurses are also important in health care as they are the initial care providers that interact with the patients (Hwang, 2015). Medical staff also maintain the patient's medical information.

On an organisational level, the management of the health care organisation is also an influential stakeholder. Governing bodies and senior management define the goals of the organisation, and ensure that these goals are met (Chenot, 2007). They are also the ones who approve an organisation's budget allocation. Therefore, costly initiatives which aim to promote patient safety will have to be approved by the management. On the other hand, costs incurred from medical

errors and adverse events are also reviewed by the organisation's governing bodies (Filippidis et al., 2016).

Information Technology (IT) has an increasing role in the health care industry as new advances in technology are being developed and used. Medical records and information are now stored in information systems and accessed using computers. Aside from ensuring that these systems are functioning correctly, software developers should implement security measures in order to prevent security attacks (Sametinger, Rozenblit, Lysecky, & Ott, 2015). The IT department of the health care organisation should also be able to properly maintain these systems and ensure the security and availability of the medical information.

Medical devices are also widely used in the health care industry. Manufacturers of these devices should be able to ensure the quality of the devices since even minor errors can cause harmful and fatal results to the patients. If an issue regarding a medical device is identified, the manufacturer should be informed and should find a remedy for the problem, either by modifying the design of the device, repairing, or replacing the device (Rozovsky & Woods, 2005).

9.2 BENEFITS OF PATIENT SAFETY

Observing patient safety will greatly benefit a patient's health and condition. By following standard procedures and continuously monitoring patients, adverse events can be minimised. Unnecessary medical errors and deaths can be avoided. The patient's recovery process can also be sped up (Khan & Pathan, 2013). This will increase the patient's trust in the health care organisation.

9.3 PATIENT SAFETY CHALLENGES

There are many factors that can impact patient safety such as defining policies and processes, technological infrastructure and tools, and collaboration of different medical departments. Each factor has its corresponding challenges in promoting patient safety.

9.3.1 People

Ensuring patient safety can have many challenges in health care organisations. One of the main causes of AE is poor communication (Popovici et al., 2015). This can be critical during handovers such as changes in medical staff shifts and patient transfers. Incorrect transfer of information may result to diagnostic errors or preventable procedures. A study showed that 43% of surgical errors that occur in operating rooms (ORs) are due to poor communication between different medical personnel (van Beuzekom, Boer, Akerboom, & Hudson, 2012). Aside from human error, poor communication can be caused by lack of appropriate and intuitive tools and unstandardised communication processes. Different definition of concepts and inconsistent language may also be contributing to the problem as there is still a lack of standardised taxonomies across various medical fields (McElroy, Woods, Yanes, Skaro, Daud, Curtis, Wymore, Holl, Abecassis, & Ladner, 2016). In order to address this challenge, the World Health Organisation (WHO) World Alliance for Patient Safety developed the International Classification for Patient Safety (ICPS) which is a framework of standardised medical concepts and terms.

Human factors such as behaviours and systems that can impact a person's performance can also affect patient safety (Fortune et al., 2013). These can be attributed to a person's cognitive and social skills. If any of these factors are substandard, it can pose a challenge to patient safety. The person's working environment may also be a factor, such as poor working conditions, lack of training, and insufficient staffing. In hospitals in the United States, understaffing of nurses is ranked as one of the most significant threats to patient safety (van Beuzekom et al., 2012).

9.3.2 Process

Another challenge is to ensure that the organisation's efforts towards patient safety meet all levels by having different areas and departments take accountability (Zimmerman et al., 2006). One reason is because physicians and other health care staff can have busy schedules and their engagement in collaborative meetings and discussions are less prioritised. For low to middle-income countries in the Eastern Mediterranean Region, more focus is given to

building infrastructures that encourage patient safety such as laboratories (Saleh, Alameddine, Mourad, & Natafgi, 2015). The development of these facilities to encourage a patient safety culture will cost an organisation a significant amount. Health care organisations will require expenditure in order to fund new facilities, purchase new technologies, and develop modern patient-care programs (Youngberg, 2010). Therefore, these initiatives will require the approval of senior management, which can be quite difficult (Ford & Savage, 2008). The success of the implementation of these initiatives will be dependent on the commitment and support of the management.

One of the ways to encourage patient safety is to report adverse events and share the information to other departments and health care organisations. This is to promote collaboration and to learn from others' experiences. However, this can be a challenge due to legal requirements to keep patient data confidential (Rozovsky & Woods, 2005). Medical information is sensitive, and patients usually like to keep their information private. Apart from data privacy concerns, health care organisations and staff also fear that reporting medical errors and adverse events can damage their reputation. It can be perceived as admitting to a liability that results in blaming a physician or medical staff and implementing disciplinary and corrective actions (Rozovsky & Woods, 2005).

9.3.3 Technology

Different information systems are being used by medical departments to manage the huge volumes of information available. Since the vast amounts of data come from multiple resources, one challenge is the lack of data standards. These can become an obstacle in sharing information between different health care facilities, laboratories, and even pharmacies (Aspden, Corrigan, Wolcott, & Erickson, 2003). This is critical in health care as different medical departments need to collaborate when caring for a patient. At the minimum, a health organisation must ensure that its data types and terminologies are standardised, and that the way that data is transmitted from one system to another is clearly defined (Aspden et al., 2003).

Medical devices and systems can also be susceptible to security attacks. The data that is stored and transmitted can be compromised if perpetrators are able to launch a successful attack. Manufacturers of medical devices have not considered the dangers of cyber security attacks in their design, making these

devices vulnerable to cyber criminals (Williams & Woodward, 2015). Due to the small size and limited capacity of these devices, traditional security measures such as antivirus software or intrusion detection tools cannot be used. Despite these challenges, it is critical that medical devices and systems used in health care organisations ensure data confidentiality and integrity (Khan & Pathan, 2013). In order to protect the patient's data privacy, communication over different channels should be encrypted and privacy policies should be in place to prevent unauthorised access to the data. Since devices and systems in health care can be critical in the patient safety, availability should also be ensured. Unfortunately, medical devices have limited resources and adequate security measures may not be implemented. The wireless communication channel of medical devices is either not encrypted, or only uses the weak encryption of a static key (Zheng, Zhang, Yang, Valli, Shankaran, & Orgun, 2017).

Implantable Medical Devices (IMDs) such as defibrillators and pacemakers can save lives of many patients, but these can also pose risks to patient safety. Since these devices are inside a patient's body, even minor errors of the device can result to severe consequences such as loss of consciousness, and even death (Peters & Peters, 2007). For example, sutures used to close a surgery wound can carry infectious organisms, staples can leave scars, and defibrillators can short circuit, failing to deliver the intended shock to the heart. In 2006, almost 50,000 defibrillators and pacemakers were recalled by one manufacturer, with more than 50% of the devices already implanted to the patients (Peters & Peters, 2007). Biofilms which become habitats for different bacteria can also form at the surface of the medical devices. These biofilms inhibit the diffusion of antibiotics, which can eventually lead to more complications. Medical devices can also contain toxic materials such as polyvinyl chloride (PVC) which is a known carcinogen. Despite the health risk advisory issued by the Food and Drug Administration (FDA), PVC is still being used in some medical devices (Peters & Peters, 2007). Unfortunately, testing medical devices in humans can also be a challenge. Getting human-oriented test data is limited before the devices are implanted to patients.

The software of medical systems and devices may also introduce risks to patient safety. According to a study based on the FDA Recalls database, software

failures caused 64.3% of computer-related recalls from 2006 to 2011 (Alemzadeh, Raman, Kalbarczyk, & Iyer, 2013). Some examples of software failures of medical systems include unexpected system lockups and inaccurate data, or images displayed. Software failures can also have a more direct impact to patient safety, such unstoppable x-ray exposure and unrecognizable instruments that are critical to surgeries. In terms of medical devices, these have been more vulnerable to malware in the recent years due to increased interconnectivity (Sametinger et al., 2015). If the compromised device sends incorrect values to the server, the physician may prescribe erroneous treatments or device configurations that may be harmful to the patient. Unfortunately, it can be a challenge to embed security controls in medical devices due to constraints such as limited data storage and battery power.

9.4 ROLE OF INFORMATION TECHNOLOGY IN PATIENT SAFETY

With the increasing use of wireless technology and various digital devices, there is an opportunity for IT to improve communication and access to information in hospitals. According to a survey conducted on Japanese hospitals, those with excellent IT infrastructure provided a better quality of health care (Sasaki, Okumura, Yamaguchi, & Imanaka, 2016). The availability of a WLAN (Wireless Local Area Network) and accessibility of medical databases and libraries can significantly help medical staff in obtaining the latest medical information and research.

There is a lot of information used in the medical field such as patient profile and history, and information regarding medications and procedures. Information systems are used in order to store and manage these data. A study in 2016 reviewed the process of implementing an electronic medical records (EMR) system that could be used in patient mediation reconciliation (Hsu, Wang, Chen, & Hsiao, 2016). The use of EMR can reduce the instances of added or duplicated medications given to the patients.

IT is also used in the process of research and development of patient safety in organisations, as well as for feedback and reporting. For example, a web-based safety debriefing tool can be used to collect comments and concerns regarding patient safety (McElroy et al., 2016). This allows collaboration among medical

staff and provides an avenue to raise and concerns in order to improve patient care processes. Incident reporting (IR) systems are also used in many health care organisations to promote accountability and encourage a culture of patient safety (Flott, Darzi, & Mayer, 2016).

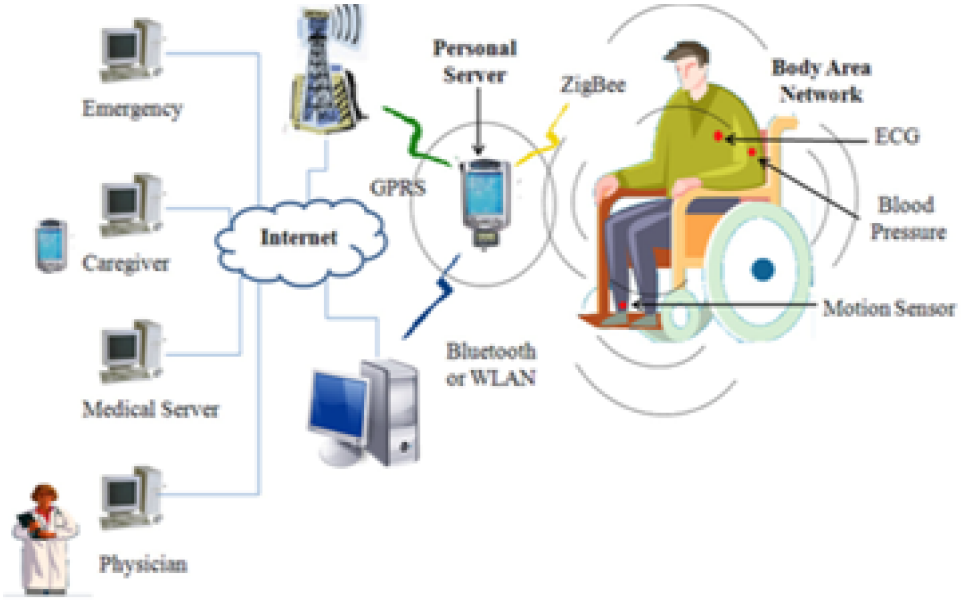


Figure 9.2: Application of WBAN (Khan & Pathan, 2013, p. 166)

Another use of IT in the improving patient safety is to use Business Intelligence (BI) in order to assist in making informed decisions (Foshay & Kuziemsky, 2014). BI can be beneficial to organisations since decisions made regarding health care and patient safety require the analysis of large amounts of useful data. Medical devices such as Wireless Body Area Sensor Networks (WBANs) are widely used to monitor the state and activities of the body (Figure 9.2). The United States purchases the most medical devices with a market sale of $148 billion and is expected to reach $185.9 billion by 2019 (Rathore, Mohamed, Al-Ali, Du, & Guizani, 2017).

WBANs can be used to monitor a person's vital signs and send the data to a Personal Server (PS) and into a medical application or a database (Khan & Pathan, 2013). This can support real time diagnosis, as well as sending an emergency alert. It can be a wearable device or an IMD. There is a wide range of IMDs that patients use, such as neuro-stimulators, gastric stimulators, insulin delivery systems, and defibrillators (Rathore et al., 2017). Figure 9.2 illustrates a sample application of a WBAN. Some medical devices can also automatically

release medication into the patient's body, which makes it more convenient for patients since their daily activities are not interrupted. Compared to traditional health care systems, medical devices are more cost effective, as it allows patients to be released from the hospital at an earlier time.

9.5 RISK MITIGATION TO IMPROVE PATIENT SAFETY

There are many risks involved in striving to improve patient safety. These risks can be classified into different domains, such as operational, financial, strategic, legal, human, and technology risks (Youngberg, 2010). Risks can come from tasks or activities, systems and processes. Some risks can exist even if controls are already implemented. Below are some mitigations that health care organisations implement in order to minimise risk. However, it should be noted that risks are always present and that having zero risks is not achievable (Youngberg, 2010).

9.5.1 People

The Security Rule of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 mandates that health care organisations have a person responsible for the security of electronic protected health information (e-PHI). The designated security officer should perform risk analysis to identify possible security risks as well as coordinate with other departments for risk management (Krager & Krager, 2016). The cost of different security measures is compared to the possible losses if a security breach happens and security controls are not in place. These controls may be administrative, physical, organisational, operational, or technical security measures.

Training of the staff is also important. The patient safety taxonomy standard used should be learned by the staff in order to better understand reports and information used by the organisation (Rozovsky & Woods, 2005). Aside from having knowledge regarding their medical practice, staff should also know how to protect crucial medical information. For example, staff should know about computer virus protection as well as how to report any suspected security breach (Krager & Krager, 2016).

Although patient safety is mostly influenced by the governing boards of health care organisations, it is important to note that cultivating patient safety should start during a medical personnel's education. The IOM states that health

professionals, particularly nurses, are not prepared to provide high quality care to patients (Chenot, 2007). Medical schools and education leaders should improve their curriculum and integrate patient safety in their framework.

9.5.2 Process

With the increased awareness in patient safety, health care organisations have been more proactive with their risk management process. According to Sandars and Cook (2007), most preventable adverse events are caused by the failure of the organisational systems and not of individual health care staff. Based on a study in 2006 regarding the risks in the UK general practice, majority of the risks are related to keeping the confidentiality, closely followed by prescribing medication and health and safety legislations (Sandars & Cook, 2007).

Therefore, the clinical risk management process is being implemented to improve patient safety. The main steps in this process are i.) identification of the risk, ii.) analysis of the risk, iii.) risk control, iv.) risk costing, v.) recording of the findings and action items, and vi.) monitoring and review of the risk assessment (Sandars & Cook, 2007).

Another approach to mitigate patient safety risks is to be more proactive. The proactive framework tries to identify and reduce the impact of risks before an incident happens by involving staff members and asking them to give feedback on a broad spectrum of aspects of the health system such as staffing, communication, and procedures (van Beuzekom et al., 2012). It focuses on the overall processes instead of taking reactive actions when a medical error occurs and blaming certain individuals. This approach encourages collaboration and makes it easier to develop patient safety culture in an organisation. One way to be more proactive and identify risk areas is to consistently file incident reports to report adverse events (Rozovsky & Woods, 2005). The information in the incident reports can be analysed in order to determine problem areas that need attention. It is important that the information is objective and should only contain facts. Aside from procedures in filing incident reports, health care organisations should also define measures for preserving the patient's medical information.

Health organisations are also aiming to improve and standardise the processes within different departments by implementing principles such as Six

Sigma (Ford & Savage, 2008). By standardizing different processes, the operations of the organisation become more efficient and the staff are following certain guidelines and best practices on how to do tasks. An example of this is adopting a standard report when doing patient handovers, such as using the START (Situation, Therapies, Anticipated course, Reconciliation, and Transfer) format (Ford & Savage, 2008). This ensures that the medical staff taking responsibility of the patient is provided with enough information and reduce the chances of making medical errors. Standard processes are also important in operating rooms. According to a study, 50% of adverse events happen in ORs (van Beuzekom et al., 2012). By standardizing OR processes, medical staff can focus on the surgery and the safety of the patient.

Organisations can also implement Enterprise Risk Management (ERM). ERM is an enterprise-wide process which involves the processes of risk identification, analysis, and prioritization, as well as implementation of risk mitigation activities (Youngberg, 2010). It is part of the organisation's strategic planning which requires the support and commitment of the senior management and executive board. In order to be successful, ERM programs need a champion that can push for the development, implementation, and evaluation these programs since these can take several years to implement. Since ERM is a broad initiative, it also focuses on collaboration between multiple cross-functional teams in the organisation. Aside from helping organisations mitigate risks, ERM can also affect an organisation's culture, making people keener on regularly monitoring and reporting their activities (Youngberg, 2010).

There are also laws and regulations regarding data privacy and security. An example is the HIPAA which is followed by hospitals, doctors, and other health care organisations (Khan & Pathan, 2013). HIPAA sets standards in terms of how medical records, billing statements and patient records are documented and handled. Health care organisations should comply with the Security Ruling of HIPAA which focuses on protecting the confidentiality, integrity and availability of e-PHI (Krager & Krager, 2016). There are also acts regarding reporting adverse events to authorities. The Safe Medical Devices Act (SMDA) requires organisations and facilities to report adverse events which involves medical devices to the FDA as well as to the manufacturer (Rozovsky & Woods, 2005).

9.5.3 Technology

Information systems have been used to store and manage patient data and medical history. Since 1991, the IOM has recommended the use of EMR in order to easily

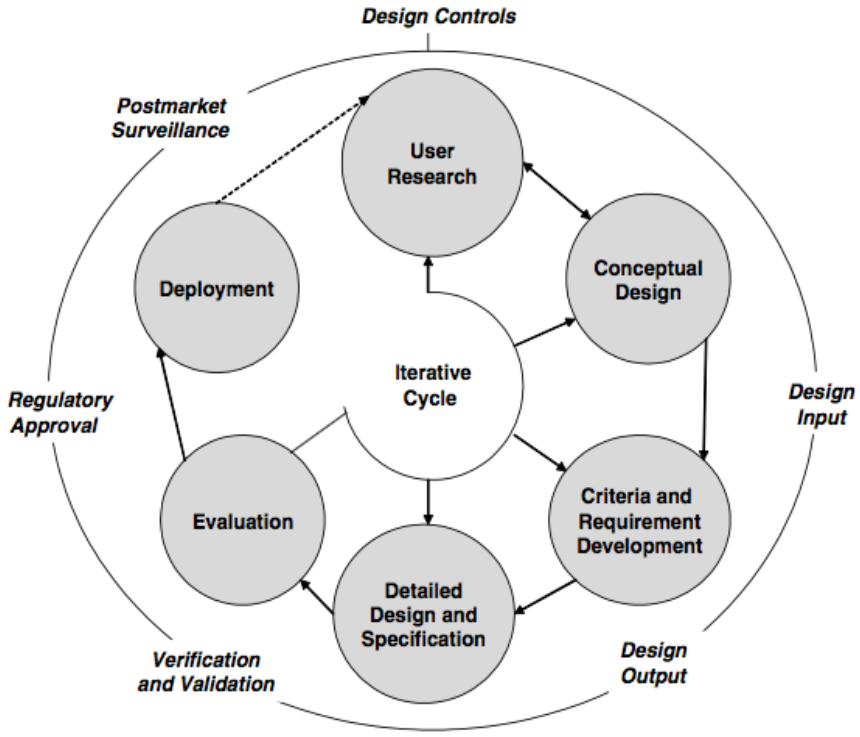


Figure 9.3 Processes in the HE74 Standard (Aspden et al., 2003, p.138)

store and access the medical data (Ford & Savage, 2008). The correctness, integrity, and completeness of the data in these systems are critical to support patient safety since these systems are used as basis for decision-making with regard to a patient's medication. The fourth Information Technology in Health Care conference examined and presented proposals to design and implement information systems in a way that would improve patient safety and reduce instances of medical errors (Aarts & Nohr, 2010).

It is important that the format of the data used is standardised. In 2003, the Consolidated Health Informatics (CHI) required federal health care services to use standard formats for messaging such as the Health Level Seven Version 2.x (HL7 V2.x) for clinical data, Logical Observation Identifiers, Names and Codes (LOINC) for laboratory results, and National Council for Prescription Drug Programs (NCPDP) for pharmacies (Aspden et al., 2003). Following these standards will support easier data collection, reporting, and reuse. Another

common standard is the RxNORM developed by the National Library of Medicine (NLM), which is a normalized form of naming clinical drugs (Aspden et al., 2003).

The security and integrity of data stored and transmitted in information systems and devices should be ensured. Security measures such as firewalls and antivirus programs should be put in place in order to prevent security attacks (Krager & Krager, 2016). Encryption can be used in order to protect the privacy of patient's medical information. The use of Message Authentication Code (MAC) can help ensure data integrity and verify that data received has not been tampered (Khan & Pathan, 2013). Access rights and data ownership should be clearly defined as well. There should be controls in place to ensure that unauthorised access is blocked. Since devices and systems in health care can be critical in the patient safety, availability should also be ensured. This can be achieved by implementing redundancy.

In terms of medical devices, human factors should be considered in the early stages of the product design (Peters & Peters, 2007). There are also standards that can be implemented when designing these devices. One is the American National Standards Institute (ANSI) / Association for the Advancement of Medical Instrumentation (AAMI) HE74 Human Factors Design Process (Aspden et al., 2003). With this process, steps and techniques are defined to analyse, design, and test systems and devices. The model in Figure 9.3 shows the iterative processes of user research, conceptual design, requirements development, design specifications, evaluation, and deployment, wherein the output of one step becomes the input for the following step. Lessons learned when solving previous problems should also be applied in future models of the devices. Analytical error reduction can be used, wherein historical and predictable errors are analysed to determine the root cause of the defects (Peters & Peters, 2007). Aside from human factors, cyber security threats and risks should also be considered in the device design. In 2014, the FDA urged medical device manufacturers to include cyber security measures in their design and plan an approach for managing vulnerabilities of their products (Zheng et al., 2017). Automation can also be implemented in manufacturing the devices. This would reduce the human errors that can happen during the assembly and testing of the device.

It is also important that medical devices and systems have audit logs to record the information's history. Logs are significant especially when an investigation of a medical error is being done. Therefore, auditing and reporting of security breaches, errors, and malfunctions to the organisation's governance team should already be part of the normal daily operations (Williams & Woodward, 2015). However, this can be challenging for IMDs due to its limited storage capacity, with 75% of its memory already used for medical functions (Rathore et al., 2017).

9.6 LEGISLATION, STANDARDS, AND CODES OF PRACTICE

During the time of this study the policy layer documentation has been continuously updated so that legislation, standards and best practice guidelines for the use of technologies in the medical environment have all been improved. In the following sub-sections a brief review of the most up to date (at the time of writing) is provided.

9.6.1 HIPAA (Health Insurance Portability and Accountability Act of 1996)

HIPAA issues mandate that doctors, medical personnel, hospitals, and other health organisations follow for handling and protecting medical information. The Privacy Rule of HIPAA provides standards for the disclosure of paper-based protected health information (PHI) (Krager & Krager, 2016). On the other hand, the Security Ruling covers e-PHI, which is PHI in electronic form. This includes text files, digital images and data stored in databases.

Security Ruling states that there should be a designated person who is responsible for the security of e-PHI. One of the security officer's responsibilities is regular checking of audit logs and reports (Krager & Krager, 2016). By reviewing these logs, it is possible to identify who accessed a medical record, what information was accessed, what was done to the data, and when it was done.
The Security Ruling also mandates that different policies should be in place for protecting medical information. This includes policies for maintaining the proper access rights of each personnel (Krager & Krager, 2016). The access rights should be changed accordingly if a staff has resigned or has changed departments. Another policy is for contingency plans, which states the procedures to be done in case of an emergency that affects the computer systems where e-PHI is stored.

Having an off-site database backup storage is one of the most common sections of a contingency plan (Krager & Krager, 2016).

Access and use of physical facilities are also discussed in the Security Ruling. Only authorised personnel should be allowed entry to facilities where computer systems are located (Krager & Krager, 2016). It is the security officer's responsibility to document this, as well as keeping an inventory of all systems containing e-PHI.

Security Ruling states that security measures should be in place, such as having firewalls and antivirus software. If the data is transmitted over the internet, the data should be encrypted.

9.6.2 New Zealand Health Information Privacy Code 1994

The New Zealand Health Information Privacy Code is a code of practice regarding how to collect and use health information as issued by the Privacy Commissioner. These may be in the form of the patient's medical history, medical test results, and medical services done. The code covers health agencies such as organisations that provide health care and services, insurers, and the Ministry of Health. The code states that a patient's health information should not be collected unless the information will be used for a lawful purpose (Slane, 1994). The health agency should collect the information directly from the concerned individual or his representative. The agency should inform the person that his information is collected, the purpose of the collecting the information, and who are the recipients of the collected information (Slane, 1994). If the concerned individual wants to view his information or to make corrections, the health agency must allow him to do so. The health agency should also ensure that measures are in place in order to protect the privacy of the information. One way of protecting health information privacy is to limit the number of people that the information will be disclosed to (Slane, 1994). Disclosure of the information should be authorised by the concerned individual of his representative as well. Once the information is no longer needed, the health agency should not keep the patient's information anymore to avoid unnecessary breaches in privacy.

9.6.3 New Zealand Health Information Governance Guidelines

The Health Information Governance Guidelines discusses practical recommendations regarding the sharing and handling of health information, especially with the increasing use of technology managing medical information. The guidelines help health organisations in New Zealand meet their responsibilities as specified by legislations such as the Health Information Privacy Code 1994 (Ministry of Health, 2017).

The guideline emphasizes on the transparency of the use of a patient's health information. The patient must be informed that his information is being used and to whom the information will be shared with (Ministry of Health, 2017). Patients should be able to access and correct their information within 20 working days after filing a request. The patient may also choose not to disclose his information. If this is the case, it should not be a hindrance in terms of receiving the treatment, unless the medical practitioner decides that the treatment is unsafe for the patient (Ministry of Health, 2017).

Health organisations should have a privacy officer who is responsible for privacy and governance issues. In line with this, defined policies and processes should be in place to ensure proper information governance (Ministry of Health, 2017). Aside from the privacy officer, staff across different departments should be knowledgeable on the policies of data sharing and privacy.

Information systems should employ role-based access control (RBAC) in order to manage access on medical information (Ministry of Health, 2017). Only authorised persons should be able to access information. Aside from implementing RBAC, physical security controls can also be used such as proximity cards and swipe cards. The information systems should also maintain an audit log which records all changes and inquiries to the health records. If the health organisation decides to store the information in a cloud environment, a risk assessment is first done prior to implementation (Ministry of Health, 2017).

9.6.4 ISO 27001

ISO2 7001 is a standard for information security which is designed to provide all kinds of organisations a model for implementing, maintaining, and monitoring an Information Security Management System (ISMS) which is a framework of

different procedures and controls involved in information risk management. (Honan, 2014). It provides best practices and standards which organisations can follow to have their ISMS certified. Aside from security policies and access controls, ISO 27001 also discusses standards for asset management, physical security, human resources security, communications management, incident management, business continuity management, information systems acquisition, and compliance (Honan, 2014). By following the ISO 27001 standard, organisations can obtain increased reliability of their security systems, as well as ensure compliance with legislation.

ISO 27001 follows the Plan, Do, Check, and Act (PDCA) model, as illustrated in Figure 10.5. In the Plan phase, the scope, objectives, and risks of the ISMS are defined. The Do phase is the implementation of the risk treatment plan. The Check phase reviews the procedures of the ISMS, and the Act phase includes the improvements identified in the previous phase in the cycle. The PDCA model ensures that the ISMS is reviewed and improved continuously (Honan, 2014).

9.6.5 ISO 31000

ISO31000 provides generic guidelines on risk management which can be adapted by any kind of organisation, regardless of industry (Cherdantseva, Burnap, Blyth, Eden, Jones, Soulsby, & Stoddart, 2016). It provides a common set of terminologies for risk management, as well as a performance criterion that organisations can follow. It states that risk management should be systematic and integral to the organisation's processes and should promote the continuous improvement of the organisation (Purdy, 2010). It follows the risk management process shown in Figure 10.6. The risk management process illustrates that communication and consultation, as well as monitoring and review should be done continuously in parallel with the rest of the phases. The process begins with identifying the goals of the organisation and the factors that might affect these objectives. The risks are identified analysed by defining the likelihood and consequences of the risks (Purdy, 2010). The risks are then evaluated by prioritising the different risks, then the selected risk treatment is tested and implemented.

Table 9.1: 20 critical controls and their effect on attack mitigation (adapted from Hardy, 2012, p. 4)

Critical Security Control	Effect on Attack Mitigation	Description
1. Inventory of Authorised and Unauthorised Devices	**Very High**	***These controls address operational conditions that are actively targeted and exploited by all threats.***
2. Inventory of Authorised and Unauthorised Software	**Very High**	
3. Secure Configurations of Hardware and Software on Laptops, Workstations and Servers	**Very High**	
4. Continuous Vulnerability Assessment and Remediation	**Very High**	
5. Malware Defenses	**High**	***These controls address known initial entry points for targeted attacks.***
6. Application Software Security	**High**	
7. Wireless Device Control	**High**	
8. Data Recovery Capability	**Moderately High to High**	
9. Security Skills Assessment and Appropriate Training to Fill Gaps	**Moderately High to High**	
10. Secure Configurations for Network Devices such as Firewalls, Routers and Switches	**Moderately High**	
11. Limitation and Control of Network Ports, Protocols and Services	**Moderately High**	
12. Controlled Use of Administrative Privileges	**Moderate to Moderately High**	***These controls reduce the attack surface, address known propagation techniques, and/or mitigate impact.***
13. Boundary Defense	**Moderate**	
14. Maintenance, Monitoring, and Analysis of Security Audit Logs	**Moderate**	
15. Controlled Access Based on the Need to Know	**Moderate**	
16. Account Monitoring and Control	**Moderate**	
17. Data Loss Prevention	**Moderately Low to Moderate**	
18. Incident Response Capability	**Moderately Low to Moderate**	
19. Secure Network Engineering	**Low**	***These controls are about optimising, validating, and/or effectively managing controls.***
20. Penetration Tests and Red Team Exercises	**Low**	

9.7 SECURITY CONTROLS TO IMPROVE PATIENT SAFETY

The main purpose of security controls is to prevent any malicious activity such as an unauthorised person is gaining access after performing reconnaissance and misuses of or manipulating target systems and devices through their vulnerabilities (Hardy, 2012). Table 9.1 presents 20 critical controls and their effect on attack mitigation.

9.8 ENTERPRISE RISK MANAGEMENT

Due to the proliferation of the Internet and cutting-edged technology, many institutions witnessed a huge use of novel technology. Meanwhile, cyber-attacks are the main risks to any organisation as these attacks can lead to serious problems for organisations, causing a huge loss (Kouns & Minoli, 2010). In order to prevent these risks, Enterprise risk management (ERM) is very important. Lechner and Gatzert (2018) claim that ERM has become increasingly popular in recent years, especially due to an increasing complexity of risks and the further development of regulatory frameworks. Obviously, ERM is beneficial to any organisation, which is proved by various studies. By conducting research on firms in different countries, Lechner and Gatzert (2018) draw a conclusion that ERM is able to increase firm value effectively. But the one drawback is that it may require higher budget. Brady (2015) primarily focused on conducting an effective risk assessment, and then on the principles of risk review. Risk assessment is that part of risk management which provides a structured process that identifies how objectives may be affected, and it analyses the risk in terms of consequences and their probabilities before deciding on whether further treatment is required. Bogodistov and Wohlgemuth (2017) propose that applying ERM is still a challenge because the potential risks are uncertain. It is this uncertainty that make it difficult to systemise these risks. Because of this, Bogodistov and Wohlgemuth (2017) believe that some factors should be taken into account, which is high likely to contribute to the risk management. On the one hand, ERM could be integrated with resource-based view, allowing the practitioners to set priorites for different risks. It is significant to set high priority for those risks which may affect the firm’s survival. On the other hand, it offers a framework to handle those uncertain risks. While structuring risks and ranking them is arguably a feasible way to

overcome the infinite number of risks, the criteria for such structuring should be rooted in the strategic considerations of the resource-based view.

Nonetheless, these cyber-attacks have threatened to these organisations. Thus, ERM has attracted more attention in recent years for the vulnerabilities in information systems which may cause a massive loss (e.g. financial and reputation, etc.) to organisations. However, in the healthcare industry, vulnerabilities in information systems (WMedSys) are likely to pose a threaten to patients' life. That is why, patient safety has been a hot topic in recent years. In many countries, there are many medical accidents caused by medical errors. Although a number of legislations and standards were enacted to avoid potential risks, most of them are abstract and general, which are designed to fit for all fields.

9.9 A PROPOSED TWO-TIER SECURITY MODEL TO IMPROVE PATIENT SAFETY

In order to improve patient safety, it is proposed that a two-tier security model can be conceptualised by integrating the proposed DFR Framework with the current ERM Framework. This proposed two-tier security model is called iCyberDFR Framework for medical information systems (WMedSys) in the healthcare industry and the low level research plan is shown in Figure 9.4.

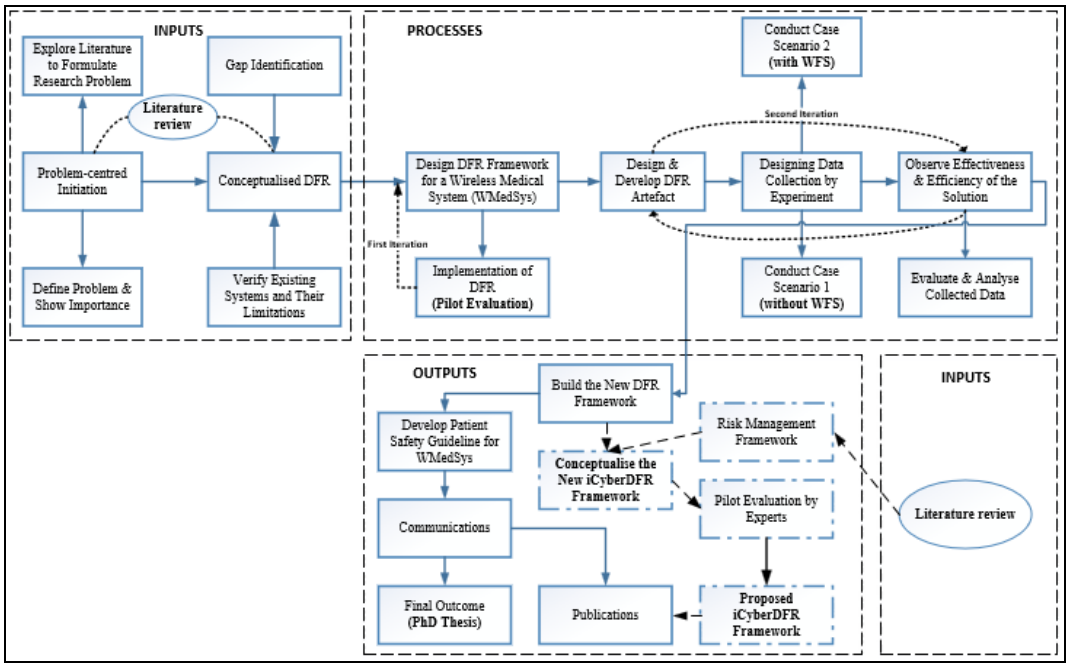


Figure 9.4: Low level research plan for a proposed iCyberDFR Framework

9.10 CONCLUSION

Chapter 9 has addressed the key issues of patient safety linking the concerns of the research questions into the practical application of this research. The balancing of positive and negative risks around IT WMedSys implementation has been weighted towards the positive benefits for services. However, this research emphasises the need to treat negative risk in order to retain the benefits of IT systems. It is helpful to review recent trends in legislation and standards writing to see that there is general public concern regarding the problem. These new and refreshed documents indicate the problem is being taken seriously and patient safety is a prioritised concern. Then, a two-tier security model is proposed to improve patient safety and it is called iCyberDFR for WMedSys. Chapter 10 now concludes the thesis by providing a summary of contributions and a list of topics for further research.

Chapter Ten

SUMMARY AND CONCLUSION

10.0 INTRODUCTION

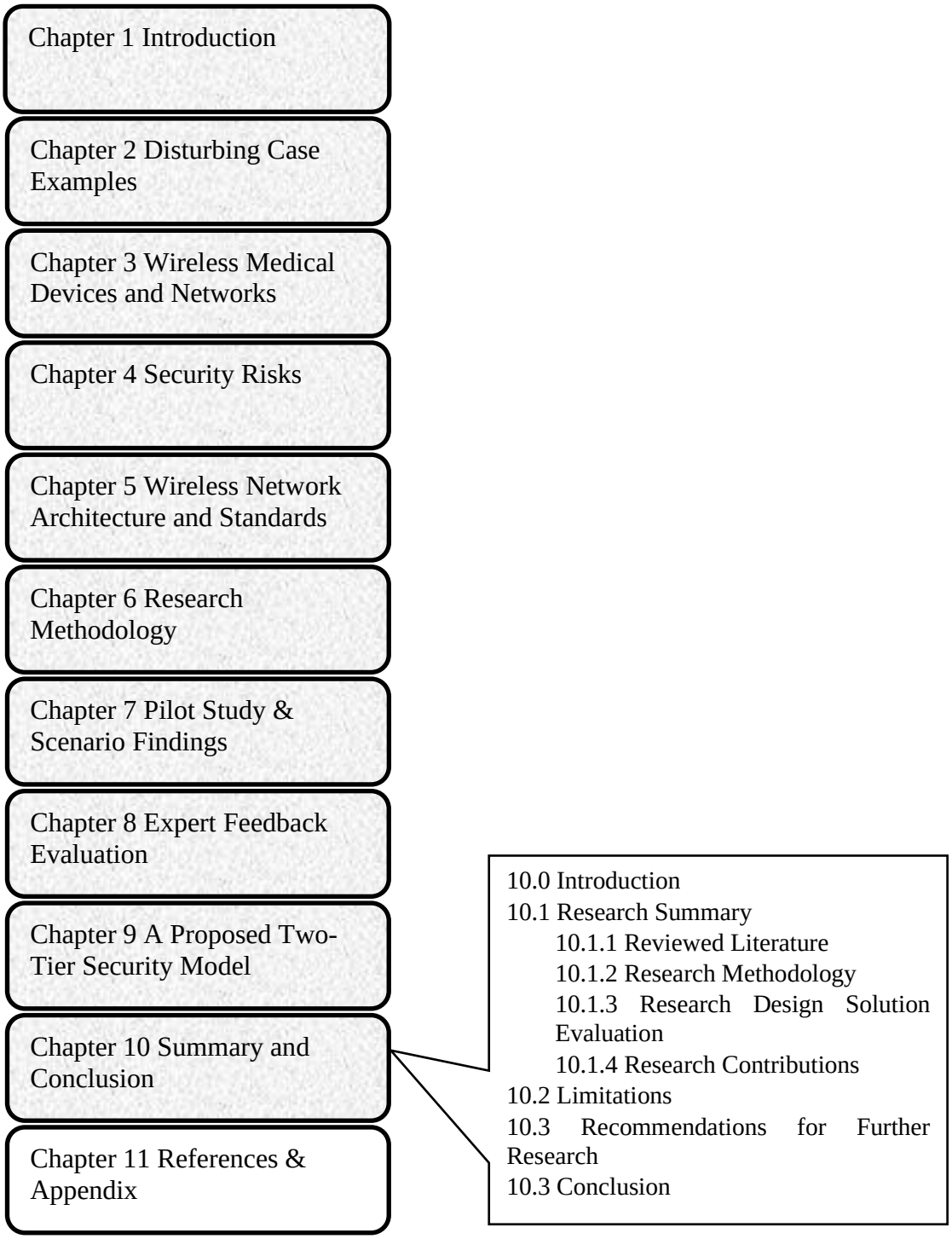


Figure 10.1: Roadmap of Chapter 10

Chapter 10 brings a conclusion to the research. The research was introduced in the Abstract and Chapter 1 as being concerned for patient safety. Chapters 2-4

established the theoretical vulnerabilities found in the technologies being used for WMedSys. Chapter 5 summarised the state of law and standards at the early time of writing that acknowledge the problem and was attempting to mitigate risks. The empirical work reported in Chapter 6 confirmed from the Pilot Study that the theoretical concerns were in real WMedSys environments. The Scenario tests took the best digitally ready design from the current literature (Figure 6.15) and subjected it to rounds of quality improvement. The practical deliverable is then a working forensically ready WMedSys module that can be inserted into current available system. It has been costed and tested in industry. This Chapter 10 is structured to review the findings and then to make recommendations for further research.

10.1 RESEARCH SUMMARY

In this research I have followed the motivation to produce a security framework that incorporates readiness for forensic investigation. The research took the lead from literature that all security provisions have the potential for failure, and hence the ability to investigate events quickly and effectively adds value to the layers of security. A forensic investigation can provide information for improving the security defences of a system, or allow the identification and prosecution of offenders. In this concluding section, summaries of the contribution of literature, the methodology, and the design solution are presented. Also the overall contribution in Figure 10.2 is reviewed.

10.1.1 Reviewed Literature

In the first and second stages of the research, a comprehensive literature review of published papers from different digital libraries and reputable journals from the past decade was conducted to give a cohesive treatment of the chosen research topic. For instance, the publications from different digital libraries such as the Institute of Electrical and Electronics Engineers (IEEE), the Association for Computing Machinery (ACM), *Springer Link, Science Direct, ProQuest Central, Digital Investigation, Google Scholar, The New England Journal of Medicine, Journal of Medical Devices: Evidence and Research, PubMed, National Institute of Standards and Technology, Cellular Telecommunications Industry Association (CTIA – The Wireless Association), ECRI Institute, Food and Drug Association –*

U.S. (FDA), and Federal Communications Commission (FCC), were searched and reviewed. Likewise, books from AUT library and Amazon website were also searched and reviewed. The searching was done by using keywords such as *WMedDs*, *Wireless Devices*, *Wireless Medical Device Security*, *Misuse Cases*, *Misuse of WMedDs and WMedSys*, *Infusion Pump*, *Pacemaker*, and so on. The literature was analysed, and the learning compounded into actions.

The result is a substantial literature contribution for the study area. The literature is referenced from Chapter 1 to 6 by critical appraisal to lift the important concepts and technical details. In Chapter 6 select research reports are also used to identify how others have approached research in this area, and to locate their network designs as starting points for the research. The Reference section documents all of these resources so that other researchers may start from a selected and focused literature in the study area. The only limitation imposed is the time dated nature of literature reviews.

10.1.2 Research Methodology

Design Science (DS) is adopted as the research methodology. DS has the benefit of managing theory and designing practical solutions to problems. It facilitates making and building solutions to problems in a way that innovation and creativity may be demonstrated. The formal processes allow artefacts to be investigated in context, and improved by design and functionality through continuous iterations and testing. In this research the characteristics of the problem area (WMedSys) shaped the testing procedures and the goals of the research. The researcher had to be flexible and to process information in order to keep the development realistic and relevant. Both innovative and confirmatory outcomes were achieved. In the research the DS research methodology was applied to a design artefact extracted from the review of related past literature. The rounds of testing included confirmation, improvement, and expert feedback. The expert feedback was particularly valuable to validate the solution that had come from theoretical constructs, and laboratory testing. The experts suggested that the last artefact was relevant and should be implemented into a live system for further evaluation.

The purpose of DS is not only to develop an artefact but also to answer the research questions and give solutions for problems. The main research question is:

“What can be improved to make digital forensic investigation more effective in a wireless medical system?” The final Figure 10.2 has the answer encapsulated in a visual communication. The implication is that if you do these things in these ways then a digital forensic investigation will be more effective in a WMedSys. In comparison to the starting point (Figure 6.5) the design has much more specific detail, more feedback loops, and a greater array of control variables. It is also costed and specified so that a person with a requirement or basic network knowledge can adopt the additional security and make use of it for improved patient safety.

My critical reflection on the methodology is simply that it works, and it allows for transition of theory into practice. The advantages advocated in the literature (see Chapter 6 DS Methodology) were apparent. The challenging part is to constantly shift in focus so that at one point the work is focused on the artefact and at another the evaluation. The evaluation leads to changes in the artefact and a new round of development and testing. The methodology is not just one thing but a set of related processes that had to be managed continuously. The processes helped to abstract from the artefact and to start to look at it objectively. As stated before, I was motivated by a desire to address safety issues and this tended to create a rush or drive to get a quick solution. The methodology slowed this momentum down so that the artefact could be matured, and multiple solutions produced. In my view patience and patient working with the DS methodology brings better results than one off attempts at solutions.

10.1.3 Research Design Solution Evaluation

The first design came from the most relevant literature reviewed in Chapter 6. The first design was shown in Figure 6.5 and then further improved by the end of the chapter through critical reflection and appraisal for the practical context. The improved design was presented in Figure 6.15. This design was used to guide the initial experimental set up. In Chapter 7 the confirmatory data from the Pilot Study showed that the theoretical claims of vulnerabilities in WMedSys were correct in practice. The scenario tests then delivered an improved design (shown in Figure 7.36) that reflected practical solutions to implementation problems. This design was then submitted to experts to gain their evaluation and suggestions for

improvement. The result of the industry feedback gives the design presented in Figure 10.2. In addition feedback from the "Communication" activities of the DS methodology have also given application and future research knowledge.

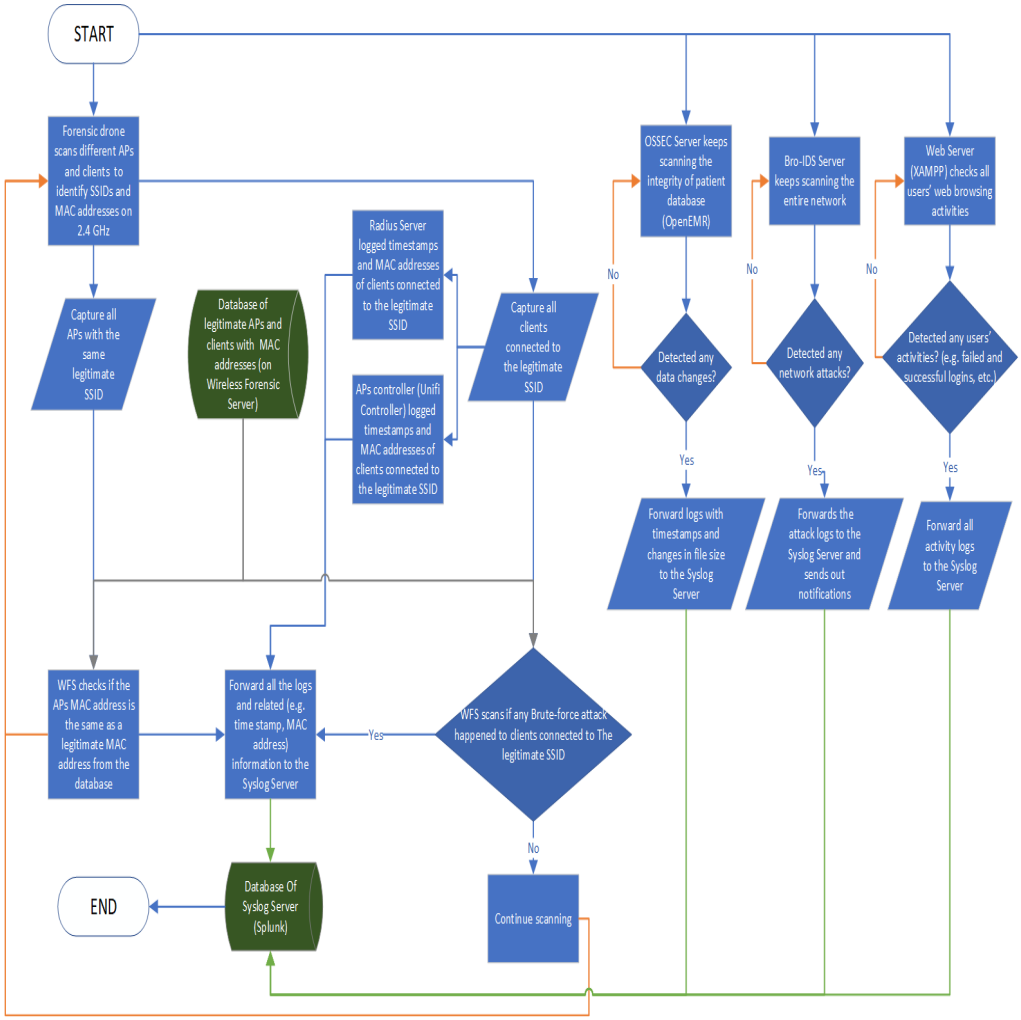


Figure 10.2: The Final Design

10.1.4 Research Contributions

The main outcomes from this Thesis are:

(i) The artefact demonstrated the proof of concept and its usefulness in DE preservation and prevention of cyber incidents from happening within an organisation

(ii) The value of the research completed is to intensify awareness of the vulnerabilities in WMedSys that can have serious consequences for patient safety.

(iii) To demonstrate the procedure (or method) for compromising a WMedSys based on WPA2-Enterprise by using freely available off-the-shelf-tools.

(iv) To heighten the security awareness about the ease of successfully compromising a WMedSys.

The other contributions from this Thesis are:

(v) A novel conceptual design of a low-cost DFR for WMedSys, which can be easily implemented and integrated to existing wireless networks in the healthcare sector.

(vi) The innovative design for digital forensic readiness provides an extra layer of protection for patients.

(vii) Providing the solution by DFR adds trust and another layer of control for the technical people responsible for maintaining security in medical environments.

(viii) An effective mitigation system has been designed and costed.

(ix) The research study forms a base platform, which could be part of risk management for improving user or patient safety.

The biggest contribution is to provide a solution. The problem of WMedSys vulnerabilities is just a fictional story on CSI or in the movies to most people, but this thesis has dispelled the myth and shown by both theory and practice that it is factual. The innovative design for forensic readiness provides an extra layer of protection for patients. Instead of people being fearful of these wireless devices the solution adds trust. It also provides another layer of control for the technical people responsible for maintaining security in medical environments. The practicality of what has been achieved and the low cost of implementation are general public benefits.

Moreover, these outcomes of the Thesis have communicated with the adequate audiences from both academic and industry in the same area and field (see List of Publications on pp. xxi-xxiii). Based on the *industry expert feedback*, they acknowledge that the outcome of this thesis is new and having a DFR system in WMedSys of any healthcare provider can fulfil not only the requirements of DE preservation, but also the prevention of a cyber incident from happening within an organisation, therefore improving patient safety.

10.2 LIMITATIONS

Most of the literature was collected in the early stages of the research and the research was designed to fill a gap in the then libraries. Continuous publishing (DS Communication) has kept the project up with current developments but there will still be more recent work by the time the Thesis is marked. One mitigating factor is that this research began when this field of WMedSys security risks was beginning to unfold. Hence, the literature has caught the wave and as a study area it is still edge cutting, but many topics have already been published to exhaustion.

Although the proposed framework is only designed for WMedSys in 2.4 GHz band, the framework can easily apply to both 2.4 GHz and 5GHz by replacing the hardware of the Pi-drone.

In the pilot and scenario tests (in Chapter 7), different attacks were carried out in very close proximity in a controlled laboratory environment. On the other hand, these attacks are feasible to perform remotely from a distant location by using a low-cost directional antenna. Similarly, a single wireless communication channel is used in the attack and multiple channels may be used by wireless clients in the real world. However, an adversary can jam non-overlapping wireless channels that are not being jammed and force the targeted wireless client to operate over the preferred channel. In addition, an adversary can apply other social engineering techniques to deceive authorised users in order to manipulate or steal recorded patient data from a WMedSys. Furthermore, the feasibility and success rate of these attacks on a WMedSys in the real world (e.g. the production network of a hospital or clinic) cannot be precisely measured as these attacks were carried on an implemented WMedSys in a controlled laboratory environment.

Another limitation is the thematic evaluation in which the proposed artefact was evaluated by the subjective method (i.e. by a group of experts) and convenience sampling method was used.

10.3 RECOMMENDATIONS FOR FURTHER RESEARCH

At the conclusion of any research project there are always things that remain untested. The scope of this research allowed the theoretical and industry testing of an artefact, but many aspects in and around the WMedSys environment require further investigation. The following points are key starters for further research:

- Assessment of Open Source solutions require testing against proprietary opportunities
- Conduct further research, the proposed Two-Tier Security Model (iCyberDFR Framework in Figure 9.4), to improve patient safety
- Continuous improvement (e.g. swappable hardware for different services) or redesign the architecture of the artefact (DFR Framework for WMedSys) based on the state of art technology like Artificial Intelligence
- The human computer interface (HCI) aspects of socio-technical implementations
- General patient safety around innovative technologies
- Standardisation developments and potential implementation of standards
- Automation of the designed system
- Continuous risk assessment framework development for the WMedSys environment to improve patient safety and contribute to the healthcare industry
- Legislation, compliance and enforcement for safety
- User awareness testing
- Education and training processes for all users
- Cryptographic defences (e.g. Hash applications)

REFERENCES

Aarts, J., & Nohr, C. (2010). From safe systems to patient safety. *Information Technology in Health Care: Socio-Technical Approaches 2010*, (p. 1-3). Amsterdam, Netherlands: IOS Press. doi:10.3233/978-1-60750-569-3-1

Ab Rahman, N. H., & Choo, K.-K. R. (2015). A survey of information security incident handling in the cloud. *Computers & security, 49*, 45-69. doi:10.1016/j.cose.2014.11.00s6

Abdullah, N. A., Zakuan, N., Khayon, M., Ariff, M. S., Bazin, N. E., & Saman, M. Z. (2012). Adoption of Enterprise Risk Management Practices in Organisation: A Review. *International Journal of Business & Information Technology, 2*(1), 1-9. Retrieved from http://ojs.excelingtech.co.uk/index.php/IJBIT

Abraham, S., & Nair, S. (2015). A Predictive Framework for Cyber Security Analytics using Attack Graphs. *International Journal of Computer Networks & Communications (IJCNC), 7*(1), 1-17. doi:10.5121/ijcnc.2015.7101

Absolute Medical Services. (2016). *Infusion Pumps Overview*. Retrieved from https://www.absolutemed.com/medical-equipment-blog/infusion-pumps-overview.htm

Achi, H., Hellany, A., & Nagrial, M. (2009). Methodology and challenges in digital security forensics of wireless systems and devices. *International Conference on Computer Engineering & Systems (ICCES)* (pp. 283-287). Cairo: IEEEE.

Adelman, L., & Riedel, S. L. (1997). *Handbook for Evaluating Knowledge-Based Systems: Conceptual Framework and Compendium of Methods* (1st ed.). Berlin, Germany: Springer.

Adnan, A. H., Abdirazak, M., Sadi, A. S., Anam, T., Khan, S. Z., Rahman, M. M., & Omar, M. M. (2016). A comparative study of WLAN security

protocols: WPA, WPA2. *International Conference on Advances in Electrical Engineering (ICAEE)* (pp. 165-169). Dhaka, Bangladesh: IEEE.

Advisen Transforming Insurance. (2016). *Mitigating The Inevitable: How Organizations Manage Data Breach Exposures.* New York: Advisen Transforming Insurance.

Agarwal, M., Biswas, S., & Nandi, S. (2016). Detection of De-Authentication DoS Attacks in Wi-Fi Networks: A Machine Learning Approach. *IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 246-251). Kowloon, China: IEEE.

Agrawal, V. (2017). A Comparative Study on Information Security Risk Analysis Methods. *Journal of Computers, 12*(1), 57-67. doi:10.17706/jcp.12.1.57-67

AHIMA Work Group. (2013). Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 update). *Journal of AHIMA, 84*(8), 58-62. Retrieved from http://library.ahima.org/doc?oid=300257

Ahmed, N., & Abraham, A. (2013). Modeling Security Risk Factors in a Cloud Computing Environment. *Journal of Information Assurance and Security, 8*, 279-289. Retrieved from https://www.scopus.com

Ahmed, N., & Matulevičius, R. (2011). Towards transformation guidelines from secure tropos to misuse cases (position paper). *7th International Workshop on Software Engineering for Secure Systems* (pp. 36-42). Honolulu, HI: ACM.

Alemzadeh, H., Raman, J., Kalbarczyk, Z., & Iyer, R. (2013). Analysis of safety-critical computer failures in medical devices. *IEEE Security & Privacy, 11*(4), 14-26. doi:10.1109/MSP.2013.49

AIAA. (2013). *Framework for Aviation Cybersecurity.* Reston, Virginia: AIAA.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications Magazine, 40*(8), 102-114. doi:10.1109/MCOM.2002.1024422

Al, M., & Yoshigoe, K. (2011). Security and attacks in wireless sensor networks. *Network Security, Administration and Management: Advancing Technology and Practice*, 183-216. doi:10.4018/978-1-60960-777-7.ch010

Alblwi, S., & Shujaee, K. (2017). A Survey on Wireless Security Protocol WPA2. *International Conference on Security and Management* (pp. 12-17). Las Vegas: CSCE.

Alenezi, A., Hussein, R. K., Walters, R. J., & Wills, G. J. (2017). A Framework for Cloud Forensic Readiness in Organizations. *5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)* (pp. 199-204). San Francisco: IEEE.

Alharbi, S., Weber-Jahnke, J. H., & Traore, I. (2011). The Proactive and Reactive Digital Forensics Investigation Process: The Proactive and Reactive Digital Forensics Investigation Process:. *International Journal of Security and Its Applications, 5*(4), 59-72. doi:10.1007/978-3-642-23141-4_9

Alhumud, M. A., Hossain, M. A., & Masud, M. (2016). Perspective of health data interoperability on cloud-based Medical Cyber-Physical Systems. *IEEE International Conference on Multimedia & Expo Workshops (ICMEW)* (pp. 1-6). Seattle: IEEE.

Ali, S. M., & Soomro, T. R. (2014). Integration of Information Security Essential Controls into Information Technology Infrastructure Library – A Proposed Framework. *International Journal of Applied Science and Technology, 4*(1), 95-100. Retrieved from http://www.ijastnet.com/

AlKalbani, A., Deng, H., & Kam, B. (2014). A Conceptual Framework for Information Security in Public Organisations for E-Government Development. *25th Australasian Conference on Information Systems* (pp. 1-11). Auckland, New Zealand: Auckland University of Technology.

Alloussi, H. E., Fetjah, L., & Chaichaa, A. (2014). Securing the Payment Card Data on Cloud environment: Issues & perspectives. *IJCSNS International Journal of Computer Science and Network Security, 14*(11), 14-20. Retrieved from http://ijcsns.org/

Al-Mahrouqi, A., Abdalla, S., & Kechadi, T. (2014). Network Forensics Readiness and Security Awareness Framework. *International Conference on Embedded Systems in Telecommunications and Instrumentation (ICESTI)* (pp. 1-4). Annaba, Algeria: University of Annaba.

Al-Mahrouqi, A., Abdalla, S., & Kechadi, T. (2015). Cyberspace Forensics Readiness and Security Awareness Model. *Journal of Advanced Computer Science and Applications(IJACSA), 6*(6), 123-127. doi:10.14569/IJACSA.2015.060617

Almohri, H., Cheng, L., & Yao, D. (2017). On Threat Modeling and Mitigation of Medical Cyber-Physical Systems. *IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)* (pp. 114-119). Philadelphia: IEEE.

Alrajeh, D., Pasquale, L., & Nuseibeh, B. (2017). On evidence preservation requirements for forensic-ready systems. *11th Joint Meeting on Foundations of Software Engineering* (pp. 559-569). Paderborn: ACM.

Alruwaili, F. F., & Gulliver, T. A. (2014). ISPC: An Information Security, Privacy, and Compliance Readiness Model for Cloud Computing Services. *International Journal of Future Generation Distributed Systems (IJFGDS), 4*(4), 1-11. Retrieved from http://iartc.net/

Alruwaili, F. F., & Gulliver, T. A. (2015). SecSDLC: A Practical Life Cycle Approach for Cloud-based Information Security. *International Journal of Research in Computer and Communication Technology, 4*(2), 95-107. Retrieved from http://ijrcct.org

Altawy, R., & Youssef, A. M. (2016). Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices. *IEEE Access, 4*, 959-979. doi:10.1109/ACCESS.2016.2521727

Ameen, M. A., & Hong, C. S. (2015). An On-Demand Emergency Packet Transmission Scheme for Wireless Body Area Networks. *Sensors, 15*(12), 30584-30616. doi:10.3390/s151229819

Ameen, M. A., Liu, J., & Kwak, K. (2010). Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. *Journal of Medical Systems, 36*(1), 93-101. doi:10.1007/s10916-010-9449-4

Angela, A. I. (2014). Evaluation of Enhanced Security Solutions in 802.11-Based Networks. *International Journal of Network Security & Its Applications (IJNSA), 6*(4), 29-42. doi:10.5121/ijnsa.2014.6403

Arney, D., Venkatasubramanian, K. K., Sokolsky, O., & Lee, I. (2011). Biomedical devices and systems security. *Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)* (pp. 2376-2379). Boston: IEEE.

Aspden, P., Corrigan, J. M., Wolcott, J., & Erickson, S. M. (Eds.). (2003). Health care data standards. *Patient safety: Achieving a new standard for care* (p.127-168). Washington D.C., USA: National Academies Press.

Aubert, H. (2011). RFID technology for human implant devicesTechnologie RFID pour implants dans le corps humain. *Comptes Rendus Physique, 12*(7), 675-683. doi:10.1016/j.crhy.2011.06.004

Awan, M. S., Burnap, P., & Rana, O. (2016). Identifying cyber risk hotspots: A framework for measuring temporal variance in computer network risk. *Computers & Security, 57*, 31-46. doi:10.1016/j.cose.2015.11.003

Baldoni, R., & Montanari, L. (2016). *Italian cyber security report 2015: A national cyber security framework* (Version 1.0). Retrieved from https://www.cyberwiser.eu/news/italian-cyber-security-report-2015-national-framework

Babeanu, D., & Mares, V. (2009). Standards Review on Mission of Management Information Systems Audit. *Journal of Applied Quantitative MEthods, 4*(4), 422-428. Retrieved from http://www.jaqm.ro

Bailey, E., & Becker, J. D. (2014). A Comparison of IT Governance and Control Frameworks in Cloud Computing. *Twentieth Americas Conference on Information System* (pp. 1-16). Savannah: Association for Information Systems (AIS).

Baines, J. L. (2013). *Defining university IT security today and tomorrow.* Raleigh: NC State Univeristy.

Baker, G. R. (2006). Patient Safety Papers. *Healthcare Quarterly Special Issues, 9,* 1-144. Retrieved from http://www.longwoods.com/publications/healthcare-quarterly

Baker, M., Salmon, T., & Murphy, D. (2016). *Reducing cyber risk in the legal sector – The blurred boundaries of trust.* Singapore: LogRhythm.

Banitsas, K., Istepanian, R. S., & Tachakra, S. (2002). Applications of medical wireless LAN systems (MedLAN). *Journal of Medical Marketing: Device, Diagnostic and Pharmaceutical Marketing, 2*(2), 136-142. doi:10.1057/palgrave.jmm.5040067

Barach, P. (2002). Lessons from the USA. In S. Emslie, K. Knox, & M. Pickstone (Eds), *Improving patient safety: Insights from American, Australian and British healthcare* (pp. 43-57). United Kingdom: ECRI Europe.

Barnes, D. M. (2015). *Cybersecurity and medical devices.* Utica: Utica College.

Barske, D., Stander, A., & Jordaan, J. (2010). A Digital Forensic Readiness framework for South African SME's. *Information Security for South Africa (ISSA)* (pp. 1-6). Sandton, Johannesburg, South Africa: IEEE.

Baskerville, R., Pries-Heje, J., & Venable, J. (2011). A Risk Management Framework for Design Science Research. *44th Hawaii International Conference on System Sciences (HICSS)* (pp. 1-10). Kauai: IEEE.

Beasley, M., Branson, B., & Hancock, B. (2017). *The State of Risk Oversight: An Overview of Enterprise Risk Management Practices (7th Edition).* Raleigh: NC STATE Poole College of Management Enterprise Risk Management Initiative.

Benchikha, N., Krim, M., Zeraoulia, K., & Benzaid, C. (2016). IWNetFAF: An Integrated Wireless Network Forensic Analysis Framework. *Cybersecurity and Cyberforensics Conference (CCC)* (pp. 35-40). Amman, Jordan : IEEE.

Berg, H.-P. (2010). *Risk management: Procedures, Methods and Experiences*. Retrieved from http://www.gnedenko-forum.org/Journal/2010/022010/RTA_2_2010-09.pdf

Beuzekom, M. V., Boer, F., Akerboom, S., & Hudson, P. (2012). Patient safety in the operating room: an intervention study on latent risk factors. *BMC Surgery, 12*(10), 1-11. doi:10.1186/1471-2482-12-10

Bharathy, G. K., & McShane, M. K. (2014). Applying a Systems Model to Enterprise Risk Management. *Engineering Management Journal, 26*(4), 38-64. doi:10.1080/10429247.2014.11432027

Blass, G. (2012). *HIPAA, HITECH, & Audit Readiness.* Chicago, Illinois: Healthcare Information and Management Systems Society.

Bogodistov, Y., & Wohlgemuth, V. (2017). Enterprise risk management: A capability-based perspective. *The Journal of Risk Finance, 18*(3), 234-251.

Borek, A., Helfert, M., Ge, M., & Parlikad, A. K. (2011). An Information Oriented Framework for Relating IS/IT Resources and Business Value. *3th International Conference on Enterprise Information Systems* (pp. 1-10). Beijing: ACM.

Borek, A., Wooaall, P., Gosaen, M., & Parlikad, A. K. (2011). Managing information risks in asset management — Experiences from an in-depth case study in the utility industry. *IET and IAM Asset Management Conference* (pp. 1-6). London: IEEE.

Borek, A., Woodall, P., & Parlikad, A. K. (2011). A Risk Management Approach to Improving Information Quality for Operational and Strategic Management. *18th European Operations Management Association (EUROMA) conference* (pp. 1-10). Cambridge: European Operations Management Association.

Bosetti, L. (2015). Risk Management Standards in Global Markets. *3rd Virtual Multidisciplinary Conference* (pp. 81-86). At Zilina, Slovakia: QUAESTI.

Boulos, M. N., & Berry, G. (2012). Real-time locating systems (RTLS) in healthcare: a condensed primer. *International Journal Of Health Geographics, 11*(25), 18-20. doi:10.1186/1476-072X-11-25

Bowman, S. (2013). Impact of Electronic Health Record Systems on Information Integrity: Quality and Safety Implications. *Perspectives in Health Information Management, 10*(1c), 1-19. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3797550/

Brady, J. (2015). *Risk Assessment: Issues and Challenges*. Retrieved from https://www.ispe.gr.jp/ISPE/07_public/pdf/201506_en.pdf

Bro. (2016). The Bro network security monitor. Retrieved from https://www.bro.org/downloads/release/bro-2.4.1.tar.gz

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning, 48*(4), 265-276. doi:10.1016/j.lrp.2014.07.005

Brownlee, N., & Guttman, E. (1998). Expectations for computer security incident response. Retrieved from https://tools.ietf.org/html/rfc2350

Bruce, G. (2015). *Information Security ISO Standards.* New York City: Deloitte.

Bulbul, H. I., Batmaz, I., & Ozel, M. (2008). Wireless network security: comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols. *1st International Conference on Forensic Applications and Techniques in Telecommunications, Information, and Multimedia and Workshop.* Adelaide, Australia: ACM.

Bundesamt für Sicherheit in der Informationstechni. (2008). *BSI-Standard 100-1: Information Security Management Systems (ISMS).* Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI).

Burleson, W., & Carrara, S. (2014). *Security and Privacy for Implantable Medical Devices.* Berlin: Springer.

Burleson, W., Clark, S. S., Ransford, B., & Fu, K. (2012). Design challenges for secure implantable medical devices. *49th ACM/EDAC/IEEE Design Automation Conference (DAC)* (pp. 12-17). San Francisc: IEEE.

Business Wire. (2012). VeriTeQ Acquisition Corporation acquires implantable, FDA-cleared VeriChip technology and Health Link personal health record from PositiveID Corporation. Retrieved from https://www.businesswire.com/news/home/20120117005610/en/VeriTeQ-Acquisition-Corporation-Acquires-Implantable-FDA-Cleared-VeriChip

Butcher, D., li, X., & Guo, J. (2007). Security Challenge and Defense in VoIP Infrastructures. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 38*(6), 1152-1162. doi:10.1109/TSMCC.2007.905853

Cagalaban, G., & Kim, S. (2011). Towards a secure patient information access control in ubiquitous healthcare systems using identity-based signcryption. *13th International Conference on Advanced Communication Technology (ICACT)* (pp. 863-867). Seoul, South Korea: IEEE.

Cagalaban, G., & Kim, S. (2011). Towards a secure patient information access control in ubiquitous healthcare systems using identity-based signcryption. *13th International Conference on Advanced Communication Technology (ICACT)* (pp. 863-867). Seoul, South Korea: IEEE.

Cai, M., Wu, Z., & Zhang, J. (2014). Research and Prevention of Rogue AP Based MitM in Wireless Network. *Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)* (pp. 538-542). Guangdong, China: IEEE.

Calder, A. (2013). *Nine Steps to Success An ISO27001:2013 Implementation Overview*. Ely, Cambridgeshire: IT Governance .

Caneil, M., & Gilis, J.-L. (2010). *Attacks against the WiFi protocols WEP and WPA*. Retrieved from https://matthieu.io/dl/wifi-attacks-wep-wpa.pdf

Carlson, F. R. (2014). *Security Analysis of Cloud Computing*. Retrieved from https://arxiv.org/ftp/arxiv/papers/1404/1404.6849.pdf

Cassola, A., Robertson, W., Kirda, E., & Noubir, G. (2013). *A practical, targeted, and stealthy attack against WPA enterprise authentication.* Boston: Northeastern University.

Cavallari, R., Martelli, F., Rosini, R., Buratti, C., & Verdone, R. (2011). A survey on wireless body area networks. *Journal of Wireless Networks, 17*(1), 1-18. doi:10.1007/s11276-010-0252-4

Censi, F., Calcagnini, G., Mattei, E., Triventi, M., & Bartolini, P. (2010). RFID in healthcare environment: electromagnetic compatibility regulatory issues. *2010 Annual International Conference of the IEEE Engineering in Medicine and Biology* (pp. 352-355). Buenos Aires, Argentina: IEEE.

Center for Internet Secuirty. (2013). *Critical Controls for Effective Cyber Defense.* East Greenbush, New York: Center for Internet Secuirty.

CESG. (2015). *Technology and information risk management.* Gloucestershire: CESG.

CESG Enquiries. (2015). *Good Practice Guide Forensic Readiness.* Gloucestershire: Crown.

CESG Enquiries. (2015). *IA Implementation Guide Forensic Readiness Planning.* Gloucestershire: Crown.

Chapin, D. A., & Akridge, S. (2005). How Can Security Be Measured ? *Information System Control Journal, 2*, 1-6. Retrieved from www.isaca.org

Chen, B., Varkey, J. P., Pompili, D., Li, J. K., & Marsic, I. (2010). Patient vital signs monitoring using Wireless Body Area Networks. *IEEE 36th Annual Northeast Bioengineering Conference (NEBEC)* (pp. 1-2). New York: IEEE.

Chen, D., Soong, S.-j., Grimes, G. J., & Orthner, H. F. (2004). Wireless local area network in a prehospital environment. *BMC Medical Informatics and Decision Making, 4*(12), 1-9. doi:10.1186/1472-6947-4-12

Chen, H. (2017). Applications of Cyber-Physical System: A Literature Review. *Journal of Industrial Integration and Management, 2*(3), 1-28. doi:10.1142/S2424862217500129

Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. (2011). Body Area Networks: A Survey. *Mobile Networks and Applications, 16*(12), 171-193. doi:10.1007/s11036-010-0260-8

Chen, P.-y., Kataria, G., & Krishnan, R. (2011). Correlated Failures, Diversification, and Information Security Risk Management. *MIS Quarterly, 35*(2), 397-422. doi:10.2307/23044049

Chenot, T. M. (2007). *Frameworks for patient safety in the nursing curriculum (Doctoral dissertation*, University of North Florida). Retrieved from https://digitalcommons.unf.edu/etd/236/

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security, 56*, 1-27. doi:10.1016/j.cose.2015.09.009

Choejey, P., Fung, C. C., Wong, K. W., Murray, D., & Xie, H. (2015). Cybersecurity Practices for E-Government: An Assessment in Bhutan. *10th International Conference on e-Business (iNCEB2015)* (pp. 1-8). Bangkok: ACM.

Cisco. (2017). *Cisco 2017 Cyber Security Report.* Elmwood Park: InfoSec Institute.

Civil Air Navigation Services Organisation. (2014). *CANSO Cyber Security and Risk Assessment Guide.* Amsterdam: Civil Air Navigation Services Organisation (CANSO).

Clark, S. S., & Fu, K. (2012). Recent results in computer security for medical devices. *MobiHealth 2011. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 83*, 111-118. doi:10.1007/978-3-642-29734-2_16

Clifford, A., McCalman, J., Bainbride, R., & Tsey, K. (2015). Interventions to improve cultural competency in health care for Indigenous peoples of Australia, New Zealand, Canada and the USA: a systematic review. *International Journal for Quality in Health Care,, 27*(2), 89-98. doi:10.1093/intqhc/mzv010

Cline, B. (2009). *G22 - A Security and Compliance Risk ManagementFramework for Health Care.* Rolling Meadows: ISACA.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*(2), 544-546. doi:10.1016/j.future.2017.07.060

Conti, M., Mancini, L. V., Spolaor, R., & Verde, N. V. (2016). Analyzing Android Encrypted Network Traffic to Identify User Actions. *IEEE Transactions on Information Forensics and Security, 11*(1), 114-125. doi:10.1109/TIFS.2015.2478741

Cope, P., Campbell, J., & Hayajneh, T. (2017). An investigation of Bluetooth security vulnerabilities. *IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 1-7). Las Vegas: IEEE.

Costello, G. J. (2017). *Aristotle's Phronesis: Seeking Philosophical Foundations for Design Science Research*. Retrieved from https://www.researchgate.net/publication/318722910_Aristotle%27s_Phronesis_Seeking_Philosophical_Foundations_for_Design_Science_Research

Craven, C., Byrne, K., Sims-Gould, J., & Martin-Matthews, A. (2012). Types and patterns of safety concerns in home care: staff perspectives. *International Journal for Quality in Health Care, 24*(5), 525-531. doi:10.1093/intqhc/mzs047

Creswell, J. W. (2013). *Research Design Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). Thousand Oaks,CA: Sage.

Cuomo, A. M., & Lawsky, B. M. (2014). *Report on Cyber Security in the Banking Sector.* New York: New York State Department of Financial Services.

Cusack, B., & Kyaw, A. K. (2014). Managing wireless security risks in medical services. In P. A. H. Williams (Ed.), *Proceedings of the 3rd Australian eHealth Informatics and Security Conference (AeHIS)*, (pp. 14-21). Perth, Western Australian: Security Research Centre (SECAU), Edith Cowan University.

Cusack, B., & Kyaw, A. K. (2012). Forensic readiness for wireless medical systems. In A. Woodward (Ed.), *Proceedings of the 10th Australian Digital Forensics Conference*, (pp. 21-32). Perth, Western Australia: SECAU – Security Research Centre, Edith Cowan University.

CyberSecurity Malaysia. (2013). *ISMS Implementation Guideline_a practical approach.* Selangor Darul Ehsan, Malaysia: CyberSecurity Malaysia.

CYFOR. (2017). *Specialists in Organisational Forensic Readiness Planning and Implementation*. Retrieved from http://cyfor.co.uk/digital-forensics/forensic-readiness-planning/

Cypher, D., Chevrollier, N., Montavont, N., & Golmie, N. (2006). Prevailing over wires in healthcare environments: benefits and challenges. *IEEE Communications Magazine*, *44*(4), 56-63. doi:10.1109/MCOM.2006.1632650

Dallas, M. (2013). *Management of Risk: Guidance for Practitioners and the international standard on risk management, ISO 31000:2009.* London: The Stationery Office.

Dargie, W., & Poellabauer, C. (2010). *Fundamentals of Wireless Sensor Networks: Theory and Practice.* Singapore: John Wiley & Sons Ltd.

Darknet. (2016). MANA toolkit – Rogue access point (evilAP) and MiTM attack tool. Retrieved from https://www.darknet.org.uk/2016/09/mana-toolkit-rogue-access-point-evilap-mitm-attack-tool/

Darwish, A., & Hassanien , A. E. (2011). Wearable and Implantable Wireless Sensor Network Solutions for Healthcare Monitoring. *Sensors*, *11*(6), 5561-5595. doi:10.3390/s110605561

Das, A. K., Zeadally, S., & Wazid, M. (2017). Lightweight authentication protocols for wearable devices. *Computers & Electrical Engineering, 63*, 196-208. doi:10.1016/j.compeleceng.2017.03.008

David, D. S., & Jeyachandran, A. (2016). A comprehensive survey of security mechanisms in healthcare applications. *International Conference on Communication and Electronics Systems (ICCES)* (pp. 1-6). Coimbatore, India: IEEE.

David, Y., & Judd, T. M. (2006). Management and assessment of medical technology. In J. D. Bronzino (Ed.), *The biomedical engineering handbook: Medical devices and systems* (3rd ed., pp. 75-1--75-14). Florida: CRC Press.

De Marco, L., Ferrucci, F., & Kechadi, M. (2014). Reference architecture for a cloud forensic readiness system. *EAI Endorsed Transactions on Security and Safety, 2014*, 1-9.

Delmastro, F. (2012). Pervasive communications in healthcare. *Computer Communications, 35*(11), 1284-1295. doi:10.1016/j.comcom.2012.04.018

Deloitte. (2016). *Cyber crisis management Readiness, response, and recovery.* New York City: Deloitte.

Denning, T., Borning, A., Friedman, B., Gill, B. T., Kohno , T., & Maisel, W. H. (2010). Patients, pacemakers, and implantable defibrillators: human values and security for wireless implantable medical devices. *SIGCHI Conference on Human Factors in Computing Systems* (pp. 917-926). Atlanta, Georgia: ACM.

Denning, T., Matsuoka, Y., & Kohno, T. (2009). Neurosecurity: security and privacy for neural devices. *Neurosurgical Focus, 27*(1), E7. doi:10.3171/2009.4.FOCUS0985

Devaraj, S. J., & Ezra, K. (2011). Current trends and future challenges in wireless telemedicine system. *3rd International Conference on Electronics Computer Technology (ICECT)* (pp. 417-421). Hong Kong, China: IEEE.

Dhama, S. (2014). *A Practical Approach to Distributed WPA/WPA2 Cracking with CUDA.* San Luis Obispo: California Polytechnic State University.

Diksha, N., & Shubham, A. (2006). Backdoor Intrusion in Wireless Networks-problems and solutions. *International Conference on Communication Technology, ICCT '06* (pp. 1-4). Guilin, China: IEEE.

Djemame, K., Armstrong, D. J., Kiran, M., & Jiang, M. (2011). A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems. *The Second International Conference on Cloud Computing, GRIDs, and Virtualization* (pp. 119-126). Rome: IARIA.

Dogaru, D. I., & Dumitrache, I. (2015). Cyber-physical systems in healthcare networks. *E-Health and Bioengineering Conference (EHB)* (pp. 1-4). Iasi, Romania : IEEE.

Dong, P., Han, Y., Guo, X., & Xie, F. (2015). A Systematic Review of Studies on Cyber Physical System Security. *International Journal of Security and Its Applications, 9*(1), 155-164. doi:10.14257/ijsia.2015.9.1.17

Dong, T., & Yadav, S. B. (2014). A Comprehensive Framework for Comparing System Security Risk Assessment Methods. *Twentieth Americas Conference on Information Systems* (pp. 1-8). Savannah: Association for Information Systems (AIS).

Earle, A. E. (2006). *Wireless security handbook* (1st ed.). Boca Raton, Florida: Auerbach Publications, Taylor & Francis Group.

EC-Council. (2010). *Ethical Hacking & Countermeasures Secure Network Infrastructures.* Boston: Cengage.

EC-Council. (2011). *Disaster Recovery.* Boston: Cengage.

Eden, P., Blyth, A., Burnap, P., Cherdantseva, Y., Jones, K., Soulsby, H., & Stoddart, K. (2016). Forensic readiness for SCADA/ICS incident response. *4th International Symposium for ICS & SCADA Cyber Security Research* (pp. 1-9). Belfast: ACM.

Ehlinger, S. (2017, December 4). Former employee reportedly steals mental health data on 28,434 Bexar County patients. *San Antonio Express News*. Retrieved from

https://www.expressnews.com/business/local/article/Former-employee-reportedly-steals-mental-health-12405113.php

Ellouze, N., Allouche, M., Ahmed, H. B., Rekhis, S., & Boudriga, S. (2013). Security of implantable medical devices: limits, requirements, and proposals. *Security and Communication Networks, 7*(12), 2475–2491. doi:10.1002/sec.939

Ellouze, N., Rekhis, S., Boudriga, N., & Allouche, M. (2017). Cardiac Implantable Medical Devices forensics: Postmortem analysis of lethal attacks scenarios. *Digital Investigation, 21*, 11-30. doi:10.1016/j.diin.2016.12.001

Elouze, N., Rekhis, S., Boudriga, N., & Allouche, M. (2017). Cardiac implantable medical devices forensics: Postmortem analysis of lethal attacks scenarios. Digital Investigation, 21, 11-30. doi:10.1016/j.diin.2016.12.001

Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security, 52*, 70-89. doi:10.1016/j.cose.2015.04.003

Elyas, M., Maynard, S. B., Ahmad, A., & Lonie, A. (2014). Towards A Systemic Framework for Digital Forensic Readiness. *Journal of Computer Information Systems, 54*(3), 97-105. doi:10.1080/08874417.2014.11645708

Emslie, S., Knox, K., & Pickstone, M. (2002). *Improving Patient Safety: Insights from American, Australian and British healthcare.* Welwyn Garden City: ECRI Europe.

Endicott-Popovsky, B. E., & Frincke, D. A. (2006). Embedding Forensic Capabilities into Networks: Addressing Inefficiencies in Digital Forensics Investigations. *IEEE Information Assurance Workshop* (pp. 133-139). West Point: IEEE.

Endicott-Popovsky, B., Frincke, D. A., & Taylor, C. A. (2007). A theoretical framework for organizational network forensic readiness. *Journal of Computers, 2*(3), 1-11. Retrieved from http://www.jcomputers.us/

Eren, H. (2006). *Wireless Sensors and Instruments: Networks, Design, and Applications* (1st ed.). Boca Raton, Florida: CRC Press.

European Data Protection Supervisor. (2019). The history of the general data protection regulation. Retrieved from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Evangelopoulou, M., & Johnson, C. W. (2015). Empirical Framework for Situation Awareness Measurement Techniques in Network Defense. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (pp. 1-4). London: IEEE.

Evesti, A., Suomalainen, J., & Savola, R. (2014). Security Aspects of Short-Range Wireless Communication – Risk Analysis for the Healthcare Application. *International Journal of Intelligent Computing Research (IJICR), 5*(2), 1-16. Retrieved from http://infonomics-society.org/ijicr/

Fachkha, C., & Debbabi, M. (2016). Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization. *IEEE Communications Surveys & Tutorials, 18*(2), 1197-1227. doi:10.1109/COMST.2015.2497690

Faris, S., Hasnaoui, S. E., Medromi, H., Iguer, H., & Sayouti, A. (2014). Toward an Effective Information Security Risk Management of Universities' Information Systems Using Multi Agent Systems, Itil, Iso 27002,Iso 27005. *International Journal of Advanced Computer Science and Applications (IJACSA), 5*(6), 114-118. Retrieved from http://thesai.org/Publications/IJACSA

Federici, C. (2013). AlmaNebula: A Computer Forensics Framework for the Cloud. *Procedia Computer Science, 19*, 139-146. doi:10.1016/j.procs.2013.06.023

Filippidis, F. T., Mian, S. S., & Millett, C. (2016). Perceptions of quality and safety and experience of adverse events in 27 European Union healthcare systems, 2009–2013. *International Journal for Quality in Health Care, 28*(6), 721-727. doi:10.1093/intqhc/mzw097

Filkins, B. (2014). *Health Care Cyberthreat Report Widespread Compromises Detected, Compliance Nightmare on Horizon.* Bethesda: SANS Institute.

Fisher, J. A., & Monahan,, T. (2012). Evaluation of real-time location systems in their hospital contexts. *International Journal of Medical Informatics, 81*(10), 705-712. doi:10.1016/j.ijmedinf.2012.07.001

Fitzmaurice, J. M. (2006). Computer-based patient records. In J. D. Bronzino (Ed.), *The biomedical engineering handbook: Medical devices and systems* (3rd ed., pp. 41-1--41-16). Florida: CRC Press.

Flick, U. (2015). *Introducing Research Methodology: A Beginner's Guide to Doing a Research Project* (2nd ed.). Thousand Oaks, CA: Sage.

Flott , K., Darzi, A., & Mayer, E. (2016). Evaluation framework for patient safety incident reporting systems. *International Journal for Quality in Health Care, 28*(1), 8-9. doi:10.1093/intqhc/mzw104.7

Flott, K., Darzi, A., & Mayer, E. (2016). ISQUA16-1828 Evaluation framework for patient safety incident reporting systems. *International Journal for Quality in Health Care, 28*(suppl_1), 8-9.

Fluhrer, S., Mantin, I., & Shamir, A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. *8th Annual International Workshop Selected Areas in Cryptography (SAC)* (pp. 1-23). Toronto: Selected Areas in Cryptography.

Ford, E. W., & Savage, G. T. (2008). Patient safety: State-of-the-art in health care management and future directions. In Patient Safety and Health Care Management (pp. 1-14). United Kingdom: Emerald Group Publishing Limited.

Forsberg, E. M., Shelley-Egan, C., Thorstensen, E., Landeweerd, L., & Hofmann, B. (2017). *Evaluating Ethical Frameworks for the Assessment of Human Cognitive Enhancement Applications* (1st ed.). Berlin, Germany: Springer.

Fortune, P. M., Davis, M., Hanson, J., & Phillips, B. (Eds.). (2013). Human factors in the health care setting: A pocket guide for clinical instructors. West Sussex, UK: John Wiley & Sons Ltd.

Foshay, N., & Kuziemsky, C. (2014). Towards an implementation framework for business intelligence in healthcare. *International Journal of Information Management, 34*(1), 20-27. doi:10.1016/j.ijinfomgt.2013.09.003

Frankel, S., Eydt , B., Owens, L., & Scarfone, K. (2007). *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.* Gaithersburg, Maryland: National Institute of Standards and Technology.

Fraser, J., Simkins, B., & Narvaez, K. (2014). *Implementing Enterprise Risk Management: Case Studies and Best Practices.* Hoboken, New Jersey: Wiley.

Frelinger, B. (2012). *COBIT Case Study: Building Acceptance and Adoption of Governance of Enterprise IT*. Retrieved from http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Building-Acceptance-and-Adoption-of-Governance-of-Enterprise-IT.aspx?utm_referrer=

Freudenthal, E. A., Herrera, D. A., Kautz, F., Natividad, C., Ogrey, A., Sipla, J., . . . Estevez, L. (2007). *Evaluation of HF RFID for implanted medical applications [UTEP-CS-07-36]*. Texax, El Paso: University of Texas, Department of Computer Science.

Fu, K. (2009). Inside risks: Reducing risks of implantable medical devices. *Communications of the ACM - One Laptop Per Child: Vision vs. Reality, 52*(6), 25-27. doi:10.1145/1516046.1516055

Fu, K., & Blum , J. (2013). Controlling for cybersecurity risks of medical device Software. *Communications of the ACM, 56*(10), 35-37. doi:10.1145/2508701

Fulford, M. (2016). *HITRUST Certification Improves Healthcare Cyber Security*. Retrieved from https://www.lbmcinformationsecurity.com/blog/hitrust-certification-improves-healthcare-cyber-security

Gaffo, F. H., & Barros, R. M. (2012). GAIA risks - a service-based framework to manage project risks. *XXXVIII Conferencia Latinoamericana En Informatica (CLEI)* (pp. 1-10). Medellin, Colombia: IEEE.

Garrett , B., & Jackson , C. (2006). A mobile clinical e-portfolio for nursing and medical students, using wireless personal digital assistants (PDAs). *Nurse Educ Today, 26*(8), 647-654. doi:10.1016/j.nedt.2006.07.020.S0260-6917(06)00120-1

Gawanmeh, A., Al-Hamadi, H., Al-Qutayri, M., Chin, S.-K., & Saleem, K. (2015). Reliability analysis of healthcare information systems: State of the art and future directions. *17th International Conference on E-health Networking, Application & Services (HealthCom)*, (pp. 68-74). Boston: IEEE.

Gaynor, M., Bass, C., & Duepner, B. (2015). A tale of two standards: strengthening HIPAA security regulations using the PCI-DSS. *Health Systems, 4*(2), 111-123. doi:10.1057/hs.2014.17

Ge, M., Hong, J. B., Guttmann, W., & Kim, D. S. (2017). A framework for automating security analysis of the internet of things. *Journal of Network and Computer Applications*, 1-60. doi:10.1016/j.jnca.2017.01.033

Gill , G., Gallo , S., & Rijnders , Q. (2016). *Achieving Digital Forensic Readiness.* Sydney: KPMG.

Giraldo, J., Sarkar, E., Cardenas, A. A., Maniatakos, M., & Kantarcioglu, M. (2017). Security and Privacy in Cyber-Physical Systems: A Survey of Surveys. *IEEE Design & Test, 34*(4), 7-17. doi:10.1109/MDAT.2017.2709310

Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., & Fu, K. (2011). They can hear your heartbeats: non-invasive security for implantable medical devices. In *ACM SIGCOMM 2011 conference* (pp. 2-13). New York, NY: ACM.

Golmie, N., Chevrollier, N., & Rebala, O. (2003). Bluetooth and WLAN coexistence: challenges and solutions. *IEEE Wireless Communications, 10*(6), 22-29. doi:10.1109/MWC.2003.1265849

Government Communications Security Bureau. (2015). *NZISM New Zealand Information Security Manual.* Wellington: Government Communications Security Bureau.

Goyal, P., Batra, S., & Singh, A. (2010). A literature review of security attack in mobile ad-hoc networks. *International Journal of Computer Applications, 9*(12), 11-15. doi:10.5120/1439-1947

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly, 37*(2), 337-355. Retrieved from https://www.misq.org/

Grim, L., & Vandenbrink, R. (2014). *IDS: File Integrity Checking.* Bethesda: SANS Institute.

Grimes, S. L. (2011). Using 80001 to manage medical devices on the IT network. *Journal of Biomedical Instrumentation & Technology, 45*(s2), 23-26. doi:10.2345/0899-8205-45.s2.23

Grimvall, G., Holmgren, A., Jacobsson, P., & Thedéen, T. (2010). *Risks in Technological Systems.* Berlin: Springer.

Grispos, G., Garcia-Galan, J., Pasquale, L., & Nuseibeh, B. (2017). Are You Ready? Towards the Engineering of Forensic-Ready Systems. *IEEE 11th International Conference on Research Challenges in Information Science* (pp. 328 - 333). Brighton: IEEE .

Grobler, C. P., & Louwrens, C. P. (2007). Digital Forensic Readiness as a Component of Information Security Best Practice. *IFIP International Information Security Conference* (pp. 13-24). Boston: Springer.

Grobler, C. P., Louwrens, C. P., & Solms, S. H. (2010). A Multi-component View of Digital Forensics. *ARES '10 International Conference on Availability, Reliability, and Security* (pp. 647-652). Krakow, Poland: IEEE.

Grobler, M., & Villiers, C. D. (2017). Shaping solutions with a community: the research design using design science research (DSR) and case study research with an ICT4D project. *International Conference on Information Resources Management (CONF-IRM)* (pp. 1-12). Santiago: CONF-IRM.

Gunes, V., Peter, S., Givargis, T., & Vahid, F. (2014). A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems. *KSII Transactions on Internet and Information Systems*, 4242-4268. doi:10.3837/tiis.2014.12.001

Gupta, S., & Saini, A. K. (2013). Information System Security and Risk Management: Issues and Impact on Organizations. *Global Journal of Enterprise Information System, 5*(1), 31-35. doi:10.18311/gjeis/2013/3144

Habash, R. W., Groza, V., & Burr, K. (2013). Risk Management Framework for the Power Grid Cyber-Physical Security. *British Journal of Applied Science & Technology, 3*(4), 1070-1085. doi:10.9734/BJAST/2013/3682

Hajdarevic, K., Kozaric, K., & Hadzigrahic, J. (2012). Architecture and Infrastructure for Governing Information Security In Central Banks. *Journal of Central Banking Theory and Practice*, 5-17. Retrieved from http://www.ijcb.org/

Halamka, J., Juels, A., Stubblefield, A., & Westhues, J. (2006). The security implications of VeriChip cloning. *Journal of the American Medical Informatics Association, 13*(6), 601–607. doi:10.1197/jamia.m2143

Halperin, D., Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., . . . Maisel, W. H. (2008). Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. *IEEE Symposium on Security and Privacy (sp 2008)* (pp. 129-142). Oakland: IEEE.

Han, S., Xie, M., Chen, H.-H., & Ling, Y. (2014). Intrusion Detection in Cyber-Physical Systems: Techniques and Challenges. *IEEE Systems Journal, 8*(4), 1052-1062. doi:10.1109/JSYST.2013.2257594

Hänel, T., & Felden, C. (2017). Design and Evaluation of an Analytical Framework to Analyze and Control Production Processes. *Procedia CIRP, 62*, 141-146. doi:10.1016/j.procir.2016.06.052

Hanna, S., Rolles, R., Markham, A. M., Poosankam, P., Fu, K., & Song, D. (2011). Take two software updates and see me in the morning: the case for

software security evaluations of medical devices. *HealthSec'11 Proceedings of the 2nd USENIX conference on Health security and privacy* (pp. 6-6). San Francisco: ACM.

Hansen, J. A., & Hansen, N. M. (2010). A taxonomy of vulnerabilities in implantable medical devices. *Second annual workshop on Security and privacy in medical and home-care systems* (pp. 13-20). Chicago: ACM.

Haque, S. A., Aziz, S. M., & Rahman, M. (2014). Review of Cyber-Physical System in Healthcare. *International Journal of Distributed Sensor Networks, 10*(4), 1-20. doi:10.1155/2014/217415

Harbawi, M., & Varol, A. (2017). An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. In *5th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-6). Tirgu Mures, Romania: IEEE.

Hardy, K., & Runnels , A. (2014). *Enterprise Risk Management: A Guide for Government Professionals.* Hoboken, New Jersey: Wiley.

Harpes, C., Schaff, G., Martins, M., Kordy, B., Trujillo, R., & Ionita, D. (2014). *Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security: Currently established risk-assessment methods.* Brussel: EC-DG CONNECT.

Hasan, R., Zawoad, S., Noor, S., Haque, M. M., & Burke, D. (2016). How Secure is the Healthcare Network from Insider Attacks? An Audit Guideline for Vulnerability Analysis. *IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)* (pp. 417-422). Atlanta: IEEE.

Hassen, S. S., & Zakaria, M. S. (2013). Managing University IT Risks in Structured and Organized Environment. *Research Journal of Applied Sciences, Engineering and Technology, 6*(12), 2270-2276. Retrieved from https://www.scopus.com

Haufe, K., Dzombeta, S., & Brandis, K. (2014). Proposal for a Security Management in Cloud Computing for Health Care. *The Scientific World Journal, 2014*, 1-7. doi:10.1155/2014/146970

Heartfield, R., & Loukas, G. (2016). A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys (CSUR), 48*(3), 1-38. doi:10.1145/2835375

Heslop, L., Weeding, S., Dawson, L., Fisher, J., & Howard, A. (2010). *Implementation* issues for mobile-wireless infrastructure and mobile health care computing devices for a hospital ward setting. *Journal of Medical Systems, 34*(4), 509-518. doi:10.1007/s10916-009-9246-y

Hermans, J., Tinholt, M. W., & de Wit, J. (2015). Achieving digital forensic readiness. Retrieved from https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/Achieving-Digital-Forensic-Readiness-12-9-2015.pdf

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems, 19*(2), 2007. Retrieved from http://aisel.aisnet.org/sjis/

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75-105.

Hewitt, M., & Keen, C. (2009). *How to Search and Critically Evaluate Research Literature.* Nottingham: The NIHR RDS for the East Midlands / Yorkshire & the Humber.

Hewlett Packard. (2014). *Breach Response: How to Prepare for the Inevitable.* Palo Alto, California: Hewlett Packard.

Hewlett Packard. (2015). *Behind the Mask: The Changing Face of Hacking.* Palo Alto, California: Hewlett Packard.

Hewlett Packard. (2016). *HPE Security Research: Cyber Risk Report 2016.* Palo Alto, California: Hewlett Packard.

HITRUST Alliance. (2016). *Risk Analysis Guide for HITRUST Organizations & Assessors.* Frisco: HITRUST Alliance.

HM Government. (2015). *2015 Information Security Breaches Survey: Technical Report.* London: HM Government.

Hoglund, D. (2007). Wireless technology infrastructure: A business strategy. *Journal of Biomedical Instrumentation & Technology, 41*(6), 457-460.

Honan, B. (2010). *ISO27001 in a Windows Environment: The Best Practice Handbook for a Microsoft Windows Environment* (2nd ed.). Ely, Cambridgeshire: IT Governance.

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law, 1–34.* doi:10.1080/13600834.2019.1573501

Honan, B. (2014). An introduction to ISO27001. *ISO27001 in a Windows environment: The best practice handbook for a Microsoft Windows environment* (p. 33-43). United Kingdom: IT Governance Publishing.

Hsu, C.-N., Wang, Y.-C. L., Chen, I.-L., & Hsiao, S.-C. (2016). Implement External Electronic Medication Records To Promote Effective Hospital Medication Reconciliation. *International Journal for Quality in Health Care, 28*(1), 12. doi:10.1093/intqhc/mzw104.13

Hsu, C. N., Wang, Y. C. L., Chen, I. L., & Hsiao, S. C. (2016). ISQUA16-2073 Implementing external electronic medication records to promote effective hospital medication reconciliation. International Journal for Quality in Health Care, 28(suppl_1), 12.

Hu, F., Lu, Y., Vasilakos, A. V., Hao, Q., Ma, R., Patil, Y., . . . Xiong, N. N. (2016). Robust Cyber–Physical Systems: Concept, models, and implementation. *Future Generation Computer Systems, 56,* 449-475. doi:10.1016/j.future.2015.06.006

Huang, A. R., & Segal, B. (2011). A literature review of the safety of medical body area network devices in magnetic resonance imaging. *5th International Symposium on Medical Information & Communication Technology (ISMICT)* (pp. 127-129). Montreux, Switzerland: IEEE.

Huang, H., Gong, T., Ye, N., Wang, R., & Dou, Y. (2017). Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System. *IEEE Transactions on Industrial Informatics, 13*(3), 1227-1237. doi:10.1109/TII.2017.2687618

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security - A Survey. *IEEE Internet of Things Journal, PP*(99), 1-1. doi:10.1109/JIOT.2017.2703172

Hutchins, M. J., Bhinge, R., Micali, M. K., Robinson, S. L., Sutherland, J. W., & Dornfeld, D. (2015). Framework for Identifying Cybersecurity Risks in Manufacturing. *Procedia Manufacturing, 1*, 47-63. doi:10.1016/j.promfg.2015.09.060

Hwang, H., Jung, G., Sohn, K., & Park, S. (2008). A study on MITM (Man in the Middle) vulnerability in wireless network using 802.1X and EAP. In Kuinam J. Kim & Okhuen Ha Los (Eds.), *Proceedings of 2008 International Conference on Information Science and security,* (pp. 164-170). Alamitos, CA: IEEE Computer Society.

Hwang, J.-I. (2015). What are hospital nurses' strengths and weaknesses in patient safety competence? Findings from three Korean hospitals. *International Journal for Quality in Health Care,, 27*(3), 232-238. doi:10.1093/intqhc/mzv027

IBM. (2016). *The Evolving Face of Cyberthreats.* Armonk, New York: IBM.

Ieong, R. S. C. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation, 3S*(2006), S29-S36. doi:10.1016/j.diin.2006.06.004

InfoSec Institue. (2017). *10 Best Practices for Healthcare Security*. Retrieved from http://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/

Ionita, D. (2013). *Current Established Risk Assessment Methodologies and Tools.* Enschede, Netherlands: University of Twente.

ISACA. (2010). *Process Health Assessment Discussion Worksheet.* Rolling Meadows, Illinois: ISACA.

ISACA. (2010). *The Business Model for Information Security.* Rolling Meadows, Illinois: ISACA.

ISACA. (2012). *Calculating Cloud ROI: From the Customer Perspective.* Rolling Meadows, Illinois: ISACA.

ISACA. (2013). *Secuirty As A Service: Business Benefit With Security, Gorvernance and Assurance Perspective.* Rolling Meadows, Illinois: ISACA.

Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K.-S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access, 3*, 678-708. doi:10.1109/ACCESS.2015.2437951

International Organisation for Standardisation (ISO). (2013). *Information technology - Security techniques - Code of practice for information security controls.* Geneva: ISO.

Jain, J. (2017). *Cracking a WPA2 Encryption Password File*. Retrieved from http://resources.infosecinstitute.com/cracking-wpa2-encryption-password-file/#gref

Jain, P. C. (2014). Wireless body area network for medical healthcare. *IETE Technical Review, 28*(4), 362-371. doi:10.4103/0256-4602.83556

Janoff, C., & McGlothin, B. (2015). *Cisco Compliance Solution for HIPAA Security Rule Design and Implementation Guide.* Elmwood Park: Cisco.

Jayaratna , N. (1994). *Understanding and Evaluating Methodologies: Nimsad, a Systematic Framework* (1st ed.). New York City: McGraw-Hill.

Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science.* Springer: Berlin, Germany.

Jovanov, E., Raskovic , D., Price, J., Chapman , J., Moore, A., & Krishnamurthy, A. (2011). Patient monitoring using personal area networks of wireless intelligent sensors. *Biomedical Sciences Instrumentation, 37*, 373-378.

Retrieved from https://www.ncbi.nlm.nih.gov/labs/journals/biomed-sci-instrum/

Jula, A., Sundararajan, E., & Othman, Z. (2014). Cloud computing service composition: A systematic literature review. *Expert Systems with Applications, 41*(8), 3809-3824. doi:10.1016/j.eswa.2013.12.017

Julisch, K., Suter, C., Woitalla, T., & Zimmermann, O. (2011). Compliance by Design - Bridging the Chasm between Auditors and IT Architects. *Computers and Security, 30*(6), 410-426. doi:10.1016/j.cose.2011.03.005

Kacic, M., Hanacek, P., Henzl, M., & Jurnecka, P. (2013). Malware injection in wireless networks. *IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)* (pp. 483-487). Berlin, Germany: IEEE.

Kalniņš, R., Puriņš, J., & Alksnis, G. (2017). Security Evaluation of Wireless Network Access Points. *Applied Computer Systems, 21*(1), 38-45. doi:10.1515/acss-2017-0005

Kanhere, V. (2009). Driving Value from Information Security A Governance Perspective. *ISACA Journal, 2*, 1-4. Retrieved from https://www.isaca.org/pages/default.aspx

Kao, H. Y., Yu, M. C., Masud, M., Wu, W. H., Chen, L. J., & Wu, Y. C. (2016). Design and evaluation of hospital-based business intelligence system (HBIS): A foundation for design science research methodology. *Computers in Human Behavior, 62*, 495-505. doi:10.1016/j.chb.2016.04.021

Karie, N. M., & Venter, H. S. (2015). Taxonomy of Challenges for Digital Forensics. *Journal of Forensic Sciences, 60*(4), 885-893. doi:10.1111/1556-4029.12809

Karie, N. M., Kebande, V. R., & Venter, H. S. (2017). Taxonomy for Digital Forensic Evidence. *Pan-African Conference on Science Computing and Telecommunications (PACT)* (pp. 1-8). Nairobi, Kenya: IEEE.

Karygiannis, A. T., & Owens , L. (2002). *NIST Special Publication 800-48: Wireless Network Security - 802.11, Bluetooth and Handheld Devices.* Gaithersburg, Maryland: National Institute of Standards and Technology.

Kaspersky. (2016). *Damage Control: The Cost of Security Breaches IT Security Risks Special Report Series.* Moscow: Kaspersky.

Katal, A., Wazid, M., & Goudar, R. H. (2012). Enhanced Security Framework for Cloud Computing. *2nd International Conference on Computational Intelligence and Information Technology* (pp. 365-370). Chennai, India: Springer.

Katzis, K., Jones, R. W., & Despotou, G. (2017). Totally Connected Healthcare with TV White Spaces. *Stud Health Technol Inform, 238,* 68-71. Retrieved from https://www.ncbi.nlm.nih.gov/

Kebande, V. R., & Venter, H. S. (2014). A Cloud Forensic Readiness Model Using a Botnet as a Service. *International Conference on Digital Security and Forensics (DigitalSec2014)* (pp. 1-10). Ostrava, Czech Republic: SDIWC.

Kebande, V. R., & Venter, H. S. (2015). A Functional Architecture for Cloud Forensic Readiness Large-scale Potential Evidence Analysis. *14th European Conference on Cyber Warfare and Security (ECCWS)* (pp. 1-11). Hertfordshire, Hatfield: ACM.

Kebande, V. R., & Venter, H. S. (2016). Requirements for Achieving Digital Forensic Readiness in the Cloud Environment using an NMB Solution. *11th International Conference on Cyber Warfare and Security* (pp. 1-9). Boston: ACPI.

Kebande, V. R., Karie, N. M., Omeleze, S. (2016). A mobile forensic readiness model aimed at minimising cyber bullying. *International Journal of Computer Applications, 140*(1), 28-33.

Kebande, V. R., Karie, N. M., & Venter, H. S. (2016). A generic Digital Forensic Readiness model for BYOD using honeypot technology. In *Proceedings of IST-Africa Week Conference* (pp. 1-12). Durban, South Africa: IEEE.

Kebande, V. R., Ntsamo, H. S., & Venter, H. S. (2016). Towards a prototype for Achieving Digital Forensic Readiness in the Cloud using a Distributed NMB Solution. *15th European Conference on Cyber Warfare and Security (ECCWS)* (pp. 1-10). Munich: ACM.

Keller, R., & König, C. (2014). A Reference Model to Support Risk Identification in Cloud Networks. *Thirty Fifth International Conference on Information Systems* (pp. 1-19). Auckland: Auckland University of Technology.

Kendrick, R. (2010). *Cyber Risks for Business Professionals: A Management Guide.* Ely, Cambridgeshire: IT Governance.

Kerikmäe, T., & Rull, A. (2016). *The Future of Law and eTechnologies* (1st ed.). Berlin, Germany: Springer.

Kestle, R., & Self, R. (2014). *The Role of IS Assurance & Security Management. IT Practices For SME Success*. Retrieved from https://computing.derby.ac.uk/ojs/index.php/itpsme/article/view/15

Khan, J. Y., & Yuce , M. R. (2010). Wireless Body Area Network (WBAN) for Medical Applications. In D. Campolo, *New Developments in Biomedical Engineering* (pp. 591-628). London: InTech.

Khan, J. Y., Yuce, M. R., Bulge, G., & Harding, B. (2012). Wireless Body Area Network (WBAN) Design Techniques and Performance Evaluation. *Journal of Medical Systems, 36*(3), 1441-1457. doi:10.1007/s10916-010-9605-x

Khan, S., & Pathan, A. K. (2013). Security and privacy in wireless body area networks for health care applications. *Wireless networks and security* (p. 165-187). Berlin: Springer.

Khan, M. (2017). *Understanding Security Risk Concepts*. Retrieved from http://resources.infosecinstitute.com/understanding-security-risk-concepts/

Khan, S., Gani, A., Wahab, A. W., Bagiwa, M. A., Shiraz, M., Khan, S. U., . . . Zomaya, A. Y. (2016). Cloud Log Forensics: Foundations, State of the

Art, and Future Directions. *ACM Computing Surveys (CSUR), 49*(1), 1-44. doi:10.1145/2906149

Khurana, H., Basney, J., Bakht, M., Freemon, M., Welch, V., & Butler, Y. (2009). Palantir: a framework for collaborative incident response and investigation. *8th Symposium on Identity and Trust on the Internet* (pp. 38-51). Gaithersburg, Maryland: ACM.

Kierkegaard, P. (2011). Electronic health record: Wiring Europe's healthcare. *Computer Law & Security Review, 27*(5), 503-515. doi:10.1016/j.clsr.2011.07.013

King, A. L., Feng, L., & Lee, I. (2013). *Assuring the Safety of On-Demand Medical Cyber Physical Systems.* Philadelphia: University of Pennsylvania.

King, T. (2015). *Digital Forensic Readiness.* Birmingham: West Midlands Police.

Kocabas, O., Soyata, T., & Aktas, M. K. (2016). Emerging Security Mechanisms for Medical Cyber Physical Systems. *IEEE/ACM Transactions on Computational Biology and Bioinformatics, 13*(3), 401-416. doi:10.1109/TCBB.2016.2520933

Konstantinou, C., Maniatakos, M., Saqib, F., Hu, S., Plusquellic, J., & Jin, Y. (2015). Cyber-physical systems: A security perspective. *20th IEEE European Test Symposium (ETS)* (pp. 1-8). Cluj-Napoca, Romania: IEEE.

Kostadinov, D. (2017). *Mobile, Smartphone & BYOD*. Retrieved from http://resources.infosecinstitute.com/category/enterprise/securityawareness/mobile-smartphone-and-byod/

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques* (2nd ed.). Delhi: New Age International.

Kouns, J., & Minoli, D. (2010). *Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams.* Hoboken, New Jersey: Wiley.

KPMG. (2017). *Forensic Readiness.* Bern: KPMG.

Krager, D., & Krager, C. (2016). Security rule explained. *HIPAA for health care professionals* (p. 82-108). NY, USA: Delmar, Cengage Learning.

Kramer, D. B., Baker, M., Ransford, B., Molina-Markham, A., Stewart, Q., Fu, K., & Reynolds, M. R. (2012). Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. *PLoS ONE, 7*(7), 1-7. doi:10.1371/journal.pone.0040200

Kumkar, V., Tiwari, A., Tiwari, P., Gupta, A., & Shrawne, S. (2012). Vulnerabilities of wireless security protocols (WEP and WPA2). *International Journal of Advanced Research in Computer Engineering & Technology, 1*(2), 34-38. Retrieved from http://ijarcet.org/

Künzle, B., Kolbe, M., & Grote, G. (2010). Ensuring patient safety through effective leadership behaviour: A literature review. *Safety Science, 48*(1), 1-17. doi:10.1016/j.ssci.2009.06.004

Kurian, J., & Singh, M. (2014). A Framework for Analysing Types of User Information on Social Networking Sites. *25th Australasian Conference on Information Systems* (pp. 1-10). Auckland, New Zealand: Auckland University of Technology.

Kusuda, Y. (2005). A further step beyond wireless capsule endoscopy. *Sensor Review, 25*(4), 259–260.

Kyaw, A. K., & Cusack, B. (2014). Security challenges in pervasive wireless medical systems and devices. In *Proceedings of the 11th International Conference on High-capacity Optical Networks and Emerging/Enabling Technologies (HONET-PfE 2014)*, (pp. 178 – 185). United States of America: IEEE.

Kyaw, A. K., Truong, H. P, & Joseph, J. (2018). Low-Cost Computing Using Raspberry Pi 2 Model B. *Journal of Computers, 13*(3), 287-299. doi:10.17706/jcp.13.3.287-299

Kyaw, A. K., Tian, Z., & Cusack, B. (2016). Wi-Pi: a study of WLAN security in Auckland City. *IJCSNS International Journal of Computer Science and Network Security, 16*(8), 68-80.

Lac, M., Sukunesan, S., Cain, A., Vasa, R., & Mouzakis, K. (2014). Mobile Learning in Corporate Businesses: A review of literature focusing on journal articles. *25th Australasian Conference on Information Systems* (pp. 1-10). Auckland, New Zealand: Auckland University of Technology.

Lalla, H., Flowerday, S., Sanyamahwe, T., & Tarwireyi, P. (2012). A Log File Digital Forensic Model. *8th International Conference on Digital Forensics (DF)* (pp. 247-259). Pretoria, South Africa.: Springer.

Latré, B., Braem, B., Moerman, I., Blondia, C., & Demeester, P. (2011). A survey on wireless body area networks. *Journal of Wireless Networks, 17*(1), 1-18. doi:10.1007/s11276-010-0252-4

Lechner, P., & Gatzert, N. (2018). Determinants and value of enterprise risk management: empirical evidence from Germany. *The European Journal of Finance, 24*(10), 867-887. doi:10.1080/1351847X.2017.1347100

Lee, I., & Sokolsky, O. (2010). Medical Cyber Physical Systems. *47th Design Automation Conference (DAC '10)* (pp. 743-748). Anaheim: ACM.

Lee, I., Sokolsky, O., Chen, S., Hatcliff, J., & Jee, E. (2012). *Challenges and Research Directions in Medical Cyber-Physical Systems.* Philadelphia: University of Pennsylvania.

Lee, J. H., & Pack, S. (2017). *Quality, Reliability, Security and Robustness in Heterogeneous Networks* (1st ed.). Berlin, Germany: Springer.

Lehembre, G. (2005). *Wi-Fi security – WEP, WPA and WPA2.* Warsaw: Hakin9.

Li, C., Raghunathan, A., & Jha, N. K. (2011). Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. *13th IEEE International Conference on e-Health Networking Applications and Services (Healthcom)* (pp. 150-156). Columbia, MO: IEEE.

Li, C., Zhang, M., Raghunathan, A., & Jha, N. K. (2014). Attacking and defending a diabetes therapy system. *Security and Privacy for Implantable Medical Devices*, 175-193. doi:10.1007/978-1-4614-1674-6_8

Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. *IEEE Wireless Communications, 17*(1), 1536-1284. doi:10.1109/MWC.2010.5416350

Li, S., Hu, F., & Li, G. (2011). Advances and challenges in body area network. *Communications in Computer and Information Science, 226*(2011), 58-65. doi:10.1007/978-3-642-23235-0_8

Li, Z., Pan, H., Liu, W., Xu, F., Cao, Z., & Xiong, G. (2017). A network attack forensic platform against HTTP evasive behavior. *The Journal of Supercomputing, 73*(7), 3053-3064. doi:10.1007/s11227-016-1924-3

Liao, Y.-C., & Langweg, H. (2016). Evidential Reasoning for Forensic Readiness. *Journal of Digital Forensics, Security and Law, 11*(1), 37-52. Retrieved from http://ojs.jdfsl.org

Lim, S. R. (2015). Identifying management factors for digital incident responses on Machine-to-Machine services. *Digital Investigation, 14*, 46-52. doi:10.1016/j.diin.2015.07.003

Lim, S., Oh, T. H., Choi, Y. B., & Lakshman, T. (2010). Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring. *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC)* (pp. 327-332). Newport Beach: IEEE.

Lin, C. C., Lee, R. G., & Hsiao, C. C. (2008). A pervasive health monitoring service system based on ubiquitous network technology. *International Journal of Medical Informatics, 77*(7), 461-469. doi:10.1016/j.ijmedinf.2007.08.012

Liolios, C., Doukas, C., Fourlas, G., & Maglogiannis, I. (2010). An overview of body sensor networks in enabling pervasive healthcare and assistive environments. *3rd International Conference on Pervasive Technologies Related to Assistive Environments* (pp. 23-25). New York: ACM.

Liu, C. C., Chang, C. H., Su, M. C., Chu, H. T., & Hung, S. H. (2011). RFID-initiated workflow control to facilitate patient safety and utilization efficiency in operation theatre. *International Journal of Computer*

Methods and Programs in Biomedicine, 104(3), 435-442. doi:10.1016/j.cmpb.2010.08.017

Lloyd. (2015). *SOCIETY & SECURITY: Business Blackout.* Cambridge: University of Cambridge.

LOGalyze. (2012). The LOGalyze installation manual. Retrieved from https://www.logalyze.com/installation-manual/finish/1-documentation/12-logalyze-installation-manual

LogRhythm. (2014). *Automation Suite for NIST Cyber Security Framework.* Boulder, Colorado: LogRhythm.

LogRythm. (2014). *SANS "Top 20" Critical Controls for Cyber Defense.* Singapore: LogRythm.

Loughlin, S., & Williams, J. S. (2011). The Top 10 Medical Device Challenges. *Biomedical Instrumentation & Technology, 45*(2), 98-104. doi:10.2345/0899-8205-45.2.98

Louisot, J.-P., & Ketcham, C. H. (2014). *ERM - Enterprise Risk Management: Issues and Cases.* Hoboken, New Jersey: Wiley.

Iucaskauffman. (2013). *WiFi security: history of insecurities in WEP, WPA and WPA2*. Retrieved from http://security.blogoverflow.com/2013/08/wifi-security-history-of-insecurities-in-wep-wpa-and-wpa2/

Luckett, P., McDonald, J. T., & Glisson, W. B. (2017). Attack-Graph Threat Modeling Assessment of Ambulatory Medical Devices. *50th Hawaii International Conference on System Sciences* (pp. 3648-3657). Waikoloa: Shidler.

Lukyanenko, R., Samuel, B. M., & Parsons, J. (2018). Artifact Sampling: Using Multiple Information Technology Artifacts to Increase Research Rigor. *51st Hawaii International Conference on System Sciences (HICSS 2018)* (pp. 1-10). Hawaii: Urban Center for Computation and Data.

Lun, Y. Z., D'Innocenzo, A., Malavolta, I., & Benedetto, M. D. (2016). *Cyber-Physical Systems Security: a Systematic Mapping Study*. Ithaca: Cornell University Library.

Luthfi, A., & Prayudi, Y. (2015). Process Model of Digital Forensics Readiness Scheme (DFRS) as a Recommendation of Digital Evidence Preservation. *Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec)* (pp. 117-122). Jakarta, Indonesia: IEEE.

Ma, W.-M. (2010). Study on Architecture-Oriented Information Security Risk Assessment Model. *2nd International Confernce Computational Collective Intelligence* (pp. 218-266). Taiwan: Springer.

Macchi,, L., Pietikäinen,, E., Reiman, T., Heikkilä, J., & Ruuhilehto, K. (2011). *Patient safety management: Available models and systems.* Espoo, Finland: VTT Technical Research Centre of Finland.

Maedche, A., Brocke, J. V., & Hevner, A. (2017). *Designing the Digital Transformation.* Berlin, Germany: Springer.

Mahncke, R. J., & Williams, P. A. (2014). Developing and Validating a Healthcare Information Security Governance Framework. *Journal of Health Informatics, 8*(2), 1-13. Retrieved from www.eJHI.net

Mahopo, B., Abdullah, H., & Mujinga, M. (2015). A formal qualitative risk management approach for IT security. *Information Security for South Africa (ISSA)* (pp. 1-8). Johannesburg, South Africa: IEEE.

Maisel, W. H., & Kohno, T. (2010). Improving the security and privacy of implantable medical devices. *New England Journal of Medicine, 362*(13), 1164-1166. doi:10.1056/NEJMp1000745

Makutsoane, M. P., & Leonard, A. (2014). A conceptual framework to determine the digital forensic readiness of a Cloud Service Provider. *Portland International Conference on Management of Engineering & Technology (PICMET)* (pp. 3313-3321). Kanazawa, Japan: IEEE.

Majchrowski, B. (2010, June). Real-time locating systems: Measuring the benefits. *Journal of Material Management in Health Care, 2010*(June), 18-20.

Malasri, K., & Wang, L. (2009). Securing wireless implantable devices for healthcare: Ideas and challenges. *IEEE Communications Magazine, 47*(7), 74-80. doi:10.1109/MCOM.2009.5183475

Maloney, J. (2009). *Security Metrics Roadmap: A Guide for Information Security Professionals.* Santa Fe: The Santa Fe Group.

Marco, L. D., Ferrucci, F., & Kechadi, T. (2014). Reference Architecture for a Cloud Forensic Readiness System. *e-Scripts ICST Transactions on Security and Safety*, 1-9. Retrieved from https://www.insight-centre.org

Marco, L. D., Kechadi, M.-T., & Ferrucci, F. (2013). Cloud Forensic Readiness: Foundations. *International Conference on Digital Forensics and Cyber Crime*, 237-244. doi:10.1007/978-3-319-14289-0_16

Marlabs. (2015). *HITRUST Common Security Framework (CSF) Assessment.* Piscataway, New Jersey: Marlabs.

Martini, B., & Choo, K. K. (2012). An integrated conceptual digital forensic framework for cloud computing. *The International Journal of Digital Forensics & Incident Response, 9*(2), 71-80. doi:10.1016/j.diin.2012.07.001

Maxim Integrated. (2013). *Overview - Infusion pumps*. Retrieved from http://www.maximintegrated.com/solutions/infusion/

Mcelroy, L. M., Woods, D. M., Yanes, A. F., Skaro, A. I., Daud, A., Curtis, T., . . . Ladner, D. P. (2016). Applying the WHO conceptual framework for the International Classification for Patient Safety to a surgical population. *International Journal for Quality in Health Care, 28*(2), 166-174. doi:10.1093/intqhc/mzw001

Meditology Services, & Trend Micro. (2014). *Architecting Security to Address Compliance for Healthcare Providers.* Shibuya, Tokyo: Trend Micro.

Meingast, M., Roosta, T., & Sastry, S. (2006). Security and Privacy Issues with Health Care Information Technology. *28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society* (pp. 5453-5458). New York: IEEE.

Mekhaznia, T., & Zidani, A. (2015). Wi-Fi security analysis. *Procedia Computer Science, 73*, 172-178. doi:10.1016/j.procs.2015.12.009

Ministry of Health (2017). HISO 10064:2017 Health Information Governance Guidelines.

Min, K.-S., Chai, S.-W., & Han, M. (2015). An International Comparative Study on Cyber Security Strategy. *International Journal of Security and Its Applications, 9*(2), 13-20. doi:10.14257/ijsia.2015.9.2.02

Mora, J., & Lueg, L. (2017). Pyrit package description. Retrieved from https://tools.kali.org/wireless-attacks/pyrit

Moramarco, S. (2017). *Phishing and Security Awareness Best Practices for Healthcare*. Retrieved from http://resources.infosecinstitute.com/phishing-security-awareness-best-practices-healthcare/

Mouhtaropoulos, A., Dimotikalis, P., & Li, C. T. (2013). Applying a Digital forensic readiness framework: Three case studies. *IEEE International Conference on Technologies for Homeland Security (HST)* (pp. 217-223). Waltham, MA: IEEE.

Mouhtaropoulos, A., Grobler, M., & Li, C.-T. (2011). Digital Forensic Readiness: An Insight into Governmental and Academic Initiatives. *European Intelligence and Security Informatics Conference (EISIC)* (pp. 191-196). Athens, Greece: IEEE.

Mouhtaropoulos, A., Li, C.-T., & Grobler, M. (2014). Digital Forensic Readiness: Are We There Yet? *Journal of International Commercial Law and Technology, 9*(3), 173-179. Retrieved from http://www.jiclt.com

Mouton, F. (2012). *Digital Forensic Readiness for Wireless Sensor Network Environments.* Pretoria: University of Pretoria.

Mouton, F., & Venter, H. S. (2011). A prototype for achieving digital forensic readiness on wireless sensor networks. *AFRICON* (pp. 1-6). Livingstone, Zambia: IEEE.

Muhammad, S., Furqan, Z., & Guha, R. (2005). Wireless sensor network security: a secure sink node architecture. *24th IEEE International Performance,*

Computing, and Communications Conference (pp. 371-376). Phoenix: IEEE.

Muñoz, J., Alonso, J. V., García, F. Q., Costas, S., Pillado, M., Javier, F., . . . Bravo, C. L. (2013). A Cognitive Mobile BTS Solution with Software-Defined Radioelectric Sensing. *Sensors (Basel), 13*(2), 2051–2075. doi:10.3390/s130202051

Muthu, S. P., & Pavithran, S. (2015). Advanced attack against wireless networks WEP, WPA/WPA2-Personal and WPA/WPA2-Enterprise. *International Journal of Scientific & Technology Research, 4*(8), 147-152. Retrieved from http://www.ijstr.org/

Nakhila, O., Attiah, A., Jinz, Y., & Zou, C. (2015). Parallel active dictionary attack on WPA2-PSK Wi-Fi networks. *IEEE Military Communications Conference* (pp. 665-670). Tampa: IEEE.

Napier, J. (Ed.). (2011). *NICS forensic readiness guidelines* (Version 1.0). http://studyres.com/download/4392801

Natalizio, E., Loscrí, V., & Aloi, G. (2010). The practical experience of implementing a GSM BTS through open software/hardware. *3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL)* (pp. 1-5). Rome, Italy: IEEE.

Newbold, S. K. (2003). New uses for wireless technology. *Nursing Management, 34*, 22-23. Retrieved from http://journals.lww.com/nursingmanagement/pages/default.aspx

Ng, H. S., Sim, M. L., & Tan, C. M. (2006). Security issues of wireless sensor networks in healthcare applications. *BT Technology Journal, 24*(2), 138-144. doi:10.1007/s10550-006-0051-8

Ng, J. W., Lo, B. P., Wells, O., Sloman, M., Peters, N., Darzi, A., . . . Yang, G. Z. (2004). *Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon).* London: Imperial College London.

Ngobeni, S. J., & Venter, H. S. (2009). The Design of a Wireless Forensic Readiness Model (WFRM). *Information Security South Africa Conference* (pp. 1-17). Johannesburg, South Africa: ISSA.

Ngobeni, S., Venter, H., & Burke, I. (2010). A Forensic Readiness Model for Wireless Networks. *IFIP Advances in Information and Communication Technology*, *337*, 107-117. doi:10.1007/978-3-642-15506-2_8

Ngoc, T. V. (2008). *Medical Applications of Wireless Networks.* St. Louis, MO: Washington University in St. Louis.

Niemöller, C., Metzger, D., & Thomas, O. (2017). Design and Evaluation of a Smart-Glasses-based Service Support System. *13th International Conference on Wirtschaftsinformatik* (pp. 106-120). Gallen, Switzerland: AIS Electronic Library.

Nimgaonkar, S., Kotikela, S., & Gomathisankaran, M. (2012). CTrust: A Framework for Secure and Trustworthy Application Execution in Cloud Computing. *International Conference on Cyber Security (CyberSecurity)* (pp. 24-31). Alexandria: IEEE.

Nita, L., Cretu, M., & Hariton, A. (2011). System for remote patient monitoring and data collection with applicability on E-health applications. *7th International Symposium on Advanced Topics in Electrical Engineering (ATEE)* (pp. 1-4). Bucharest, Romania: IEEE.

Nnoli, H., Lindskog, D., Zavarsky, P., Aghili, S., & Ruhl, R. (2012). The Governance of Corporate Forensics Using COBIT, NIST and Increased Automated Forensic Approaches. *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)* (pp. 734-741). Amsterdam, Netherlands: IEEE.

Noman, S. A., Qasaimeh, M., Al-Qassas, R., & Noman, H. A. (2017). Mitigating Evil Twin attacks in wireless 802.11 networks at Jordan. *IJCSI International Journal of Computer Science Issues*, *14*(1), 60-68. doi:10.20943/01201701.6068

Noor, M. M., & Hassan, W. H. (2013). Current Threats of Wireless Networks. *3rd International Conference on Digital Information Processing and Communications* (pp. 704-713). Dubai: Society of Digital Information and Wireless Communications (SDIWC).

Noorzaie, I. (2006). *Survey paper: medical applications of wireless networks*. Retrieved from http://www.cs.wustl.edu/~jain/cse574-06/medical_wireless.htm

Nunamaker, J. F. Jr., Chen, M., and Purdin, T. D. M. (1990). Systems Development in Information Systems Research, *Journal of Management Information Systems, 7*(3), 89-106.

Nyamagwa, M., Liu, J., Liu, A., & Uehara, T. (2014). Cloudforen: A novel framework for digital forensics in cloud computing. *Journal of Harbin Institute Of Technology, 1*(6), 39-45. doi:10.11916/j.issn.1005-9113.2014.06.008

Offensive Security. (2016, November). Kali tools: hostapd-wpe package description. Retrieved from https://tools.kali.org/wireless-attacks/hostapd-wpe

Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009). Outline of a design science research process. *4th International Conference on Design Science Research in Information Systems and Technology* (pp. 1-11). New York: ACM.

Ohigashi, T., & Morii , M. (2009). *A Practical Message Falsification Attack on WPA.* Higashihiroshima: Hiroshima University.

OpenEMR. (2016, May). OpenEMR 4.1.2 users guide. Retrieved from http://www.open-emr.org/wiki/index.php/OpenEMR_4.1.2_Users_Guide

OpenEMR. (2014a). OpenEMR downloads. Retrieved from http://www.open-emr.org/wiki/index.php/OpenEMR_Downloads

OpenEMR. (2014b). OpenEMR 4.1.2 XAMPP package installation. Retrieved from https://www.open-emr.org/wiki/index.php/OpenEMR_4.1.2_XAMPP_Package_Installation

OSSEC. (2019). Getting started with OSSEC. Retrieved from https://ossec-docs.readthedocs.io/en/latest/manual/non-technical-overview.html

Pace, P., & Loscri, V. (2012). OpenBTS: A Step Forward in the Cognitive Direction. *21st International Conference on Computer Communications and Networks (ICCCN)* (pp. 1-6). Munich: IEEE.

Paquette, A. (2011). Design of a pragmatic test lab for evaluating and testing wireless medical devices. *IEEE 37th Annual Northeast Bioengineering Conference (NEBEC)* (pp. 1-2). Troy, New York: IEEE.

Paquette, A., Painter, F., & Jackson, J. L. (2011). Management and risk assessment of wireless medical devices in the hospital. *Journal of Biomedical Instrumentation & Technology, 45*(3), 243-248. doi:10.2345/0899-8205-45.3.243

Parkinson, M. J., & Baker, N. J. (2005). IT and Enterprise Governance. *Information Systems Control Journal, 3*, 1-5. Retrieved from https://www.isaca.org/Journal/archives/Pages/default.aspx

Parlak, S., Sarcevic, A., Marsic, I., & Burd, R. S. (2012). Introducing RFID technology in dynamic and time-critical medical settings. *Journal of Biomedical Informatics, 45*(5), 958-974. doi:10.1016/j.jbi.2012.04.003

Paterson, K. G., Poettering, B., & Schuldt, J. C. (2014). Plaintext recovery attacks against WPA/TKIP. *Fast Software Encryption* (pp. 325-349). Heidelberg: Springer.

Paul, N., & Klonoff, D. C. (2010). *Insulin Pump System Security and Privacy*. Retrieved from https://web.eecs.utk.edu/~pauln/papers/paul-klonoff-healthsec-2010.pdf

Pederson, P. (2014). *A Cost-Efficient Approach to High Cyber Security Assurance in Nuclear Power Plants.* Wilmington: The Langner Group.

Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems, 24*(3), 45-78. doi:10.2753/MIS0742-1222240302

Pescatore, J. (2017). *Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017.* Bethesda: SANS Institute.

Petersen, C., & Bhalotra, S. (2015). *The Cyber-Threat Risk - Oversight Guidance for CEOs and Boards.* Singapore: LogRhythm.

Peters, G. A., & Peters, B. J. (2007). Medical devices. *Medical error and patient safety: Human factors in medicine* (p.59-78). Florida, USA: CRC Press.

Petković, M. (2009). Remote patient monitoring: Information reliability challenges. *9th International Conference on Telecommunication in Modern Satellite, Cable, and Broadcasting Services* (pp. 295-301). Nis, Serbia : IEEE.

Phifer, L. (2003). *WLAN security: Best practices for wireless network security*. Retrieved from http://searchsecurity.techtarget.com/WLAN-security-Best-practices-for-wireless-network-security

Piggin, R. (2017). *Cybersecurity of medical devices: Addressing patient safety and the security of patient health information.* London: BSI Group.

Pironti, J. P. (2005). Key Elements of an Information Security Program. *Information System Control Journal, 1*, 1-6. Retrieved from https://www.isaca.org/Journal/archives/Pages/default.aspx

Pisa, C., Caponi, A., Dargahi, T., Bianchi, G., & Melazzi, N. B. (2016). WI-FAB: attribute-based WLAN access control, without pre-shared keys and backend infrastructures. *8th ACM International Workshop on Hot Topics in Planet-scale mObile computing and online Social neTworking* (pp. 31-36). Paderborn: ACM.

Ponemon Institute. (2015). *2015 Cost of Cyber Crime Study: Global.* Palo Alto, California: Hewlett Packard Enterprise.

Ponemon Institute. (2015). *2015 Cost of Data Breach Study: Global Analysis.* Armonk, New York: IBM.

Ponemon Institute. (2016). *2016 Global Encryption Trends Study.* Plantation, Florida: Thales e-Security.

Ponemon Institute. (2016). *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data.* Traverse City, Michigan: Ponemon Institute.

Popovici, I., Morita, P. P., Doran, D., Lapinsky, S., Morra , D., Shier, A., . . . Cafazzo, J. A. (2015). Technological aspects of hospital communication challenges: an observational study. *International Journal for Quality in Health Care, 27*(3), 183-188. doi:10.1093/intqhc/mzv016

Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2015). A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia. *Computer Network and Information Security, 11*, 1-8. doi:10.5815/ijcnis.2015.11.01

PRIMIS. (2014). *Security and Confidentiality of Practice Data Policy: Statement of compliance and Applications for data access forms.* Nottingham: The University of Nottingham.

Pritchard, C. L. (2014). *Risk Management: Concepts and Guidance* (5th ed.). Boca Raton, Florida: CRC Press.

Privacy Commissioner. (2017). Health information privacy code 1994: Incorporating amendments No 2, No 3, No 4, No 5, No 6, No 7, No 8 and No 9. Retrieved from https://www.privacy.org.nz/assets/Files/Codes-of-Practice-materials/Consolidated-HIPC-current-as-of-28-Sept-17.pdf

Purdy, G. (2010). ISO 31000:2009 - for Risk ManagementSetting a New Standard. *Risk Analysis, 30*(6), 881-886. doi:10.1111/j.1539-6924.2010.01442.x

PwC. (2014). *US cybercrime: Rising risks, reduced readiness Key findings from the 2014 US State of Cybercrime Survey.* London: PWC.

PwC. (2016). *Security Framework: A Guide For Business leaders* . Santa Clara, CA: Palo Alto Networks.

Pyrek, K. M. (2017). *Healthcare Crime: Investigating Abuse, Fraud, and Homicide by Caregivers* (1st ed.). Boca Raton: CRC Press.

Quadri, A. T., Komal, M., & Khalil, Z. (2015). A Comprehensive Study on Risk Analysis and Risk Management in IT Industry. *International Journal of Computer and Communication System Engineering (IJCCSE), 2*(4), 561-568. Retrieved from http://www.ijccse.com

Quinn, S. (2018, January 15). Hospital pays $55,000 ransom; no patient data stolen. *Daily Reporter*. Retrieved from http://www.greenfieldreporter.com/2018/01/16/01162018dr_hancock_health_pays_ransom/

Radcliffe, J. (2011). *Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System.* Las Vegas: Black Hat Security.

Radivilova, T., & Hassan, H. A. (2017). Test for penetration in Wi-Fi network: Attacks on WPA2-PSK and WPA2-enterprise. *International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)* (pp. 1-4). Odessa, Ukraine: IEEE.

Rahman, A. F. A., Ahmad, R., & Ramli, S. N. (2014). In *16th International Conference on Advanced Communication Technology*, Pyeongchang, 2014, pp. 177-180. doi: 10.1109/ICACT.2014.6778944

Rahman, N. H. (2016). An evidence-*based cloud incident handling framework.* Adelaide: University of South Australia.

Rahman, N. H., Cahyani, N. D., & Choo, K. K. (2016). Cloud incident handling and forensic-by-design: cloud storage as a case study. *Concurrency and Computation: Practice and Experience*, 1-16. doi:10.1002/cpe.3868

Rahman, N. H., Glisson, W. B., Yang, Y., & Choo, K. K. (2016). Forensic-by-Design Framework for Cyber-Physical Cloud Systems. *IEEE Cloud Computing, 3*(1), 50-59. doi:10.1109/MCC.2016.5

Rajan, R. D. (2013). Wireless-enabled remote patient monitoring solutions. *Medical Design Technology*. Retrieved from https://www.mdtmag.com/article/2013/05/wireless-enabled-remote-patient-monitoring-solutions

Raju, B. K., & Geethakumari, G. (2016). An advanced forensic readiness model for the cloud environment. *International Conference on Computing, Communication and Automation (ICCCA)* (pp. 765-771). Noida, India: IEEE.

Ramachandran, V. (2011). *Backtrack 5 Wireless Penetration Testing: Beginner's Guide.* Birmingham: Packt Publishing.

Ransford, B., Clark, S. S., Kune, D. F., Fu, K., & Burleson, W. P. (2014). Design challenges for secure implantable medical devices. In W. Burleson, & S. Carrara (Eds.), *Security and Privacy for Implantable Medical Devices* (pp. 157-173). New York: Springer.

Rathore, H., Mohamed, A., Al-Ali, A., Du, X., & Guizani, M. (2017). A review of security challenges, attacks and resolutions for wireless medical devices. *13th International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 1495-1501). Valencia, Spain: IEEE.

Rathore, H., Mohamed, A., Al-Ali, A., Du, X., & Guizani, M. (2017, June). A review of security challenges, attacks and resolutions for wireless medical devices. In *Wireless Communications and Mobile Computing Conference*, 13, 1495-1501. doi:10.1109/IWCMC.2017.7986505

Rebollo, O., Mellado, D., & Fernandez-Medina, E. (2014). ISGcloud: a Security Governance Framework for Cloud Computing. *The Computer Journal Advance Access*, 1-22. doi:10.1093/comjnl/bxu141

Rebollo, O., Mellado, D., & Fernández-Medina, E. (n.d.). A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment. *Journal of Universal Computer Science, 18*(6), 798-815. doi:10.3217/jucs-018-06-0798

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology, 58*, 44-57. doi:10.1016/j.infsof.2014.10.003

Rebollo, O., Mellado, D., Sanchez, L. E., & Fernández-Medina, E. (2011). Comparative Analysis of Information Security Governance Frameworks:

A Public Sector Approach. *11th European Conference on e-Coverment (ECEG'11)* (pp. 1-10). Ljubljani, Slovenia: ECDG.

Reddy, K., & Vehter, H. S. (2013). The architecture of a digital forensic readiness management system. *Computers & Security, 32*, 73-89. doi:10.1016/j.cose.2012.09.008

Reddy, K., & Venter, H. (2009). A Forensic Framework for Handling Information Privacy Incidents. *IFIP International Conference on Digital Forensics* (pp. 143-155). Orlando, Florida: Springer.

Reggiani, M. (2016). *A brief introduction to Forensic Readiness*. Retrieved from http://resources.infosecinstitute.com/a-brief-introduction-to-forensic-readiness/#gref

Reis, A. L., Selva, A. F., Lenzi, K. G., Barbin, S. E., & Meloni, L. G. (2012). Software defined radio on digital communications: A new teaching tool. In Proceedings of the *IEEE 13th Annual Wireless and Microwave Technology Conference (WAMICON)* (pp. 1-8). Cocoa Beach: IEEE.

Ren, Y., Werner, R., Pazzi, N., & Boukerche, A. (2010). Monitoring patients via a secure and mobile healthcare system. *IEEE Wireless Communications, 17*(1), 1536-1284. doi:10.1109/MWC.2010.5416351

Reserve Bank of India. (2011). *Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds.* Mumbai: Reserve Bank of India.

Rimawati, Y., & Sutikno, S. (2016). The assessment of information security management process capability using ISO/IEC 33072:2016 (Case study in Statistics Indonesia). *International Conference on Information Technology Systems and Innovation (ICITSI)* (pp. 1-6). Bandung, Indonesia: IEEE.

Rodrigues, G. A., Albuquerque, R. d., Deus, F. E., Sousa Jr., R. T., Júnior, G. A., Villalba, L. J., & Kim, T.-H. (2017). Cybersecurity and Network Forensics: Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection. *Applied Sciences, 7*(10), 1-29. doi:10.3390/app7101082

Rohin, S., Narasimman, S. L., & Prabhakar, R. (2016). Preclusion of WPS and WPA Attacks Using Anomaly Detection. *International Journal of Advances in Cloud Computing and Computer Science (IJACCCS), 2*(5), 12-17. Retrieved from http://troindia.in/

Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence, 2*(3), 1-28. Retrieved from http://www.ijde.org/

Rozovsky, F., & Woods, J. (Ed.). (2005). *The handbook of patient safety compliance: A practical guide for health care organizations*. CA, USA: Jossey-Bass.

Rushanan, M., Rubin, A. D., Kune, D. F., & Swanson , C. M. (2014). SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. *IEEE Symposium on Security and Privacy* (pp. 524-539). SAN JOSE: IEEE.

Sachowski, J., & Ivtchenko, D. (2016). *Implementing Digital Forensic Readiness* (1st ed.). Amsterdam, Netherlands: Elsevier.

Sagahyroon, A., Aloul, F., Aloul, A. R., Bahrololoum, M. S., Makhsoos, F., & Hussein, N. (2011). Monitoring patients' signs wirelessly. In *1st Middle East Conference on Biomedical Engineering (MECBME)* (pp. 283-286). United States of America: IEEE. doi: 10.1109/MECBME.2011.5752121

Saleem, S., Ullah, S., & Kwak, K. S. (2010). Towards security issues and solutions in Wireless Body Area Networks. In C. Yuan, L. Tsay, F. Wang, F. Ko, J. Zhan, Y. Na, … Y. Sohn (Eds.), *Proceedings of the 6th International Conference on Networked Computing (INC2010)* (pp. 1-4). Gyeongju, South Korea: IEEE.

Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics, 9*(2), 107-118. doi:10.1016/j.aci.2011.05.002

Saleh, S., Alameddine, M., Mourad, Y., & Natafgi, N. (2015). Quality of care in primary health care settings in the Eastern Mediterranean region: a

systematic review of the literature. *International Journal for Quality in Health Care, 27*(2), 79-88. doi:10.1093/intqhc/mzu103

Salman, S. (2017). *COBIT 5 for Risk: Making Sense of IT Risk Management*. Retrieved from http://www.isaca.org/COBIT/focus/Pages/cobit-5-for-risk-making-sense-of-it-risk-management.aspx

Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security challenges for medical devices. Communications of the ACM, 58(4), 74-82. doi:10.1145/2667218

Sandars, J., & Cook, G. (2007). *ABC of patient safety*. Massachusetts, USA: Blackwell Publishing, Inc.

Sari, A., & Karay, M. (2015). Comparative Analysis of Wireless Security Protocols: WEP vs WPA. *International Journal of Communications, Network and System Sciences, 8*, 483-491. doi:10.4236/ijcns.2015.812043

Sasaki , N., Okumura , A., Yamaguchi , N., & Imanaka, Y. (2016). Hospital Information Technology Infrastructure Affects Quality of Care. *International Journal for Quality in Health Care, 28*(1), 62. doi:10.1093/intqhc/mzw104.98

Satti, R. S., & Jafari, F. (2016). Reviewing Existing Forensic Models to Propose a Cyber Forensic Investigation Process Model for Higher Educational Institutes. *International Journal of Computer Network and Information Security(IJCNIS), 5*, 16-24. doi:10.5815/ijcnis.2015.05.03

Scarfone, K., Dicoi, D., Sexton, M., & Tibbs, C. (2008, July). *NIST Special Publication 800-48 Revision 1: Guide to Securing Legacy IEEE 802.11 Wireless Networks*. Gaithersburg, Maryland: National Institute of Standards and Technology.

Schneidewind, N. (2009). Metrics for mitigating cybersecurity threats to networks. *IEEE Internet Computing, 14*(1), 1089-7801. doi:10.1109/MIC.2010.14

Sedlack, D. J. (2016). Understanding Cyber Security Perceptions Related to Information Risk in a Healthcare Setting. *Twenty-second Americas*

Conference on Information Systems (pp. 1-10). San Diego: Association for Information Systems.

Seepers, R. M., Strydis, C., Sourdis, I., & Zeeuw, C. I. (2017). Enhancing Heart-Beat-Based Security for mHealth Applications. *IEEE Journal of Biomedical and Health Informatics , 21*(1), 254-262. doi:10.1109/JBHI.2015.2496151

Sepehrdad, P., Sušil, P., Vaudenay, S., & Vuagnoux, M. (2013). Smashing WEP in a Passive Attack. *Fast Software Encryption (FSE)* (pp. 115-178). Berlin: Springer.

Sepehrdad, P., Susil, P., Vaudenay, S., & Vuagnoux, M. (2015). Tornado attack on RC4 with applications to WEP & WPA. *IACR Cryptology ePrint Archive, 2015*, 1-65. Retrieved from https://www.iacr.org/newsletter/v17n1/eprint.html

Sfar, A. R., Natalizio, E., Challal, Y., & Chtouroua, Z. (2017). A Roadmap for Security Challenges in Internet of Things. *Digital Communications and Networks*, 1-31. doi:10.1016/j.dcan.2017.04.003

Shakeel, I. (2017). *Top 5 Free Intrusion Detection Tools for Enterprise Network*. Retrieved from http://resources.infosecinstitute.com/top-5-free-intrusion-detection-tools-enterprise-network/

Shared Assessments. (2010). *Evaluating Cloud Risk for the Enterprise: A Shared Assessments Guide.* Santa Fe: The Santa Fe Group.

Shayan, J., Azarnik, A., Chuprat, S., Karamizadeh, S., & Alizadeh, M. (2013). Identifying Benefits and Risks Associated with Utilizing Cloud Computing. *The International Journal of Soft Computing and Software Engineering [JSCSE], 3*(3), 416-421. doi:10.7321/jscse.v3.n3.63

Sitnikova, E., & Asgarkhani, M. (2014). A strategic framework for managing internet security. *11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)* (pp. 947-955). Xiamen, China: IEEE.

Slay, J., & Turnbull, B. (2006). The need for a technical approach to digital forensic evidence collection for wireless technologies. *IEEE Information Assurance Workshop* (pp. 124-132). West Point: IEEE.

Slane, B. (1994). New Zealand Health Information Privacy Code. Retrieved from https://www.privacy.org.nz/

Smith, B., Austin, A., Brown, M., King, J. T., Lankford, J., Meneely, A., & Williams, L. (2010). Challenges for protecting the privacy of health information: required certification can leave common vulnerabilities undetected. In *SPIMACS '10 Proceedings of the second annual workshop on Security and privacy in medical and home-care systems* (pp. 1-12). Chicago: ACM.

Snare. (2014). Snare agents. Retrieved from https://www.snaresolutions.com/products/snare-agents/

Söderholm, P., & Karim, R. (2010). An Enterprise Risk Management framework for evaluation of eMaintenance. *1st international workshop and congress on eMaintenance* (pp. 133-140). Luleå, Sweden: Scandinavia's northernmost University of Technology.

Sokolsky, O., Lee, I., & Heimdahl, M. (2011). *Challenges in the Regulatory Approval of Medical Cyber-Physical Systems.* Philadelphia: University of Pennsylvania.

Sommer, P. (2012). *Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations Security Advisers and Lawyers.* Swindon: Assurance Advisory Council (IAAC).

Song, Y., & Pang, Y. (2014). How to Manage Cloud Risks Based on the BMIS Model. *Journal of Information Processing Systems, 10,* 132-144. doi:10.3745/JIPS.2014.10.1.132

Sopra Group, & Napier, J. (2011). *NICS Forensics Readiness Guidelines.* Belfast: Commission for Victims and Survivors.

Splunk. (2016). Get started Splunk Enterprise. Retrieved from https://www.splunk.com/en_us/download/splunk-enterprise.html

Stošić, L., & Bogdanović, M. (2012). RC4 stream cipher and possible attacks on WEP. *International Journal of Advanced Computer Science and Applications (IJACSA), 3*(3), 110-114. doi:10.14569/IJACSA.2012.030319

Stubblefield, A., Ioannidis, J., & Rubin, A. D. (2004). A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). *ACM Transactions on Information and System Security (TISSEC), 7*(2), 319-332 . doi:10.1145/996943.996948

Sule, D. (2014). Importance of Forensic Readiness. *ISACA Journal, 1*(2014), 1-5. Retrieved from https://www.isaca.org/Journal/archives/2014/Volume-1/Pages/JOnline-Importance-of-Forensic-Readiness.aspx

Swedberg, C. (2015). GS1 US Survey Finds Strong RFID Adoption. *RFID Journal*, 1-4. Retrieved from http://www.rfidjournal.com/articles/view?12837

Swedberg, C. (2015). North York General Hospital Uses RFID to Restock Medication Trays. *RFID Journal*, 1-3. Retrieved from http://www.rfidjournal.com/

Tata Consultancy Services. (2012). *Telecommunication Networks: Security Management.* Mumbai: Tata Consultancy Services.

TechAmerica Foundation. (2011). *Cloud First Buyer's Guide for Government.* Washington, D.C: TechAmerica Foundation.

TechTarget. (2016). *Security Wake-Up Call: Cyber Attacks Ring Alarm Bells.* Singapore: TechTarget.

Tedesco, D., Hernandez-Boussard, T., Carretta, E., Rucci, P., Rolli, M., Denia, P. D., . . . Fantini, M. P. (2016). Evaluating patient safety indicators in orthopedic surgery between Italy and the USA. *International Journal for Quality in Health Care, 28*(4), 486-491. doi:10.1093/intqhc/mzw053

Tews, E., & Beck, M. (2009). Practical attacks against WEP and WPA. In *ACM Proceedings of Conference on Wireless Network Security* (pp. 79-86). Zurich: ACM. doi:10.1145/1514274.1514286

Thamilarasu, G. (2016). iDetect: an intelligent intrusion detection system for wireless body area networks. *International Journal of Security and Networks, 11*(1/2), 89-93. doi:10.1504/IJSN.2016.075074

The National Archives. (2011). *Digital Continuity to Support Forensic Readiness.* Richmond: The National Archives.

The National Science Foundation. (2012). *Wireless sensors: from medicine to motion*. Retrieved from http://www.nsf.gov/news/special_reports/liberty/03_technology_02.jsp

Theoharidou, M., Papanikolaou, N., Pearson, S., & Gritzalis, D. (2013). Privacy Risk, Security, Accountability in the Cloud. *IEEE International Conference on Cloud Computing Technology and Science* (pp. 177-184). Washington, DC: ACM.

Thitchener, K., & Herco, F. (2016). Speaking Up for Patient Safety Survey. *International Journal for Quality in Health Care, 28*(1), 50. doi:10.1093/intqhc/mzw104.78

Thorpe, S., Ray, I., & Grandison, T. (2013). *A Synchronized Log Cloud Forensic Framework.* Fort Collins: Colorado State University.

Todo, Y., Ozawa, Y., Ohigashi, T., & Morii, M. (2012). Falsification attacks against WPA-TKIP in a realistic environment. *IEICE Transactions on Information and Systems*, *E95-D*(2), 588-595. doi:10.1587/transinf.E95.D.588

Tomcsanyi, D. P., & Lueg, L. (2010). *Taking a different approach to attack WPA2-AES, or the born of the CCMP known-plain-text attack*. Retrieved from https://www.hwsw.hu/kepek/hirek/2011/05/wpa2aes_ccmp_known_plaintext.pdf

Topol, E. J. (2011). The digital wireless revolution: wireless devices and their applications in healthcare. *Futurescan 2011: Healthcare trends and implication 2010-2016*, 37-42. Retrieved from https://www.acfas.org/FutureScan/

Toreini, P., & Morana, S. (2017). Designing attention-aware business intelligence and analytics dashboards. *12th International Conference on Design Science Research in Information Systems and Technology* (pp. 64-72). Karlsruhe, Germany: Karlsruher Institut für Technologie (KIT).

Troshani, I., Rampersad, G., & Wickramasinghe, N. (2011). On Cloud Nine? An Integrative Risk Management Framework for Cloud Computing. *24th Bled eConference - eFuture: Creating Solutions for the Individual, Organisations and Society* (pp. 15-26). Bled: Bled eCommerce Conference.

Tsitroulis, A., Lampoudis, D., & Tsekleves, E. (2014). Exposing WPA2 security protocol vulnerabilities. *International Journal of Information and Computer Security, 6*(1), 93-107. doi:10.1504/IJICS.2014.059797

Tu, M., Xu, D., Butler, E., & Schwartz, A. (2012). Forensic Evidence Identification and Modeling for Attacks against a Simulated Online Business Information System. *Journal of Digital Forensics, Security and Law, 7*(4), 73-98. doi:10.15394/jdfsl.2012.1134

Turab, N., Aljawarneh, S., & Masadeh, S. (2010). A study of secure deployment of wireless technology in the medical fields. In *ISWSA '10 Proceedings of the 1st International Conference on Intelligent Semantic Web-Services and Applications* (pp. 1-4). New York: ACM.

Tzeng, S., Chen, W., & Pai, F. (2008). Evaluating the business value of RFID: evidence from five case studies. *International Journal of Production Economics, 11*(2), 601-613. doi:10.1016/j.ijpe.2007.05.009

Ullah, S., Higgins, H., Braem, B., Latré, B., Blondia, C., Moerman, I., . . . Kwak, K. S. (2012). A Comprehensive Survey of Wireless Body Area Networks. *Journal of Medical Systems, 36*(3), 1065-1094. doi:10.1007/s10916-010-9571-3

US Health & Human Services. (2010). *Guidance on Risk Analysis Requirements under the HIPAA Security Rule.* Washington, D.C.: US Health & Human Services.

Valero, M., Jung, S. S., Uluagac, A. S., Li, Y., & Beyah, R. (2012). Di-Sec: A distributed security framework for heterogeneous Wireless Sensor Networks. *IEEE INFOCOM* (pp. 585-593). Orlando: IEEE.

Van Beuzekom, M., Boer, F., Akerboom, S., & Hudson, P. (2012). Patient safety in the operating room: An intervention study on latent risk factors. *BMC Surgery, 12*(1), 10.

Van Staden, F. R., & Venter, H. S. (2014). *Implementing Digital Forensic Readiness for Cloud Computing Using Performance Monitoring Tools.* Pretoria: University of Pretoria.

Vanhoef, M., & Piessens, F. (2013). Practical verification of WPA-TKIP vulnerabilities. *8th ACM SIGSAC symposium on Information, computer and communications security* (pp. 427-436). Hangzhou, China: ACM.

Vanhoef, M., & Piessens, F. (2014). *Advanced Wi-Fi attacks using commodity hardware.* Leuven, Belgium: Departement Computerwetenschappen - KU Leuven.

Vanhoef, M., & Piessens, F. (2017). Key reinstallation attacks: Forcing nonce reuse in WPA2. *ACM SIGSAC Conference on Computer and Communications Security* (pp. 1313-1328). Dallas: ACM.

Vanhoef, M., & Ronen, E. (2019). *Dragonblood: A security analysis of WPA3's SAE handshake* (2019/383). Retrieved from Cryptology ePrint Archive website: https://eprint.iacr.org/2019/383

Varshney, U. (2003). Pervasive healthcare. *IEEE Computers, 36*(12), 138-140. doi:10.1109/MC.2003.1250897

Varshney, U. (2007). Pervasive healthcare and wireless health monitoring. *Journal of Mobile Networks and Applications, 12*(2-3), 113-127. doi:10.1007/s11036-007-0017-1

Vassis, D., Belsis, P., Skourlas, C., & Pantziou, G. (2010). Providing advanced remote medical treatment services through pervasive environments. *Journal of Personal and Ubiquitous Computing, 14*(6), 563-537. doi:10.1007/s00779-009-0273-0

Vegh, L., & Miclea, L. (2015). Improving the Security of a Cyber-Physical System using Cryptography, Steganography and Digital Signatures. *International Journal of Computer and Information Technology, 4*(2), 427-434. Retrieved from https://www.ijcit.com/

Veltsos, C. (2011). *Security and attacks in wireless sensor networks.* Hershey, Pennsylvania: IGI Global.

Venable, J. R. (2010). Design Science Research Post Hevner et al: Criteria, Standards, Guidelines, and Expectations. *nternational Conference on Design Science Research in Information Systems* (pp. 109-123). St. Gallen, Switzerland: Springer.

Viehböck, S. (2011). *Brute forcing Wi-Fi Protected Setup*. Retrieved from https://packetstorm.foofus.com/papers/wireless/viehboeck_wps.pdf

Vincent, C., & Williams, J. (2011). *Clinical Risk Management: Enhancing Patient Safety* (2nd ed.). London: BMJ Books.

Virginio , L. A., & Ricarte, I. L. (2015). Identification of Patient Safety Risks Associated with Electronic Health Records: A Software Quality Perspective. *MEDINFO 2015: eHealth-enabled Health, 216*, 55-59. doi:10.3233/978-1-61499-564-7-55

Vohradsky, D. (2012). *Cloud Risk—10 Principles and a Framework*. Retrieved from https://www.isaca.org/Journal/archives/2012/Volume-5/Pages/Cloud-Risk-10-Principles-and-a-Framework-for-Assessment.aspx

Wagner, T., Lindstadt, C., Jeon, Y., & Mackert, M. (2016). Implantable Medical Device Website Efficacy in Informing Consumers Weighing Benefits/Risks of Health Care Options. *Journal of Health Communication, 21*(2), 121-126. doi:10.1080/10810730.2016.1201173

Wake, T. (2012). *Security is not a tool and your tools are not security*. Mold: Halkyn Consulting.

Wake, T. (2015). *Security Essentials for the Small – Medium Business.* Mold: Halkyn Consulting.

Wake, T. (2015). *Security Risk Management - an Introduction*. Retrieved from http://www.halkynconsulting.co.uk/security-resources/downloads/risk_management_developing_framework.pdf

Waliullah, M., & Gan, D. (2014). Wireless LAN Security Threats & Vulnerabilities: A Literature Review. *International Journal of Advanced Computer Science and Applications (IJACSA), 5*(1), 176-183. Retrieved from http://thesai.org/Publications/IJACSA

Waliullah, M., Moniruzzaman, A. B., & Rahman, M. S. (2015). An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network. *International Journal of Future Generation Communication and Networking*, *8*(1), 9-18. doi:10.14257/ijfgcn.2015.8.1.02

Wang, S., Zhang, X., Zhang, Y., Wang, L., Yang, J., & Wang, W. (2017). A Survey on Mobile Edge Networks: Convergence of Computing, Caching and Communications. *IEEE Access, 5*, 6757-6779. doi:10.1109/ACCESS.2017.2685434

Wang, Y., Jin, Z., & Zhao, X. (2010). Practical Defense against WEP and WPA-PSK Attack for WLAN. *6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)* (pp. 1-4). Chengdu, China: IEEE.

Wara, Y. M., & Singh, D. (2015). A Guide to Establishing Computer Security Incident Response Team (CSIRT) For National Research and Education Network (NREN). *African Journal of Computing & ICT, 8*(2), 1-9. Retrieved from www.ajocict.net

Watfa, M. K., & Safa, H. (2009). Security in wireless LANs. In Y. Zhang, L. T. Yang & J. Ma (Eds.), *Unlicensed mobile access technology: protocols, architecture, security, standards and applications* (pp. 207-227). Milton Park, United States of America: Auerbach Publications, Taylor & Francis Group.

White, D., & de Villiers, I. (2016). The MANA toolkit. Retrieved from https://github.com/sensepost/mana

White, D., & de Villiers, I. (2014, August). *Manna from heaven: Improving the state of wireless rogue AP attacks*. Speech presented at the DEF CON 22, Las Vegas, United States of America. Abstract retrieved from https://www.defcon.org/html/defcon-22/dc-22-speakers.html#DWhite

Wi-Fi Alliance. (2018, January). Wi-Fi® introduces security enhancements. Retrieved from https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements

Williams, M. G. (2015). A Risk Assessment on Raspberry PI using NIST Standards. *International Journal of Computer Science and Network Security (IJCSNS), 15*(6), 22-30. Retrieved from http://paper.ijcsns.org

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Medical Devices: Evidence and Research, 8*, 305-316.

Witters, D. (2011). Wireless medical systems: Risks, challenges, and opportunities. *Journal of Biomedical Instrumentation & Technology: Managing Medical Devices on the IT Network, 45*(s), 45-52. doi:10.2345/0899-8205-45.s2.49

Wójtowicz, S., & Belka, R. (2014). Analysis of selected methods for the recovery of encrypted WEP key. *SPIE Proceedings, 9290*(92902Z), 1-7. doi:10.1117/12.2075251

Wu, F., & Eagles, S. (2016). Cybersecurity for Medical Device Manufacturers: Ensuring Safety and Functionality. *Biomedical Instrumentation & Technology, 50*, 23-34. doi:10.2345/0899-8205-50.1.23

Yang, T. A., & Zahur, Y. (2004). Wireless LAN security and laboratory designs. *The Journal of Computing Sciences in Colleges, 19*(3), 44-60. Retrieved from https://www.ccsc.org/publications/

Yao, L., Liu, B., Wu, G., Yao, K., & Wang, J. (2011). A biometric key establishment protocol for body area networks. *International Journal of Distributed Sensor Networks, 2011*, 1-10. doi:10.1155/2011/282986

Yaseen, M., Saleema, K., Orgund, M. A., Derhab, A., Abbas, H., Al-Muhtadi, J., . . . Rashid, I. (2017). Secure Sensors Data Acquisition and Communication

Protection in eHealthcare: Review on State of the Art. *Telematics and Informatics*, 1-27. doi:10.1016/j.tele.2017.08.005

Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks, 52*(2008). doi:10.1016/j.comnet.2008.04.002

Yoe, C. (2011). *Principles of Risk Analysis: Decision Making Under Uncertainty* (1st ed.). Boca Raton, Florida: CRC Press.

Younis, O., & Moayeri, N. (2016). Cyber-physical systems: A framework for dynamic traffic light control at road intersections. *IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1-6). Doha, Qatar: IEEE.

Youngberg, B. J. (Ed.). (2010). Enterprise risk management: The impact on healthcare organizations. *Principles of risk management and patient safety* (p. 115-134). Massachusetts, USA: Jones & Bartlett Publishers.

Yuce, M. R., & Khan, J. Y. (2012). *Wireless body area networks: Technology, implementation, and applications.* Danvers, United States of America: Pan Stanford Publishing.

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & Alvarenga, S. C. (2016). A Survey of Intrusion Detection in Internet of Things. *Journal of Network and Computer Applications*, 1-46. doi:10.1016/j.jnca.2017.02.009

Zeadally, S., Isaac, J. T., & Baig, Z. (2016). Security attacks and solutions in electronic health (E-health) systems. *Journal of Medical Systems*, *40*(263), 1-12. doi:10.1007/s10916-016-0597-z

Zhang, J., Duong, T. Q., Woods, R., & Marshall, A. (2017). Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview. *Entropy*, *19*, 1-16. doi:10.3390/e19080420

Zhang, J., Johnson,, T. R., Patel, V. L., Paige, D. L., & Kubose, T. (2003). Using usability heuristics to evaluate patient safety of medical devices. *Journal of Biomedical Informatics, 36*(2003), 23-30. doi:10.1016/S1532-0464(03)00060-1

Zhang, Z., Wang, H., Vasilakos, A. V., & Fang, H. (2012). ECG-Cryptography and Authentication in Body Area Networks. *IEEE Transactions on Information Technology in Biomedicine, 16*(6), 1070-1078. doi:10.1109/TITB.2012.2206115

Zheng, G., Shankaran, R., Orgun, M. A., Qiao, L., & Saleem, K. (2017). Ideas and challenges for securing wireless implantable medical devices: A review. *IEEE Sensors Journal, 17*(3), 562-576. doi: 10.1109/JSEN.2016.2633973

Zheng, G., Zhang, G., Yang, W., Valli, C., Shankaran, R., & Orgun, M. A. (2017, September). From WannaCry to WannaDie: Security trade-offs and design for implantable medical devices. In *Communications and Information Technologies (ISCIT), 17*, 1-5.

Zhong, F., & Rohde, M. E. (2014). Cloud Computing and ERP: A Framework of Promises and Challenges. *25th Australasian Conference on Information Systems* (pp. 1-10). Auckland, New Zealand: Auckland University of Technology.

Zimmerman, R., Christoffersen, E., Shaver, J., & Smith, T. (2006). A framework for local accountability for patient safety. *Healthcare Quarterly, 9*, 65-68.

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE, 104*(9), 1727-1765. doi:10.1109/JPROC.2016.2558521

Zurawski, J. (2015). *Cybersecurity: Protecting Against Things that go "bump" in the Net*. Retrieved from http://docplayer.net/8283926-Cybersecurity-protecting-against-things-that-go-bump-in-the-net.html

APPENDIX A

ETHICS EXCEPTIOIN

EXCEPTIONS TO ACTIVITIES REQUIRING AUTEC APPROVAL

The following activities do not require AUTEC approval:

6.7. Where a professional or expert opinion is sought, except where this is part of a study of the profession or area of expertise.

-

See more detail at:
http://www.aut.ac.nz/researchethics/guidelines-and-procedures/exceptions-to-activities-requiring-autec-approval-6

APPENDIX B

Pilot Study

The local area network (LAN) topology diagram of a pilot study consists of different Syslog and Microsoft Windows servers, and OpenEMR as shown in Figure B1.

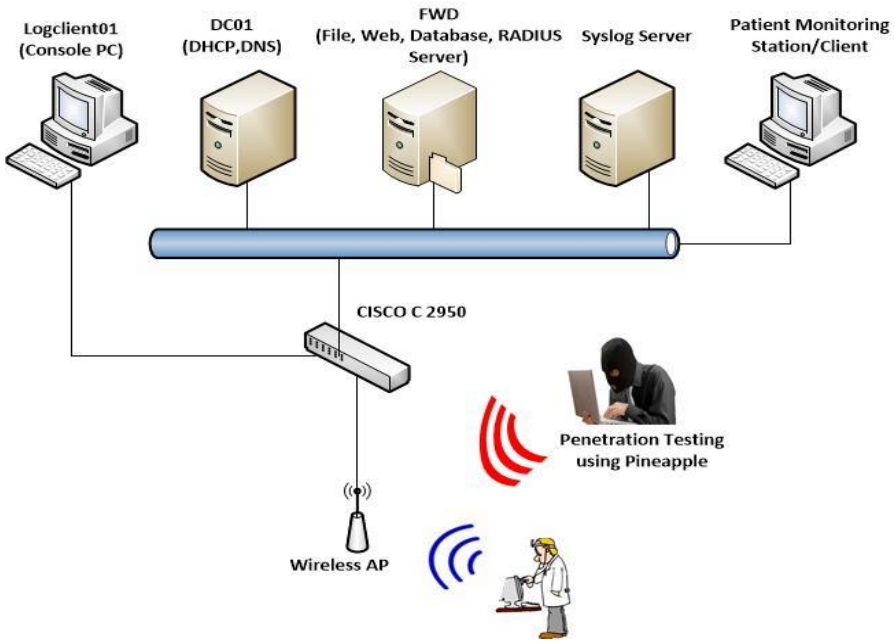


Figure B1: Network topology diagram

Table B1: Internet Protocol (IP) Addressing Scheme

Network	172.16.50.0/24
IP address Range	172.16.50.1 to 172.16.50.255
Broadcast Address	172.16.50.255
Usable IP Address Range	172.16.50.1 to 172.16.50.254
Subnet mask	255.255.255.0
Gateway IP Address	172.16.50.254

Table B2: Host Details

Service	IP Address	Computer-Name
Active Directory Domain Services (ADDS)	172.16.50.1/24	DC01
Domain Name System (DNS) Server	172.16.50.1/24	DC01
Dynamic Host Configuration Protocol (DHCP) Server	172.16.50.1/24	DC01
File Server	172.16.50.2/24	FWD
Remote Authentication Dial-In User Service (RADIUS) Server	172.16.50.2/24	FWD
Web Server	172.16.50.2/24	FWD
Wireless Access Point	172.16.50.4/24	TEST-91
XAMPP Web Host	172.16.50.5/24	Logclient01
Syslog server- LOGalyze	172.16.50.12/24	Logsrv01
Syslog Server- Snare Backlog	172.16.50.12/24	Logsrv02
Syslog Server- rsyslog	172.16.50.13/24	Logsrv04

Appendix B1: Configuring logging on CISCO Catalyst Switch

To enable logging on the CISCO switch, *logging x.x.x.x* (where x.x.x.x is the IPv4 address of the syslog server) command is applied from the global configuration mode. Then, the commands such as *logging buffered size* and *logging trap debugging* are used to set the maximum buffer size of 16384 bytes and force the switch to send debugging trap to the syslog server (IP address: 172.16.5.12), respectively (Figure A1.1).

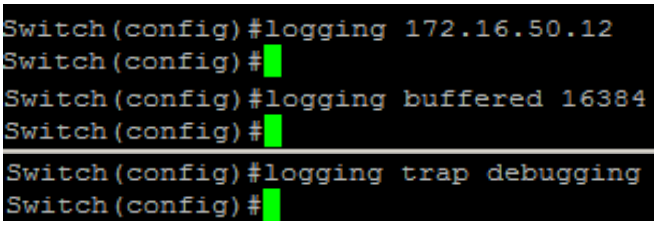


Figure B1.1: Logging configuration on the switch

Appendix B2: Configuring port spanning or mirroring on CISCO Catalyst Switch 2950

To capture the network traffic passing through a CISCO switch, the port spanning (also referred to as port mirroring or monitoring) needs to be enabled on a live port used during communication. Hence, the following commands are used to enable port spanning.

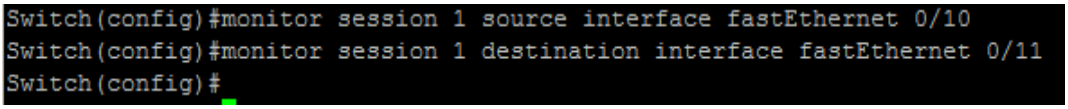


Figure B2.1: Enabling port spanning on the switch

Note: LAN cable from the WAP is connected to the source port and the monitoring PC running the Wireshark application should be connected to the destination port.

Appendix B3: Installing and configuring AD DS and DNS on Server 2008 R2

Active Directory Domain Services (AD DS) is installed on a member that runs Windows Server 2008 R2 server (IP address: 172.16.50.1) by using the Active Directory Domain Services Installation Wizard (dcpromo.exe). After installing AD DS successfully, the member server becomes the primary domain controller (DC01).

Installation Procedure

(i) Run dcpromo.exe, and then click OK.

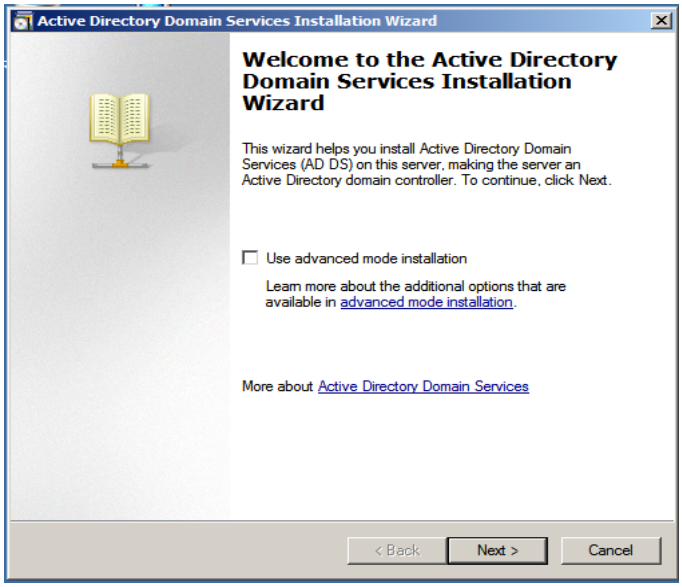


Figure B3.1: AD DS installation wizard

(ii) On the "Choose a Deployment Configuration" page, select "create a new domain in a new forest".

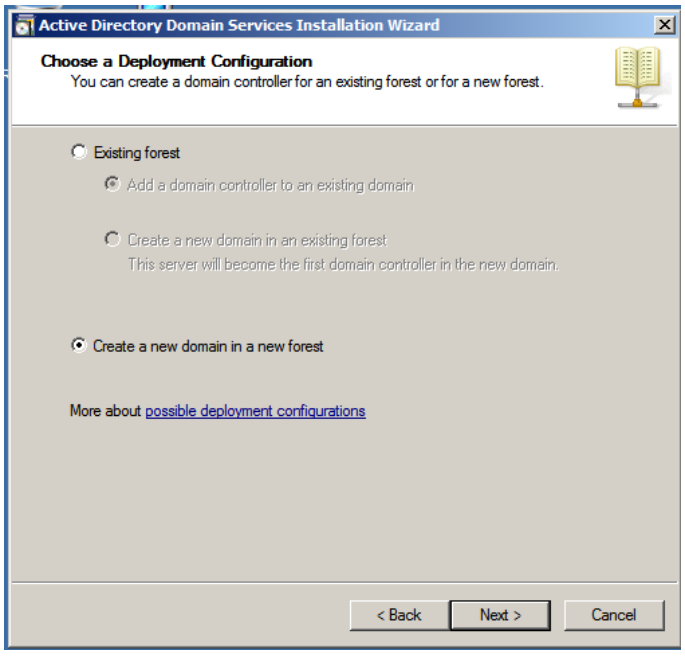


Figure B3.2: Choosing deployment configuration option

(iii) On the "Name the Forest Root Domain" page (Figure B3.3), provide a fully qualified domain name (test.com) for a new forest.

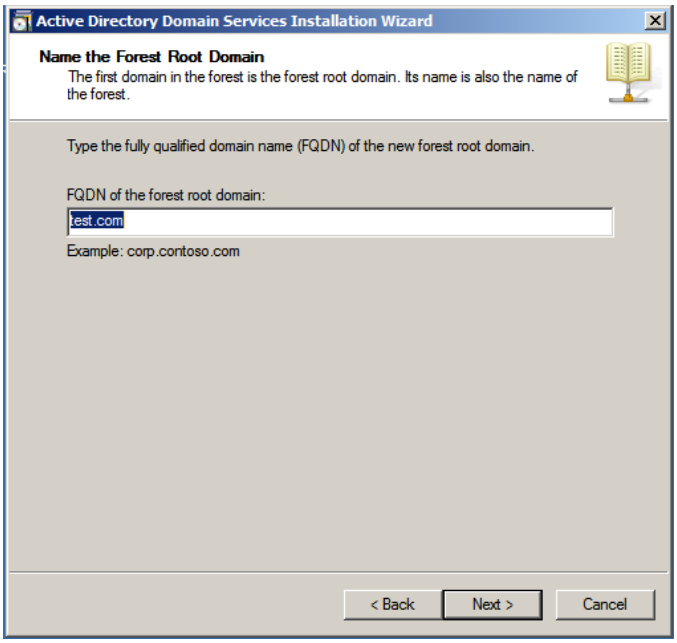


Figure B3.3: Naming test.com as the forest root domain

(iv) Then, Windows Server 2008 R2 is selected for the "Forest Functional Level".

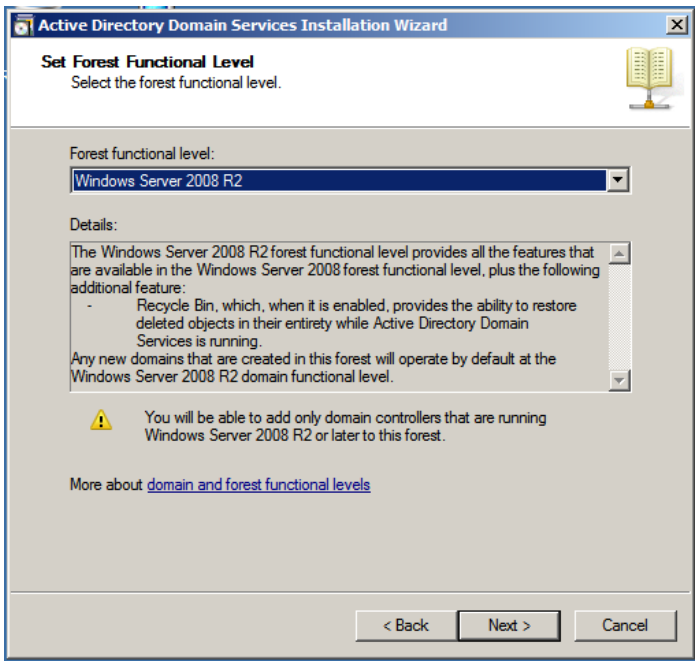


Figure B3.4: Selecting Windows Server 2008 R2 as the forest functional level

(v) On the "Additional Domain Controller Option" page, select DNS server as an additional option for the Domain Controller (DC01). The Global Catalog will be auto selected as the first DC in forest must have a Global Catalog.

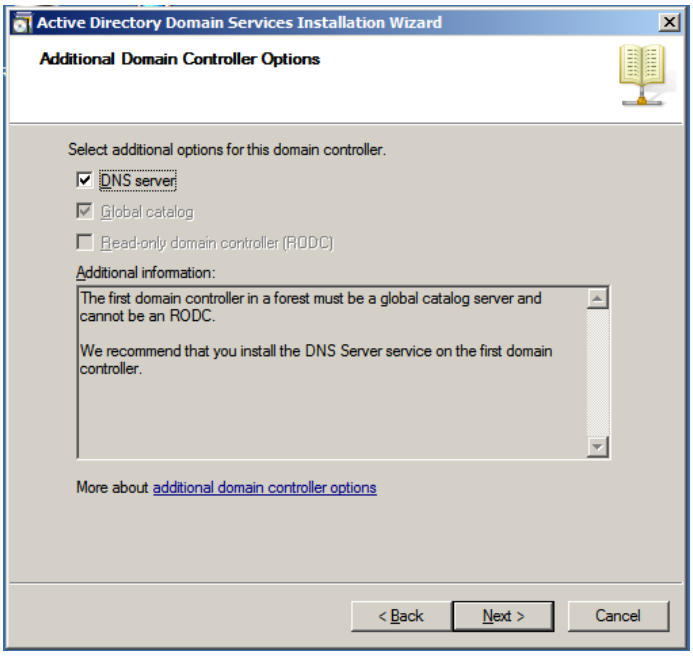


Figure B3.5: Installing DNS Server on Windows Server 2008 R2

(vi) On the "**Location for Database, Log Files, and SYSVOL"** page, type or browse to the volume and folder locations for the database, log files, and SYSVOL files, and then click **Next**.

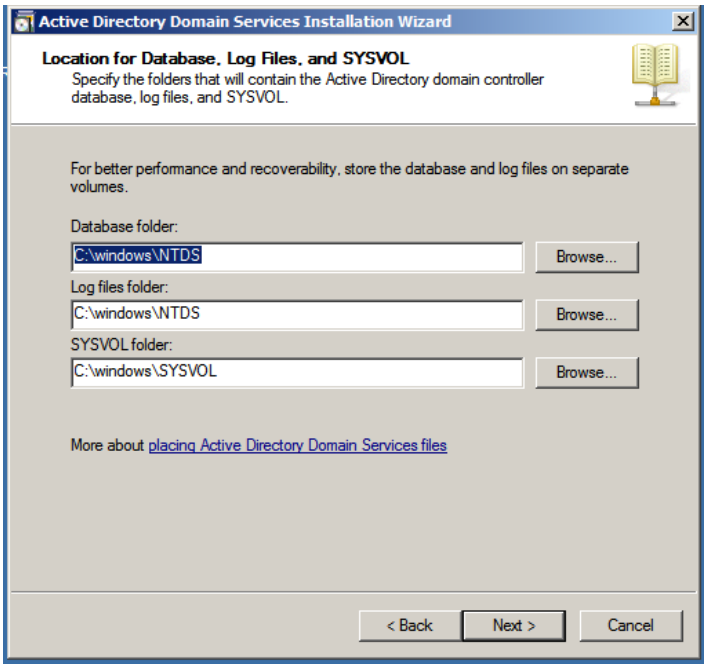


Figure B3.6: Choosing locations for database, log files and SYSVOL folders

(vii) On the **"Directory Services Restore Mode Administrator Password"** page, type and confirm the restore mode password.

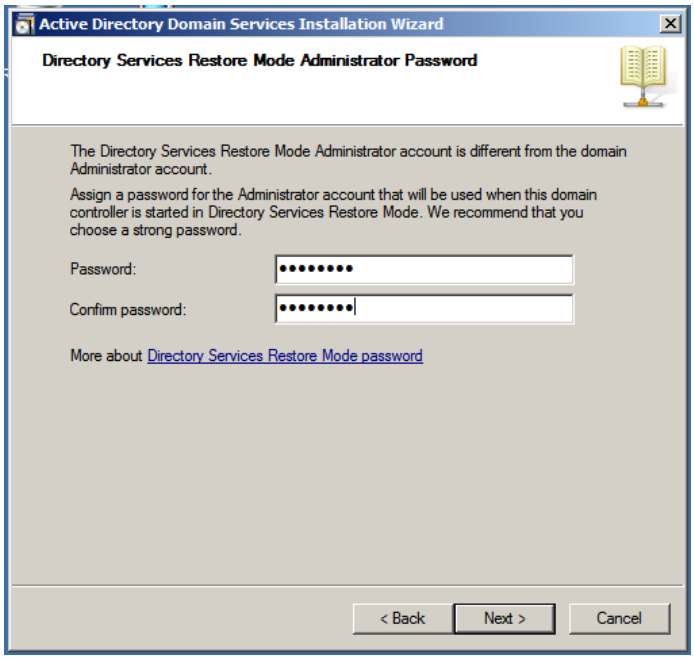


Figure B3.7: Setting up an administrator password for DS restore Mode

(viii) On the "Summary" page, review the installation selections. After ensuring the selections, click ***Next*** and ***Finish*** to install AD DS and DNS.

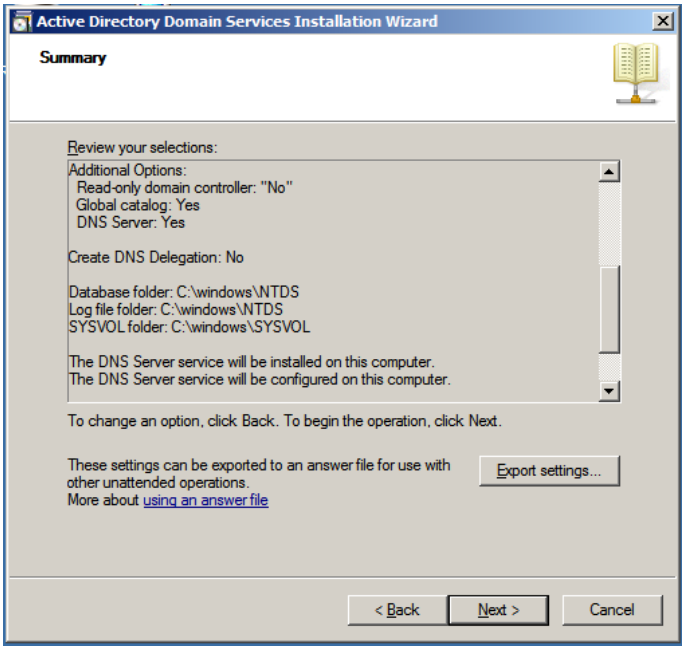


Figure B3.8: Installation summary page

Figure B3.9: Completing AD DS installation wizard

Appendix B4: Installing and configuring DHCP server on DC01

(i) To install DHCP service on DC01, open the Server Manager and right click on roles, and then select add roles.

(ii) Afterwards, select the DHCP Server role to be installed.

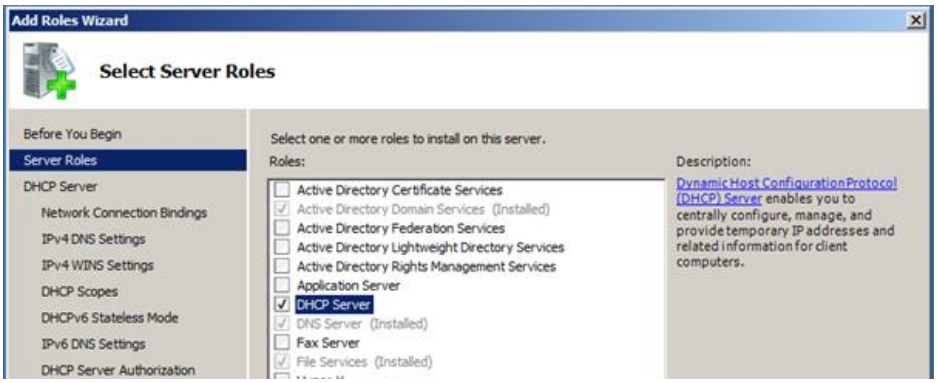


Figure B4.1: Selecting DHCP Server role

(iii) Select the DC's IP address (172.16.50.1) for the network connection binding that can be used to service DHCP clients within the LAN.

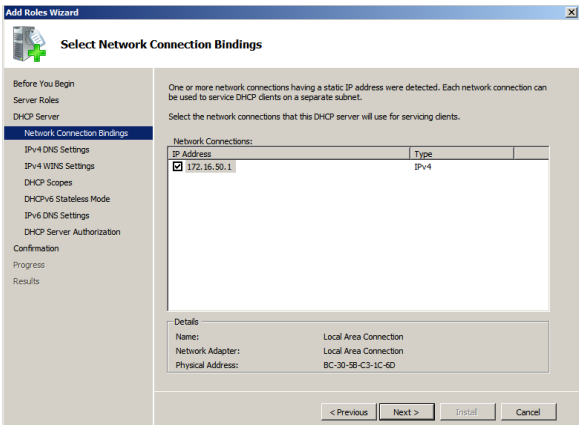


Figure B4.2: Selecting DC's IP address for network connection binding

(iv) DC's IP address is also chosen as a preferred DNS server IP address.

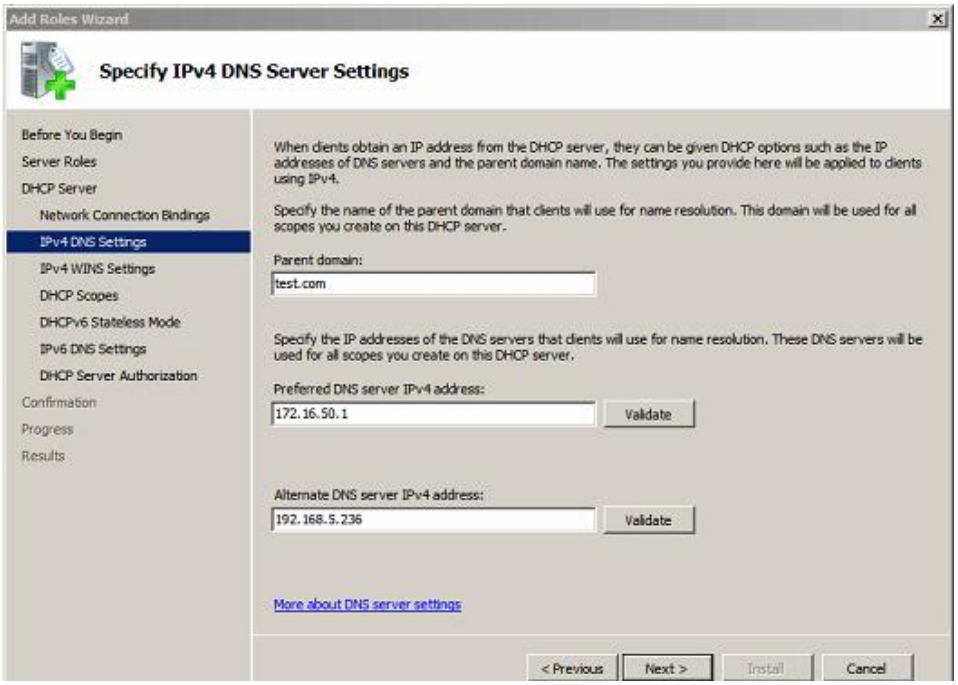


Figure B4.3: Specifying DC's IP address as the preferred DNS server IP address

(v) Click ***Next*** to skip the WINS setup and configure settings for DHCP server (as shown in Figure B4.4) after creating a DHCP Scope by clicking on the ***Add*** button.

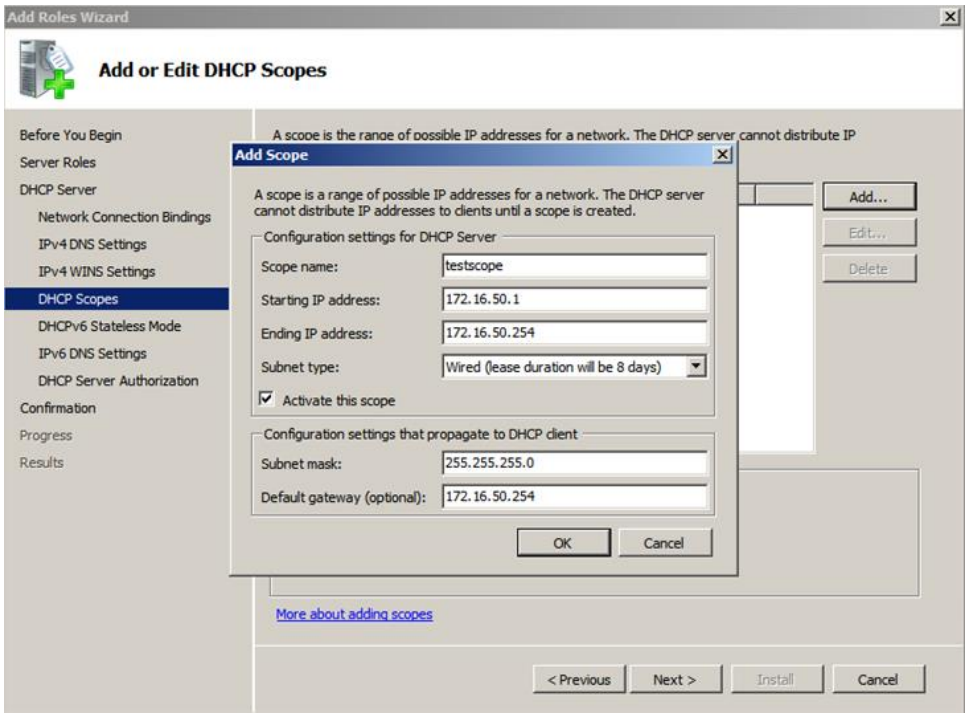


Figure B4.4: Configuring settings for DHCP server

(vi) Then, select the option to disable DHCP stateless mode for this server.

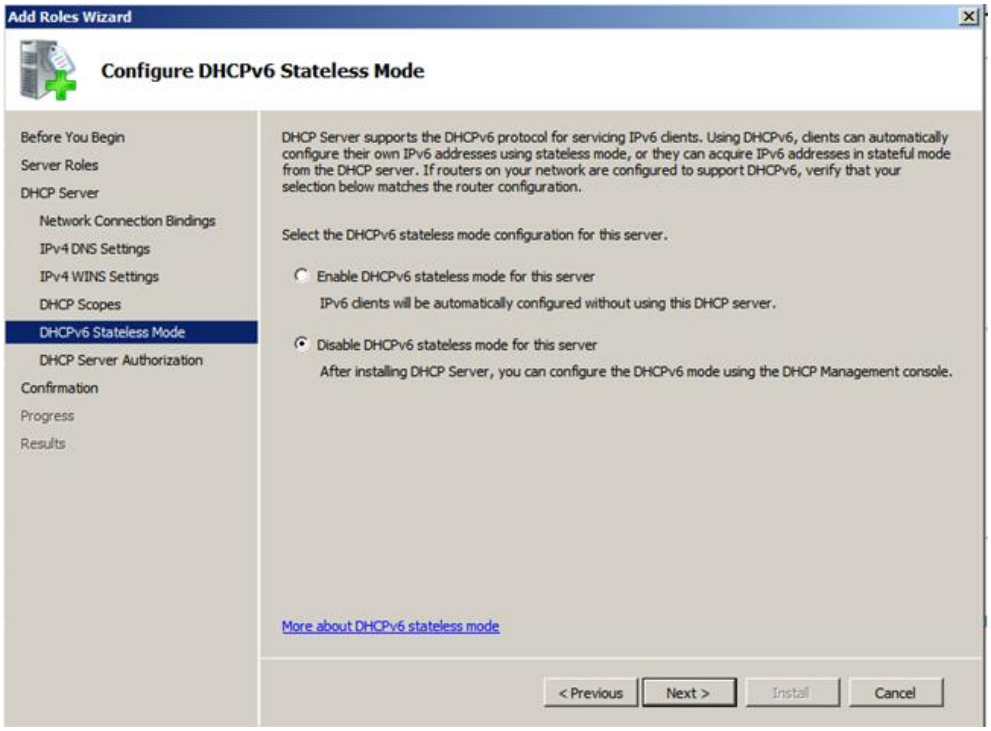


Figure B4.5: Configuring DHCPv6 stateless mode

(vii) On the "Authorise DHCP Server" page, the user credentials should be specified to authorise this DHCP server in AD DS (Figure B4.6).

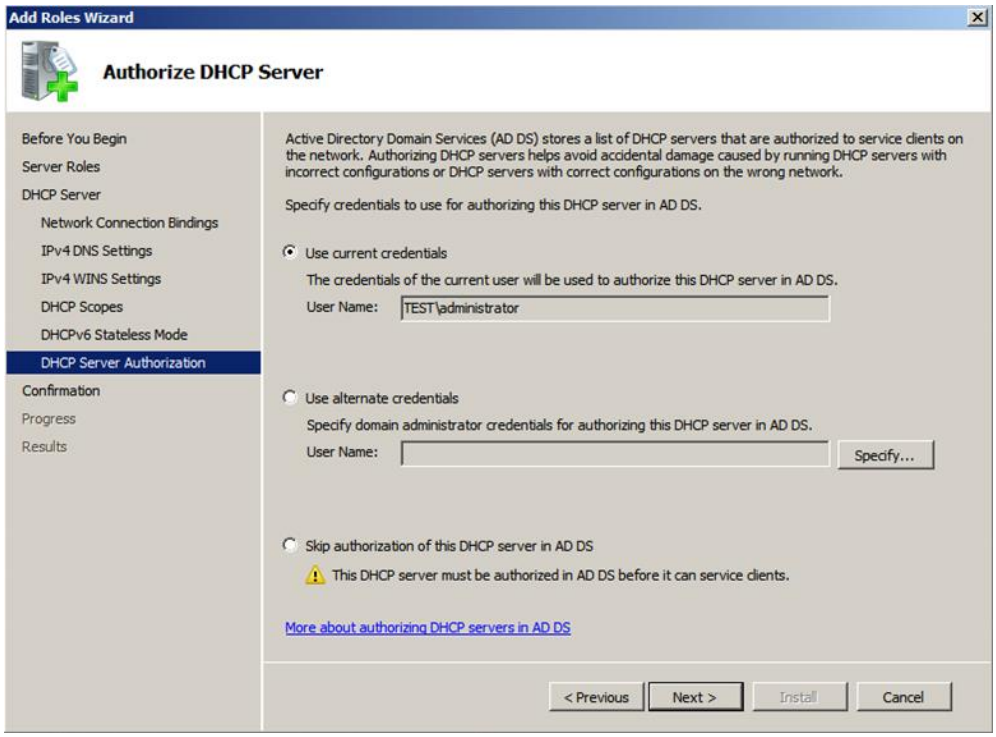


Figure B4.6: Specifying the current user for DHCP server authorisation

(viii) On the "Confirm Installation Selections" page, click on ***Install*** button to start installation of DHCP server on DC01 after confirming installation selections (Figure A4.7). Once the installation is completed without errors, the result for DHCP server installation can be seen as the "installation succeeded" (Figure B4.8).

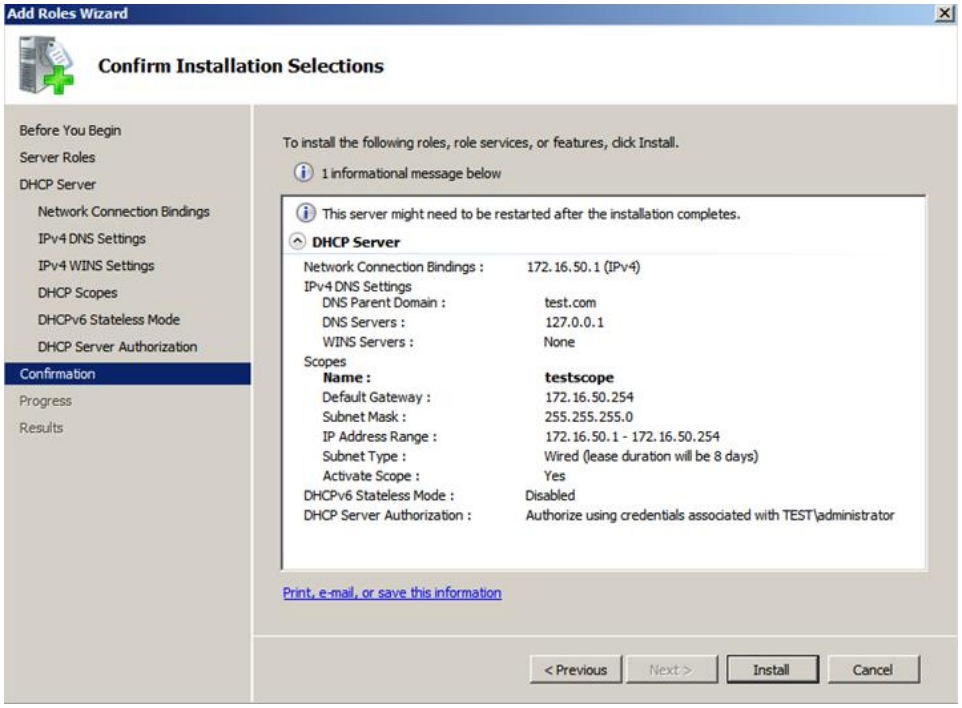


Figure B4.7: Details of DHCP server

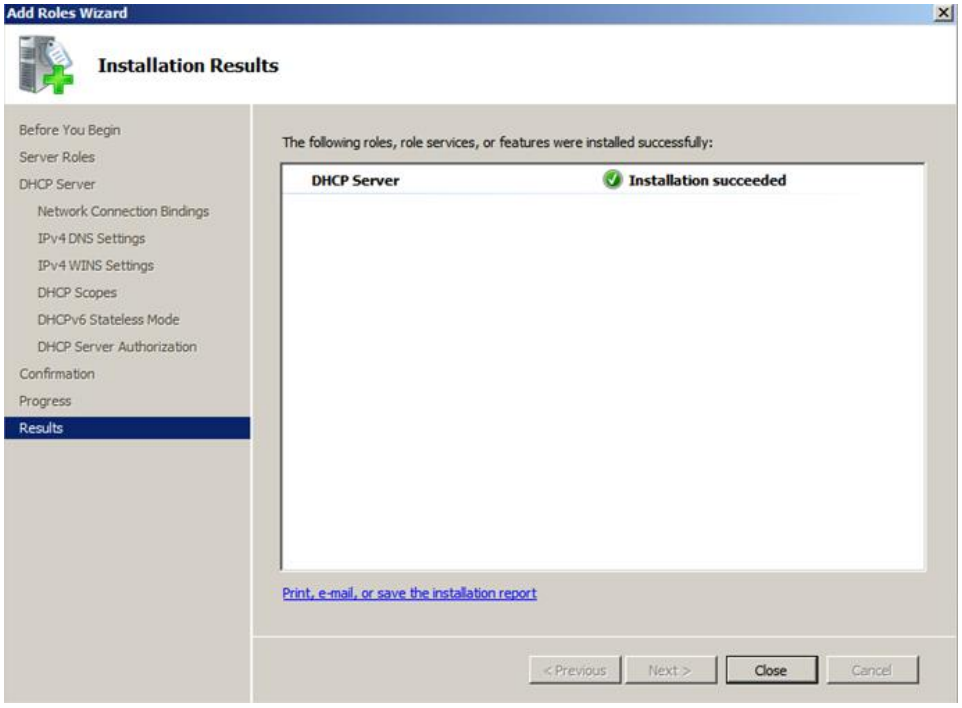


Figure B4.8: DHCP installation result

Appendix B5: Installing Network Policy and Access Services Server on Microsoft Server 2008 R2

(i) First go to "Server Manager" and click on "Add Roles" to select Network Policy and Access Services (NPAS) under the "Server Roles".

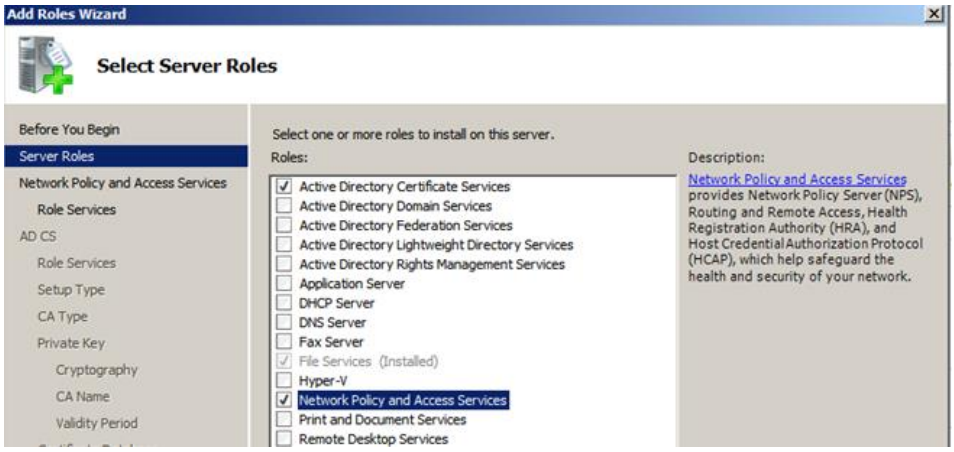


Figure B5.1: Selecting NPAS server role

(ii) Web Server (IIS) role service is installed for Host Credential Authorisation Protocol or HCAP (Figure B5.2) by clicking "Add Required Role Services" and then click on ***Next*** button.

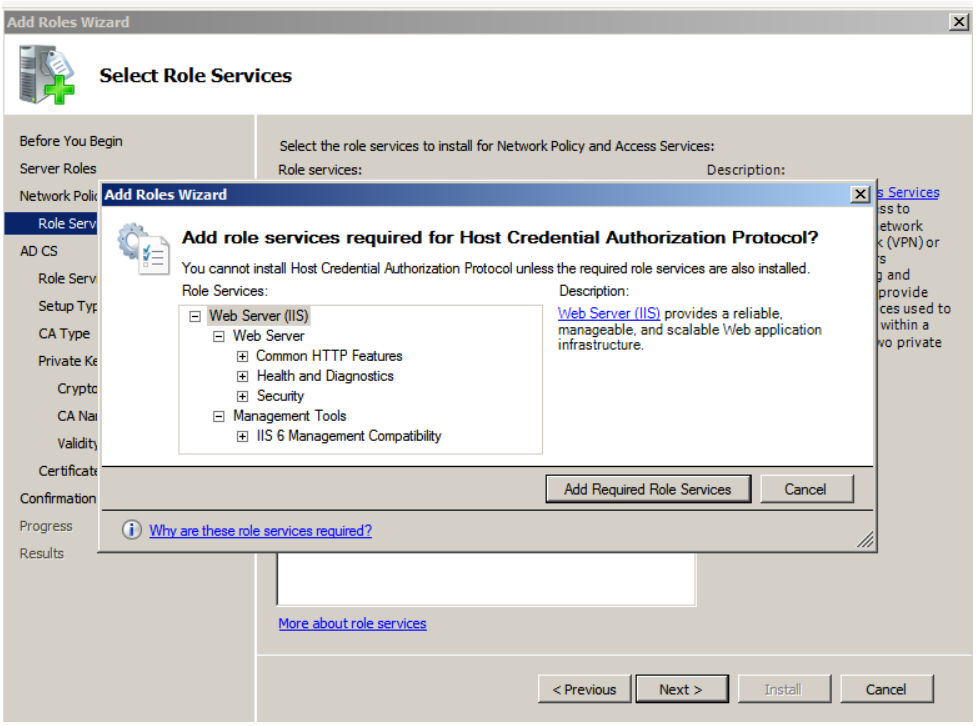


Figure B5.2: Installing IIS

(iii) On the "Select Server Roles" page, check Network Policy and Access Services.

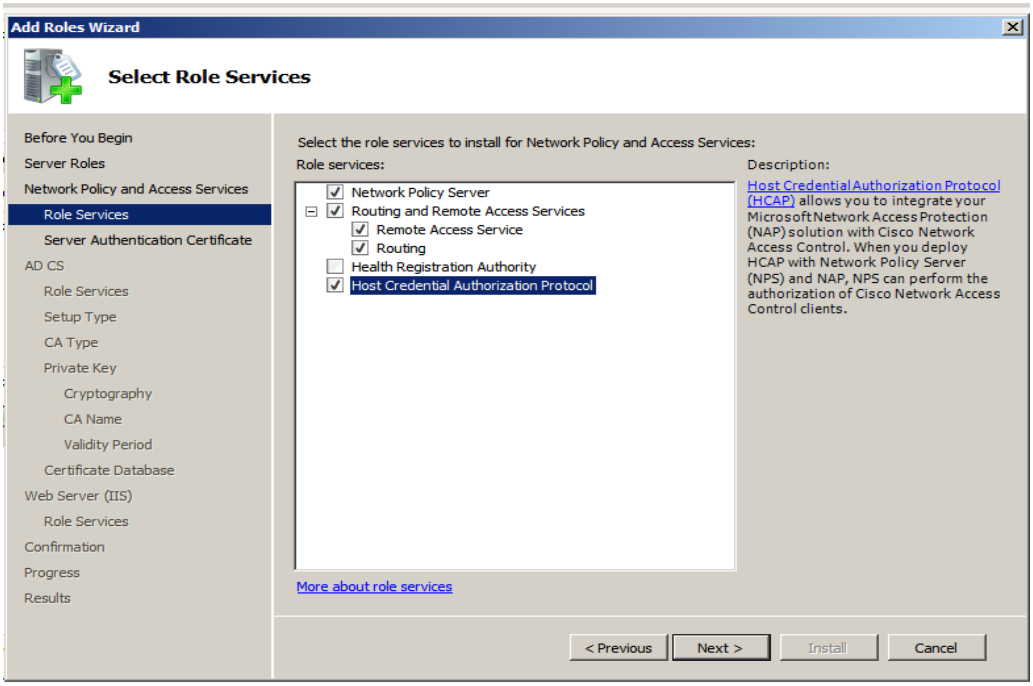


Figure B5.3: Selecting HCAP

(iv) On the "Choose a Server Authentication Certificate for SSL Encryption" page, select the radio button "Create a self-signed certificate for SSL encryption".

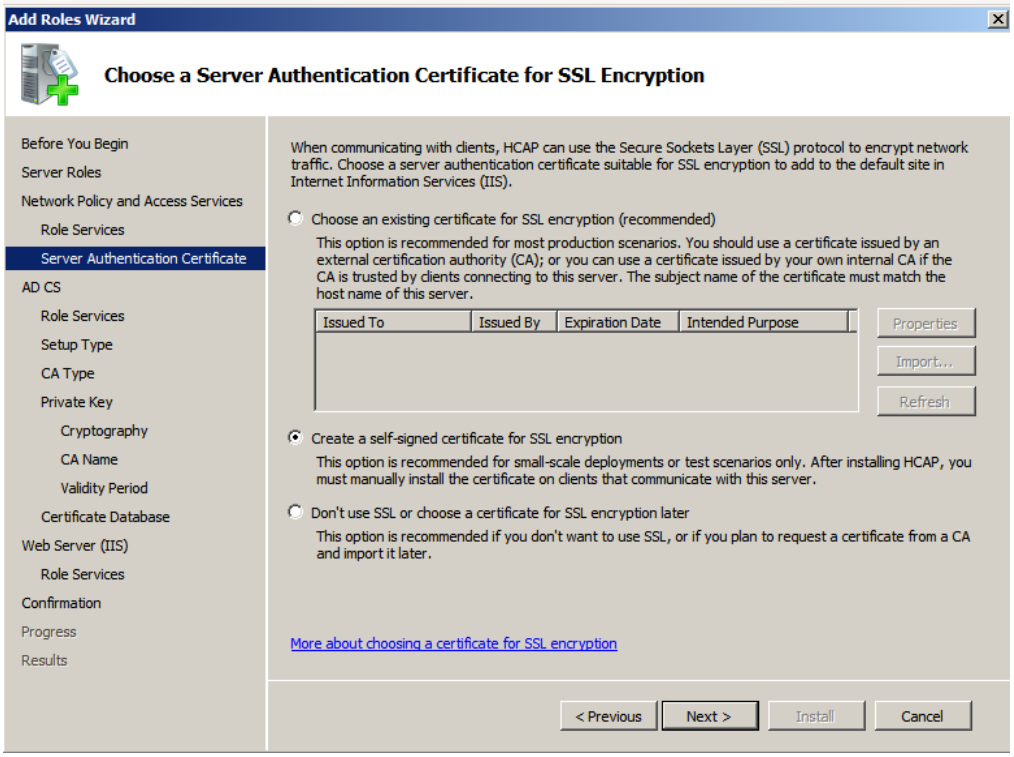


Figure B5.4: Creating a server authentication certificate

(v) On the “Introduction to Active Directory Certificate Services” page, the system will prompt an information about Active Directory Certificate Services and then click ***Next*** to proceed further.

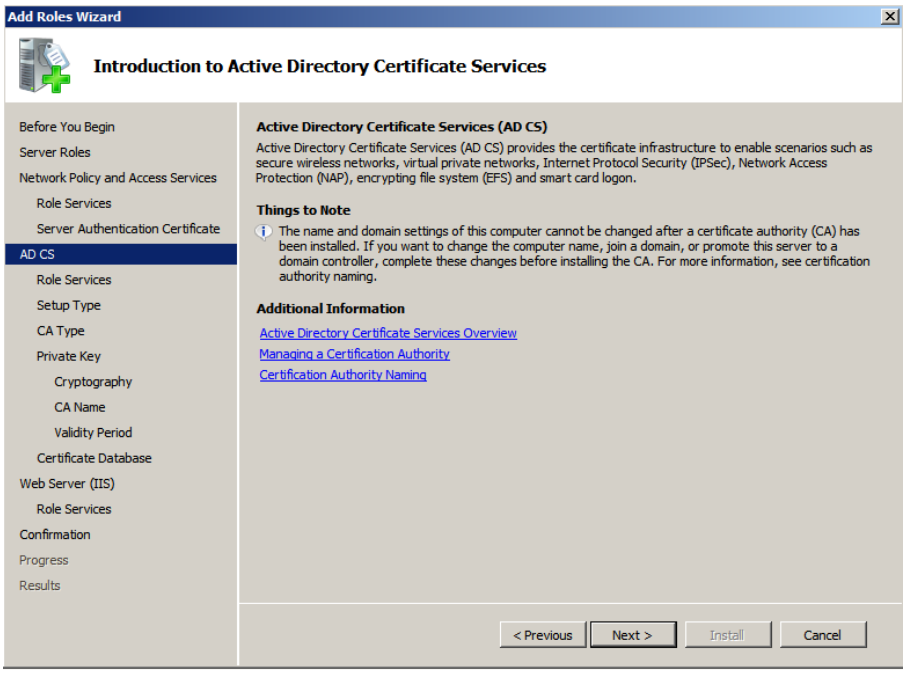


Figure B5.5: ADCS certificate

(vi) On the “Active Directory Certificate Services: Role Service” page, select the “Certification Authority (CA)” role service, which will help to issue and manage certificate.

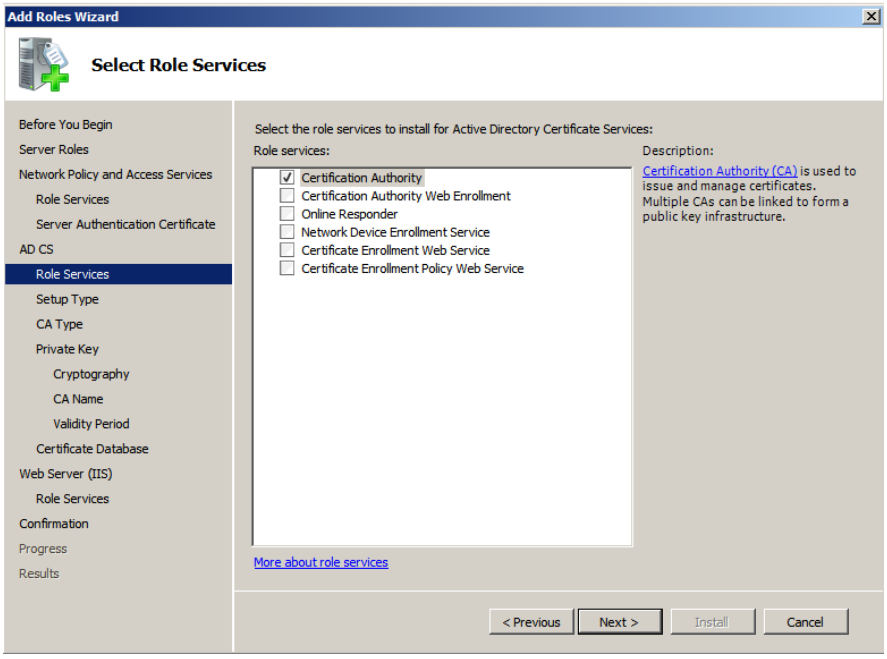


Figure B5.6: Selecting CA role service

(vii) On the “Specify Setup Type” page, check radio button “Standalone” to enable CA to issue or manage certificates without use of Directory Service.

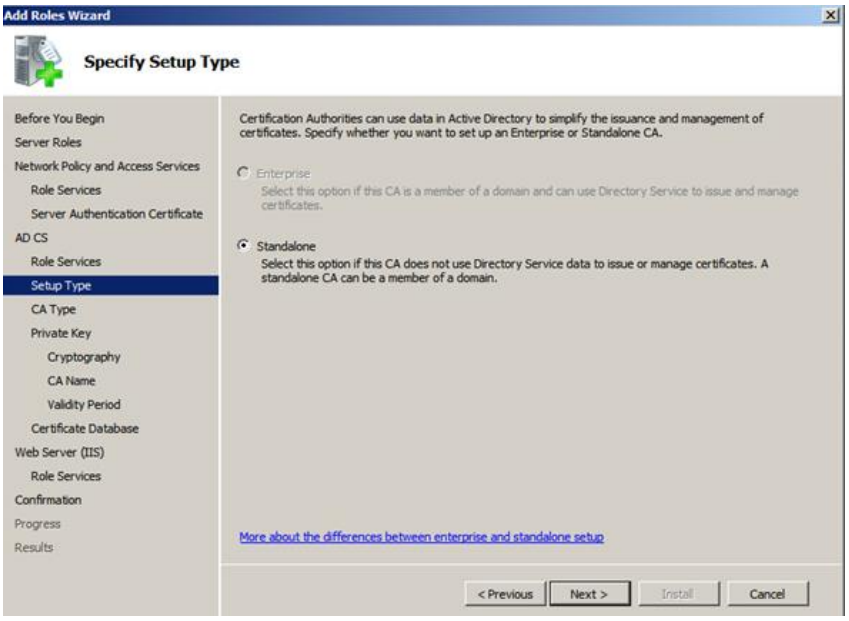


Figure B5.7: Selecting the setup type as a Standalone CA

(viii) Then, “Root CA” is selected to specify CA type, as we are installing the first and only certification authority in a public key infrastructure. Then click on ***Next*** button.

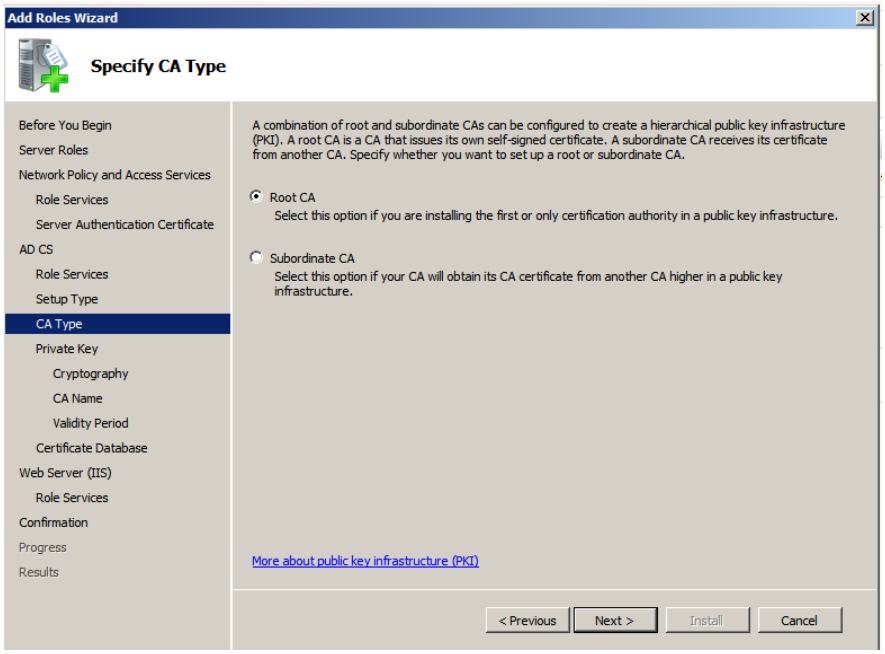


Figure B5.8: Selecting Root CA

(ix) On the “Private Key” page, select “Create a new private key” for generating and issuing certificates to clients.

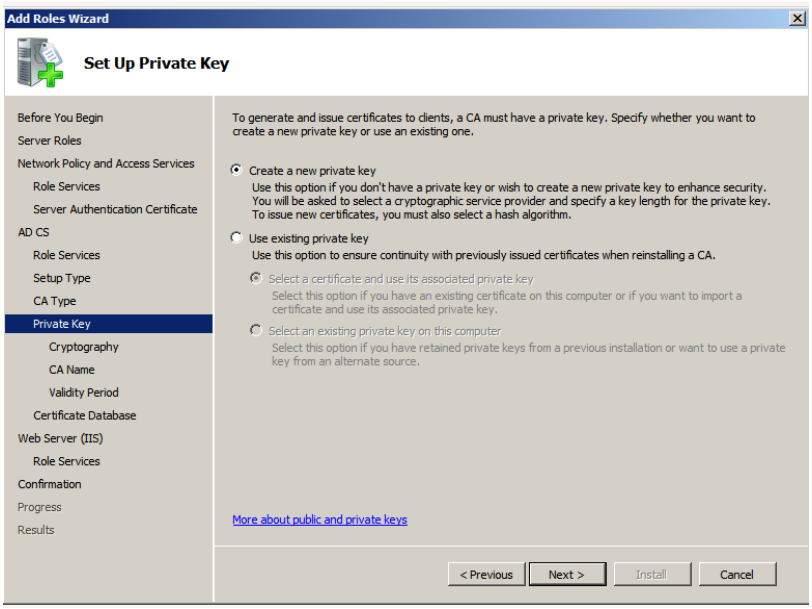


Figure B5.9: Setting up a new private key

(x) Then, configure a cryptographic service provider (CSP), hash algorithm and key character length as shown in Figure B5.10.

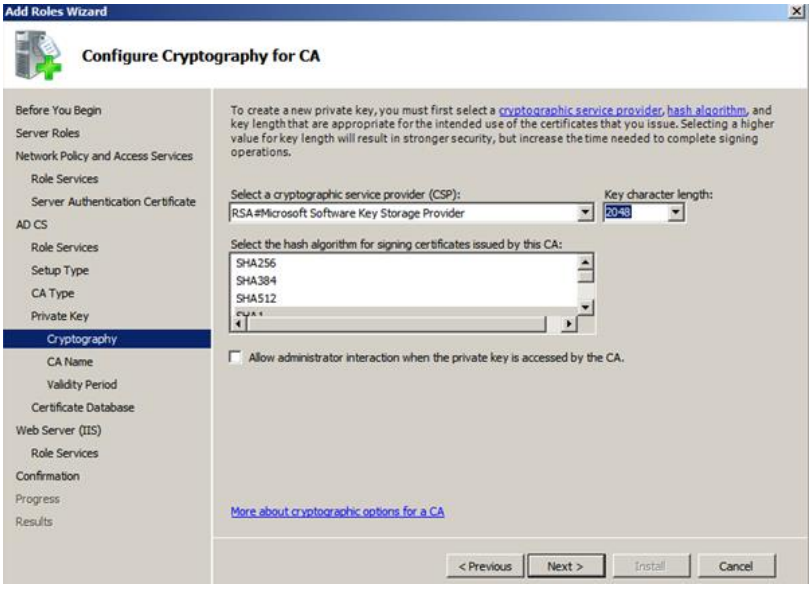


Figure B5.10: Configuring cryptography for CA

(xi) CA Name is configured as shown in as shown in Figure B5.11.

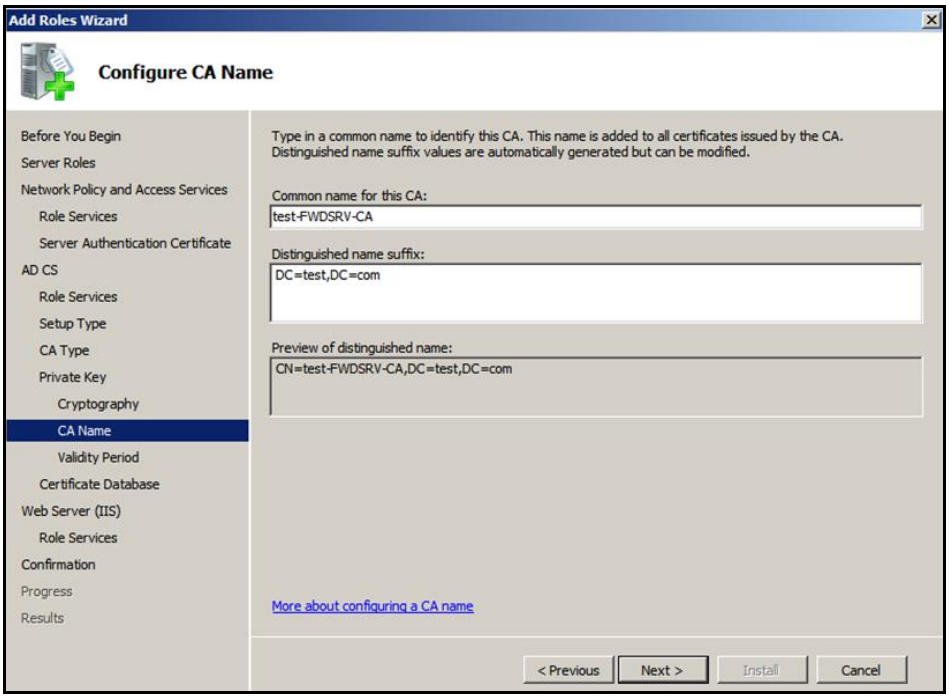


Figure B5.11: Configuring CA name

(xii) Ensure to key the validity period 5 years for the certificate generated for this CA and click on ***Next*** button.

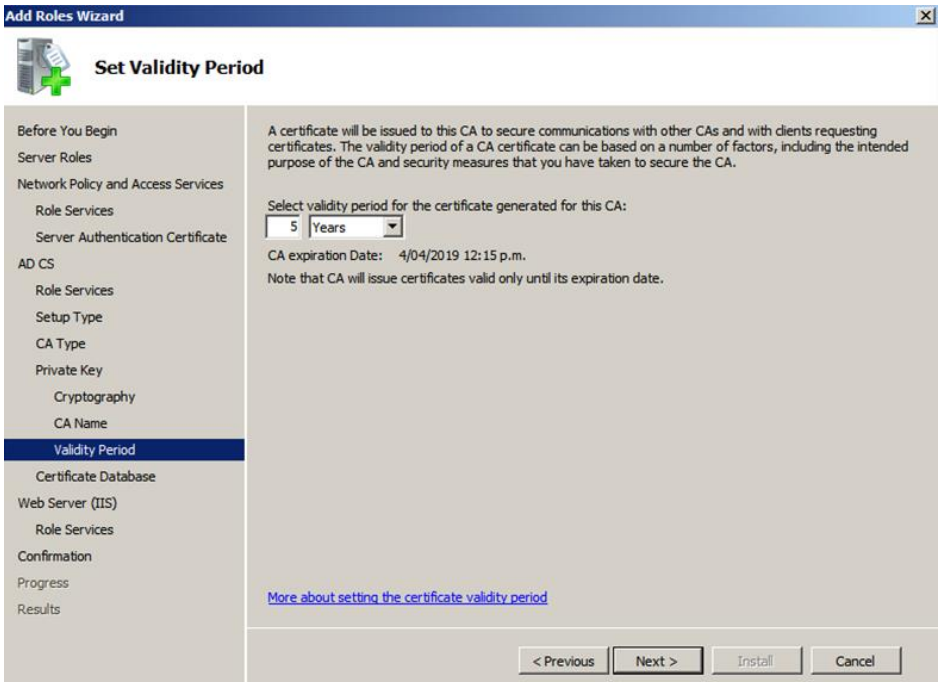


Figure B5.12: Configuring the validity period for CA

(xiii) When configuring locations for CA database and log file, select the default path and click on ***Next*** button.

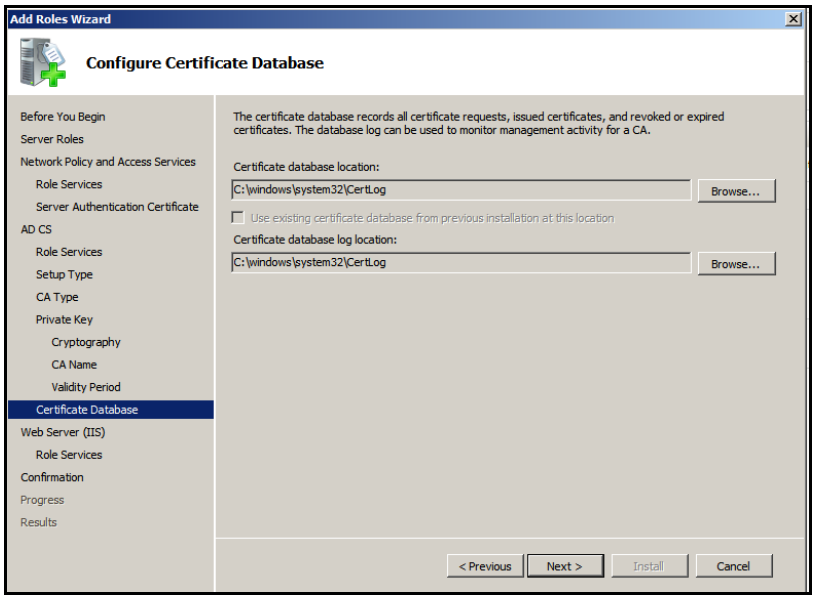


Figure B5.13: Configuring certificate database

(xiv) On the "Role Services" page, select the required role services for IIS and click on ***Next*** button.

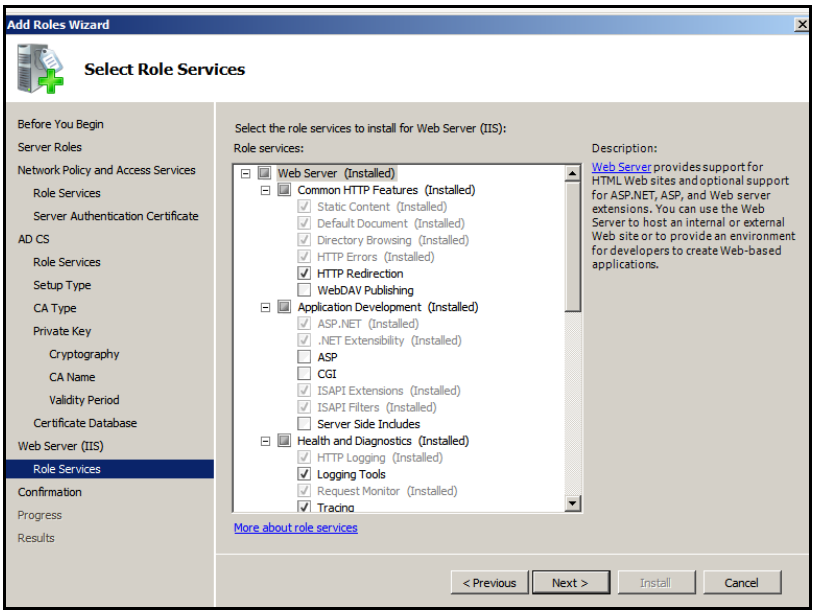


Figure B5.14: Selecting role services required for IIS

(xv) Then, confirm installation selections of all selected options and click on the ***Install*** button (see Figure B5.15)

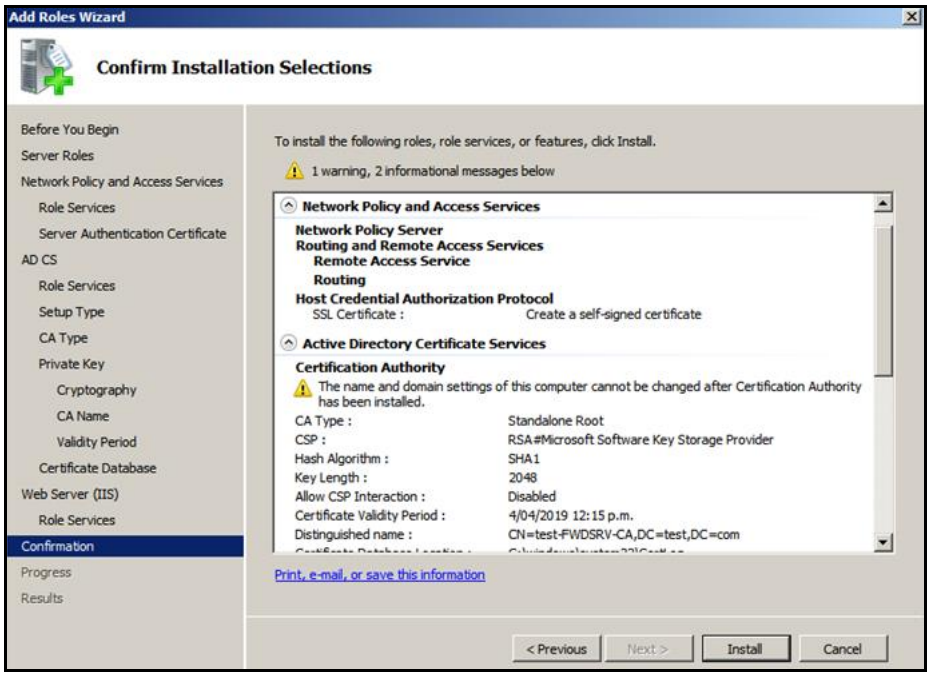


Figure B5.15: Confirming NPAS installation selections

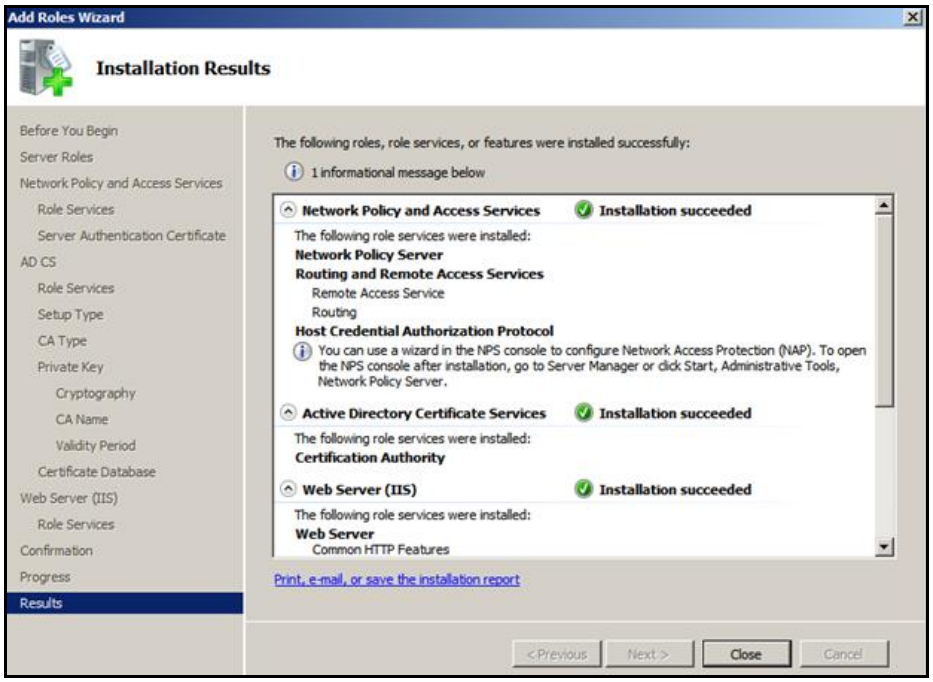


Figure B5.16: Screenshot of successful NPAS installation

Appendix A6: Configuring Network Policy Server on Microsoft Server 2008 R2

(i) First of all, open the "Server Manager" and expend NPAS (see Figure B6.1) to configure the network policy server (NPS).

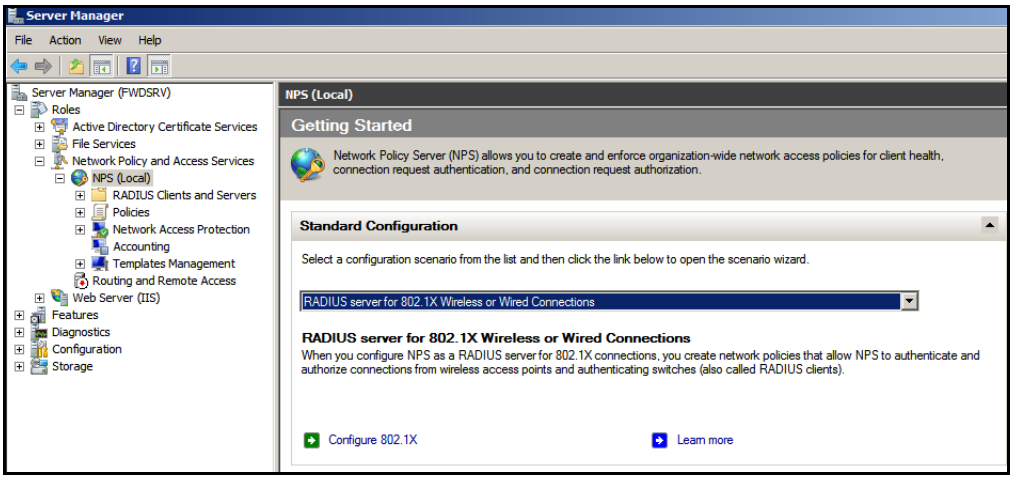


Figure B6.1: Configuring NPS for RADIUS

(ii) Then, select the "Secure Wireless Connection" under the type of 802.1X connections.

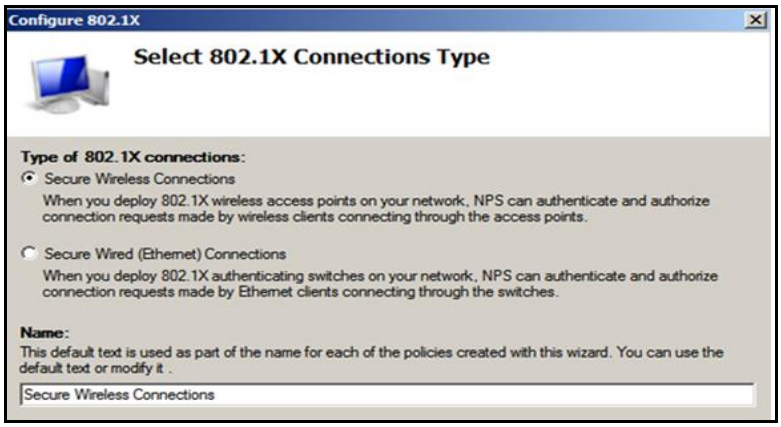


Figure B6.2: Selecting 802.1X connection type

(iii) Afterwards, click on "Add New Radius Client" and click on ***Next*** after specifying a RADIUS client (see Figure B6.3).

Figure B6.3: Specifying pfSense as RADIUS client

(iv) Under the "New RADIUS Client" configuration, ensure to verify IP address of pfSense (see Figure B6.3).

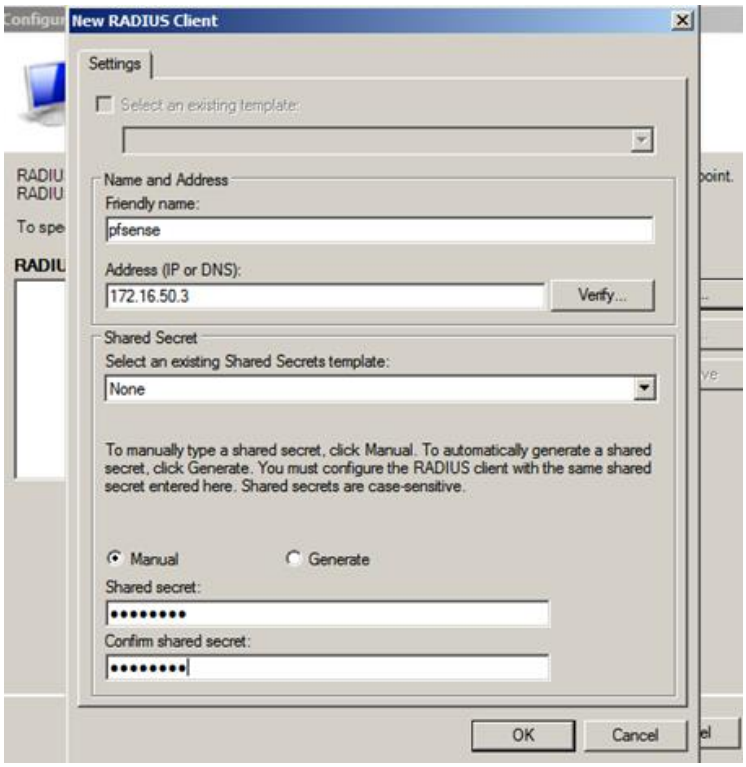


Figure B6.4: Verifying pfSense as RADIUS client

(v) On the "Configure an Authentication Method" page, select the EAP type for this policy and click on configure button.

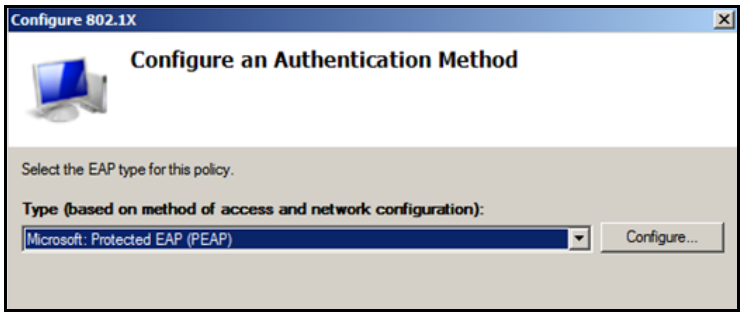


Figure B6.5: Configuring an authentication method

(vi) Go to "Edit protected EAP Properties" page, select the certificate the server should use to prove its identity to the client (Figure B6.6) and chose "Enable Fast Reconnect" option.

Figure B6.6: Selecting the certificate the server should use to prove its identity

(vii) In order to apply the policy, user groups should be selected and click next.

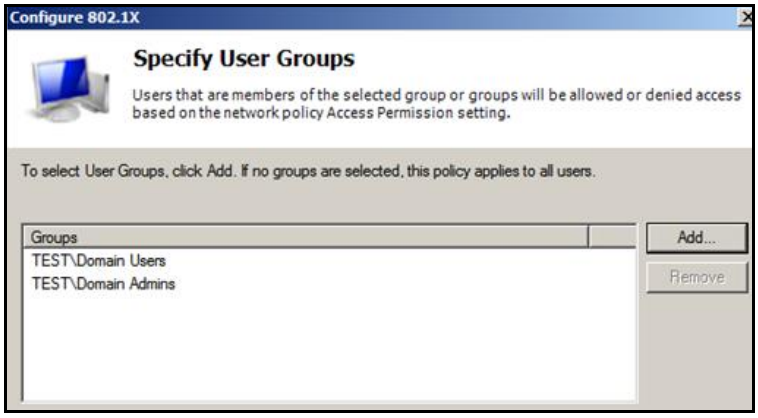


Figure B6.7: Selecting the user groups to apply the policy

(viii) Click ***Next*** buttons on "Configure Traffic Controls" (Figure B6.8) and "Summary" pages. Then, click on the ***Finish*** button to apply changes (Figures B6.9).

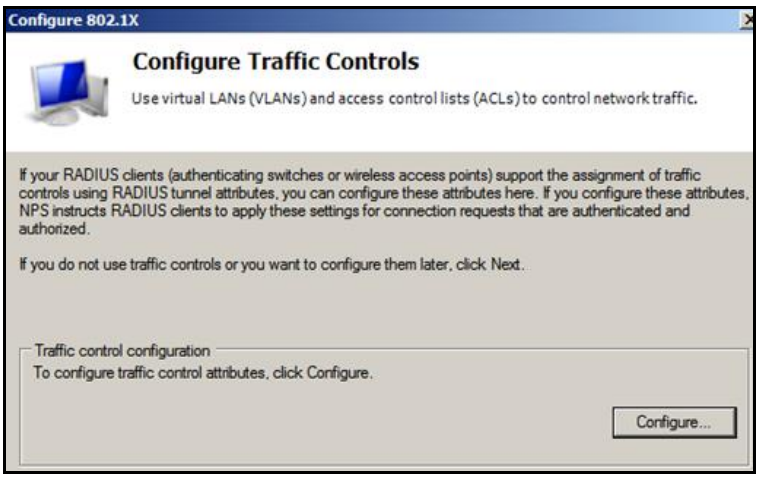


Figure B6.8: Screenshot of "Configure Traffic Controls"

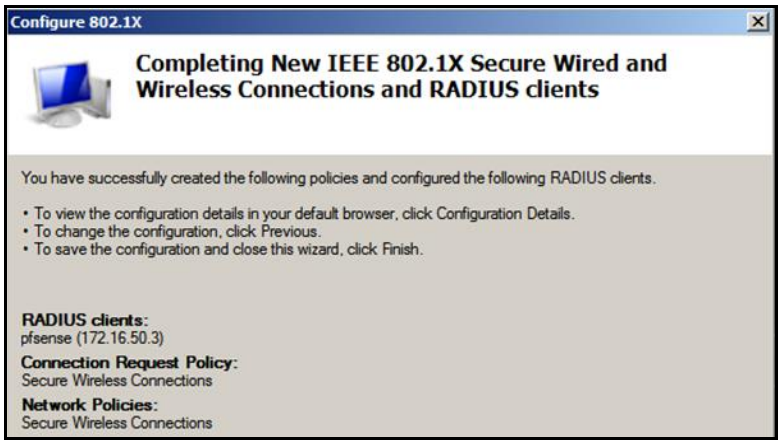


Figure B6.9: Screenshot of the successful NPS configuration

(ix) Finally, the network policy named "Secure Wireless Connections" has been configured on the server (Figure B6.10).

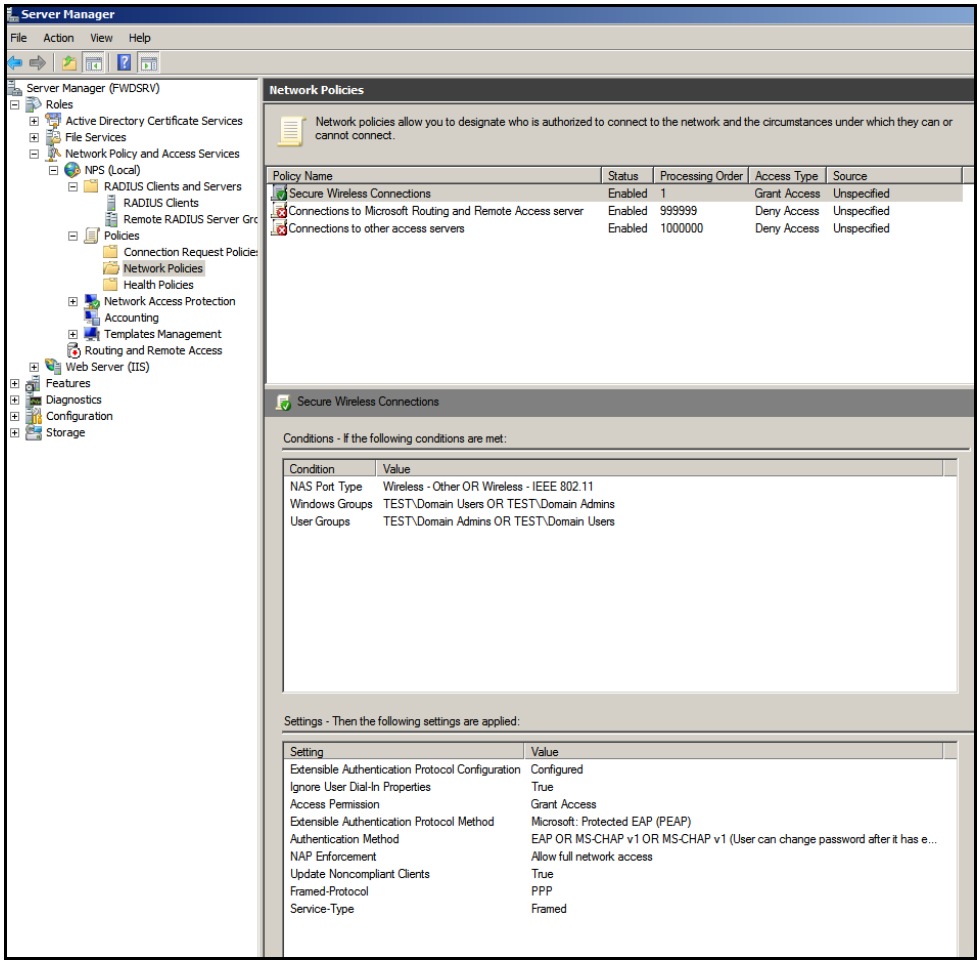


Figure B6.10: Screenshot of the network policy configuration

Appendix B7: Installation and Configuration of LOGalyze Syslog server

Two main steps to install logalyze syslog server.

- Installation of JAVA VM
- Installation of LOGalyze

Appendix B7.1: Installing JAVA package

In order to run LOGalyze, it is essential to install Java package and the steps for installation of Java package are as follows (LOGalyze, 2012, p. 6).

- "*Download Java SE 6 Update XX JRE where XX is the latest release from http://www.oracle.com/technetwork/java/javase/downloads/index.html*
- *Install the Software Development Kit (SDK) according to the instructions included with the release. The detailed installation instructions can be found in the documentation of the Java package.*
- *Set an environment variable JAVA_HOME to the path name of the directory into which you installed the SDK release*."

To set the JAVA_HOME, follow the following steps.

- Go to My Computer > Properties > Advance Settings > Environment Variables
- Add new Variable with Name=JAVA_HOME and Value=path of Java file on local machine and then add the string as path value in Systems Variables.

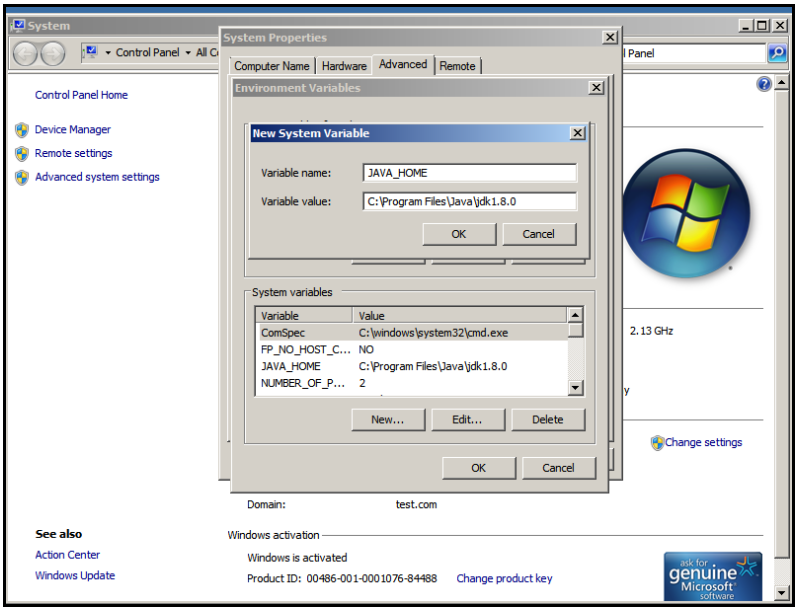


Figure B7.1: Screenshot of setting up the environment variable Java_Home

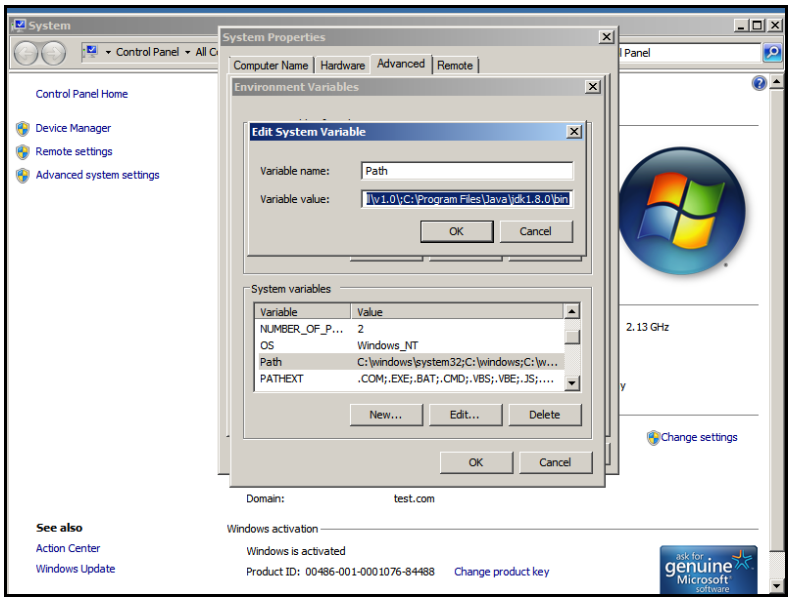


Figure B7.1.2: Screenshot of setting up the environment variable Java_Home

Appendix B7.2: Installing LOGalyze

The installation steps can be found in the latest version of LOGalyze installation manual (LOGalyze, 2012).

(i) Download a binary distribution of LOGalyze engine from http://www.logalyze.com/en/product/downloads. For Microsoft Windows platform, download logalyze-tomcat6-4.1.x-bin.zip file.

(ii) Unpack the binary distribution into the local drive (C:\).

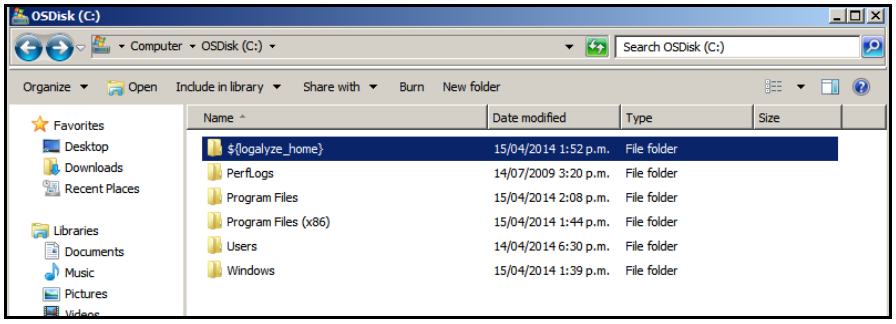


Figure B7.2: Unpacking the binary distribution

(iii) Go to ${logalyze_home}/conf/ and rename all of the files with extension .sample by removing the .sample extension (Figure B7.3).

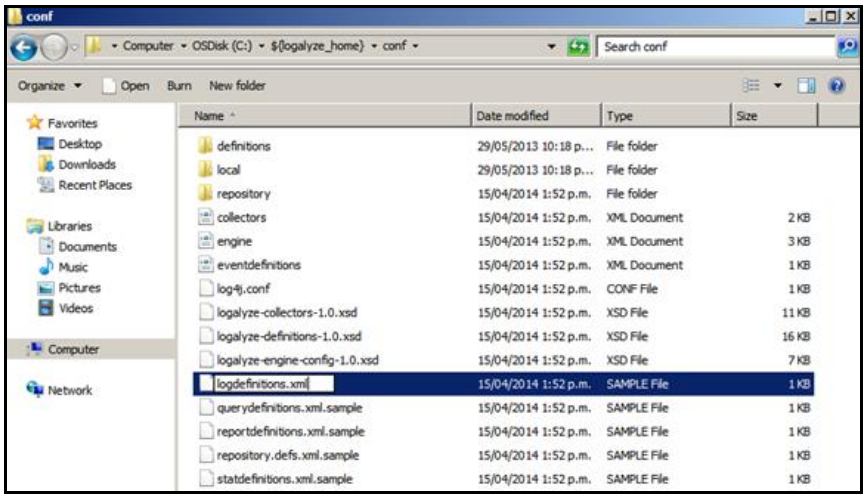


Figure B7.3: Renaming files with extension .sample

(iv) Then, edit ${logalyze_home}/bin/setenv.sh to set JAVA_HOME.

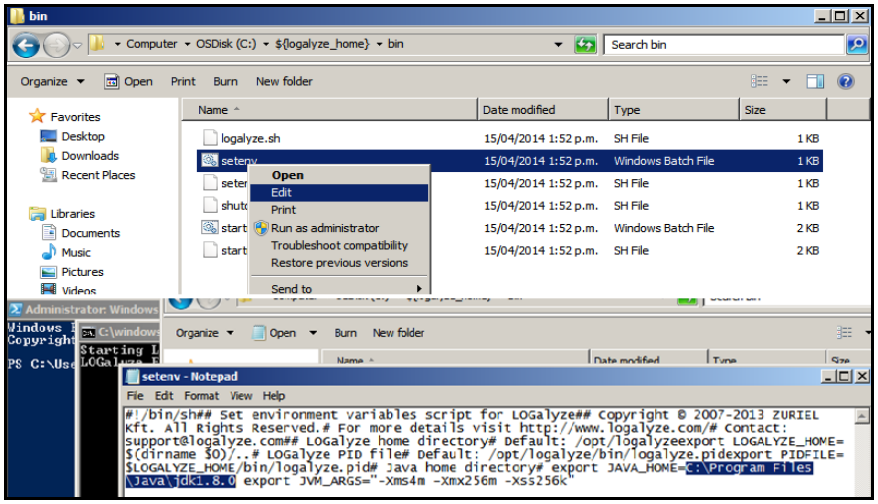


Figure B7.4: Renaming files with extension .sample

(v) In order to start LOGalyze Engine, run startup.bat (see Figure B7.5).

(vi) Similarly, run startup.bat to start LOGalyze Admin.

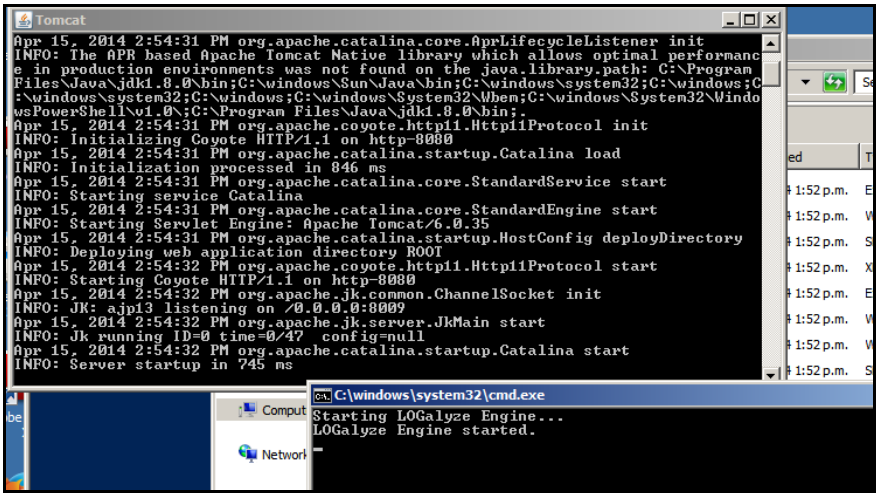


Figure B7.5: LOGalyze engine has started

(vii) Once LOGalyze Engine and Admin is running, open a web browser and visit *http://localhost:8080*. Then, the default username (admin) and password (logalyze) can be used to log into the system.

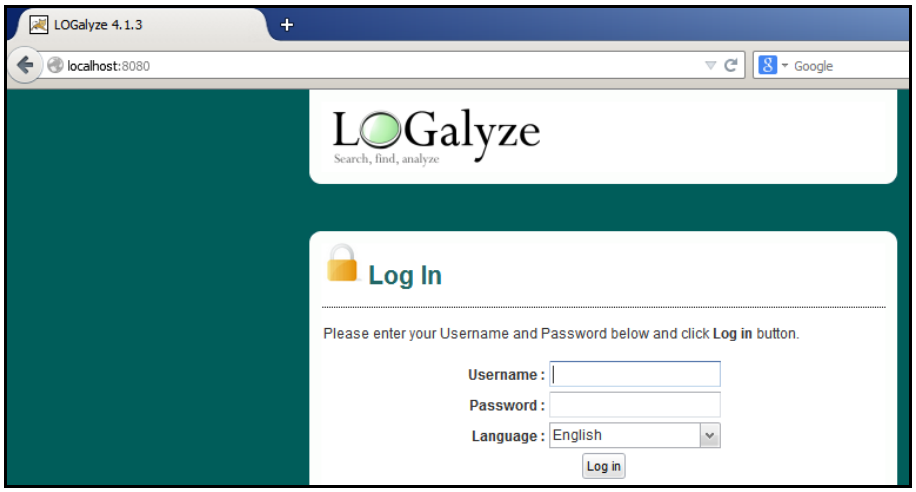


Figure B7.6: Log in page of LOGalyze server

Appendix B8: Installing and Configuring Snare BackLog Syslog Server

(i) Download Snare BackLog Server and run the executable (.exe) file

(ii) Click on the Next button to install the Snare BackLog (see Figure B8.1)

Figure B8.1: Screenshot of the Snare BackLog Setup

(iii) On the "Select Destination Location" page, give the directory location where you want to install Snare BackLog server (Figure B8.2).

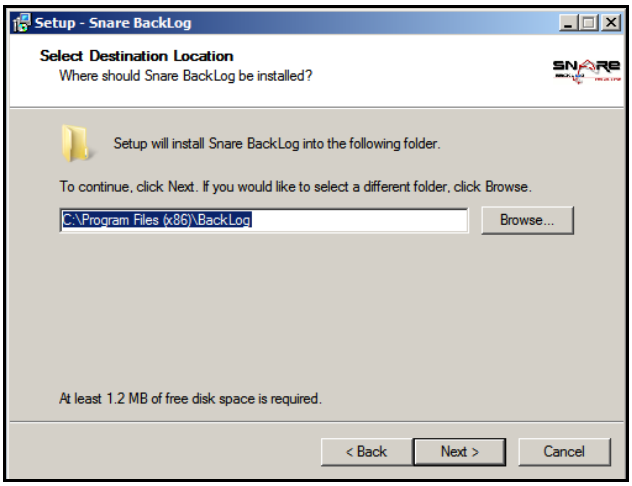


Figure B8.2: Specifying the location for Snare BackLog

(iv) The next step is to give the folder name where setup will create the program's shortcut on the "Select Start Menu Folder" page (Figure B8.3).

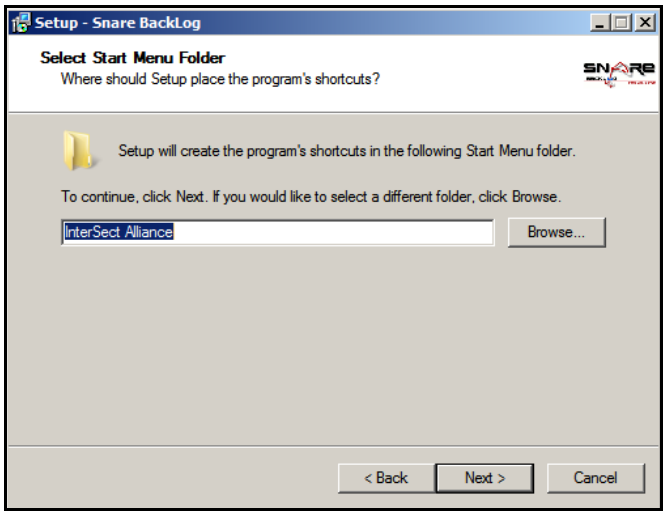


Figure B8.3: Specifying the location for Start Menu folder

(v) Then, click on the ***Next*** button after reading important information (Figure B8.4).

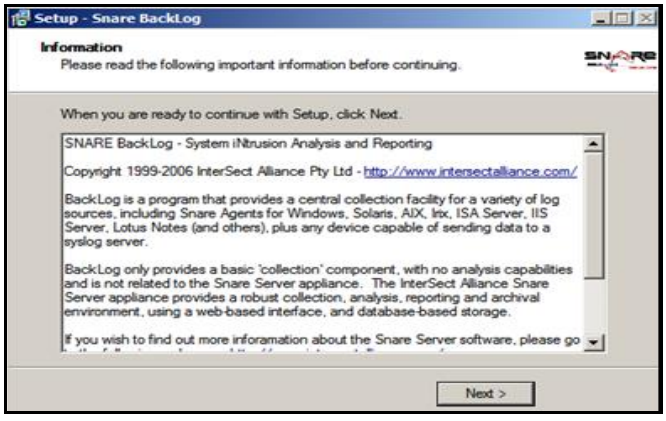


Figure B8.4: Information page of Snare BackLog setup

(vi) On the "Ready to Install" page, click on the ***Install*** button to continue with the installation.

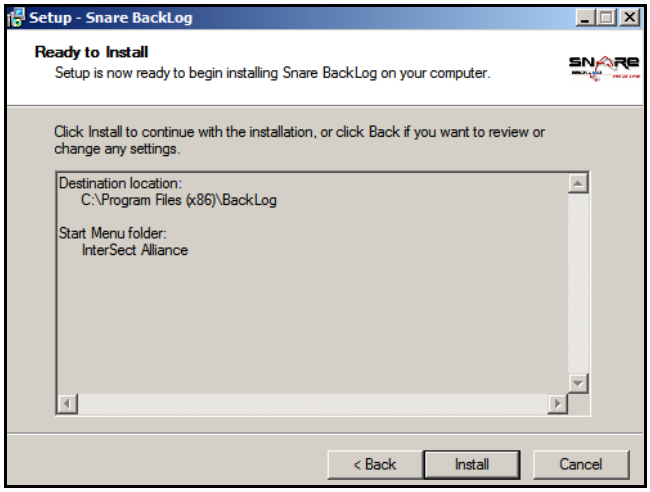


Figure B8.5: Snare BackLog is ready to install

(vii) After completing the Snare BackLog setup, click on the ***Finish*** button.

Figure B8.6: Screenshot of completing Snare BackLog setup

(viii) Finally, the Snare Backlog server is ready to use as syslog collector.

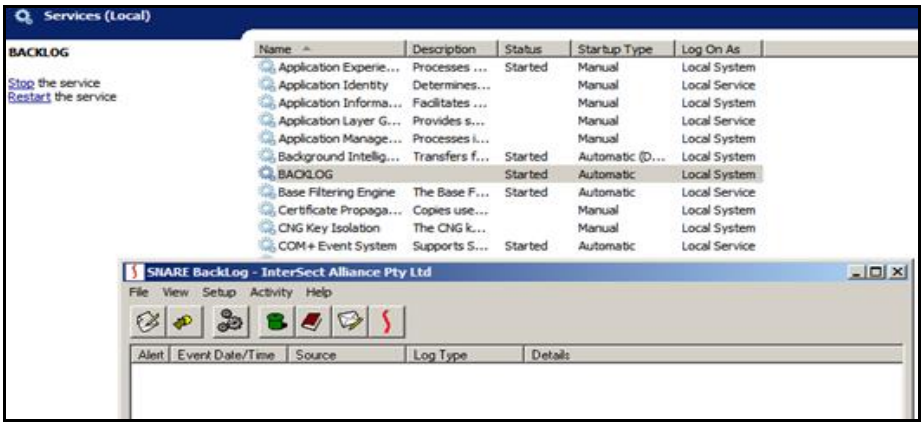


Figure B8.7: Screenshot of running Snare BackLog

Appendix B9: Installing and Configuring rsyslog server on Ubuntu Server 12.04

The following are steps to enable Ubuntu Server 12.04 LTS to collect syslogs from the network by using a centralised rsyslog collector.

(i) After installing the Ubuntu server, the system should be updated with the latest patches, and the system should be configured with static IP, subnet mask, default gateway address by using the command "sudo nano /etc/network/interfaces" (Figure B9.1).

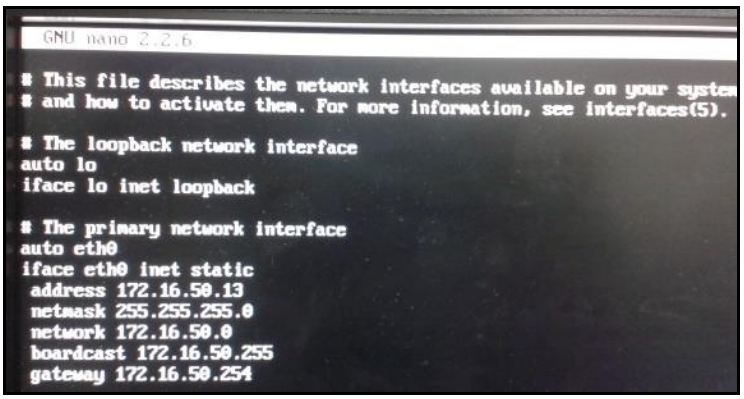


Figure B9.1: Configuring the network interface of Ubuntu Server

(ii) Save the configuration and restart the networking service using the command, "sudo /etc/init.d/networking restart".

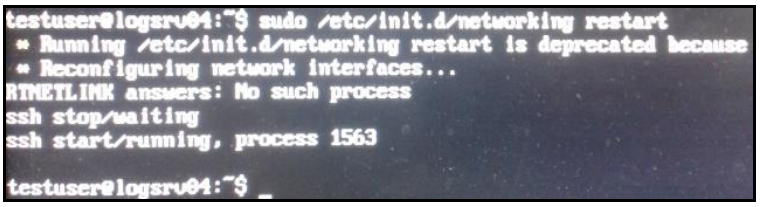


Figure B9.2: Restarting networking service

(iii) Edit the configuration file (rsyslog.conf) by using a text editor to allow the submission of system logs from clients. The command "sudo vim /etc/rsyslog.conf" is used to edit the file. Then, uncomment the following lines:

```
$ModLoad      imudp
$UDPServerRun 514
```

Also, the following lines should be added to the bottom of the configuration file.

```
$template TmplAuth,
```

"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"

(iv) Change the permissions of the /var/log directory to allow syslog the ability create or change sub-directories and files by using the command “cd /var && sudo chown syslog:syslog log”.

(v) Save the changes made to the rsyslog.conf file and restart the rsyslog service by using the command “sudo service rsyslog restart”.

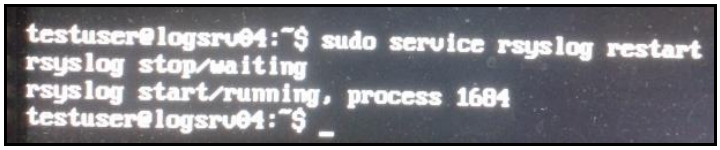


Figure B9.3: Restarting networking service

(vi) The next step is to configure clients to forward logs to the newly configured Syslog server. For all Unix/Linux-based clients, rsyslog.conf file or syslog.conf file should firstly be edited and uncomment the following lines (x.x.x.x being the IP address of syslog server) by using the “sudo nano /etc/rsyslog.conf” command.

. @logserver (replace "logserver" with x.x.x.x)

(vii) Restart the rsyslog/syslog service by using the command “sudo service rsyslog restart” (Figure B9.3)

(vii) Then, it is essential to verify logs are being forwarded to the syslog server. On the **s**yslog server**,** check the "/var/log" directory to see whether client log directories have been created by using the commands “cd /var/log” and list the file using “ls”, then view the syslog file using “cat” command.

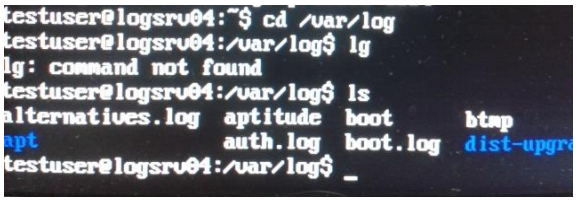


Figure B9.4: Verifying whether logs are being forwarded to the syslog server

Unfortunately, Windows-based systems do not natively play nice with Syslog servers. However, an agent-based service called "Snare" can be installed to manage and export log files to the centralised syslog server.

Appendix B10: Installing and configuring Snare syslog clients on hosts running Microsoft Windows Operating Systems.

(i) Download Snare client Setup (.exe) file from https://www.snaresolutions.com/products/snare-agents/ and run it on Windows-based hosts, where you want to enable syslog client service. Once the installation is completed, Snare syslog clients will convert Window's events into syslog format and will forward the logs to a desired syslog server over the local network by using UDP port 514.

Figure B10.1: Screenshot of Snare Agent setup

(ii) On the "License Agreement" page, read the detail carefully. Then, check "I accept the agreement" and click on the ***Next*** button (Figure B10.2).

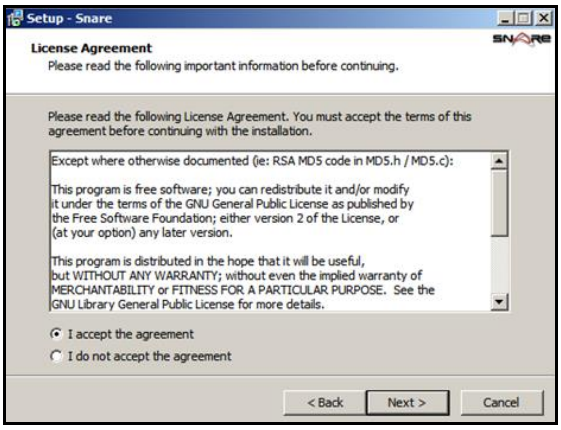


Figure B10.2: Screenshot of accepting the license agreement

(iii) On "Snare Auditing" page, select "Yes" for Snare to take control of host's EventLog configuration and click on the ***Next*** button (Figure B10.3).

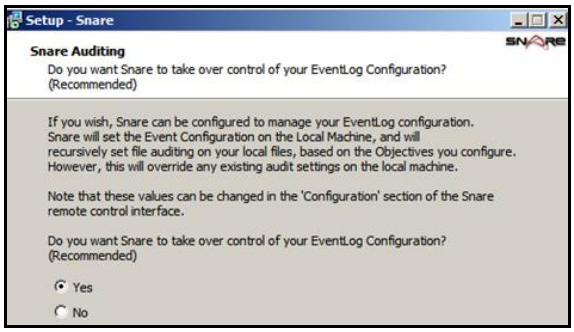


Figure B10.3: Allowing Snare to take over control of EventLog configuration

(iv) The next step is to create service account credentials for administration. However, it is recommended to select "Use System Account" option (Figure B10.4).

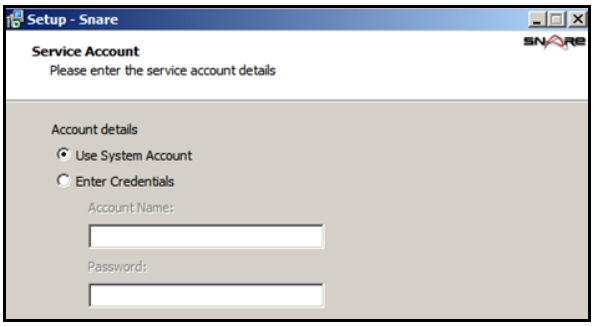


Figure B10.4: Creating a service account

(v) The remote administration using web-console should be enabled and also the password for remote login should be created (Figure B10.5). Then click on the ***Next*** button.

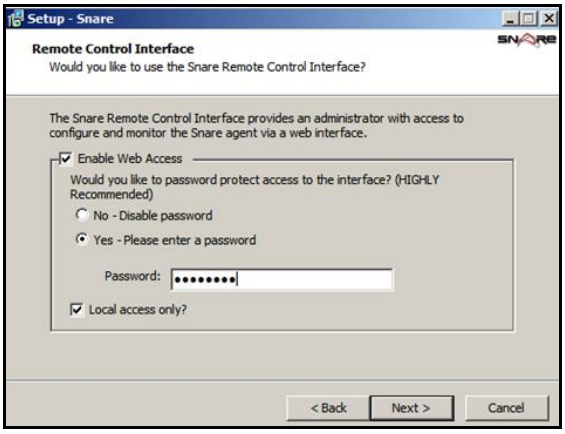


Figure B10.5: Enabling the Snare remote control interface

(vi) On the "Select Destination Location" page, the location of a folder to store Snare installation files is required to specify and click on the ***Next*** button (Figure B10.6). It is important to note that at least 1.3 MB of free disk space is required).

Figure B10.6: Selecting the location of the folder to store Snare installation files

(vii) The location of a folder where Snare setup will create program's shortcut needs to be selected and click on the ***Next*** button (Figure B10.7).

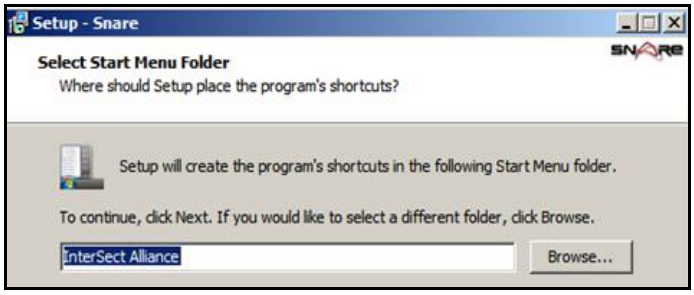


Figure B10.7: Selecting the location of the Start Menu folder

(viii) Click on the ***Install*** button to begin the installation of Snare.

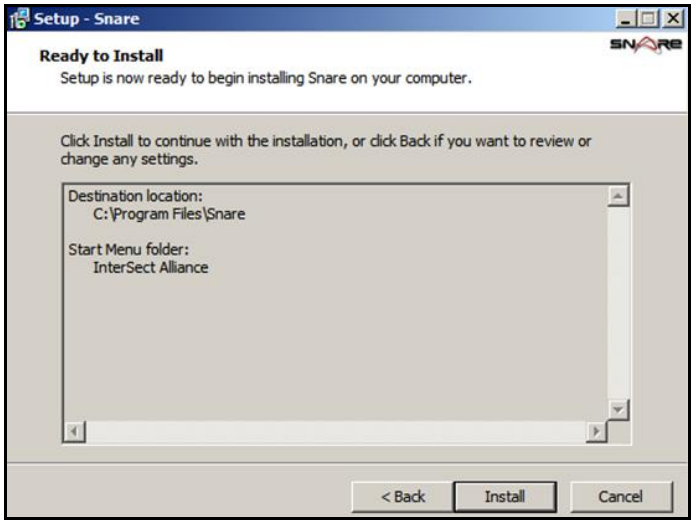


Figure B10.8: Snare is ready to be installed

(ix) Once the installation has finished (Figure B10.9), click on the ***Finish*** button to exit Setup.

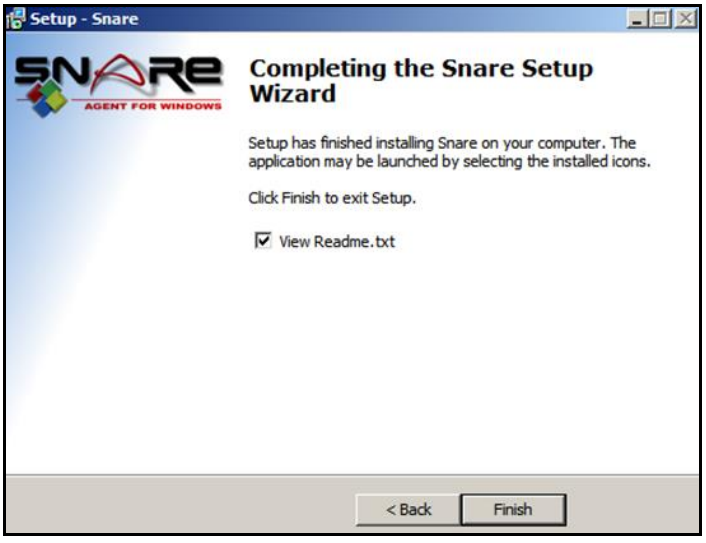


Figure B10.9: Setup has completed installing Snare

(x) To configure Snare client, open a web browser and connect the "localhost" via port 6161 (Figure B10.10).

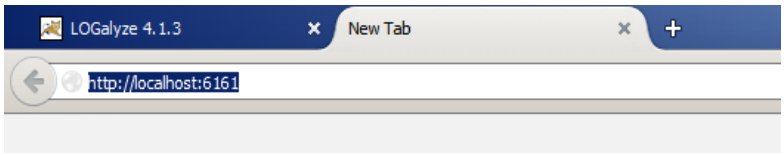


Figure B10.10: Accessing Snare client by using a web browser

(xi) Enter credentials by using ***Snare*** as the username and password which was created during the installation. Then, click on "Network Configuration" menu (Figure B10.11).

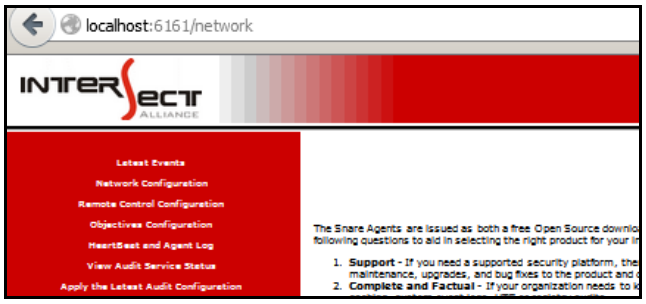


Figure B10.11: Screenshot of the Snare client

(xii) Afterwards, the destination Snare server's IP address should be provided and change the network configuration as shown in Figure B10.12. Then, the network configuration file should be saved.

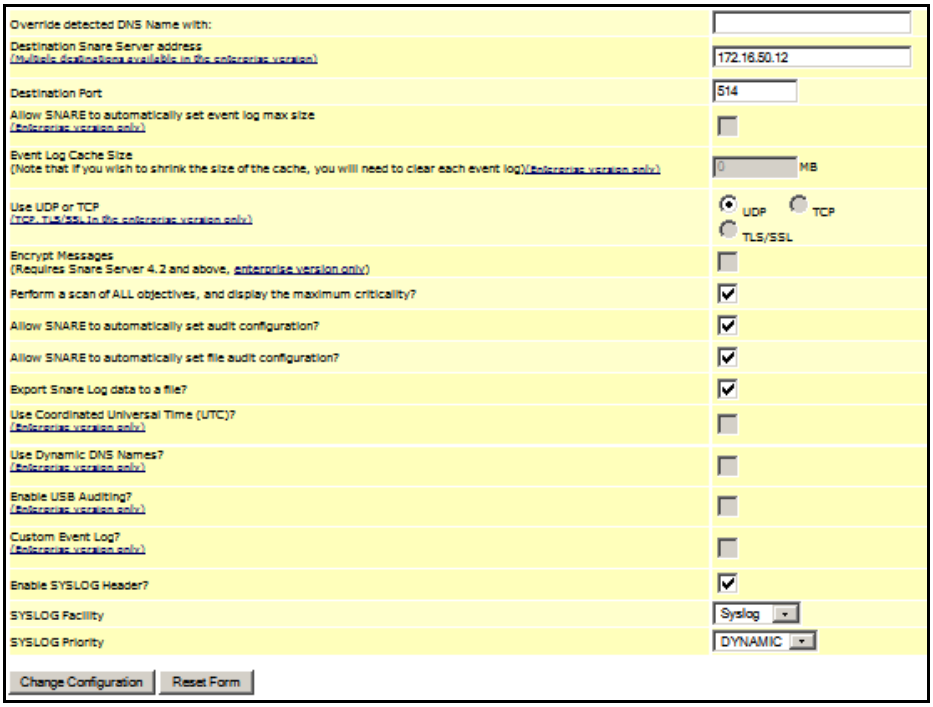


Figure B10.12: Screenshot of the Snare Agent's network configuration file

(xiii) Finally, click on the "Apply the Latest Audit Configuration" menu to apply changes to the system.

Figure B10.13: Applying the latest configuration

Appendix B11: Configuring Windows Firewall settings for Syslog client/server

To enable syslog clients to forward logs to the Syslog server, it is required to create a firewall rule to open UDP port 514 in outbound direction on clients. Similarly, UDP port 514 should be opened in both directions on the syslog server.

(i) On the server side, go to the advanced settings of the Windows Firewall by opening: **Start > Control panel > Firewall > Advanced settings.**

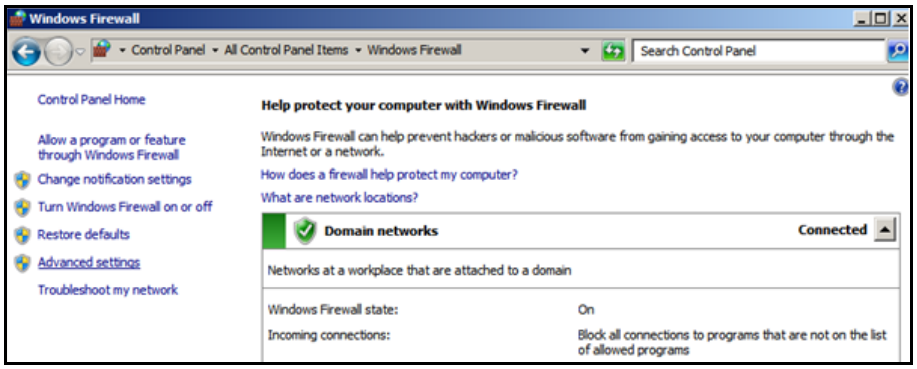


Figure B11.1: Screenshot of Windows Firewall

(ii) Right click on "Inbound Rules" and select "New Rule".

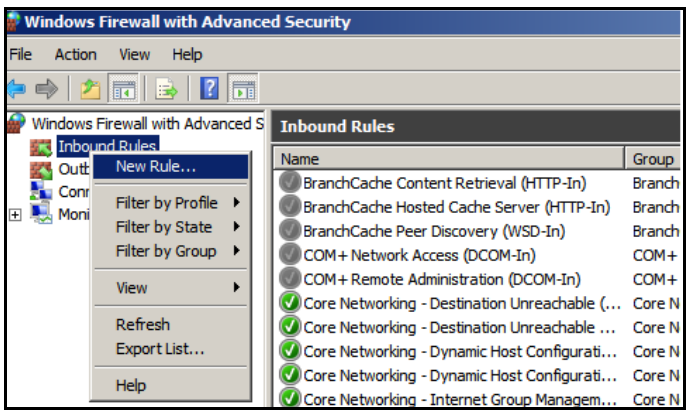


Figure B11.2: Creating a new Firewall rule

(iii) Then, the type of rule to create is "Port" in this case and click on the ***Next*** button (Figure B11.3).

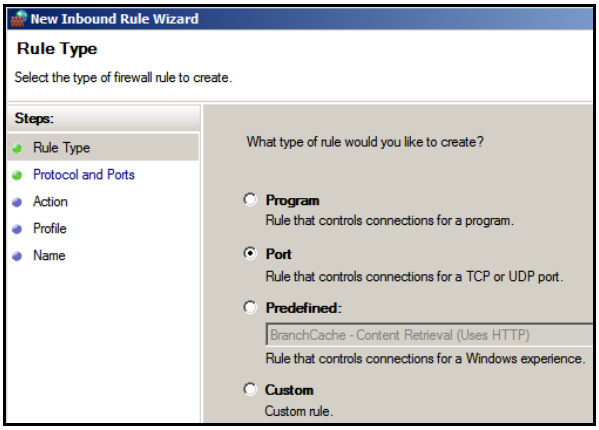


Figure B11.3: Creating an inbound port-based Firewall rule

(iv) On the "Protocol and Ports" page, UDP is selected and the specific local port number entered is 514 to specify protocol and port number accordingly.

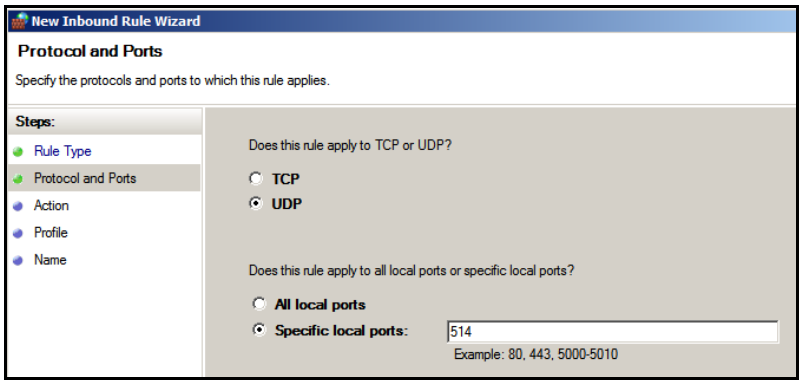


Figure B11.4: Specifying protocol and port number for Firewall rule

(v) On the "Action" page, "allow the connection" is selected for the action to be taken when connection matches the specified conditions (Figure B11.5) and then click on the ***Next*** button.

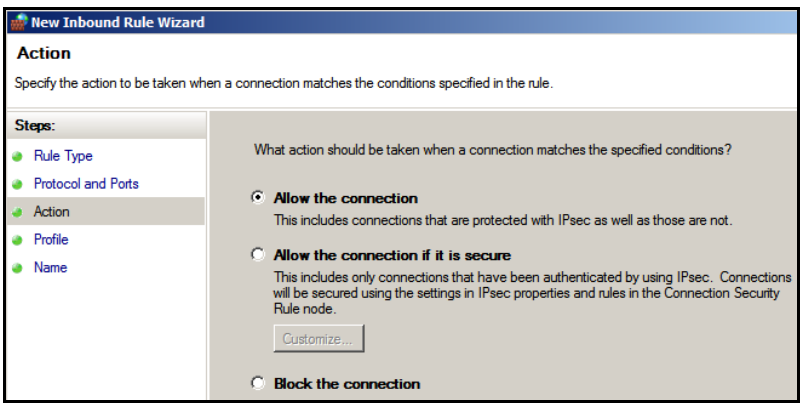


Figure B11.5: Selecting the action to be taken for a new Firewall rule

(vi) On the "Profile" page, the profile for which this rule applies should be configured as shown in Figure B11.6.

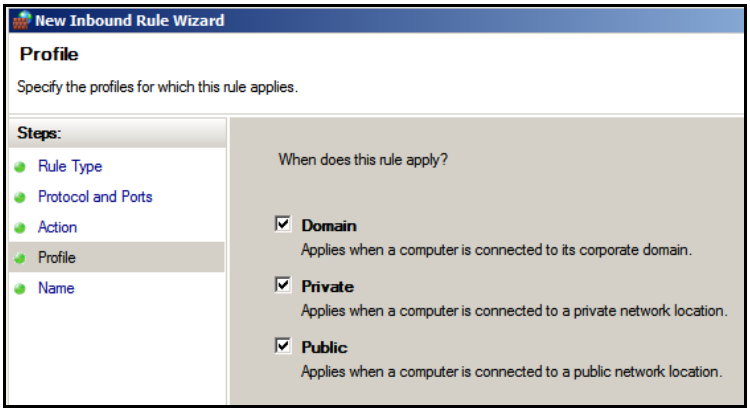


Figure B11.6: Configuring the profiles for which a new Firewall rule applies to

(vii) Then, the unique name for Firewall rule is given as "Snare Syslog UDP 514".

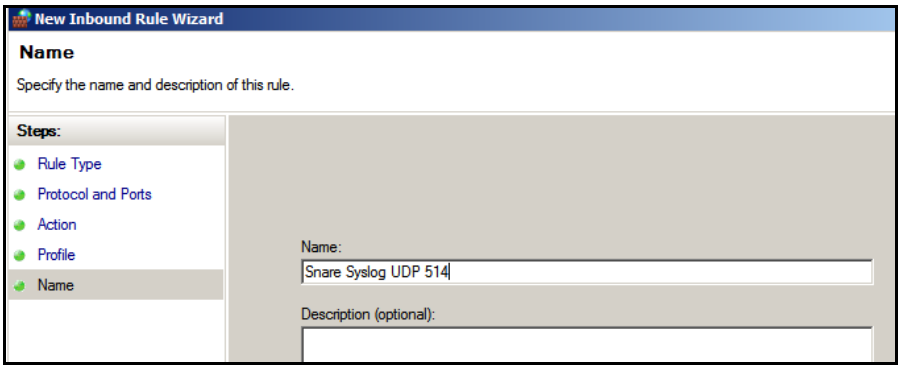


Figure B11.7: Giving the name of Firewall rule

(viii) In the same procedure, outbound rules for the Syslog server and clients are created to enable the communication between syslog forwarder and collector.

Appendix B12: Installing and configuring OpenEMR

Before installing OpenEMR web application, we need pre-installed OpenEMR with the XAMPP package, which can be download from http://www.open-emr.org/wiki/index.php/OpenEMR_Downloads.

(i) The first step is to download OpenEMR (openemr-4.1.2.zip).

(ii) The downloaded OpenEMR archive is extracted and the name of the directory "openemr-4.1.2" is changed to just openemr.

(iii) Then, the extracted "openemr" folder is moved to the Web Server root directory as shown in Figure B12.1.

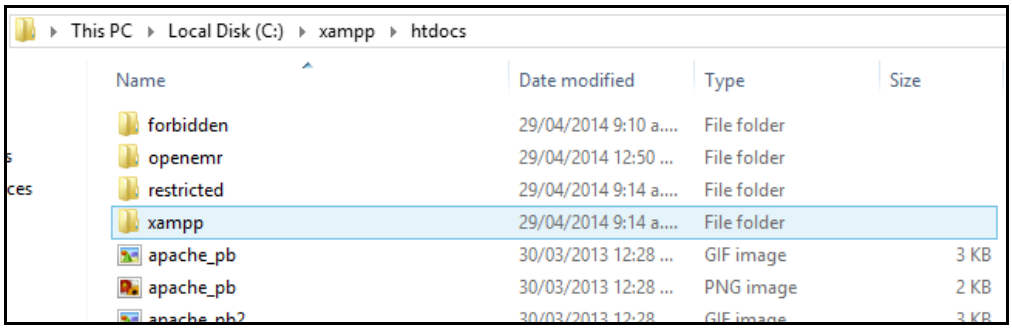


Figure B12.1: Location of the extracted OpenEMR folder

(iv) To configure the Install through the web graphical user interface (GUI), follow the instruction from https://www.open-emr.org/wiki/index.php/OpenEMR_4.1.2_XAMPP_Package_Installation (OpenEMR, 2014b).

(v) Once the installation is done without errors, the successful installation of OpenEMR can be observed on the final configuration page (Figure B12.2) . This final installation page gives additional information and instructions including OpenEMR admin username and password, along with a link to start OpenEMR.

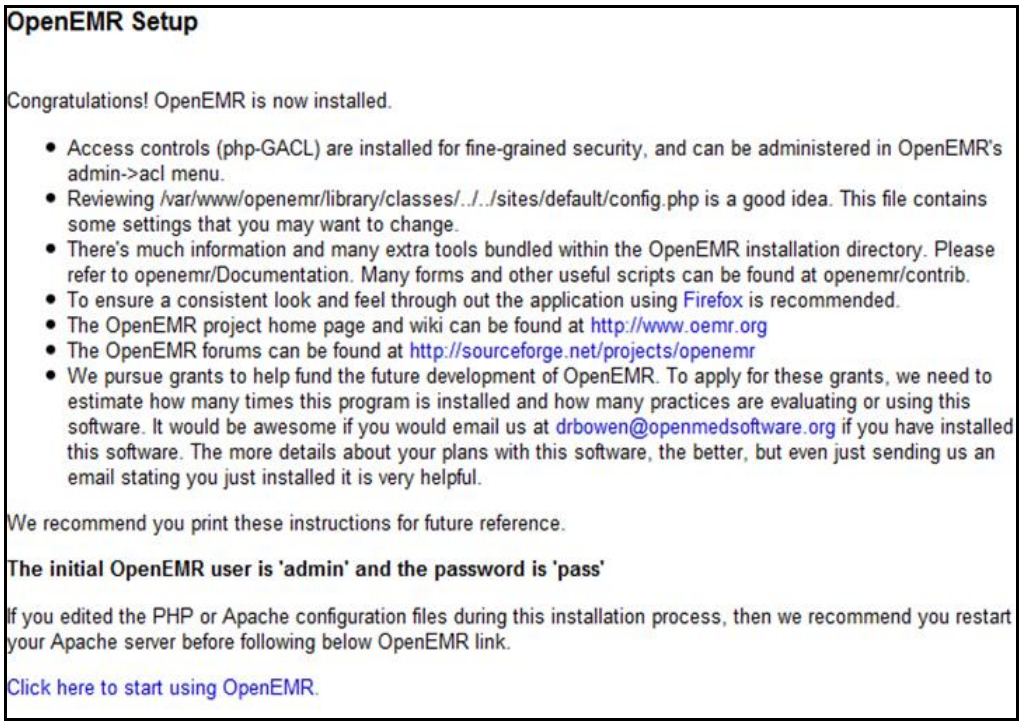


Figure B12.2: Screenshot of the successful OpenEMR installation

APPENDIX C

Budget for Final Proposal

& Cost Benefit Analysis (CBA)

The main purpose of CBA is to find out whether the open-source and low-cost proposed Digital Forensic Readiness (DFR) System is suitable to replace the commercial solutions available in the market. The CBA will include all hardware and software components, which will be used in the Forensic Readiness System.

Table C1: Cost Benefit Analysis

Component	Digital Forensic Readiness System with Ubiquiti RouterStation Pro (as of 2 July 2014)			Digital Forensic Readiness System with Raspberry Pi 3 (as of 9 July 2016)			Digital Forensic Readiness System with Raspberry Pi 3, IDS (Bro) and IPS (OSSEC) (as of 9 July 2016)		
	Devices and Software	**Qty**	**Price (NZD)**	**Devices**	**Qty**	**Price (NZD)**	**Devices**	**Qty**	**Price (NZD)**
Hardware	Ubiquity XR2 XtremerRange2 600mW	2	$105.08	Raspberry Pi 3 (including case)	1	$100.00	Raspberry Pi 3 (including case)	1	$100.00
	Ubiquiti POE-48-24W-G 0.5A PoE	1	$35.10	Strontium 16GB SD card	1	$17.60	Strontium 16GB SD card	1	$17.60
	RP-SMA Female Bulkhead to MMCX Male Pigtail	2	$34.20	TP-LINK TL-WN722N	2	$40.00	TP-LINK TL-WN722N	2	$40.00
	Ubiquiti RouterStation Pro	1	$176.61	Dell OptiPlex 745	1	$181.80	Dell OptiPlex 745	1	$181.80
	Dell OptiPlex 745	1	$181.80				HP EliteDesk 800 G1 DM	1	$1,500.00
Software	Ubuntu Linux GUI		Free	Kali Linux 2016 for ARM		Free	Kali Linux 2016 for ARM		Free
	OpenWRT		Free	Kali Linux 2016		Free	Kali Linux 2016		Free
	Kismet		Free	Kismet		Free	Kismet		Free
							Windows 10 Enterprise and Hyper-V		$300.00

							Bro (Version 2.4.1)		Free
							OSSEC (Version 0.9)		Free
Total			**$532.79**			**$339.00**			**$2,139.00**

Table C1 explains the total cost of an individual system and the cost of hardware and software for all three DFR systems tested in the laboratory environment.

Table C2: Total cost comparison of the proposed low-cost DFR system with Cisco's commercial DFR systems

	Forensic Readiness System with Raspberry Pi 3 and IDS (Bro) and IPS (OSSEC) (as of 9 July 2016)			**Commercial Forensic Readiness System Cisco (Low-end; as of 27 December 2018)**			**Commercial Forensic Readiness System Cisco (High-end; as of 27 December 2018)**		
	Devices and Software	*Quantity*	*Price (NZD)*	*Devices and Software*	*Quantity*	*Price (NZD)*	*Devices and Software*	*Quantity*	*Price (NZD)*
Hardware Components	Raspberry Pi 3 included cases	1	$100.00	Cisco Aironet AP2802I	1	$1,332.95	Cisco Aironet 4800	1	$2,937.60
	Strontium 16GB SD card	1	$17.60	Cisco 5520 Wireless Controller support 50 AP w/rack kit TAA	1	$22,658.31	Cisco 8540 Wireless Controller support 50 AP w/rack kit TAA	1	$61,765.22
	TP-LINK TL-WN722N	2	$40.00	Cisco MSE 3355	1	$24,202.03	Cisco MSE 3365	1	$35,765.11
	Dell OptiPlex 745	1	$181.80						
	HP EliteDesk 800 G1 DM	1	$1,500.00						
Software Components	Kali Linux 2016 for ARM		Free	Cisco Prime Infrastructure Base (v. 3.x) 1		$93.50	Cisco Prime Infrastructure Base		$93.50

				license			(v. 3.x) 1 license		
	Kali Linux 2016		Free	Cisco Mobility Services Engine Virtual Appliance License		$5,412.93	Cisco Mobility Services Engine Virtual Appliance License		$5,412.93
	Kismet		Free						
	Windows 10 Enterprise and Hyper-V		$300.00						
	Bro (Version 2.4.1)		Free						
	OSSEC (Version 0.9)		Free						
TOTAL			**$2,139.00**			**$53,699.72**			**$105,974.36**

Table C2 presents the total cost comparison of the proposed low-cost DFR system with Cisco's DFR systems. It details the cost of each factor including hardware and software for all three alternative different systems. The proposed low-cost DFR system for WMedSys includes the open source hardware and software solutions. On the other hand, Cisco's commercial DFR solutions are based on the low-end and high-end of Cisco devices. Based on staff's ability and company's finance, the cost for staff training will also be different. The cost factors for staff payment, staff training, and system or devices maintained will not be included in calculating the total cost.

Table C3: Total cost comparison of the experimented DFR systems with Cisco's commercial DFR systems

	Forensic Readiness System with Ubiquiti RouterStation Pro (as of 2 July 2014)	**Forensic Readiness System with Raspberry Pi-3 (as of 9 July 2016)**	**Forensic Readiness System with Raspberry Pi-3 and IDS (Bro) and IPS (OSSEC) (as of 9 July 2016)**	**Commercial Forensic Readiness System Cisco (Low-end; as of 27 December 2018)**	**Commercial Forensic Readiness System Cisco (High-end; as of 27 December 2018)**
Total Cost of 20 Wireless Access Points (including the power supply)	NZ$ 7,019.80	NZ$ 3,152.00	NZ$ 3,152.00	NZ$ 26,659.00	NZ$ 58,752.00
Total Cost of the Forensic Readiness System	NZ$ 7,201.60	NZ$ 3,333.80	NZ$ 5,133.80	NZ$ 79,025.77	NZ$ 161,608.80

Table C3 describes the total cost of the tested DFR systems with Cisco's commercial DFR systems by using 20 APs. According to the experiments and calculated CBA results, the proposed low-cost DFR system with Raspberry Pi 3, IDS (Bro) and IPS (OSSEC) has the most cost effective compared to other solutions.

APPENDIX D

Evaluation Feedback from Experts on the Proposed Digital Forensic Ready (DFR) Framework Artefact

Table D1: Expert 1's Evaluation Feedback

No.	Description	Expert's Answer
DFR Framework for WMedSys: Overall Evaluation		
1	Overall, how effective do you think the proposed DFR Framework artefact would be in the production environment in case of preserving potential digital evidence?	The propose DFR Framework is effective for wireless attacks through the drone and the forensic server, and effective for the internal and Internet attacks, through the IDS server and agents.
2	Are the defined components of the proposed DFR Framework artefact clear and relevant to what you observe?	The components proposed by the framework are clearly explained in a diagram and text.
3	Do you think the provided requirements helpful and adequate in designing DFR Framework artefact for WMedSys?	I think the DFR Framework requirements are adequate for designing an artefact for any wireless medical system.
4	Do you think the proposed artefact is useful and realistic in improving/addressing user/patient safety?	I think the proposed artefact is realistic in addressing patient safety since it could be integrated with existing systems.
5	How easy or difficult do you think it is to implement and integrate the proposed DFR Framework artefact in an existing WMedSys?	Implementing the services in the proposed framework is very easy and does not require additional skills for IT professionals/system engineers/network administrators.
6	What was an approximate time for you to follow all components of proposed DFR Framework artefact? Was it easy to understand?	It took about 30 minutes to follow all of the components of the framework; it was very easy to understand.
7	Do you think there is any area of improvement in the proposed artefact? If so, please give your suggestion.	Symbols used in the framework design should explained and be consistent. For example, the square symbol is used for branching and aggregating. Second, there should be no END symbol in the diagram since the process is non-terminating.
8	Is there any modification that should be made to any component of the proposed DFR Framework?	I don't think there is any need for more components or modification be made to the existing framework.

9	Do you think the proposed DFR Framework is effective and efficient in capturing security attacks in a WMedSys?	I think the proposed DFR Framework is as effective as the implemented IDS software, the wireless drone, and the wireless forensic server.
10	Do you think the proposed DFR Framework is effective and efficient in determining security attacks on a WMedSys?	I think the proposed DFR Framework is effective and efficient in detecting common security attacks on wireless medical networks.
11	Do you think the proposed DFR Framework is effective and efficient in addressing to improve patient/user safety?	I think The DFR Framework is comprehensive and it is an improvement on patient safety by providing awareness and training for the users and to prevent similar attacks not to be repeated to the wireless medical network.
12	Please provide your comments on the usability and ease of operation.	The framework is usable, since it does not require additional technical skills to implement.
13	Can you list the weaknesses and strengths of the proposed DFR Framework artefact for WMedSys?	Strength: low cost resources. Weaknesses: (1) There is always security risks, similar to any computer network; (2) using only the 2.4GHz band.
14	Regarding the completeness of the DFR Framework artefact for WMedSys, how do you think?	It is complete as far as I know.
15	Were the information provided related to the artefact logical and helpful?	The framework design is clear, and the accompanying documents are explaining the components of the framework clearly.
16	Is the proposed DFR Framework artefact cost effective and efficient?	The proposed DFR Framework artefacts is cost effective because it is using low costs hardware and free open source software.
17	Is the proposed artefact likely to be widely adopted and implemented in WMedSys?	It follows from (16) above that the framework is likely be adopted by healthcare providers.
18	How effective do you think the proposed DFR Framework could be if IT managers/security engineers of clinical and hospital networks starts using it in their WMedSys?	I think the DFR Framework could very effective if it was adopted by IT practitioners in healthcare.

Table D2: Expert 2's Evaluation Feedback

No.	Description	Expert's Answer
DFR Framework for WMedSys: Overall Evaluation		
1	Overall, how effective do you think the proposed DFR Framework artefact would be in the production environment in case of preserving potential digital evidence?	Yes, I think the proposed DFR framework artefact will be effective for the production environment, the operation of forensic drone and 3 servers are quite perfect to detect threat due to flow chart.
2	Are the defined components of the proposed DFR Framework artefact clear and relevant to what you observe?	Yes, clear.
3	Do you think the provided requirements helpful and adequate in designing DFR Framework artefact for WMedSys?	So far, it is OK for networking point of view. But it may need to consider some more software compatibility with HIS, RIS, PACS networks and DICOM protocol.
4	Do you think the proposed artefact is useful and realistic in improving/addressing user/patient safety?	The proposed framework is more concerning about forensic evidence. It is useful and realistic. I am thinking of prevention (network security) and investigation working together in the same network.
5	How easy or difficult do you think it is to implement and integrate the proposed DFR Framework artefact in an existing WMedSys?	Yes, it is easy to understand and implement.
6	What was an approximate time for you to follow all components of proposed DFR Framework artefact? Was it easy to understand?	Yes, it is not much difficult to understand. My background is not IT, just medical engineer and it can understand for 2 hours.
7	Do you think there is any area of improvement in the proposed artefact? If so, please give your suggestion.	Normally, a hospital network consists of Hospital Information System (HIS) /RIS and PACS servers. If your proposed artefact put these in your flow chart, then it will be more familiar chart for hospital Biomedical Medical Engineer (BME).
8	Is there any modification that should be made to any component of the proposed DFR Framework?	It is OK.
9	Do you think the proposed DFR Framework is effective and efficient in capturing security attacks on a WMedSys?	Yes, I consider it is effective.

10	Do you think the proposed DFR Framework is effective and efficient in determining security attacks on a WMedSys?	Yes, I think it is effective on detecting security attack.
11	Do you think the proposed DFR Framework is effective and efficient in addressing to improve patient/user safety?	Yes, I think it is effective and efficient for addressing common security attack.
12	Please provide your comments on the usability and ease of operation.	In X Ray, MRI images, the images and annotation are in DICOM format and so DFR application level is needed to align with the DICOM protocol.
13	Can you list the weaknesses and strengths of the proposed DFR Framework artefact for WMedSys?	Strength – easy to implement, competitive price Weakness- may need some more software modification to get deeper investigation, (some software patch which can access HL7, DICOM format).
14	Regarding the completeness of the DFR Framework artefact for WMedSys, how do you think?	Yes, the framework consideration is perfect. It may need some more alignment software patch for various protocol used in medical systems (DICOM, HL7).
15	Were the information provided related to the artefact logical and helpful?	Yes, it is.
16	Is the proposed DFR Framework artefact cost effective and efficient?	Yes, surely cost effective and efficient.
17	Is the proposed artefact likely to be widely adopted and implemented in WMedSys?	Yes, it is basic need for the field and likely to be widely adopted and implemented in WMedSys.
18	How effective do you think the proposed DFR Framework could be if IT managers/security engineers of clinical and hospital networks starts using it in their WMedSys?	I think it will help a lot of hospital and patient information security.

Table D3: Expert 3's Evaluation Feedback

No.	Description	Expert's Answer
DFR Framework for WMedSys: Overall Evaluation		
1	Overall, how effective do you think the proposed DFR Framework artefact would be in the production environment in case of preserving potential digital evidence?	I think that this framework that I see in a prototype version is very thoughtful and has a real-world application. It will need to be implemented and integrated within a robust commercial software package in order to see its real advantages. However, as a prototype I think that it clearly demonstrates the theoretical understanding and does offer businesses a new opportunity. It may be more efficient if the proposed framework is implemented in such a what that runs as a client-server. For example, collecting agents run on the client system.
2	Are the defined components of the proposed DFR Framework artefact clear and relevant to what you observe?	Yes.
3	Do you think the provided requirements helpful and adequate in designing DFR Framework artefact for WMedSys?	Yes. Further refinement can occur after more attacks are tested. However, at present it is sufficient.
4	Do you think the proposed artefact is useful and realistic in improving/addressing user/patient safety?	Yes. It is very useful and realistic in improving/addressing user/patient safety.
5	How easy or difficult do you think it is to implement and integrate the proposed DFR Framework artefact in an existing WMedSys?	It was very easy to implement and integrate. Although, it was slightly difficult to understand the framework at first. Once having better understand about the framework and how it worked, it was very easy to follow.
6	What was an approximate time for you to follow all components of proposed DFR Framework artefact? Was it easy to understand?	It took about 2 to 3 minutes once I worked out what to do.
7	Do you think there is any area of improvement in the proposed artefact? If so, please give your suggestion.	As a framework this is fine. However, there is a very possible the database will be overflowed after certain period of time. The overflowing policy should be in place if it occurs.
8	Is there any modification that should be made to any component of the proposed DFR Framework?	Currently, there is no modification needed.

9	Do you think the proposed DFR Framework is effective and efficient in capturing security attacks on a WMedSys?	Yes. It is very effective and efficient in capturing security attacks, and I think that many network security experts and digital forensic investigators will want to use it.
10	Do you think the proposed DFR Framework is effective and efficient in determining security attacks on a WMedSys?	Yes. It is very effective and efficient in determining security attacks, and I think that many network security experts and digital forensic investigators will want to use it. However, IDS database needs to be tested and customised for improvements after initial set up.
11	Do you think the proposed DFR Framework is effective and efficient in addressing to improve patient/user safety?	Yes. It is very effective and efficient in addressing to improve patient/user safety, and I think that many network security experts and digital forensic investigators will want to use it. However, IDS database needs to be tested and customised for improvements after initial set up.
12	Please provide your comments on the usability and ease of operation.	I found it easy and intuitive to use but as I said above for a commercial application, framework will need to be implemented as an integrated software.
13	Can you list the weaknesses and strengths of the proposed DFR Framework artefact for WMedSys?	Strength: It is easy to use. It does what it says. It solves a problem. As mentioned above it requires redevelopment for commercial implementation. : It is very flexible and cost-efficient. Weakness: It is hard to determine unless the prototype is implemented in a real-world scenario.
14	Regarding the completeness of the DFR Framework artefact for WMedSys, how do you think?	Yes. All instructions are very help and clear.
15	Were the information provided related to the artefact logical and helpful?	Yes. All instructions are very help and clear.
16	Is the proposed DFR Framework artefact cost effective and efficient?	Yes.
17	Is the proposed artefact likely to be widely adopted and implemented in WMedSys?	Yes, once the above improvements are implemented, networking security experts and digital forensic investigators can see the advantages of using it.

18	How effective do you think the proposed DFR Framework could be if IT managers/security engineers of clinical and hospital networks starts using it in their WMedSys?	Effectiveness improves in quality cycles so that learning would have to be built into the adoption framework to be effective. Networking experts and digital forensic investigators will determine to adopt the system once it can be implemented either to automated system or to integrate to existing system.

Table D4: Expert 4's Evaluation Feedback

No.	Description	Expert's Answer
DFR Framework for WMedSys: Overall Evaluation		
1	Overall, how effective do you think the proposed DFR Framework artefact would be in the production environment in case of preserving potential digital evidence?	The logging capability could be useful as long as it is easily searchable and filterable to effectively narrow down on a potential security event. An issue with large amounts of logging is looking for actionable data can become similar to trying to find a needle in a haystack.
2	Are the defined components of the proposed DFR Framework artefact clear and relevant to what you observe?	The components of the DFR framework appear to use well-known industry standard solutions.
3	Do you think the provided requirements helpful and adequate in designing DFR Framework artefact for WMedSys?	Yes, as this uses industry standard open-source projects.
4	Do you think the proposed artefact is useful and realistic in improving/addressing user/patient safety?	I believe the most useful component of the framework is the hashing of patient record information. Having a "known good" baseline is important and rather than trying to block all attack attempts, being able to detect modifications is critical.
5	How easy or difficult do you think it is to implement and integrate the proposed DFR Framework artefact in an existing WMedSys?	Implementing the framework should be relatively straight forward, however I'm unsure of the complexities of current WMedSys infrastructure. An assumption I would make is that current infrastructure is well-known to have poor security hygiene. Previous reports of ransomware attacks on hospital networks attests to this.
6	What was an approximate time for you to follow all components of proposed DFR Framework artefact? Was it easy to understand?	Yes, the framework is easy to understand. My understanding is fundamentally there is some 1) data collection systems 2) data processing system 3) inter-connecting systems. There is not a lot of complexity in the framework.

7	Do you think there is any area of improvement in the proposed artefact? If so, please give your suggestion.	I am unsure why wireless scanning is limited to 2.4GHz. Do all WMedSys networks operate at 2.4GHz? I'd recommend adding support for all used radio spectrums used in hospital equipment to ensure all devices can be included for forensic readiness.
8	Is there any modification that should be made to any component of the proposed DFR Framework?	Consider the robustness of using a TP-Link wireless adaptor. Will this withstand the harsh everyday requirements. Is there a more rugged option?
9	Do you think the proposed DFR Framework is effective and efficient in capturing security attacks on a WMedSys?	It is important to note that no system could ever capture all security events, especially targeted and sophisticated attacks. However, the logging and IDS systems implemented in the framework would provide a 'good enough' level of monitoring. I believe the key component is being alerted of modifications to patient records.
10	Do you think the proposed DFR Framework is effective and efficient in determining security attacks on a WMedSys?	The ability to determine a security attack relies on the capability of the IDS and the security analyst tasked with reviewing this information. It would be important to ensure the IDS is kept up to date.
11	Do you think the proposed DFR Framework is effective and efficient in addressing to improve patient/user safety?	My understanding of the most important factors to ensure patient safety would be the availability of the wireless systems (i.e. not unavailable due to ransomware) and the integrity of the data. The framework appears to focus on information collection more so that data protection. This may be in the form of critical forensic data is replicated and backed up, so it is not lost in a security incident.
12	Please provide your comments on the usability and ease of operation.	The framework should be easy to use, assuming the logging information is easily reviewable by the end security analyst. Splunk is a well-known SEIM, however it requires thoughtful configuration to reduce the 'noise' of large amounts of logging.
13	Can you list the weaknesses and strengths of the proposed DFR Framework artefact for WMedSys?	Strengths I believe include: the use of industry standard open-source projects makes it cheap and easy to implement. Weaknesses I believe relate to the availability of data. What if the systems in the framework are attacked? At what point can you trust the forensic data?

14	Regarding the completeness of the DFR Framework artefact for WMedSys, how do you think?	A mentioned, I would recommend looking at the entire radio spectrum used by wireless devices, including Wi-Fi 5GHz. Also review replication and backups to ensure the integrity of forensic data.
15	Were the information provided related to the artefact logical and helpful?	Yes, the framework follows a logical flow from data collection to systems that would make the data available to be reviewed by an analyst.
16	Is the proposed DFR Framework artefact cost effective and efficient?	Yes, it uses industry standard open-source tooling. Most of the cost of implementing the framework would be hardware. Also consider the cost of replacing failed hardware, such as in the wireless drone, this may be suspectable to failures.
17	Is the proposed artefact likely to be widely adopted and implemented in WMedSys?	I'm not sure as I don't have familiarity with this infrastructure. I suspect hospital infrastructure is often restricted by budget constraints and often built on a 'needs basis'.
18	How effective do you think the proposed DFR Framework could be if IT managers/security engineers of clinical and hospital networks starts using it in their WMedSys?	I believe the framework would assist in providing a standardised approach to forensic data collection of historically insecure devices (wireless devices). I also believe WMedSys systems require a layered approach to security and active monitoring to response to valid incidents.

Table D5: Expert 5's Evaluation Feedback

No.	Description	Expert's Answer
DFR Framework for WMedSys: Overall Evaluation		
1	Overall, how effective do you think the proposed DFR Framework artefact would be in the production environment in case of preserving potential digital evidence?	I think it will be effective in preserving digital evidence. It has the necessary and appropriate components to do this task.
2	Are the defined components of the proposed DFR Framework artefact clear and relevant to what you observe?	Yes, they are clear and relevant.
3	Do you think the provided requirements helpful and adequate in designing DFR Framework artefact for WMedSys?	Yes, they are helpful and adequate.

4	Do you think the proposed artefact is useful and realistic in improving/addressing user/patient safety?	It appears to be useful in improving patient safety. However, more evaluation (experiments, simulations) is needed to gauge the effectiveness of the artefact.
5	How easy or difficult do you think it is to implement and integrate the proposed DFR Framework artefact in an existing WMedSys?	I think it can be easily implemented and integrated in existing WMedSys.
6	What was an approximate time for you to follow all components of proposed DFR Framework artefact? Was it easy to understand?	Approximately 10 min. It was easy to understand.
7	Do you think there is any area of improvement in the proposed artefact? If so, please give your suggestion.	WPA3 can be incorporated in the artefact.
8	Is there any modification that should be made to any component of the proposed DFR Framework?	5 GHz should also be scanned as it is widely used these days.
9	Do you think the proposed DFR Framework is effective and efficient in capturing security attacks on a WMedSys?	It has appropriate servers to detect attacks like DDoS, Port Scanning. However, some performance metrics (e.g. attack detection time) which are critical for determining efficiency should be taken into account.
10	Do you think the proposed DFR Framework is effective and efficient in determining security attacks on a WMedSys?	It can determine some attacks as mentioned above.
11	Do you think the proposed DFR Framework is effective and efficient in addressing to improve patient/user safety?	It appears to be effective and efficient in improving patient safety. However, experimental results are needed to gauge the effectiveness and efficiency of this framework.
12	Please provide your comments on the usability and ease of operation.	It can easily be used. No issues with usability.
13	Can you list the weaknesses and strengths of the proposed DFR Framework artefact for WMedSys?	Strengths: Usability, easy to implement, preserving digital evidence Weaknesses: Does not consider 5GHz
14	Regarding the completeness of the DFR Framework artefact for WMedSys, how do you think?	Health care facilities have now started using SDN enabled WLANs. How about incorporating SDN in this framework?
15	Were the information provided related to the artefact logical and helpful?	Some more information regarding the novelty of the artefact would have been useful.

16	Is the proposed DFR Framework artefact cost effective and efficient?	Yes, it is certainly cost effective. However, it is difficult to comment on efficiency without any results.
17	Is the proposed artefact likely to be widely adopted and implemented in WMedSys?	It can be widely adopted because of cost effectiveness and ease of implementation.
18	How effective do you think the proposed DFR Framework could be if IT managers/security engineers of clinical and hospital networks starts using it in their WMedSys?	It appears to be effective in preserving digital evidence and detecting some attacks. IT managers may use it with some additions and modifications.

Table D6: Expert Evaluation Feedback Combined with Researcher's Comment

No.	Description	Expert 1 (Answers)	Expert 2 (Answers)	Expert 3 (Answers)	Expert 4 (Answers)	Expert 5 (Answers)	Researcher's Comment
1	Overall, how effective do you think the proposed DFR Framework artefact would be in the production environment in case of preserving potential digital evidence?	The propose DFR Framework is effective for wireless attacks through the drone and the forensic server, and effective for the internal and Internet attacks, through the IDS server and agents.	Yes, I think the proposed DFR Framework artefact will be effective for the production environment, the operation of forensic drone and 3 servers are quite perfect to detect threat due to flow chart.	I think that this framework that I see in a prototype version is very thoughtful and has a real-world application. It will need to be implemented and integrated within a robust commercial software package in order to see its real advantages. However, as a prototype I think that it clearly demonstrates the theoretical understanding and does offer businesses a new opportunity. It may be more efficient if the proposed framework is implemented in such a what that runs as a client-server. For example, collecting agents run on the client system.	The logging capability could be useful as long as it is easily searchable and filterable to effectively narrow down on a potential security event. An issue with large amounts of logging is looking for actionable data can become similar to trying to find a needle in a haystack.	I think it will be effective in preserving digital evidence. It has the necessary and appropriate components to do this task.	I do agree all experts' opinions. Especially, the Syslog server should be capable of dealing with large volume of inbound logs for storage and processing of the logs for later retrieval in an easily readable, searchable and secure format.

2	Are the defined components of the proposed DFR Framework artefact clear and relevant to what you observe?	The components proposed by the framework are clearly explained in a diagram and text.	Yes, clear.	Yes.	The components of the DFR Framework appear to use well-known industry standard solutions.	Yes, they are clear and relevant.	All experts agree to the fact that the defined components of the artefact are clear and relevant.
3	Do you think the provided requirements helpful and adequate in designing DFR Framework artefact for WMedSys?	I think the DFR Framework requirements are adequate for designing an artefact for any wireless medical system.	So far, it is OK for networking point of view. But it may need to consider some more software compatibility with HIS, RIS, PACS networks and DICOM protocol.	Yes. Further refinement can occur after more attacks are tested. However, at present it is sufficient.	Yes, as this uses industry standard open-source projects.	Yes, they are helpful and adequate.	Yes, I do agree further refinement is required for the proposed DFR Framework artefact after testing with different types of attacks on WMedSys.

4	Do you think the proposed artefact is useful and realistic in improving/addressing user/patient safety?	I think the proposed artefact is realistic in addressing patient safety since it could be integrated with existing systems.	The proposed framework is more concerning about forensic evidence. It is useful and realistic. I am thinking of prevention (network security) and investigation working together in the same network.	Yes. It is very useful and realistic in improving/ addressing user/patient safety.	I believe the most useful component of the framework is the hashing of patient record information. Having a "known good" baseline is important and rather than trying to block all attack attempts, being able to detect modifications is critical.	It appears to be useful in improving patient safety. However, more evaluation (experiments, simulations) is needed to gauge the effectiveness of the artefact.	All experts agree that the proposed artefact is useful and realistic in improving/addressing user/patient safety. However, some experts have mentioned different comments in improving the effectiveness of the artefact.
5	How easy or difficult do you think it is to implement and integrate the proposed DFR Framework artefact in an existing WMedSys?	Implementing the services in the proposed framework is very easy and does not require additional skills for IT professionals/system engineers/network administrators.	Yes, it is easy to understand and implement.	It was very easy to implement and integrate. Although, it was slightly difficult to understand the framework at first. Once having better understand about the framework and how it worked, it was very easy to follow.	Implementing the framework should be relatively straight forward, however I'm unsure of the complexities of current WMedSys infrastructure. An assumption I would make is that current infrastructure is well-known to have poor security hygiene. Previous reports of ransomware attacks on hospital networks attests to this.	I think it can be easily implemented and integrated in existing WMedSys.	All experts agree that it is easy to implement and integrate the proposed DFR Framework artefact in an existing WMedSys. However, one expert think it would be difficult as the requirement of technical skill level is high for implementing it.

6	What was an approximate time for you to follow all components of proposed DFR Framework artefact? Was it easy to understand?	It took about 30 minutes to follow all of the components of the framework; it was very easy to understand.	Yes, it is not much difficult to understand. My background is not IT, just medical engineer and it can understand for 2 hours.	It took about 2 to 3 minutes once I worked out what to do.	Yes, the framework is easy to understand. My understanding is fundamentally there is some 1) data collection systems 2) data processing system 3) inter-connecting systems. There is not a lot of complexity in the framework.	Approximately 10 min. It was easy to understand.	Overall, how effective do you think the proposed DFR Framework artefact would be in the production environment in case of preserving potential digital evidence
7	Do you think there is any area of improvement in the proposed artefact? If so, please give your suggestion.	Symbols used in the framework design should be explained and be consistent. For example, the square symbol is used for branching and aggregating. Second, there should be no END symbol in the diagram since the process is non-terminating.	Normally, a hospital network consists of Hospital Information System (HIS) /RIS and PACS servers. If your proposed artefact put these in your flow chart, then it will be more familiar chart for hospital Biomedical Engineer (BME).	As a framework this is fine. However, there is a very possible the database will be overflowed after certain period of time. The overflowing policy should be in place if it occurs.	I am unsure why wireless scanning is limited to 2.4GHz. Do all WMedSys networks operate at 2.4GHz? I would recommend adding support for all used radio spectrums used in hospital equipment to ensure all devices can be included for forensic readiness.	WPA3 can be incorporated in the artefact.	Yes, I do agree that there are a few areas of improvement in the proposed DFR Framework artefact, as it is limited to IEEE 802.11 2.4GHz band (WMedSys / HIS). For future work, it needs to be designed and tested with other frequency bands and the latest wireless security standard (WPA3-Enterprise).

8	Is there any modification that should be made to any component of the proposed DFR Framework?	I do not think there is any need for more components or modification be made to the existing framework.	It is OK.	Currently, there is no modification needed.	Consider the robustness of using a TP-Link wireless adaptor. Will this withstand the harsh everyday requirements. Is there a more rugged option?	5 GHz should also be scanned as it is widely used these days.	Most experts agree that any modification is not required to any component of the proposed artefact as it is sufficient at present to an architectural advancement.
9	Do you think the proposed DFR Framework is effective and efficient in capturing security attacks on a WMedSys?	I think the proposed DFR Framework is as effective as the implemented IDS software, the wireless drone, and the wireless forensic server.	Yes, I consider it is effective.	Yes. It is very effective and efficient in capturing security attacks, and I think that many network security experts and digital forensic investigators will want to use it.	It is important to note that no system could ever capture all security events, especially targeted and sophisticated attacks. However, the logging and IDS systems implemented in the framework would provide a 'good enough' level of monitoring. I believe the key component is being alerted of modifications to patient records.	It has appropriate servers to detect attacks like DDoS, Port Scanning. However, some performance metrics (e.g. attack detection time) which are critical for determining efficiency should be taken into account.	Most experts think the proposed DFR Framework artefact is effective and Expert 3 has stated that many security professionals and digital forensic investigator may want to use it. Expert 4 has mentioned that the components of the framework would provide 'good enough' level of monitoring. On the other hand, Expert 5 has pointed out the efficiency should be tested with other metrics.

10	Do you think the proposed DFR Framework is effective and efficient in determining security attacks on a WMedSys?	I think the proposed DFR Framework is effective and efficient in detecting common security attacks on wireless medical networks.	Yes, I think it is effective on detecting security attacks.	Yes. It is very effective and efficient in determining security attacks, and I think that many network security experts and digital forensic investigators will want to use it. However, IDS database needs to be tested and customised for improvements after initial set up.	The ability to determine a security attack relies on the capability of the IDS and the security analyst tasked with reviewing this information. It would be important to ensure the IDS is kept up to date.	It can determine some attacks as mentioned above.	All experts agree that the proposed DRF Framework is effective and efficient. However, Expert 3 and 4 pointed out the IDS component of the artefact should be kept up to date.
11	Do you think the proposed DFR Framework is effective and efficient in addressing to improve patient/user safety?	I think The DFR Framework is comprehensive and it is an improvement on patient safety by providing awareness and training for the users and to prevent similar attacks not to be repeated to the wireless medical network.	Yes, I think it is effective and efficient for addressing common security attack.	Yes. It is very effective and efficient in addressing to improve patient/user safety, and I think that many network security experts and digital forensic investigators will want to use it. However, IDS database needs to be tested and customised for improvements after initial set up.	My understanding of the most important factors to ensure patient safety would be the availability of the wireless systems (i.e. not unavailable due to ransomware) and the integrity of the data. The framework appears to focus on information collection more so that data protection. This may be in the form of critical forensic data is replicated and backed up, so it is not lost in a security incident.	It appears to be effective and efficient in improving patient safety. However, experimental results are needed to gauge the effectiveness and efficiency of this framework.	All experts agree that the proposed artefact is effective and efficient in addressing to improve patient/user safety.

12	Please provide your comments on the usability and ease of operation.	The framework is usable, since it does not require additional technical skills to implement.	In X-Ray, MRI images, the images and annotation are in DICOM format and so DFR application level is needed to align with the DICOM protocol.	I found it easy and intuitive to use but as I said above for a commercial application, framework will need to be implemented as an integrated software.	The framework should be easy to use, assuming the logging information is easily reviewable by the end security analyst. Splunk is a well-known SEIM, however it requires thoughtful configuration to reduce the 'noise' of large amounts of logging.	It can easily be used. No issues with usability.	All experts agree that the artefact is easy to use theoretically. However, the artefact should be tested in a controlled environment for proof of concept.

13	Can you list the weaknesses and strengths of the proposed DFR Framework artefact for WMedSys?	Strength: low cost resources. Weaknesses: (1) There is always security risks, similar to any computer network; (2) using only the 2.4GHz band.	Strength – easy to implement, competitive price Weakness- may need some more software modification to get deeper investigation, (some software patch which can access HL7, DICOM format)	Strength: It is easy to use. It does what it says. It solves a problem. As mentioned above it requires redevelopment for commercial implementation. It is very flexible and cost-efficient. Weakness: It is hard to determine unless the prototype is implemented in a real-world scenario.	Strengths I believe include: the use of industry standard open-source projects makes it cheap and easy to implement. Weaknesses I believe relate to the availability of data. What if the systems in the framework are attacked? At what point can you trust the forensic data?	Strengths: Usability, easy to implement, preserving digital evidence Weaknesses: Does not consider 5GHz.	All experts agree that the artefact is easy to use, easy to implement, cost effective and one of the main strengths is its design and suitable risk coverage. But the weaknesses mentioned by some experts include the artefact needs to be integrated with other hospital systems and the prototype should be thoroughly tested before commercialising it.

14	Regarding the completeness of the DFR Framework artefact for WMedSys, how do you think?	It is complete as far as I know.	Yes, the framework consideration is perfect. It may need some more alignment software patch for various protocol used in medical systems (DICOM, HL7).	Yes. All instructions are very helpful and clear.	A mentioned, I would recommend looking at the entire radio spectrum used by wireless devices, including Wi-Fi 5GHz. Also review replication and backups to ensure the integrity of forensic data.	Health care facilities have now started using Software Defined Network (SDN) enabled WLANs. How about incorporating SDN in this framework?	All experts agree that the DFR Framework artefact is complete. However, some experts recommend the proposed artefact should be tested with various protocols used in WMedSys (Expert 2), 5GHz wireless frequency band (Expert 4), and SDN (Expert 5), in addition to the automisation of residual risk management and data processing.
15	Were the information provided related to the artefact logical and helpful?	The framework design is clear, and the accompanying documents are explaining the components of the framework clearly.	Yes, it is.	Yes. All instructions are very help and clear.	Yes, the framework follows a logical flow from data collection to systems that would make the data available to be reviewed by an analyst.	Some more information regarding the novelty of the artefact would have been useful.	All experts agree that the information provided related to the artefact is logical, clear, useful and helpful.

16	Is the proposed DFR Framework artefact cost effective and efficient?	The proposed DFR Framework artefacts is cost effective because it is using low costs hardware and free open source software.	Yes, surely cost effective and efficient.	Yes.	Yes, it uses industry standard open-source tooling. Most of the cost of implementing the framework would be hardware. Also consider the cost of replacing failed hardware, such as in the wireless drone, this may be suspectable to failures.	Yes it is certainly cost effective. However, it is difficult to comment on efficiency without any results.	All experts agree that the proposed DFR Framework artefact is cost effective and efficient because the artefact uses industry standard open-source software and low-cost hardware. However, the artefact still needs to be implemented and tested.
17	Is the proposed artefact likely to be widely adopted and implemented in WMedSys?	It follows from (16) above that the framework is likely be adopted by healthcare providers.	Yes, it is basic need for the field and likely to be widely adopted and implemented in WMedSys.	Yes, once the above improvements are implemented, networking security experts and digital forensic investigators can see the advantages of using it.	I am not sure as I do not have familiarity with this infrastructure. I suspect hospital infrastructure is often restricted by budget constraints and often built on a 'needs basis'.	It can be widely adopted because of cost effectiveness and ease of implementation.	All experts agree that the proposed artefact is likely to be widely adopted if hospitals or clinics have enough budget.

18	How effective do you think the proposed DFR Framework could be if IT managers/ security engineers of clinical and hospital networks start using it in their WMedSys?	I think the DFR Framework could be very effective if it was adopted by IT practitioners in healthcare.	I think it will help a lot of hospital and patient information security.	Effectiveness improves in quality cycles so that learning would have to be built into the adoption framework to be effective. Networking experts and digital forensic investigators will determine to adopt the system once it can be implemented either to automated system or to integrate to existing system.	I believe the framework would assist in providing a standardised approach to forensic data collection of historically insecure devices (wireless devices). I also believe WMedSys systems require a layered approach to security and active monitoring to response to valid incidents.	It appears to be effective in preserving digital evidence and detecting some attacks. IT managers may use it with some additions and modifications.	All experts agree that the proposed DFR Framework artefact is very effective for IT managers/security engineers of clinical and hospital networks for risk mitigation, preserving digital evidence and patient safety.

APPENDIX E

(Scenario Test Data 1)

DATACAPTURED IN SYSLOG SERVERS AND WI-FI PINEAPPLE MARK IV

Table E1: SSL stripping attack has been captured on rsyslog server

Attack	SSL Strip (Man-in-the-Middle)	
Date	14/05/2014	
Time	14:00 to 14:30 hours	
User Detail	User host IP address	172.16.50.21
	Username	doc007
	Patient name	James
	Changed Data	BP 130

Test host IP address	172.16.42.167
Changed Data	BP 195

Log Capture at Pineapple

1970-01-01 00:50:30,319 POST Data (172.16.50.5):
new_login_session_management=1&authProvider=Default&authUser=doc007&clearPass=Password1&languageChoice=1
1970-01-01 00:50:33,984 POST Data (172.16.50.5):
drR=0&skip_timeout_reset=1
1970-01-01 00:50:34,233 POST Data (172.16.50.5):
skip_timeout_reset=1
1970-01-01 00:50:34,322 POST Data (172.16.50.5):
skip_timeout_reset=1&ajax=1
1970-01-01 00:50:53,458 POST Data (172.16.50.5):
embeddedScreen=true
1970-01-01 00:50:53,494 POST Data (172.16.50.5):
embeddedScreen=true
1970-01-01 00:51:34,934 POST Data (172.16.50.5):
skip_timeout_reset=1
1970-01-01 00:51:34,946 POST Data (172.16.50.5):
skip_timeout_reset=1&ajax=1
1970-01-01 00:52:35,261 POST Data (172.16.50.5):
skip_timeout_reset=1&ajax=1
1970-01-01 00:52:35,290 POST Data (172.16.50.5):
skip_timeout_reset=1
1970-01-01 00:53:35,646 POST Data (172.16.50.5):
skip_timeout_reset=1
1970-01-01 00:53:35,657 POST Data (172.16.50.5):
skip_timeout_reset=1&ajax=1
1970-01-01 00:53:36,757 POST Data (172.16.50.5):
form_type=0&form_title=HTN&form_diagnosis=&form_injury_grade=&form_injury_part=&form_injury_type=&form_medical_system=&form_medical_type=&form_begin=&form_end=&for

m_active=1&form_return=&form_occur=0&form_classification=0&form_reinjury_id=0&form_reaction=&form_referredby=&form_comments=&form_outcome=0&form_destination=&form_save=Save
1970-01-01 00:54:35,884 POST Data (172.16.50.5):
skip_timeout_reset=1
1970-01-01 00:54:35,896 POST Data (172.16.50.5):
skip_timeout_reset=1&ajax=1
1970-01-01 00:55:36,277 POST Data (172.16.50.5):
skip_timeout_reset=1
1970-01-01 00:55:36,311 POST Data (172.16.50.5):
skip_timeout_reset=1&ajax=1
1970-01-01 00:56:04,835 POST Data (172.16.50.5):
mode=update&id=4&pc_catid=10&facility_id=5&billing_facility=4&form_sensitivity=normal&form_referral_source=&form_date=2014-05-13&form_onset_date=&reason=Bp+195&issues%5B%5D=1&issues%5B%5D=2
1970-01-01 00:56:36,535 POST Data (172.16.50.5):
skip_timeout_reset=1
1970-01-01 00:56:36,552 POST Data (172.16.50.5):
skip_timeout_reset=1&ajax=1

Logs capture at Syslog Server

Android device GT-S7562 has established a connection with private network. At the same time, logclient01 (Host having XAMPP) has generated an event stating, “New process has been created”.

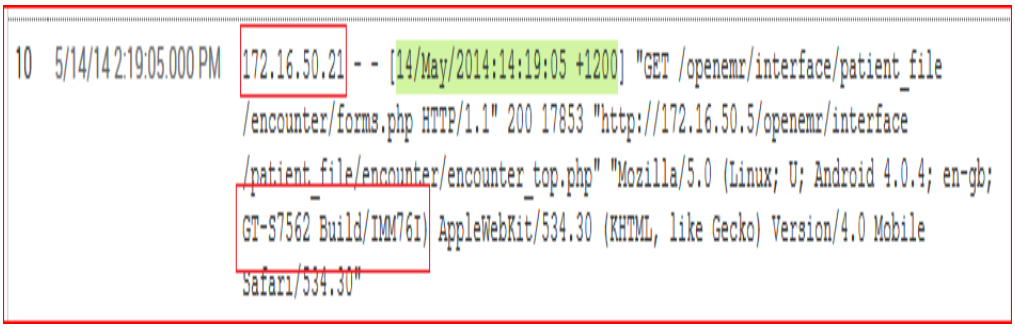


Figure E1: Log captured on the Web Server (OpenEMR)

Syslog message

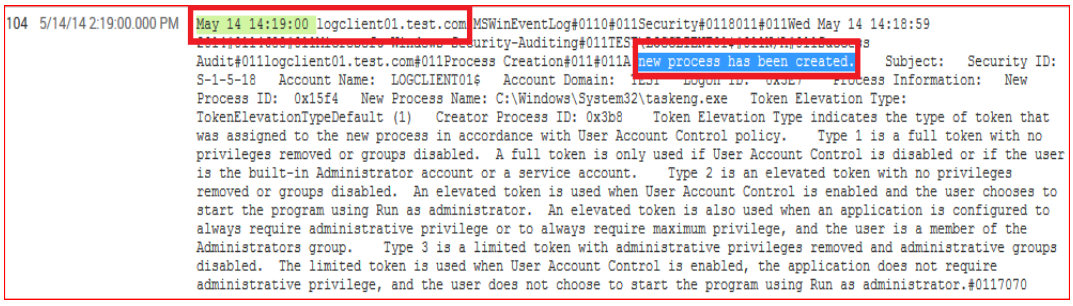


Figure E2: Syslog message

The log captured on the database server (OpenEMR) shows that a user (username doc007) with the IP address of 172.16.50.21 has entered a value BP 130 at backend database at same time.

Edit Copy Delete	260	2014-05-14 14:19:04	patient-record-insert	doc007	Default	INSERT INTO form_encounter SET date = '2014-05-13', onset_date = '', reason = 'Bp 130', facility = 'General Hospital Service location', pc_catid = '10', facility_id = '5', billing_facility = '4', sensitivity = 'normal', referral_source = '', pid = '1', encounter = '12', provider_id = '7'	NULL	1	1
Edit Copy Delete	261	2014-05-14 14:19:04	patient-record-insert	doc007	Default	insert into forms (date, encounter, form_name, form_id, pid, user, groupname, authorized, formdir) values (?, ?, ?, ?, ?, ?, ?, ?, ?, ?) ('2014-05-13','12','New Patient Encounter','4','1','doc007','Default','1','newpatient')	NULL	1	1
Edit Copy Delete	262	2014-05-14 14:19:04	patient-record-delete	doc007	Default	DELETE FROM issue_encounter WHERE pid = ? AND encounter = ? ('1','12')	NULL	1	1
Edit Copy Delete	259	2014-05-14 14:17:21	view	doc007	Default	1	NULL	0	1
Edit Copy Delete	258	2014-05-14 14:15:29	view	doc007	Default	1	NULL	0	1
Edit Copy Delete	257	2014-05-14 14:14:59	login	doc007	Default	success: 172.16.50.21	NULL	0	1

Figure E3: Log captured on the database server (OpenEMR)

Event captured on the web server (OpenEMR) shows that a user with the host IP address of 172.16.50.167 and Windows NT system has been logged in to network at same time.

175 5/14/14 2:28:38.000 PM 172.16.50.167 - - [14/May/2014:14:28:38 +1200] "GET /openemr/interface/patient_file/encounter/forms.php HTTP/1.0" 200 17853 "http://172.16.50.5/openemr/interface/patient_file/encounter/encounter_top.php" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.131 Safari/537.36"

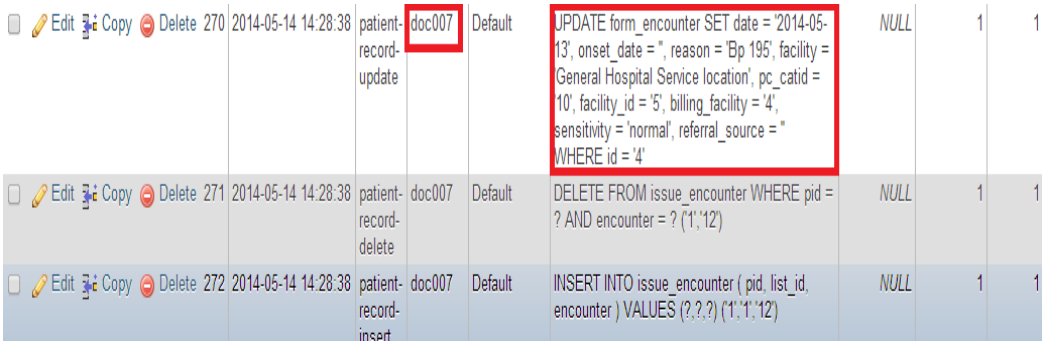
Figure E4: Log captured on the Web Server (OpenEMR)

The log captured on the dc01 (Domain Controller) shows that a remote user has logged in to network.

188 5/14/14 2:28:26.000 PM May 14 14:28:26 dc01.test.com MSWinEventLog#0111#011Security#01170414#011Wed May 14 14:28:26 2014#011#011Microsoft-Windows-Security-Auditing#011TEST\DC01$#011N/A#011Success Audit#011dc01.test.com#011Logon#011#01An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 New Logon: Security ID: S-1-5-18 Account Name: DC01$ Account Domain: TEST Logon ID: 0xee3ab0 Logon GUID: {20CAB494-DF37-F71B-DD29-8272C6B34687} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: 172.16.50.1 Source Port: 61731 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated

Figure E5: Syslog message - DC generated event for remote user

Event generated at OpenEMR database logs shows that backend database value was set to BP 195 at 14:28. The user who changed this detail was using login id "doc007"



Edit Copy Delete	270	2014-05-14 14:28:38	patient-record-update	doc007	Default	UPDATE form_encounter SET date = '2014-05-13', onset_date = '', reason = 'Bp 195', facility = 'General Hospital Service location', pc_catid = '10', facility_id = '5', billing_facility = '4', sensitivity = 'normal', referral_source = '' WHERE id = '4'	NULL	1	1
Edit Copy Delete	271	2014-05-14 14:28:38	patient-record-delete	doc007	Default	DELETE FROM issue_encounter WHERE pid = ? AND encounter = ? ('1','12')	NULL	1	1
Edit Copy Delete	272	2014-05-14 14:28:38	patient-record-insert	doc007	Default	INSERT INTO issue_encounter (pid, list_id, encounter) VALUES (?,?,?) ('1','1','12')	NULL	1	1

Figure E6: Log captured on the database server (OpenEMR)

Finding from all these logs, the backend database was changed twice using same user credentials. The value changed in the backend database could also be found from the logs.

Testing attack 2 at Snare Backlog Server

Table E2: Snare backlog

Attack	SSL Strip (Man-in-the-middle)	
Date	14/05/2014	
Time	14:30 to 14:59 hours	
User Detail	User host IP address	172.16.50.167
	Username	nurse007
	Patient name	XuAlax
	Changed Data	BP 80/120

Test host IP address	172.16.50.22
Changed Data	BP 145/80

Log Captured on the Pineapple

(Note: Time was not set properly at pineapple Mark IV; hence some time difference in following logs can be found.)

1970-01-01 01:16:08,876 POST Data (172.16.50.5):
new_login_session_management=1&authProvider=Default&authUser=nurse007&
clearPass=Password1&languageChoice=1
1970-01-01 01:16:10,204 POST Data (172.16.50.5):
drR=0&skip_timeout_reset=1
1970-01-01 01:16:10,794 POST Data (172.16.50.5):
skip_timeout_reset=1
1970-01-01 01:16:10,811 POST Data (172.16.50.5):
skip_timeout_reset=1&ajax=1
1970-01-01 01:16:21,886 POST Data (172.16.50.5):
embeddedScreen=true
1970-01-01 01:16:21,919 POST Data (172.16.50.5):
embeddedScreen=true
1970-01-01 01:16:59,116 POST Data (172.16.50.5):
embeddedScreen=true
1970-01-01 01:16:59,138 POST Data (172.16.50.5):
embeddedScreen=true
1970-01-01 01:17:10,845 POST Data (172.16.50.5):
drR=0&skip_timeout_reset=1

1970-01-01 01:17:11,033 POST Data (172.16.50.5):
skip_timeout_reset=1
1970-01-01 01:17:11,056 POST Data (172.16.50.5):
skip_timeout_reset=1&ajax=1
1970-01-01 01:17:36,818 POST Data (172.16.50.5):
embeddedScreen=true
1970-01-01 01:17:36,832 POST Data (172.16.50.5):
embeddedScreen=true
1970-01-01 01:17:59,158 POST Data (172.16.50.5):
embeddedScreen=true
1970-01-01 01:17:59,178 POST Data (172.16.50.5):
embeddedScreen=true
1970-01-01 01:18:11,108 POST Data (172.16.50.5):
drR=0&skip_timeout_reset=1
1970-01-01 01:18:11,298 POST Data (172.16.50.5):
skip_timeout_reset=1
1970-01-01 01:18:11,335 POST Data (172.16.50.5):
skip_timeout_reset=1&ajax=1
1970-01-01 01:18:36,200 POST Data (172.16.50.5):
embeddedScreen=true
1970-01-01 01:18:36,210 POST Data (172.16.50.5):
embeddedScreen=true
1970-01-01 01:19:22,650 POST Data (172.16.50.5):
new_login_session_management=1&authProvider=Default&authUser=nurse007&
clearPass=Password1&languageChoice=1
1970-01-01 01:19:23,899 POST Data (172.16.50.5):
skip_timeout_reset=1
1970-01-01 01:19:23,908 POST Data (172.16.50.5):
skip_timeout_reset=1&ajax=1
1970-01-01 01:19:24,081 POST Data (172.16.50.5):
drR=0&skip_timeout_reset=1
1970-01-01 01:19:33,068 POST Data (172.16.50.5):
embeddedScreen=true
1970-01-01 01:19:33,101 POST Data (172.16.50.5):
embeddedScreen=true
1970-01-01 01:20:25,660 POST Data (172.16.50.5):
skip_timeout_reset=1
1970-01-01 01:20:25,673 POST Data (172.16.50.5):
skip_timeout_reset=1&ajax=1
1970-01-01 01:20:43,381 POST Data (172.16.50.5):
mode=update&id=5&pc_catid=10&facility_id=5&billing_facility=4&form_sensitivity=normal&f
orm_referral_source=&form_date=2014-05-13&form_onset_date=&reason=BP+80%2F120

(Got the information about authenticated user's login ID, password and data fed to the backend database).

Logs captured on the Syslog Server

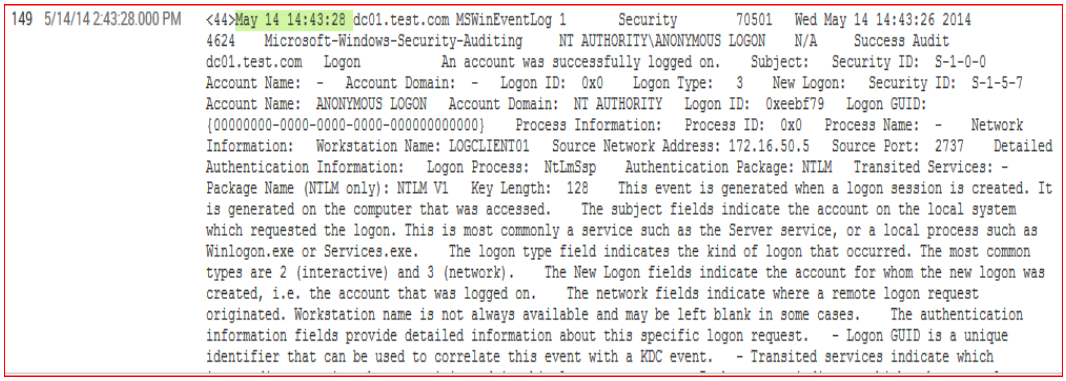


Figure E7: Syslog Message- generated by DC01

The log captured on the database server (OpenEMR) shows that a user (username nurse007) with the IP address of 172.16.50.22 has entered a value BP 80/120 at backend database.

Edit Copy Delete	282	2014-05-14 14:45:36	view	nurse007	Default	2	NULL	0	1
Edit Copy Delete	281	2014-05-14 14:45:35	login	nurse007	Default	success: 172.16.50.22	NULL	0	1
Edit Copy Delete	280	2014-05-14 14:45:22	logout	nurse007	Default	success	NULL	0	1
Edit Copy Delete	277	2014-05-14 14:45:07	patient-record-insert	nurse007	Default	INSERT INTO form_encounter SET date = '2014-05-13', onset_date = '', reason = 'BP 80/120', facility = 'General Hospital Service location', pc_catid = '10', facility_id = '5', billing_facility = '4', sensitivity = 'normal', referral_source = '', pid = '2', encounter = '13', provider_id = '8'	NULL	2	1

Figure E8: Log captured on the database server (OpenEMR)

The log captured on the web server (OpenEMR) shows that a user with Android device (IP address: 172.16.50.22) has been logged in to system at same time.

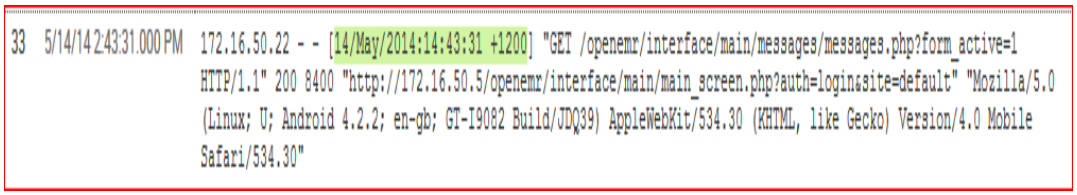


Figure E9: Log captured on the web server (OpenEMR)

From the following logs, we can see that remote user has established a connection with private network.

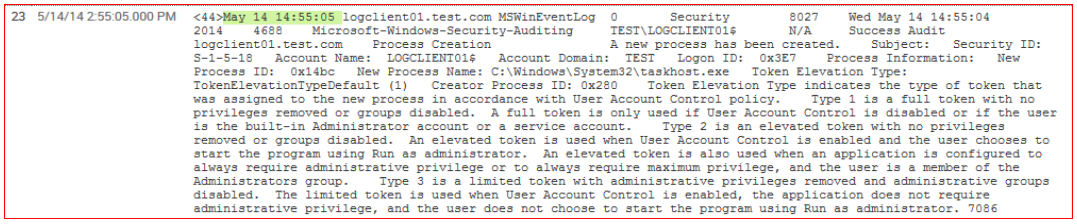


Figure E10: Syslog Message- generated by logclient01

At the same time, logclient01 (XAMPP Host) has generated an event stating, "A new process has been created." The log captured on the database server

(OpenEMR) shows that a user (username nurse007) with the IP address 172.16.167 has entered a value BP 145/80 at backend database.

Edit Copy Delete	307	2014-05-14 14:55:57	logout	nurse007	Default	success	NULL	0	1
Edit Copy Delete	305	2014-05-14 14:55:50	patient-record-update	nurse007	Default	UPDATE form_encounter SET date = '2014-05-13', onset_date = '', reason = 'BP 145/80', facility = 'General Hospital Service location', pc_catid = '10', facility_id = '5', billing_facility = '4', sensitivity = 'normal', referral_source = '' WHERE id = '5'	NULL	2	1
Edit Copy Delete	306	2014-05-14 14:55:50	patient-record-delete	nurse007	Default	DELETE FROM issue_encounter WHERE pid = ? AND encounter = ? ('2','13')	NULL	2	1
Edit Copy Delete	303	2014-05-14 14:55:15	view	nurse007	Default	2	NULL	0	1
Edit Copy Delete	304	2014-05-14 14:55:15	view	nurse007	Default	2	NULL	0	1
Edit Copy Delete	302	2014-05-14 14:55:09	login	nurse007	Default	success: 172.16.50.167	NULL	0	1
Edit Copy Delete	301	2014-05-14 14:53:52	logout	nurse007	Default	success	NULL	0	1

Figure E11: Log captured on the database server (OpenEMR)

The log captured on the web server (OpenEMR) shows that a user with Android device (IP address: 172.16.50.167) has been logged in to system at same time.

```
152  5/14/14 2:55:13.000 PM  172.16.50.167 - - [14/May/2014:14:55:13 +1200] "GET /openemr/library/js/datatables/media/images/forward_disabled.png
                             HTTP/1.1" 200 1363 "http://172.16.50.5/openemr/library/js/datatables/media/css/demo_table.css" "Mozilla/5.0 (Windows
                             NT 6.3; rv:28.0) Gecko/20100101 Firefox/28.0"
```

Figure E12: Log captured on the web server (OpenEMR)

From all these logs, we can clearly say that backend database was changed twice using same user credentials. We can also see the changed value at database logs. These changes were made using different devices having different IP addresses, which only could be possible to when some malicious activity has occurred.

APPENDIX F

(Scenario Test Data 2: Analysis of Findings)

This Appendix F presents the analysis of findings from scenario tests or experiments.

Appendix F1: Data Collection

In order to collect the experimental data, the following two fictitious case scenarios, based on previously well-cited articles (Li et al., 2014; Halperin et al., 2014; Radcliffe, 2012; Li et al., 2011), were used.

Appendix F1.1: Compromising WMedSys that utilises WPA2-PSK

Scenario 1 (WPA2-PSK): A 50-year-old Chief Executive Officer (CEO), John Lauren, from one of the fortune 500 companies, with underlying poorly controlled diabetes mellitus was on a wireless insulin pump to get better control of his blood glucose level. The insulin pump was wirelessly connected with an automatic glucose monitor. Both the pump and glucose monitor were attached to the body and the pump infuses insulin depending on the glucose level data transmitted by the glucose monitor. The pump can store up to 500 units of insulin (250 each for short acting and long acting insulin). The total daily requirement dosage of the insulin is between 0.2-05 units per kilogram based on body weight of the patient.

The higher insulin dose can induce hypoglycemia and without immediate correction of the glucose level, the patient could suffer from permanent brain injury and this could eventually lead to death. John was currently admitted to the emergency department (for seizure followed by loss of consciousness) in order to control his blood glucose level. The blood glucose level was very low. He was immediately treated with glucose bolus IV infusion and he regained conscious later with permeant neurological deficiency. In this first scenario, the emergency department John was admitted to a private clinic that deploys the wireless network based on WPA2-PSK (SSID of WLAN for WMedSys was MyWiFi-Guest).

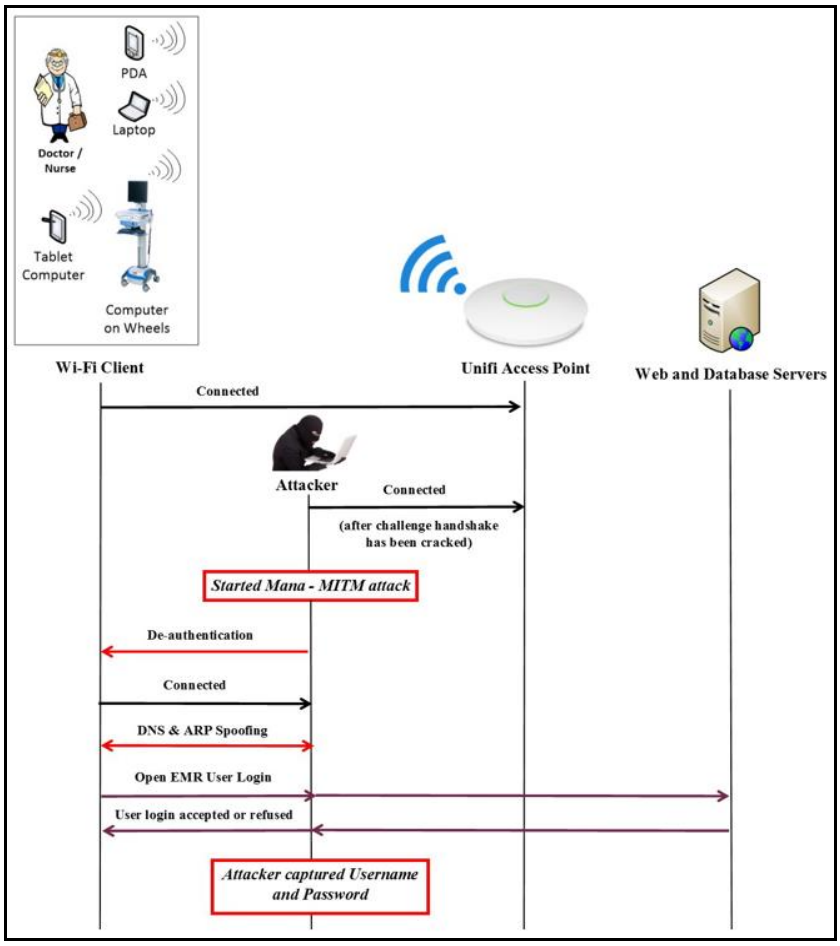


Figure F1: MITM attack carried out by a malicious attacker

Figure F1 shows the Man-in-the-Middle (MITM) attack carried out by a malicious attacker deploying the MANA Toolkit (White & de Villiers, 2014) in order to manipulate the patient's data, which was saved on the backend server (OpenEMR).

The MANA Toolkit was used to create a Fake AP with the same SSID of the legitimate AP used by the clinic. Hence, in this attack scenario, the attacker used a legitimate client login and its password. This legitimate credential was obtained after sniffing the wireless communication between a wireless client (used by a doctor who has a legitimate login username, doc007) to WAP, and performing the brute force attack to crack the password by using Aircrack-ng suite. Afterwards, the malicious attacker accessed the OpenEMR and changed the patient's physiological data (the blood glucose level). The successful MITM attack included de-authentication, DNS and ARP spoofing and capturing the packets related to authentication.

Appendix F1.2: Compromising WMedSys that utilises WPA2-Enterprise

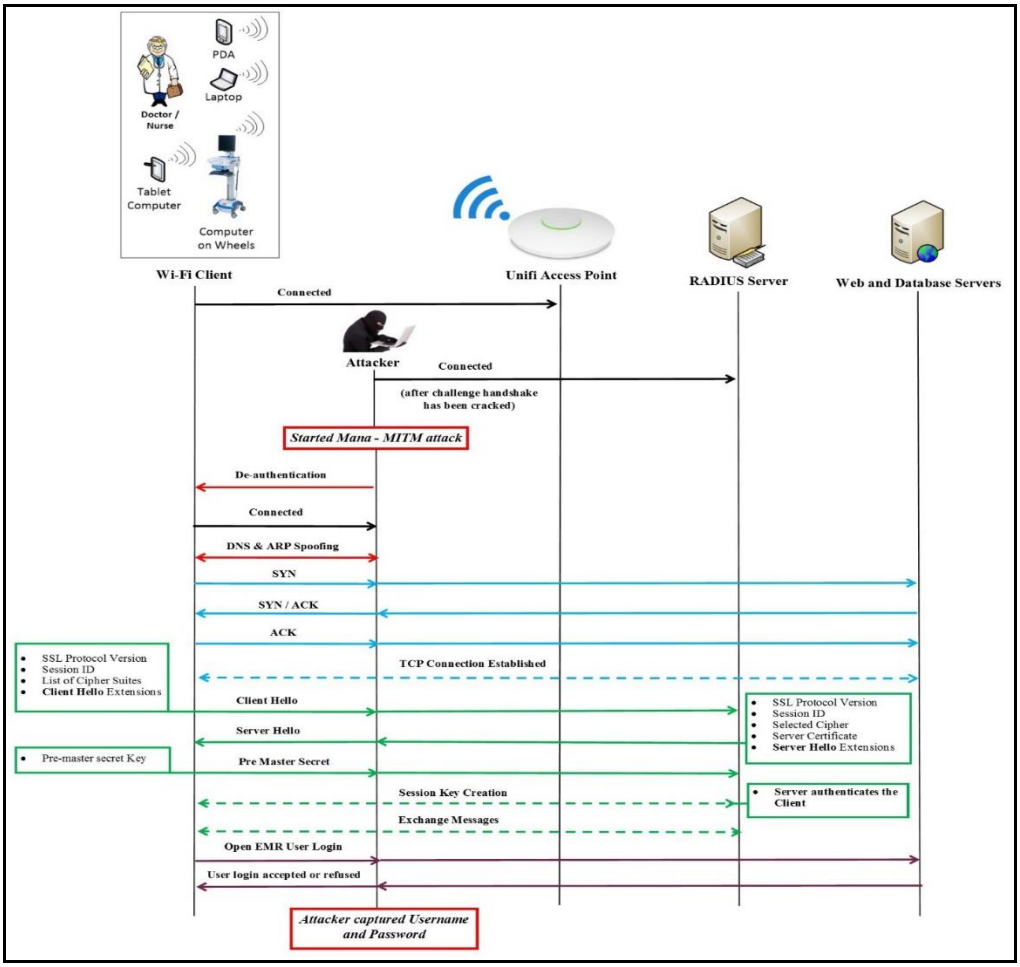


Figure F2: Man-in-the-Middle attack on a WMedSys using WPA2-Enterprise

Scenario 2 (WPA2-Enterprise): The second case scenario was related to the first research sub-question (Section 6.7). Similar to the first scenario, John Lauren was admitted to a hospital in order to control his blood glucose level. Figure F2 depicts the Man-in-the-Middle (MITM) attack carried out by a malicious attacker deploying the MANA Toolkit (White & De Villiers, 2018; White & De Villiers, 2014) in order to manipulate the patient's data from the backend server (OpenEMR), as previously mentioned in Scenario 1.

However, the WMedSys in this scenario was based on WPA2-Enterprise (WPA2-EAP), where users were authenticated by using RADIUS and AD database (SSID of WLAN for WMedSys was MyWiFi). The way in which legitimate users are authenticated against RADIUS server was stated in Hwang et al. (2018). After getting the credentials of WMedSys user (a nurse whose login username is nurse007) by using the methods (see Chapter 7), the malicious attacker amended the patient's physiological data (the blood glucose level).

Appendix F2: Findings from Attack-1: WPA2-PSK with no WFserver

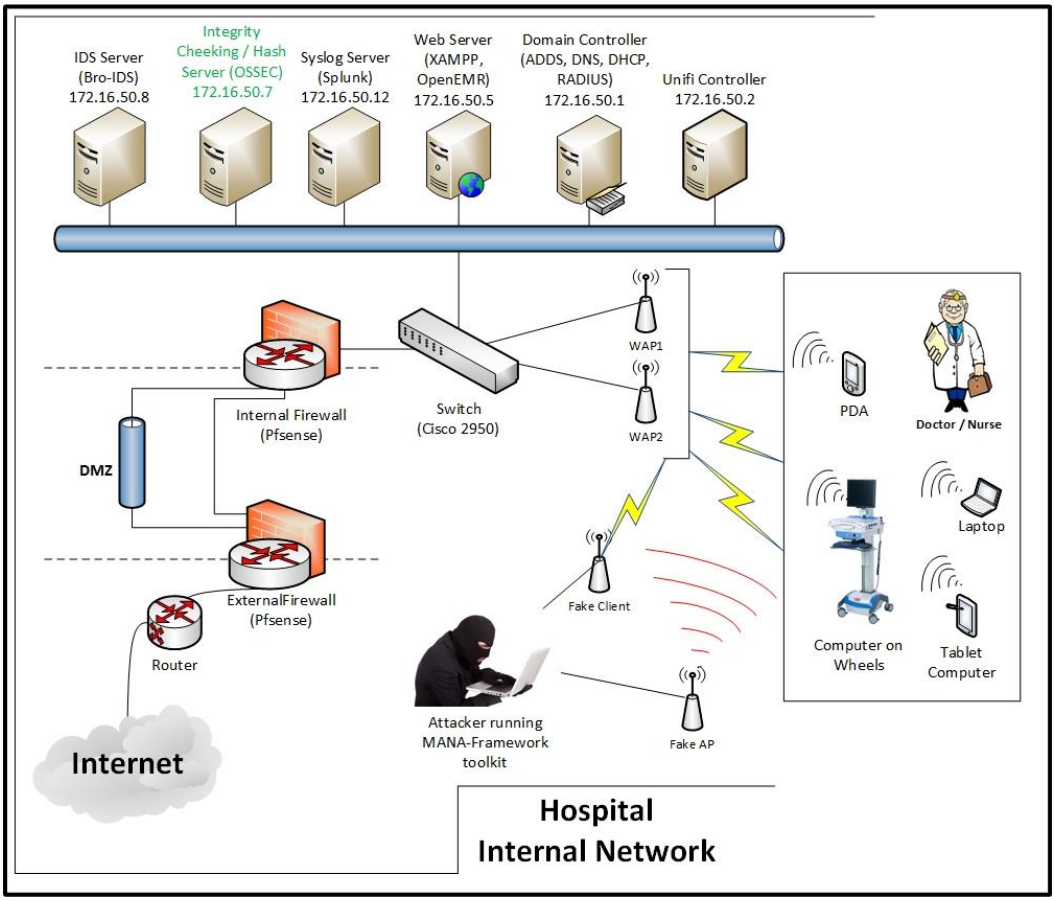


Figure F3: Experimental test-bed (WMedSys) for Attack-1 and Attack-2

After getting the legitimate username and password, the attacker logged in to OpenEMR and changed the data related to any patient. In this fictitious case scenario, the blood glucose level of the patient, John Lauren, was changed by using the captured legitimate login credentials of the doctor (name: Dr Henry Martin, login username: doc007; password: Password1) from a MITM on a WMedSys that uses WPA2-PSK.

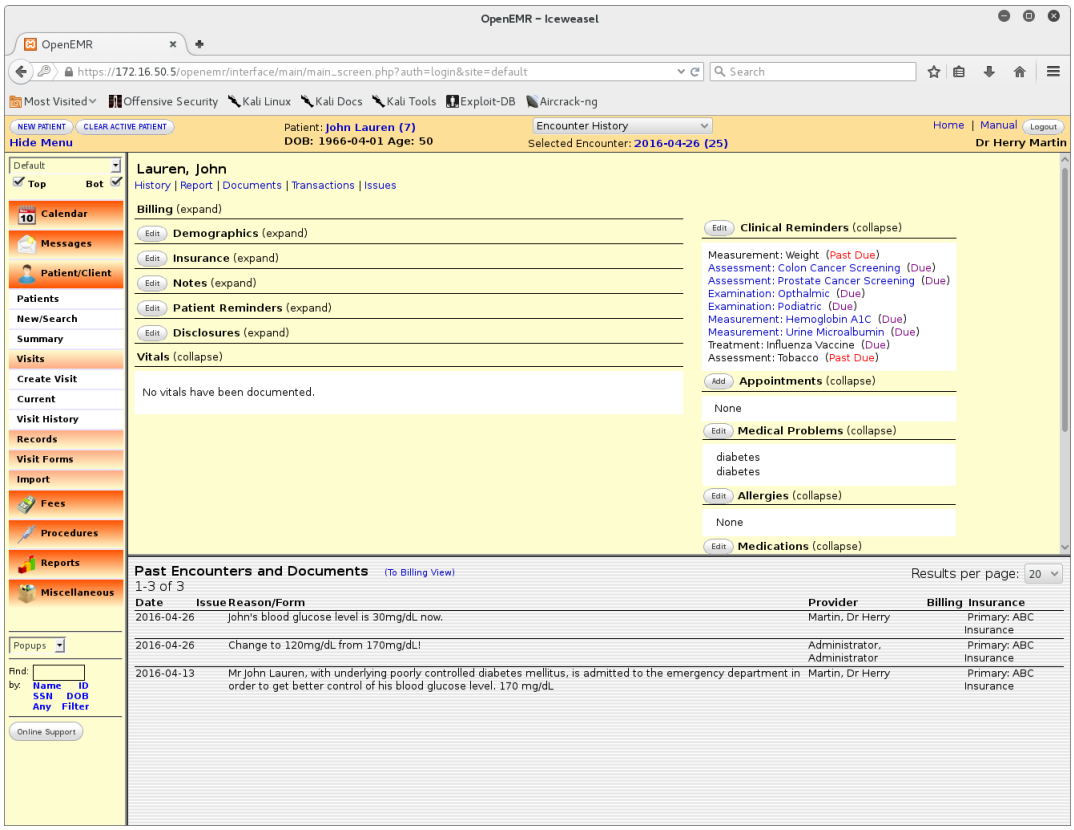


Figure F4: Screenshot of OpenEMR

After analysing the logs from Splunk, DE related to the malicious attack were found as follows.

Appendix F2.1: Attacker's PC

In this scenario, the attacker performed a MITM attack by using the Mana Toolkit. If the attacker's PC could be seized or confiscated, the login username and password could be found in the Mana Framework log (Figure F5) as the attacker logged in to OpenEMR with the obtained credentials.

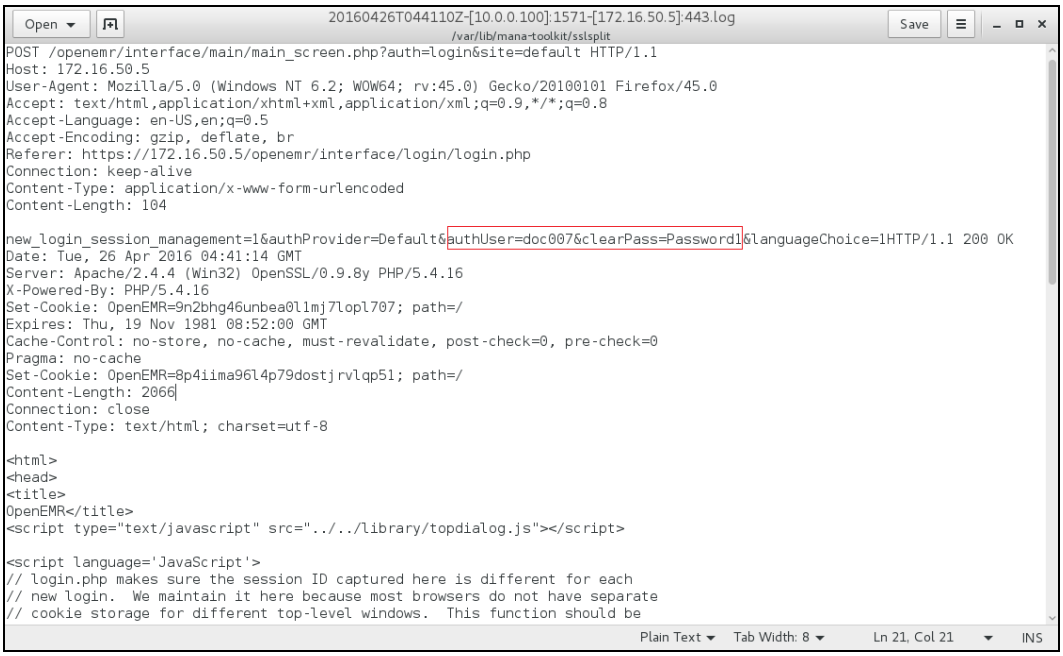


Figure F5: Login credentials found in the log of Mana Framework

Appendix F2.2: DHCP Server

DHCP server provides a centralised administration of IP address configuration and assigns IP addresses to DHCP clients along with other network parameters including the subnet mask, DNS and default gateway IP addresses. It offers not only the tracking of leased IP addresses, but also logging events relating to DHCP activities. Figure F6 shows the timestamp and IP address obtained by the attacker's computer (computer name: Kali; IP address: 172.16.50.151) from the DHCP server within WMedSys.

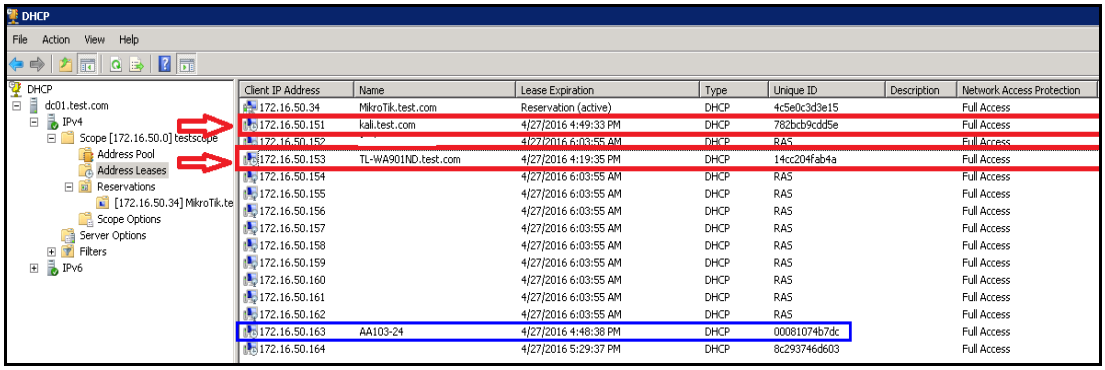


Figure F6: IP addresses distributed by the DHCP server during Attack 1

Appendix F2.3: UniFi Controller Log

UniFi Controller is a software that is installed on a networked computer (IP address: 172.16.50.2) to manage UniFi WAPs by using a web browser (Ubiquiti Networks, 2014). The details of the legitimate WAP including recent events,

alerts, settings, wireless clients, past connections and current usage can be observed by using the UniFi Controller. After investigating the details of recent events, there is an evidence that an illegitimate wireless client is associated with the WAP in WMedSys (Figure F6).

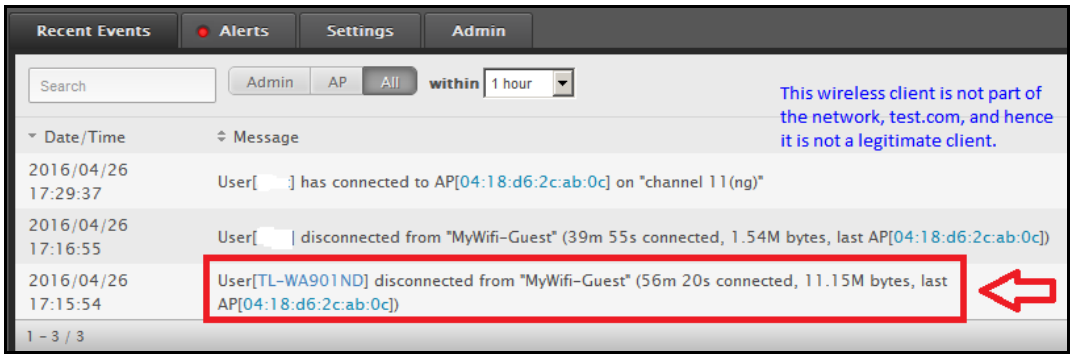


Figure F7: Evidence of an illegitimate wireless client associated with the WAP

Appendix F2.4: OpenEMR Log

Similarly, the log files from OpenEMR (IP address: 172.16.50.5) can provide details information of user's access to the patient database (DB) including login and logout timestamps of users, associated IP addresses, and records of changes or entries to the DB. Hence, the evidential trace of the login timestamp (16:51:23 on 26 April 2016) and IP address of the attacker's machine (172.16.50.151) are found in the OpenEMR log (Figure F8).

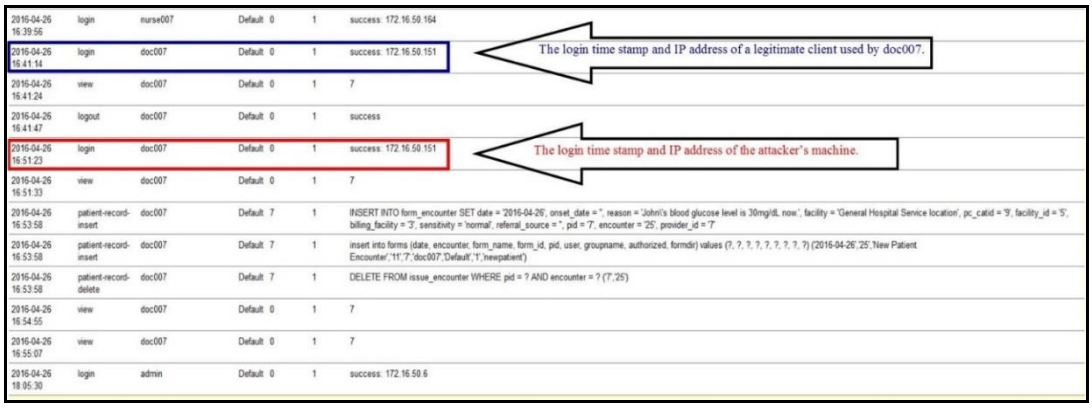


Figure F8: Evidence of login timestamp and IP address of the attacker's machine

Appendix F2.5 Syslog Server (Splunk Enterprise) Logs

A centralised syslog management system (Splunk Enterprise run on 172.16.50.12) of the WMedSys can collect, analyse and provide real-time security alerts by applications and network devices. All network devices including different servers of the WMedSys (XAMPP, OSSEC, Wireless Forensic Server, Wireless Drone,

and DHCP Server) are clients of the Splunk Enterprise and logs from these servers are set up to be forwarded to the Splunk (Figure F9).

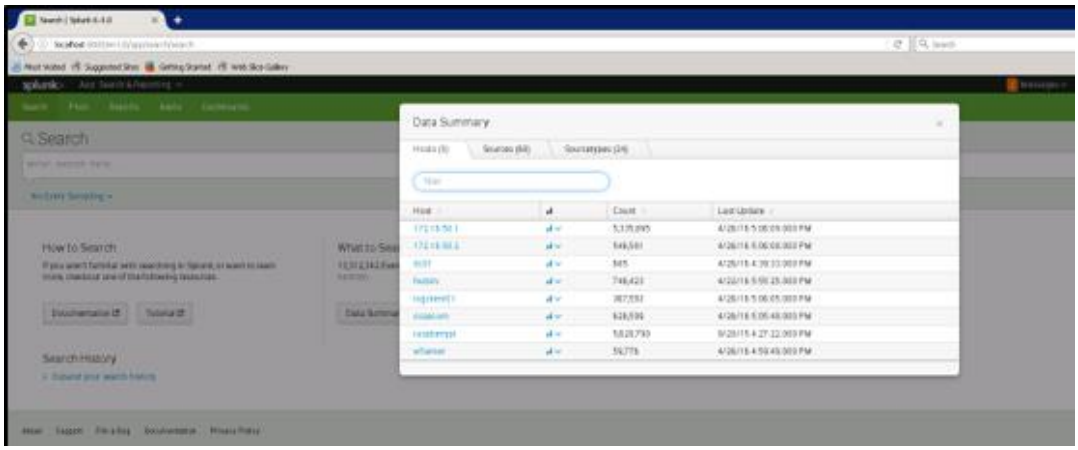


Figure F9: Clients of Splunk Enterprise

Appendix F2.6: DHCP Server Logs

Similar to the evidence found on the DHCP server (Section Appendix F2.2), DHCP server logs (Figure F10) recorded on the Splunk server confirm DE related to IP (172.16.50.151) and MAC addresses of the attacker's computer (78:2B:CB:9C:DD:5E).

dhcp.log

```
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   dhcp
#open   2016-04-26-16-19-29
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       mac     assigned_ip     lease_time      trans_id
#types  time    string  addr    port    addr    port    string  addr    interval        count
1461644369.440286       CxfWe62MoOhryAPaUh      255.255.255.255 68      172.16.50.1     67      14:cc:20:4f:ab:4a       172.16.50.153
86400.000000    887374270
1461644369.444319       CVzkMm1xpTr8DbHxIg      255.255.255.255 68      172.16.50.254   67      14:cc:20:4f:ab:4a       172.16.50.153
86400.000000    887374270
1461644423.212142       CxfWe62MoOhryAPaUh      255.255.255.255 68      172.16.50.1     67      78:2b:cb:9c:dd:5e       172.16.50.151
86400.000000    1657957670
1461644423.212142       CVzkMm1xpTr8DbHxIg      255.255.255.255 68      172.16.50.254   67      78:2b:cb:9c:dd:5e       172.16.50.151
86400.000000    1657957670
1461645058.248355       CN3G4kn0Z770mSHpf       255.255.255.255 68      172.16.50.1     67      00:08:10:74:b7:dc       172.16.50.163
86400.000000    1836702084
1461645278.700076       CIqEQjwbrP1yrTLof       255.255.255.255 68      172.16.50.1     67      00:08:10:74:b7:dc       172.16.50.163
86400.000000    851135990
1461645377.820486       C2XBQA2Re9UmEJVvu       255.255.255.255 68      172.16.50.1     67      78:2b:cb:9c:dd:5e       172.16.50.151
86400.000000    1179701062
1461645377.820486       Czpg6V2K8iwd1Xr9i5      255.255.255.255 68      172.16.50.254   67      78:2b:cb:9c:dd:5e       172.16.50.151
86400.000000    1179701062
1461645415.076344       C2XBQA2Re9UmEJVvu       255.255.255.255 68      172.16.50.1     67      8c:29:37:46:d6:03       172.16.50.164
86400.000000    1987882317
1461646112.564055       CjAxAq4eYzFYoLiQc7      255.255.255.255 68      172.16.50.1     67      00:08:10:74:b7:dc       172.16.50.163
86400.000000    3005460409
1461646167.343897       CjAxAq4eYzFYoLiQc7      255.255.255.255 68      172.16.50.1     67      78:2b:cb:9c:dd:5e       172.16.50.151
86400.000000    1235010921
1461646167.343897       CqCtfyV7hnjtWs29g       255.255.255.255 68      172.16.50.254   67      78:2b:cb:9c:dd:5e       172.16.50.151
86400.000000    1235010921
```

Figure F10: Evidence of IP and MAC addresses of the attacker's computer in DHCP server logs

Appendix F2.7: XAMPP Server Logs

XAMPP (Cross-Platform, Apache, MariaDB, PHP and Perl) is a simple web server solution (running on a networked computer with IP address of 172.16.50.5) for the WMedSys. After analysing XAMPP logs, the evidential traces of login timestamp (4:51:24 PM on 26 April 2016), username (doc007) and IP address of

the computer used by a malicious attacker who accessed OpenEMR were uncovered as shown in Figure F11.

Figure F11: Evidence found in XAMPP server log

Appendix F2.8: OSSEC Server Logs

OSSEC is a host-based intrusion detection and prevention system (HIPS). OSSEC meets the requirements of HIPAA and is capable of performing "file integrity monitoring (FIM), HIDS, log monitoring, Security Incident Management (SIM)/Security Information and Event Management (SIEM), rootkit detection and active response" (OSSEC, 2019).

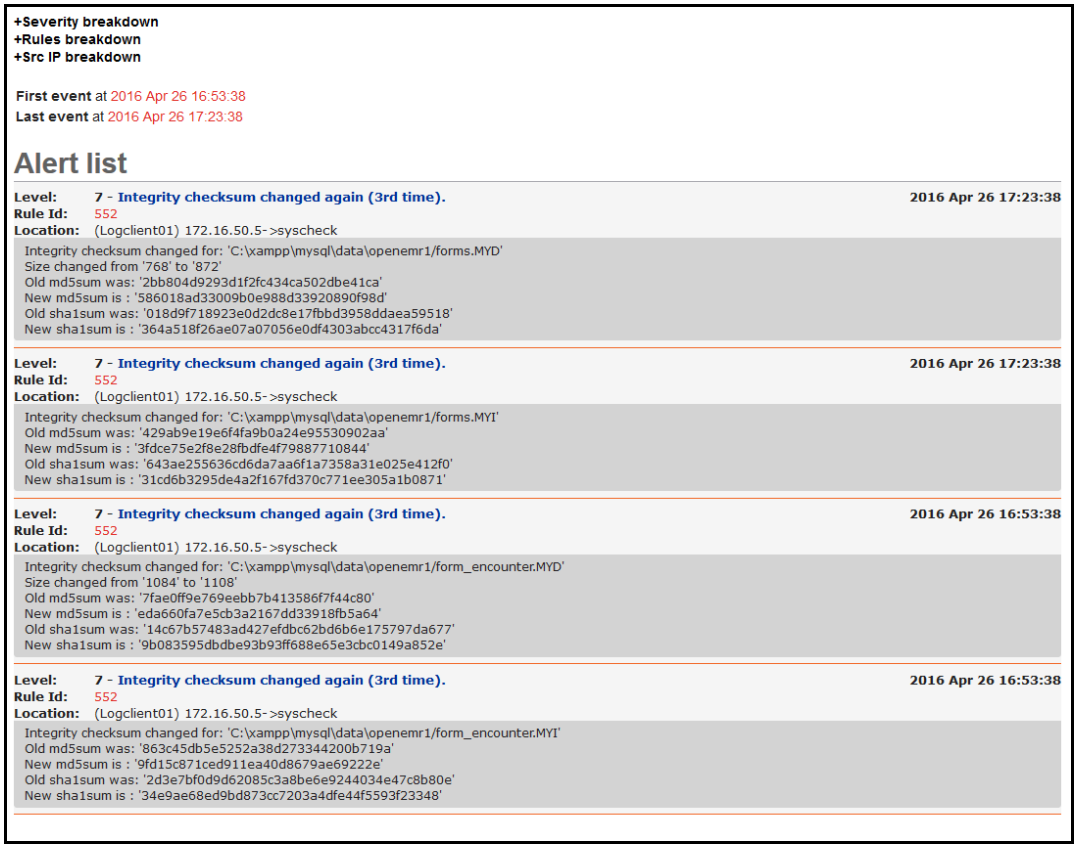


Figure F12: Evidence found in OSSEC server log

However, in the experiment, the OSSEC server (IP address: 172.16.50.7) of WMedSys was used as the FIM server in order to detect and alert changes on the patient database of OpenEMR. Hence, the log from OSSEC (Figure F12) confirms that changes to patient data was initially happened at 4:53:38 PM on 26 April 2016.

Appendix F2.9: Bro-IDS Server Logs

Moreover, the analysis of logs from Bro-IDS server by using Wireshark application (Figure F13) validated that the attacker's machine (name: Kali; IP address: 172.16.50.151) was present in the WMedSys.

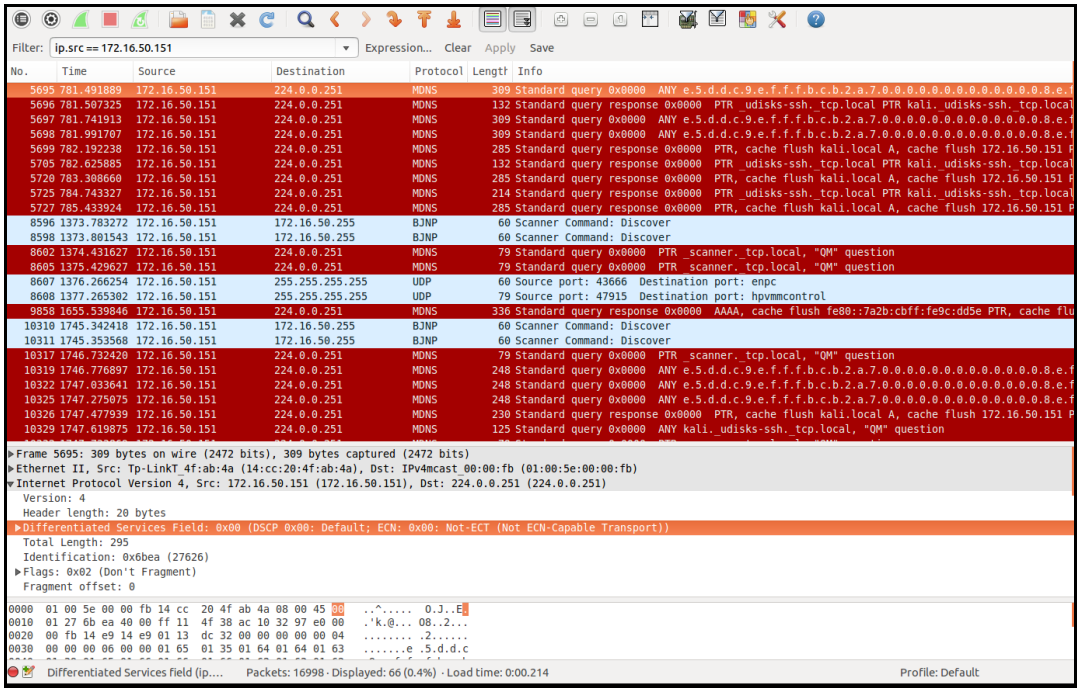


Figure F13: Evidence found in Bro-IDS server log

Appendix F.3: Findings from Attack-2: WPA2-Enterprise without WFserver

In the second attack, the WFS was not yet integrated in the WMedSys and the Unifi AP was configured with WPA2-Enterprise for Wi-Fi authentication. The attacker uses Mana Toolkit to create a Fake AP with the same SSID of legitimate APs. Once the legitimate user (username: nurse007) connects to the Fake AP and logins to OpenEMR, all data is captured by Mana Toolkit. That is how the credentials of legitimate user is captured in plain text. Then, the attacker now can use such credentials to login to OpenEMR and can change the patient's data. However, OpenEMR and XAMPP servers log the activities into the log files and OSSEC server also log changes in the hash values from the patient database file.

Similarly, logs from the Unifi controller, DHCP and RADIUS servers can be used to trace back the MAC and IP addresses of the attacker's machine. Moreover, logs from the Bro-IDS server can explain the footprint of the attacker and the type of attack used by the attacker. Hence, all these logs from servers can be found on Syslog server (Splunk) and analysed to get the information related to the attacker.

In this fictitious case scenario, the blood glucose level of the patient, John Lauren, has been changed by using the captured legitimate login credentials of the nurse (name: Rose Mary, login username: nurse007; password: Password1) from a MITM on a WMedSys that uses WPA2-Enterprise. After analysing the logs from the centralised Syslog server (Splunk), DE related to the malicious attack were found in different components of WMedSys.

Appendix F3.1: Attacker's PC

In this second attack scenario, the attacker also performs MITM attack by using Mana Toolkit. Hence, the login username and password can be found in the Mana Framework log (Figure F14) as the attacker logs in to OpenEMR with the obtained credentials.

Figure F14: Login credentials found in the log of Mana Framework

Appendix F3.2: DHCP Server

DHCP server provides a centralised administration of IP address configuration. DHCP server assigns IP addresses to DHCP clients along with other network parameters including the subnet mask, DNS and default gateway IP addresses. It offers not only the tracking of leased IP addresses, but also logging events relating to DHCP activities. The following figure shows the timestamp and IP address

obtained by the attacker's computer (computer name: Kali; IP address: 172.16.50.153) from the DHCP server within WMedSys.

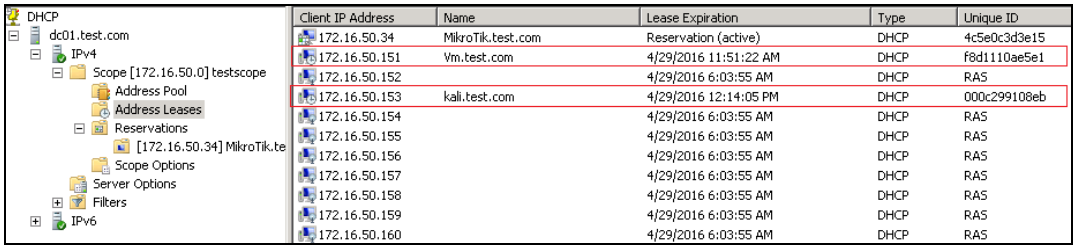


Figure F15: IP addresses distributed by the DHCP server

Appendix F3.3: UniFi Controller Log

UniFi Controller is a software that is installed on a networked computer (IP address: 172.16.50.2) to manage UniFi WAPs by using a web browser (Ubiquiti Networks, 2014). The details of the legitimate WAP including recent events, alerts, settings, wireless clients, past connections and current usage can be observed by using the UniFi Controller. After investigating the details of recent events, there is an evidence that an illegitimate wireless client is associated with the WAP (MAC address: 04:18:d6:2c:ab:0c) in WMedSys (Figure F16).

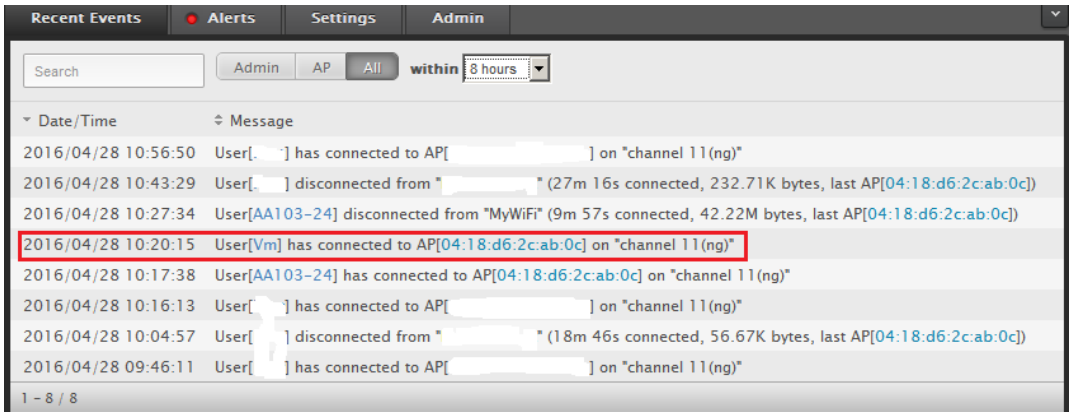


Figure F16: Evidence of illegitimate wireless client in UniFi log

Appendix F3.4: OpenEMR Log

Similarly, the log files from OpenEMR (IP address: 172.16.50.5) can provide details information of user's access to the patient database (DB) including login and logout timestamps of users, associated IP addresses, and records of changes or entries to the DB. Hence, the evidential trace of the login timestamp (12:18:43 on 28 April 2016), IP address of attacker's machine (172.16.50.153) and patient's record changes (blood glucose ready has been changed to 40mg/dL) are found in the OpenEMR log (Figure F17).

Date	Event	User	Certificate User	Group	PatientID	Success	Comments
2016-04-28 10:59:53	login	nurse007		Default	0	1	success: 172.16.50.153
2016-04-28 11:00:13	view	nurse007		Default	0	1	7
2016-04-28 12:18:43	login	nurse007		Default	0	1	success: 172.16.50.153
2016-04-28 12:19:20	view	nurse007		Default	0	1	7
2016-04-28 12:21:27	patient-record-insert	nurse007		Default	7	1	INSERT INTO form_encounter SET date = '2016-04-28', onset_date = '', reason = 'Blood glucose reading is 40mg/dL today.', facility = 'General Hospital Service location', pc_catid = '5', facility_id = '5', billing_facility = '3', sensitivity = 'normal', referral_source = '', pid = '7', encounter = '26', provider_id = '8'
2016-04-28 12:21:27	patient-record-insert	nurse007		Default	7	1	insert into forms (date, encounter, form_name, form_id, pid, user, groupname, authorized, formdir) values (?, ?, ?, ?, ?, ?, ?, ?, ?) ('2016-04-28','26','New Patient Encounter','12','7','nurse007','Default','1','newpatient')
2016-04-28 12:21:27	patient-record-delete	nurse007		Default	7	1	DELETE FROM issue_encounter WHERE pid = ? AND encounter = ? ('7','26')
2016-04-28 12:22:12	view	nurse007		Default	0	1	7
2016-04-28 12:23:23	logout	nurse007		Default	0	1	success
2016-04-28 12:58:32	login	admin		Default	0	1	success: 172.16.50.6

Figure F17: Evidence of the attacker's activities found in OpenEMR log

Appendix F3.5: XAMPP Server Logs

XAMPP (Cross-Platform, Apache, MariaDB, PHP and Perl) is a simple web server solution (running on a networked computer with IP address of 172.16.50.5) for the WMedSys. After analysing XAMPP logs on the Splunk server, the evidential traces of login timestamp (10:59:55 AM on 28 April 2016), username (nurse007) and IP address of the computer (172.16.50.153) used by a malicious attacker who accessed OpenEMR as shown in Figure F18.

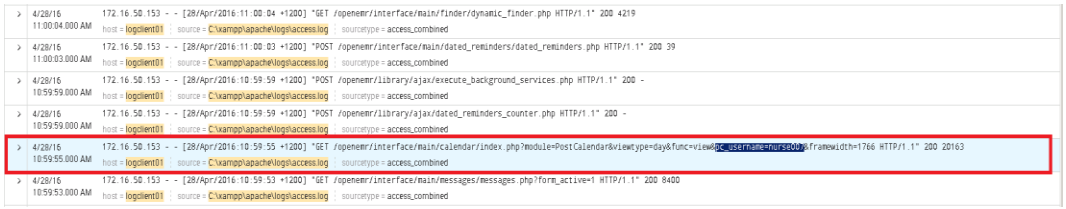


Figure F18: Evidence of the attacker's activities found in XAMPP server log

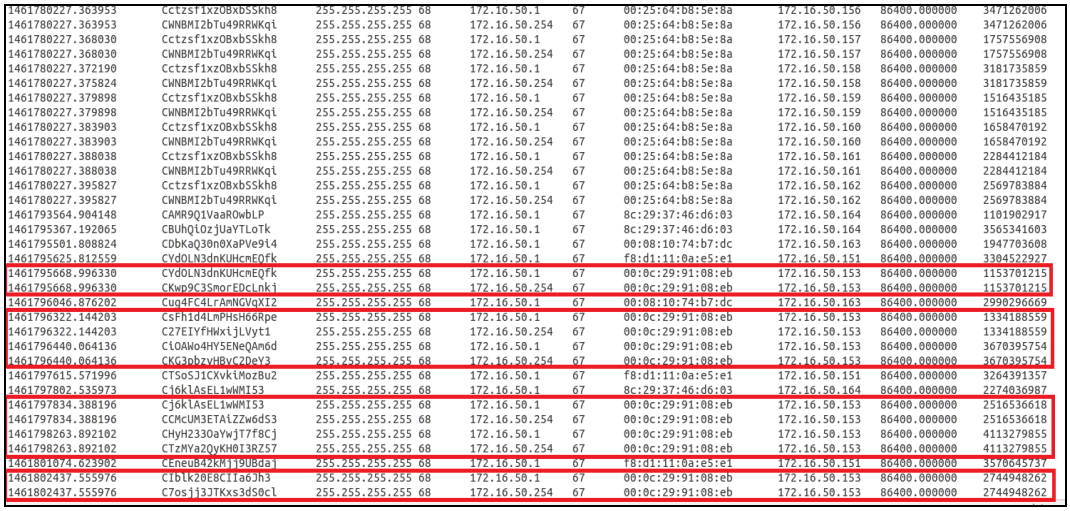
Appendix F3.6: RADIUS Server Logs

The logs from RADIUS server present the time when the attacker logins (10:20:33:846 AM on 28 April 2016) and the MAC address (F8-D1-11-0A-E5-E1) of the attacker's machine.

Figure F19: RADIUS server log

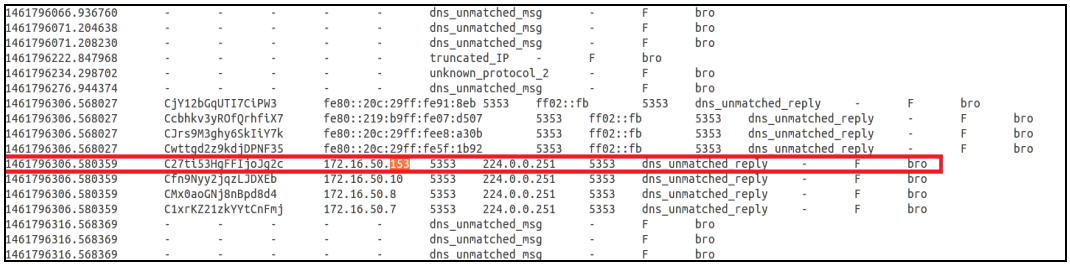
Appendix F3.7: Bro-IDS Server Logs

Moreover, the analysis of logs from Bro-IDS server (Figures F20 and F21) validated that the attacker's machine (IP address: 172.16.50.153) was present in the WMedSys.



1461780227.363953	CctzsfixzOBxbSSkh8	255.255.255.255	68	172.16.50.1	67	00:25:64:b8:5e:8a	172.16.50.156	86400.000000	3471262006
1461780227.363953	CWNBMI2bTu49RRWKqi	255.255.255.255	68	172.16.50.254	67	00:25:64:b8:5e:8a	172.16.50.156	86400.000000	3471262006
1461780227.368030	CctzsfixzOBxbSSkh8	255.255.255.255	68	172.16.50.1	67	00:25:64:b8:5e:8a	172.16.50.157	86400.000000	1757556908
1461780227.368030	CWNBMI2bTu49RRWKqi	255.255.255.255	68	172.16.50.254	67	00:25:64:b8:5e:8a	172.16.50.157	86400.000000	1757556908
1461780227.372190	CctzsfixzOBxbSSkh8	255.255.255.255	68	172.16.50.1	67	00:25:64:b8:5e:8a	172.16.50.158	86400.000000	3181735859
1461780227.375824	CWNBMI2bTu49RRWKqi	255.255.255.255	68	172.16.50.254	67	00:25:64:b8:5e:8a	172.16.50.158	86400.000000	3181735859
1461780227.379898	CctzsfixzOBxbSSkh8	255.255.255.255	68	172.16.50.1	67	00:25:64:b8:5e:8a	172.16.50.159	86400.000000	1516435185
1461780227.379898	CWNBMI2bTu49RRWKqi	255.255.255.255	68	172.16.50.254	67	00:25:64:b8:5e:8a	172.16.50.159	86400.000000	1516435185
1461780227.383903	CctzsfixzOBxbSSkh8	255.255.255.255	68	172.16.50.1	67	00:25:64:b8:5e:8a	172.16.50.160	86400.000000	1658470192
1461780227.383903	CWNBMI2bTu49RRWKqi	255.255.255.255	68	172.16.50.254	67	00:25:64:b8:5e:8a	172.16.50.160	86400.000000	1658470192
1461780227.388038	CctzsfixzOBxbSSkh8	255.255.255.255	68	172.16.50.1	67	00:25:64:b8:5e:8a	172.16.50.161	86400.000000	2284412184
1461780227.388038	CWNBMI2bTu49RRWKqi	255.255.255.255	68	172.16.50.254	67	00:25:64:b8:5e:8a	172.16.50.161	86400.000000	2284412184
1461780227.395827	CctzsfixzOBxbSSkh8	255.255.255.255	68	172.16.50.1	67	00:25:64:b8:5e:8a	172.16.50.162	86400.000000	2569783884
1461780227.395827	CWNBMI2bTu49RRWKqi	255.255.255.255	68	172.16.50.254	67	00:25:64:b8:5e:8a	172.16.50.162	86400.000000	2569783884
1461793564.904148	CAMR9Q1VaaROwbLP	255.255.255.255	68	172.16.50.1	67	8c:29:37:46:d6:03	172.16.50.164	86400.000000	1101902917
1461795367.192065	CBUhQiOzjUaYTLoTk	255.255.255.255	68	172.16.50.1	67	8c:29:37:46:d6:03	172.16.50.164	86400.000000	3565341603
1461795501.808824	CDbKaQ30n0XaPVe9i4	255.255.255.255	68	172.16.50.1	67	00:08:10:74:b7:dc	172.16.50.163	86400.000000	1947703608
1461795625.812559	CYdOLN3dnKUHcmEQfk	255.255.255.255	68	172.16.50.1	67	f8:d1:11:0a:e5:e1	172.16.50.151	86400.000000	3304522927
1461795668.996330	CYdOLN3dnKUHcmEQfk	255.255.255.255	68	172.16.50.1	67	00:0c:29:91:08:eb	172.16.50.153	86400.000000	1153701215
1461795668.996330	CKwp9C3SmorEDcLnki	255.255.255.255	68	172.16.50.254	67	00:0c:29:91:08:eb	172.16.50.153	86400.000000	1153701215
1461796046.876202	Cuq4FC4LrAmNGVqXI2	255.255.255.255	68	172.16.50.1	67	00:08:10:74:b7:dc	172.16.50.163	86400.000000	2990296669
1461796322.144203	CsFh1d4LmPHsH66Rpe	255.255.255.255	68	172.16.50.1	67	00:0c:29:91:08:eb	172.16.50.153	86400.000000	1334188559
1461796322.144203	C27EIYfHWxijLVyt1	255.255.255.255	68	172.16.50.254	67	00:0c:29:91:08:eb	172.16.50.153	86400.000000	1334188559
1461796440.064136	CiOAWo4HYSENeQAm6d	255.255.255.255	68	172.16.50.1	67	00:0c:29:91:08:eb	172.16.50.153	86400.000000	3670395754
1461796440.064136	CKG3pbzvHBvC2DeY3	255.255.255.255	68	172.16.50.254	67	00:0c:29:91:08:eb	172.16.50.153	86400.000000	3670395754
1461797615.571996	CTSoSJ1CXvkiMozBu2	255.255.255.255	68	172.16.50.1	67	f8:d1:11:0a:e5:e1	172.16.50.151	86400.000000	3264391357
1461797802.535973	Cj6klAsEL1wWMI53	255.255.255.255	68	172.16.50.1	67	8c:29:37:46:d6:03	172.16.50.164	86400.000000	2274036987
1461797834.388196	Cj6klAsEL1wWMI53	255.255.255.255	68	172.16.50.1	67	00:0c:29:91:08:eb	172.16.50.153	86400.000000	2516536618
1461797834.388196	CCMcUM3ETAiZZw6dS3	255.255.255.255	68	172.16.50.254	67	00:0c:29:91:08:eb	172.16.50.153	86400.000000	2516536618
1461798263.892102	CHyH233OaYwjT7f8Cj	255.255.255.255	68	172.16.50.1	67	00:0c:29:91:08:eb	172.16.50.153	86400.000000	4113279855
1461798263.892102	CTzMYa2QyKH0I3RZS7	255.255.255.255	68	172.16.50.254	67	00:0c:29:91:08:eb	172.16.50.153	86400.000000	4113279855
1461801074.623902	CEneuB42kMjj9UBdaj	255.255.255.255	68	172.16.50.1	67	f8:d1:11:0a:e5:e1	172.16.50.151	86400.000000	3570645737
1461802437.555976	CIblk20E8CIIa6Jh3	255.255.255.255	68	172.16.50.1	67	00:0c:29:91:08:eb	172.16.50.153	86400.000000	2744948262
1461802437.555976	C7osjj3JTKxs3dS0cl	255.255.255.255	68	172.16.50.254	67	00:0c:29:91:08:eb	172.16.50.153	86400.000000	2744948262

Figure F20: Evidence of the attacker's machine found in Bro-IDS server log



1461796066.936760	-	-	-	-	-	dns_unmatched_msg	-	F	bro				
1461796071.204638	-	-	-	-	-	dns_unmatched_msg	-	F	bro				
1461796071.208230	-	-	-	-	-	dns_unmatched_msg	-	F	bro				
1461796222.847968	-	-	-	-	-	truncated_IP	-	F	bro				
1461796234.298702	-	-	-	-	-	unknown_protocol_2	-	F	bro				
1461796276.944374	-	-	-	-	-	dns_unmatched_msg	-	F	bro				
1461796306.568027	CjY12bGqUTI7CiPW3	fe80::20c:29ff:fe91:8eb	5353	ff02::fb	5353	dns_unmatched_reply	-	F	bro				
1461796306.568027	Ccbhkv3yROfQrhfiX7	fe80::219:b9ff:fe07:d507	5353	ff02::fb	5353	dns_unmatched_reply	-	F	bro				
1461796306.568027	CJrs9M3ghy6SkIiY7k	fe80::20c:29ff:fee8:a30b	5353	ff02::fb	5353	dns_unmatched_reply	-	F	bro				
1461796306.568027	Cwttqd2z9kdjDPNF3S	fe80::20c:29ff:fe5f:1b92	5353	ff02::fb	5353	dns_unmatched_reply	-	F	bro				
1461796306.580359	C27ti53HQFFIjoJq2c	172.16.50.150	5353	224.0.0.251	5353	dns_unmatched_reply	-	F	bro				
1461796306.580359	Cfn9Nyy2jqzLJDXEb	172.16.50.10	5353	224.0.0.251	5353	dns_unmatched_reply	-	F	bro				
1461796306.580359	CMx0aoGNj8nBpd8d4	172.16.50.8	5353	224.0.0.251	5353	dns_unmatched_reply	-	F	bro				
1461796306.580359	C1xrKZ21zkYYtCnFmj	172.16.50.7	5353	224.0.0.251	5353	dns_unmatched_reply	-	F	bro				
1461796316.568369	-	-	-	-	-	dns_unmatched_msg	-	F	bro				
1461796316.568369	-	-	-	-	-	dns_unmatched_msg	-	F	bro				
1461796316.568369	-	-	-	-	-	dns_unmatched_msg	-	F	bro				

Figure F20: Evidence of the attacker's machine found in Bro-IDS server log

Appendix F4: Findings from Attack-3: WPA2-PSK with WF server

In the third scenario, the WFS is integrated in the WMedSys. The attacker used Mana Toolkit to create a Fake AP with the same SSID of legitimate AP. After capturing the credentials of a legitimate user in plain texts, the attacker uses those credentials to login to OpenEMR and change the patient's data. The patient victim of this attack was John Lauren (fictitious name) whose blood glucose reading was updated by the nurse (nurse007) at 19:01:54 on 2 May 2016. However, the attacker changed John's blood glucose reading to 30 mg/dL by using the obtained credentials of legitimate user (nurse007) at 19:20:00 on 2 May 2016.

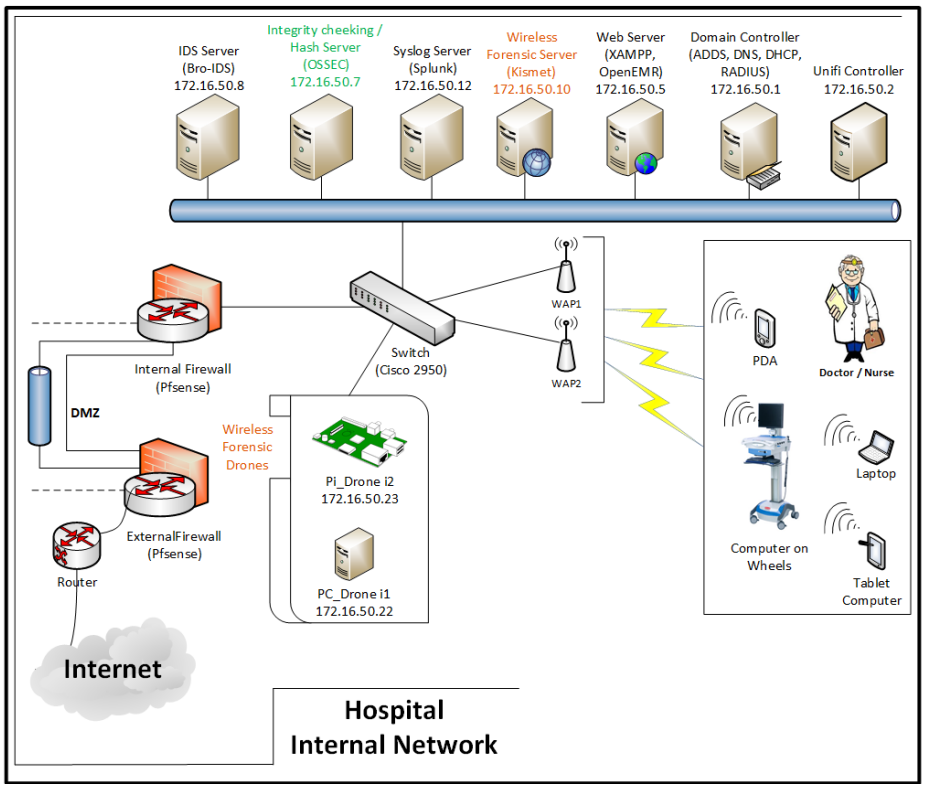


Figure F22: Experimental test-bed (WMedSys) for Attack 3

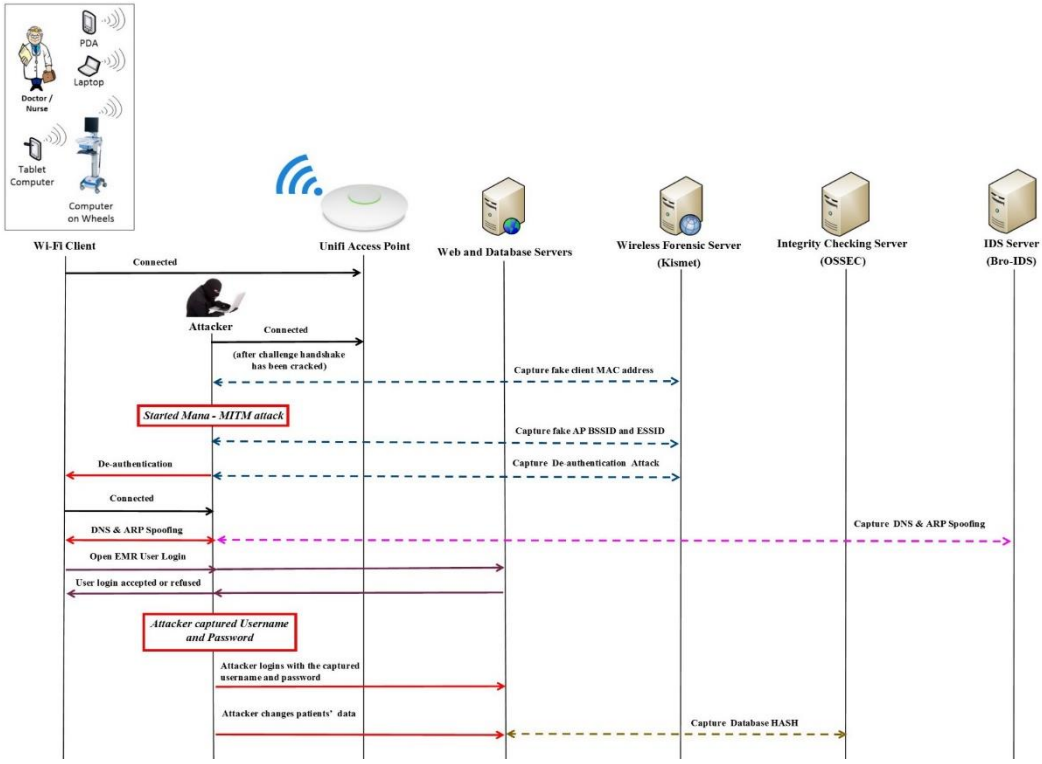


Figure F23: Man-in-the-Middle attack on a WMedSys with Wireless Forensic Server (WPA2-PSK)

DE related to the malicious attack were found in the following components of WMedSys.

Appendix F4.1: Attacker's PC

In this third attack scenario, the attacker also performed a MITM attack by using Mana Toolkit. After analysing, the login username and password were found in the Mana Framework log (Figure F24) as the attacker logged in to OpenEMR with the obtained credentials.

Figure F24: Login credentials found in the log of Mana Framework

Appendix F4.2: DHCP Server

In DHCP server log, it shows the timestamp and IP address obtained by the attacker's computer (computer name: Kali; IP address: 172.16.50.164).

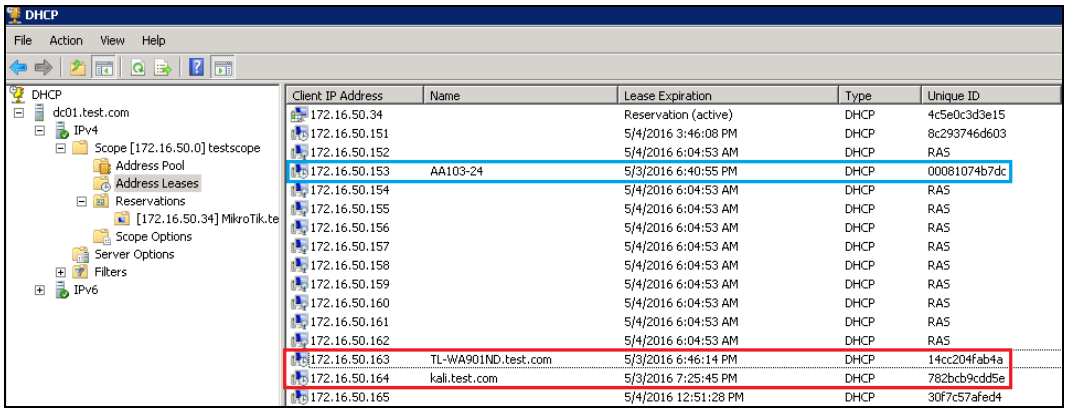


Figure F25: IP addresses distributed by the DHCP server

Appendix F4.3: UniFi Controller Log

After investigating, there was also a DE in which an illegitimate wireless client was associated with the WAP (MAC address: 04:18:d6:2c:ab:0c) from 18:46:10 on 2 May 2016 in WMedSys (Figure F26).

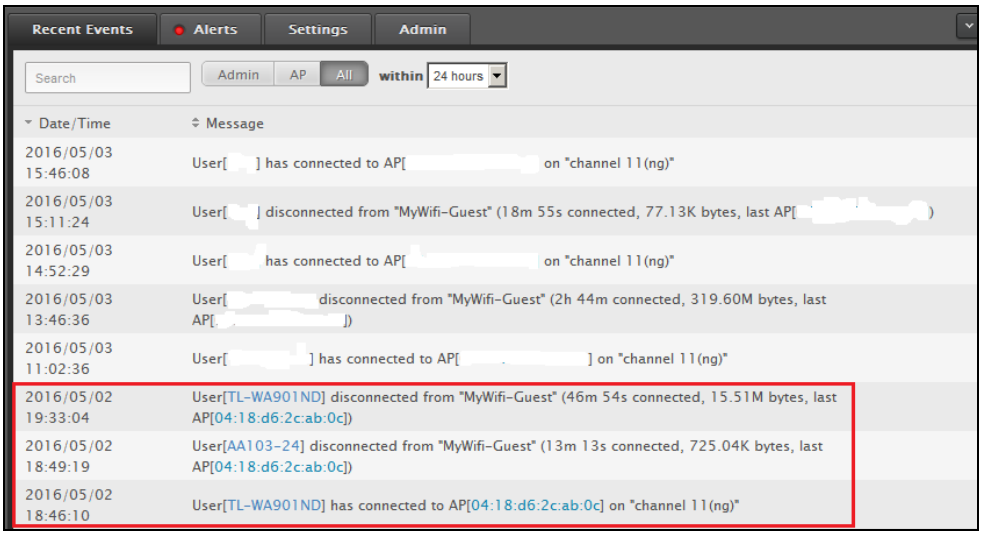


Figure F26: Evidence found in UniFi log

Appendix F4.4: OpenEMR Log

Similarly, the log files from OpenEMR (IP address: 172.16.50.5) provided the evidential trace of the login timestamp (19:18:56 on 2 May 2016), IP address of attacker's machine (172.16.50.164) and patient's record changes (blood glucose ready has been changed from 110 mg/dL to 30mg/dL) in the OpenEMR (Figure F27).

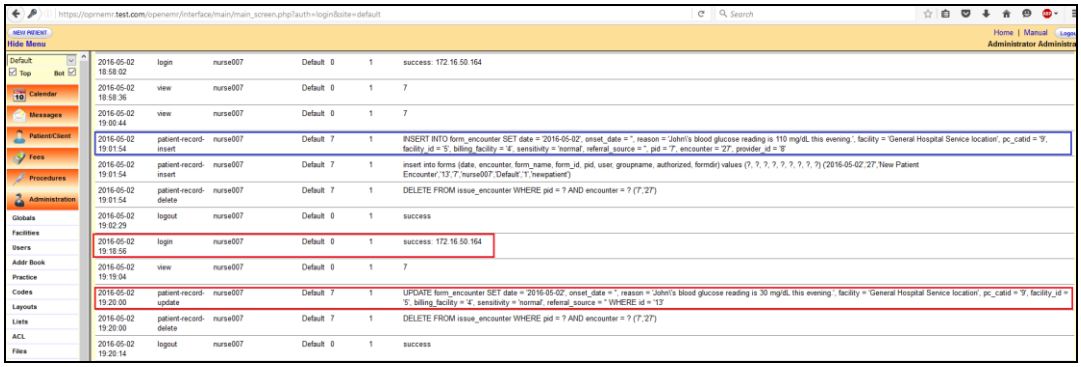


Figure F27: Evidence found in OpenEMR log

Appendix F4.5: XAMPP Server Logs

DE from the XAMPP web server logs uncovered the evidential traces of login timestamp (7:18:57 PM on 2 May 2016) of the nurse (nurse007) and IP address of the computer (172.16.50.164) used by a malicious attacker who accessed OpenEMR (Figure F28).

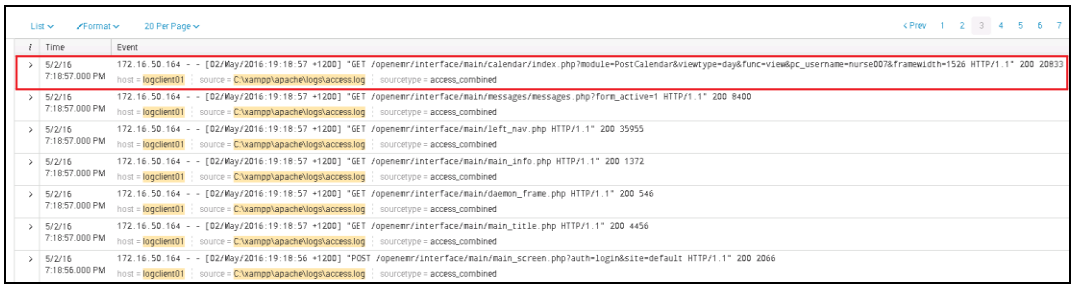


Figure F28: Evidence found in XAMPP server log

Appendix F4.6: Wireless Forensic Server (WFserver) Logs

Figure F29 showed the screenshot of the graphical interface of WFserver in WMedSys. In WFserver logs, MAC addresses of the Fake AP and the fake client were found as shown in Figures F30 and F31.

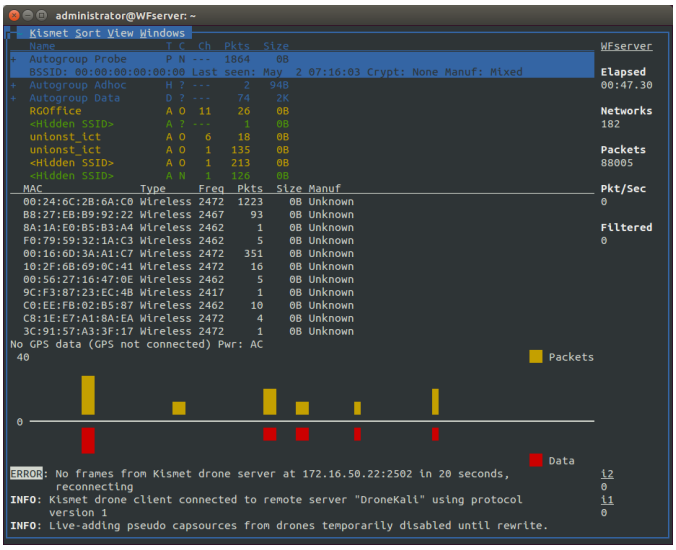


Figure F29: Screenshot of wireless forensic server in action

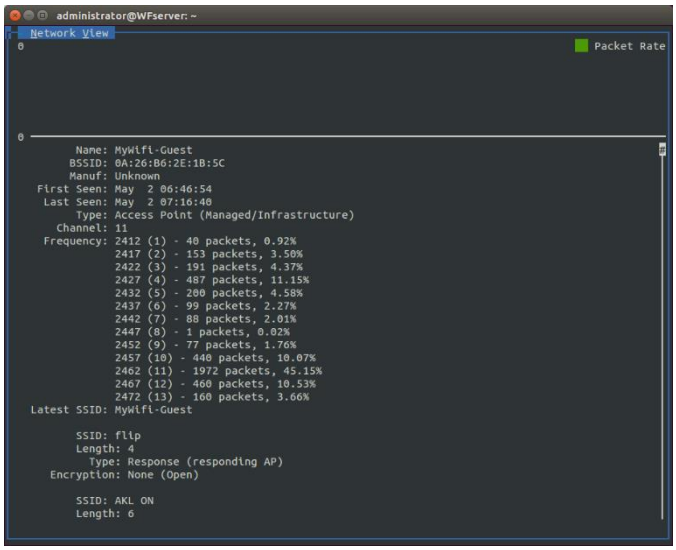


Figure F30: Wireless forensic server captures the Fake AP

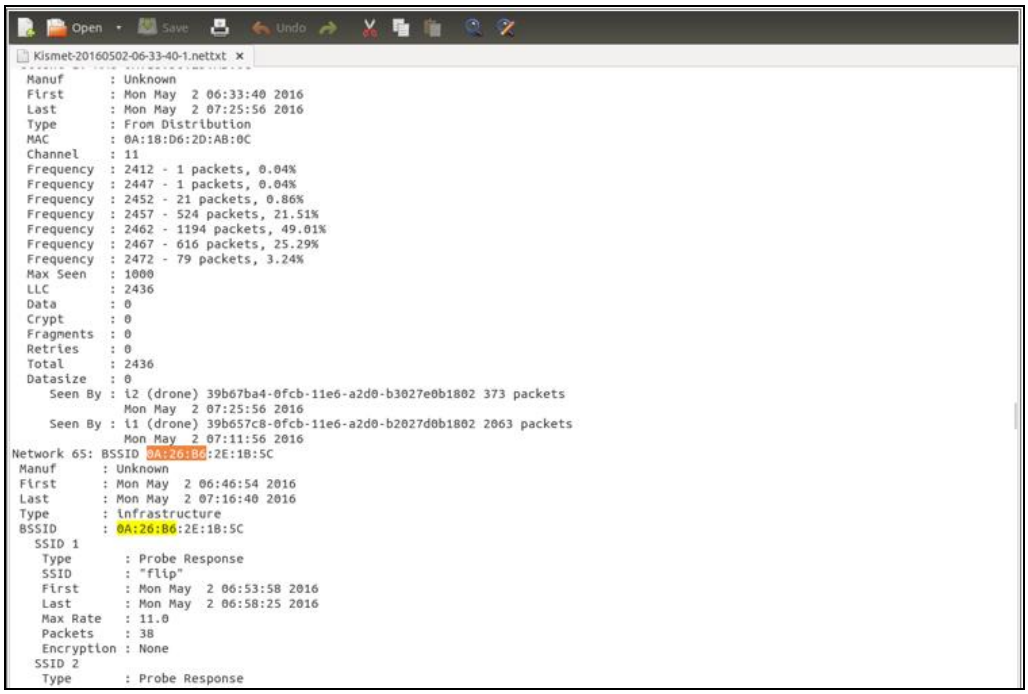


Figure F31: Wireless forensic server captures the Fake AP

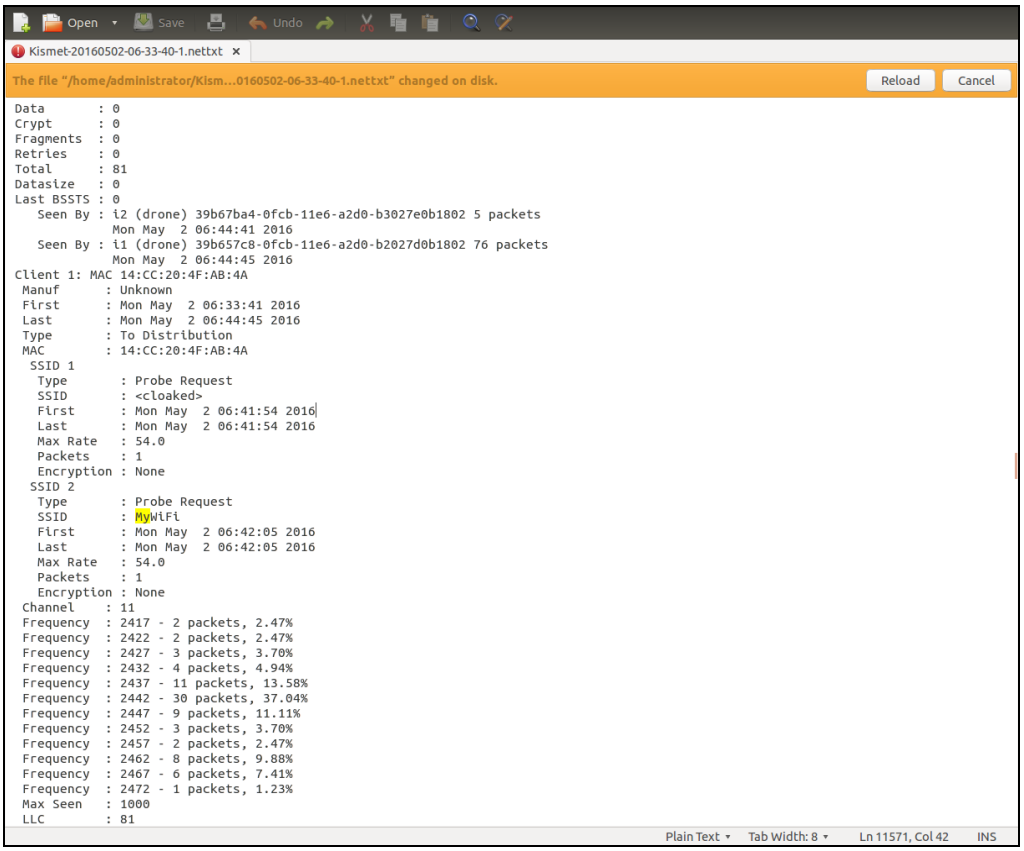


Figure F32: Wireless forensic server captures fake client

Figure F33 also showed the alert that WFserver recognised an impersonation attack in WMedSys.

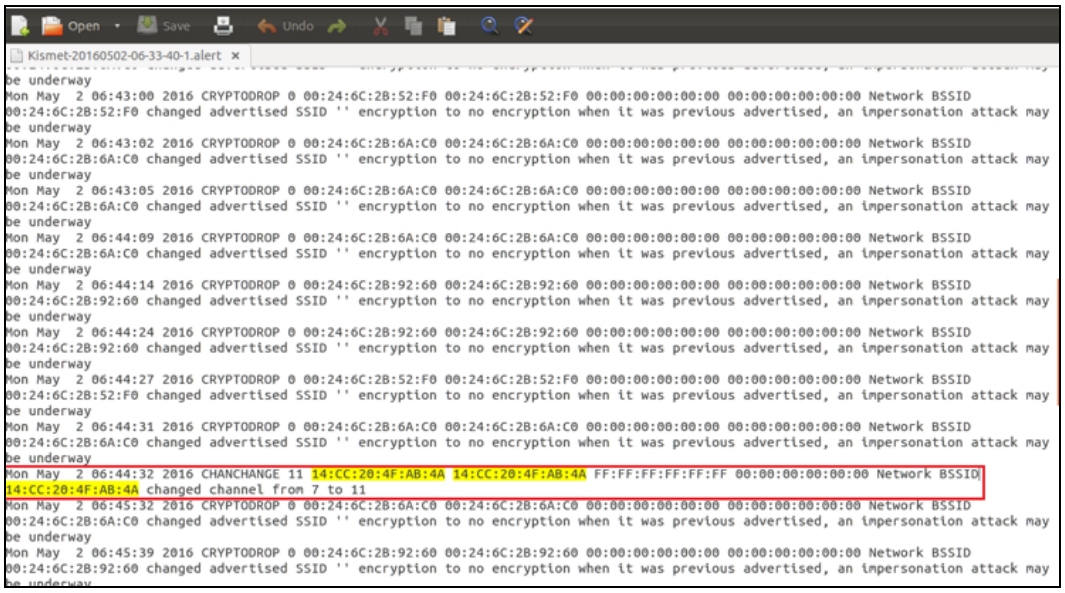


Figure F33: Wireless forensic server captures the Fake AP

In the Wireshark logs created by WFserver (Figure F34), it was found that there were the broadcast messages initiated by the Fake AP with a MAC address, 0a:26:b6:2e:1b:5c.

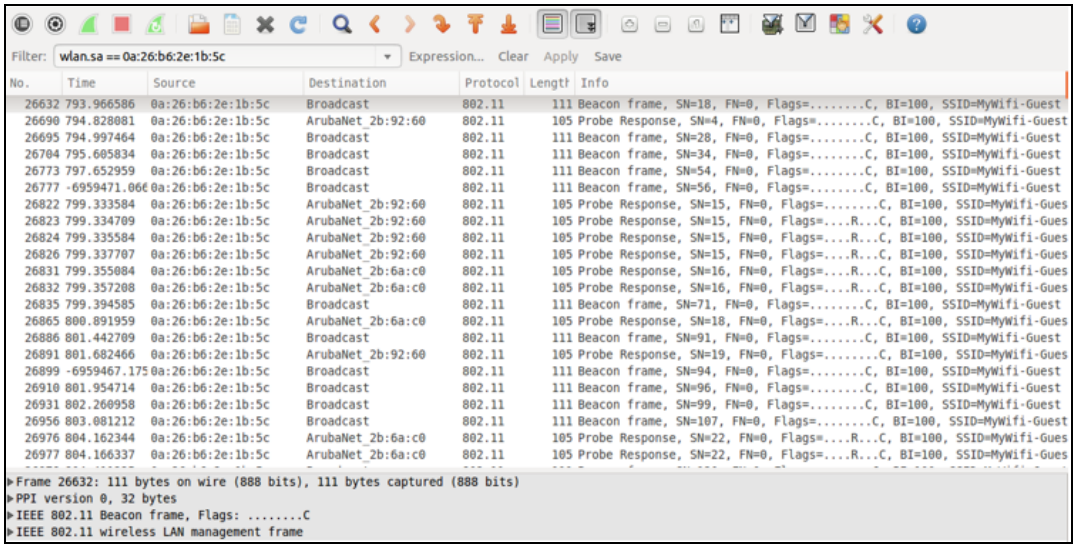


Figure F34: Broadcast messages by Fake AP found in the Wireshark log

Moreover, an evidence of the association of the fake client (MAC address: 14:cc:20:4f:ab:4a) machine used by an attacker to the legitimate AP (MAC address: 0e:18:d6:2d:ab:0c) was also found in the Wireshark logs created by WFserver (Figure F35).

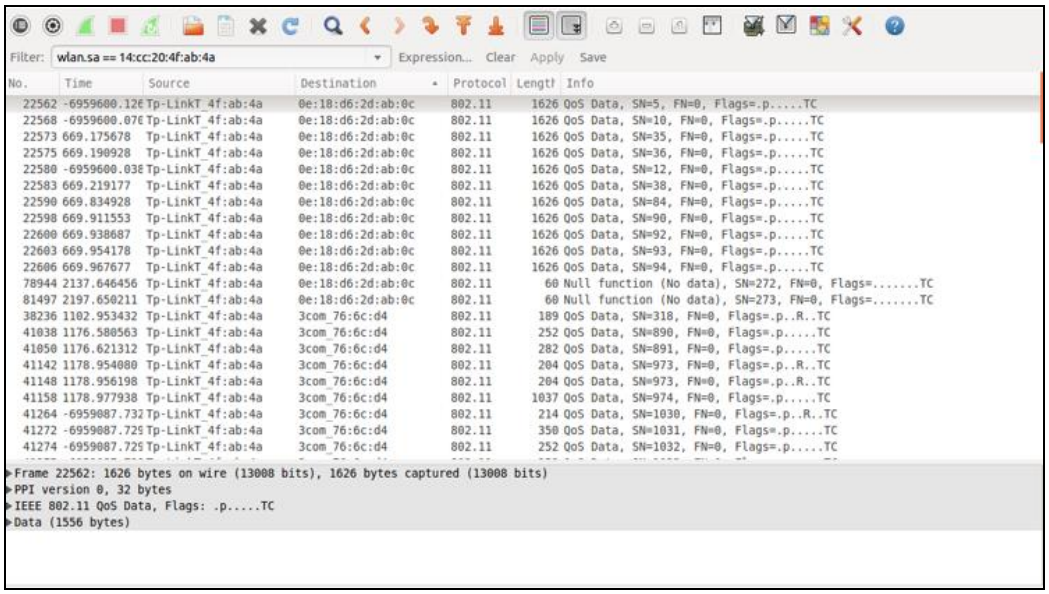


Figure F35: Evidence of association of the fake client to the legitimate AP

Appendix F4.7: Bro-IDS Log

After analysing the logs from Bro-IDS, it was noted that Bro-IDS server only captured the DHCP request from the client machine used by an attacker (Figure F36).

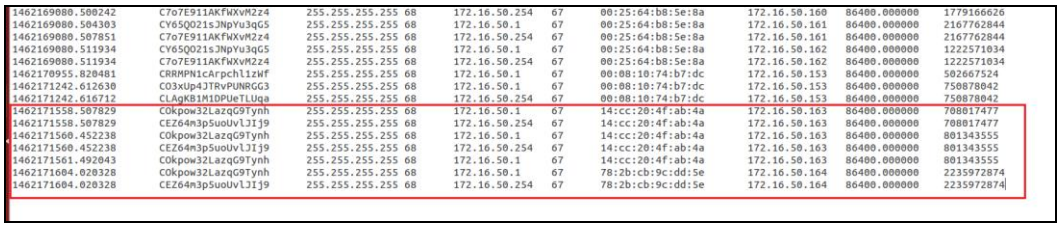


Figure F36: Evidence of DHCP requests from the fake client

Appendix F5: Findings from Attack-4: WPA2-Enterprise with WF server

In this fourth attack scenario, the Wireless Forensic Server (IP Address: 172.16.50.10) and File Monitoring Server (SolarWinds with IP Address of 172.16.50.4) were integrated in the hospital network system (WMedSys) and the UniFi AP was also configured with WPA2-EAP for Wi-Fi authentication. The attacker used a fake client login to the network with the username and password, which had been brute-forced by Asleap tool. After logging to the system, the attacker used Mana Toolkit to create a Fake AP with the same SSID of legitimate AP. At this stage, the legitimate user (username: doc007) was connected to the Fake AP and the communicated data was captured by MANA-toolkit framework.

After capturing the credentials of a legitimate user, the attacker used those credentials to login to OpenEMR and change the patient's data.

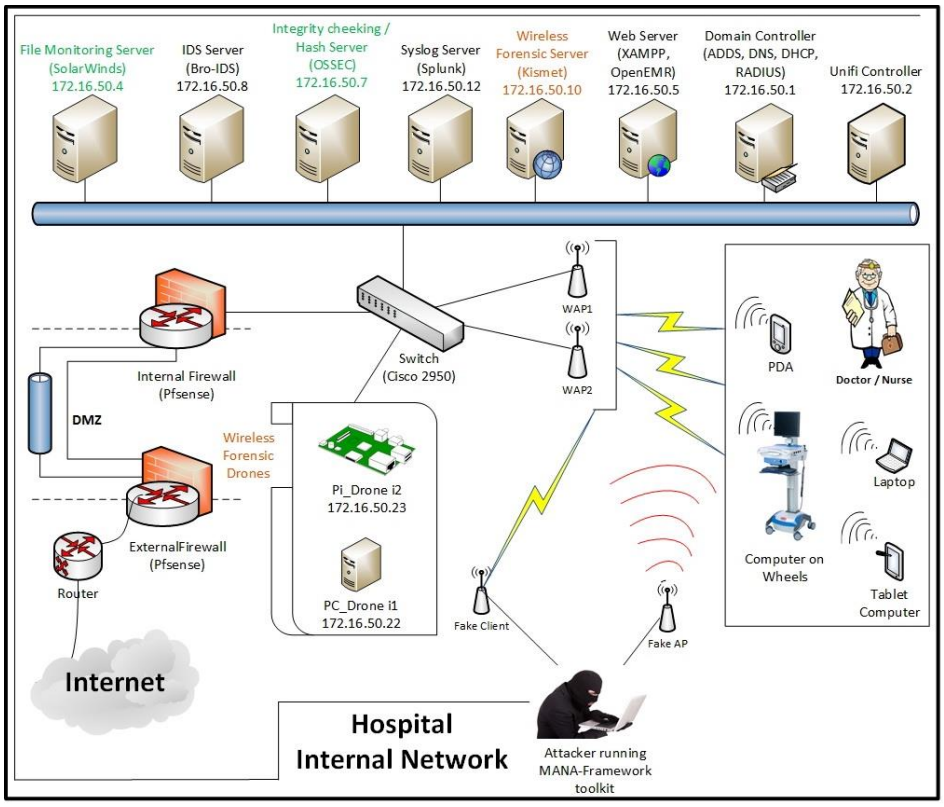


Figure F37: Experimental test-bed (WMedSys) for Attack 4

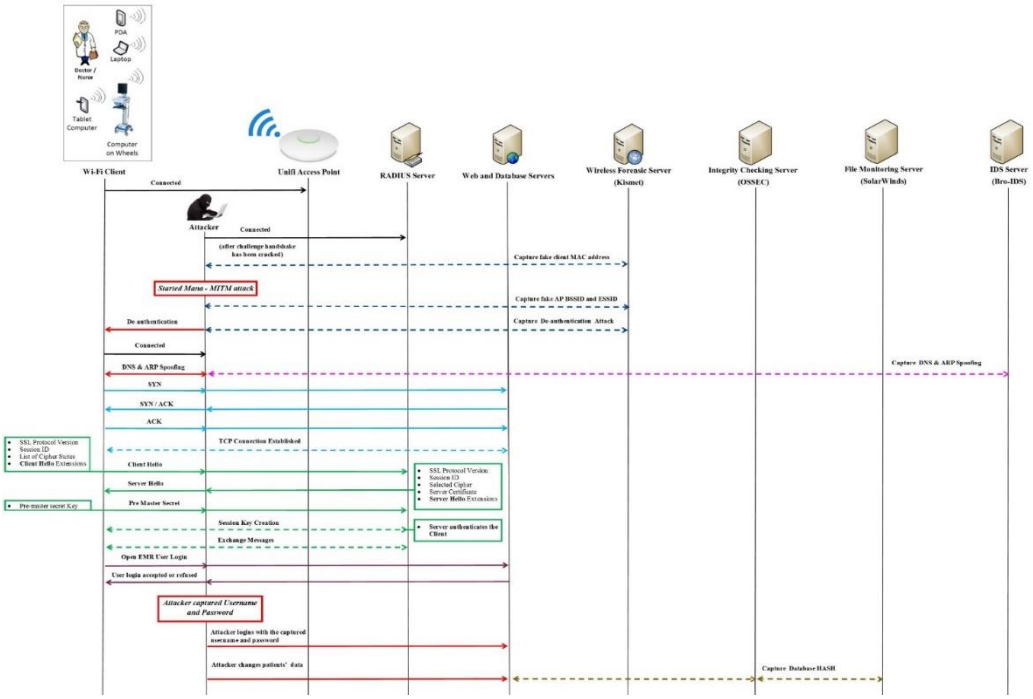


Figure F38: Man-in-the-Middle attack on a WMedSys with Wireless Forensic Server (WPA2-Enterprise)

The patient victim of this attack was John Lauren (fictitious name) whose blood glucose reading was updated to 20 mg/dL by the nurse (Rose Mary) on 2 May 2016 (Figure F39). However, the attacker changed John's blood glucose reading to 200 mg/dL by using the obtained credentials of legitimate user (doc007) at 16:14:12 on 19 May 2016 (Figure F43).

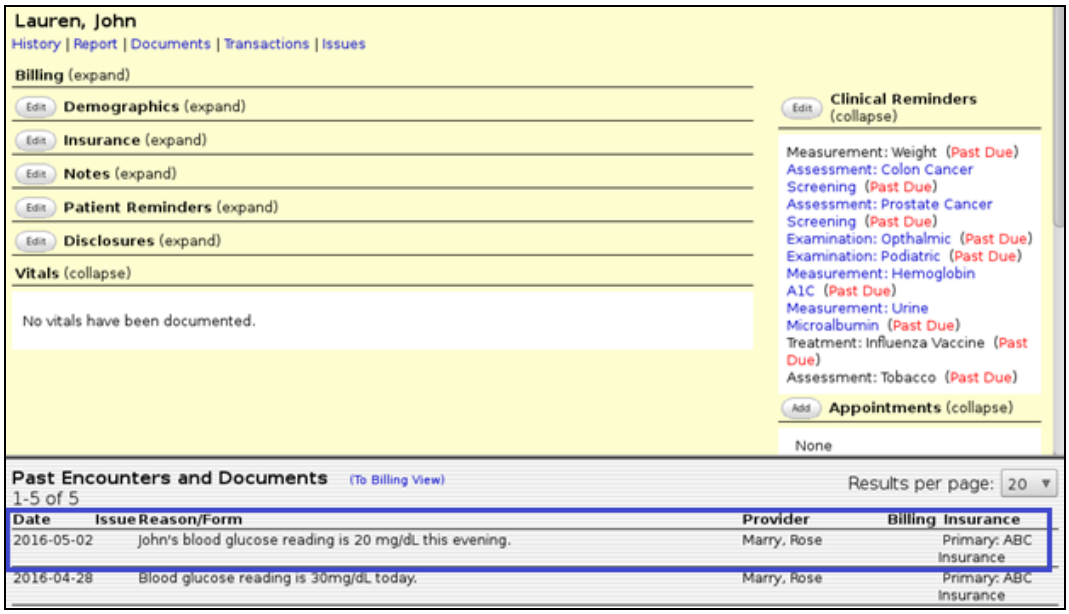


Figure F39: Patient's data before the attack

Nevertheless, OpenEMR and XAMPP servers logged the activities into the log files. Similarly, the OSSEC and SolarWinds servers also logged changes to the patient's database in hash values for integrity checking. Moreover, the Unifi controller, DHCP and RADIUS servers' logs were used to trace back MAC and IP addresses of the machine used by the attacker. In addition, Bro-IDS server's logs were used for finding out the footprint of the attacker and the type of attack used by the attacker. Furthermore, the logs captured by Wireless Forensic Server were used to identify the Fake AP and fake client activities in WMedSys. As a result of all logs from components of WMedSys were configured to be forwarded to the centralised Syslog server (Splunk), findings after the analysis of logs are listed in the following sub-sections.

Appendix F5.1: Attacker's PC

In this attack scenario, the attacker performed MITM attack by using Mana Toolkit. Hence, the login username and password were found in the Mana Framework log (Figure F40) as the attacker logged in to OpenEMR with the obtained credentials.

Figure F40: Login credentials found in the log of Mana Framework

Appendix 5.2: DHCP Server Log

In DHCP server log (Figure F41), it showed the timestamp and IP address obtained by the attacker's computer (computer name: Kali VM with the IP address of 172.16.50.163, which run on the physical machine AA103-21 with the IP address of 172.16.50.153).

Client IP Address	Name	Lease Expiration	Type	Unique ID
172.16.50.34		Reservation (active)	DHCP	4c5e0c3d3e15
172.16.50.151	Computer-on-Wheels.test.com	5/20/2016 6:19:46 PM	DHCP	00081074b7dc
172.16.50.152		5/20/2016 6:08:18 PM	DHCP	RAS
172.16.50.153	AA103-21	5/20/2016 6:03:02 PM	DHCP	f8d1110ae5e1
172.16.50.154		5/20/2016 6:07:18 PM	DHCP	RAS
172.16.50.155		5/20/2016 6:07:48 PM	DHCP	RAS
172.16.50.156		5/20/2016 6:07:18 PM	DHCP	RAS
172.16.50.157		5/20/2016 6:07:18 PM	DHCP	RAS
172.16.50.158		5/20/2016 6:07:18 PM	DHCP	RAS
172.16.50.159		5/20/2016 6:07:18 PM	DHCP	RAS
172.16.50.160		5/20/2016 6:07:18 PM	DHCP	RAS
172.16.50.161		5/20/2016 6:07:18 PM	DHCP	RAS
172.16.50.162		5/20/2016 6:07:18 PM	DHCP	RAS
172.16.50.163	kali.test.com	5/20/2016 6:03:35 PM	DHCP	000c293075e8
172.16.50.164		5/20/2016 5:53:23 PM	DHCP	000c29cb5fc2

Figure F41: IP addresses distributed by the DHCP server during Attack 4

Appendix 5.3: UniFi Controller Log

The log from UniFi Controller exposed that the evidence of the attacker's machine (computer name: AA103-21; MAC address: f8:d1:11:0a:e5:e1) and the timestamp when attacker logged in to the WMedSys.

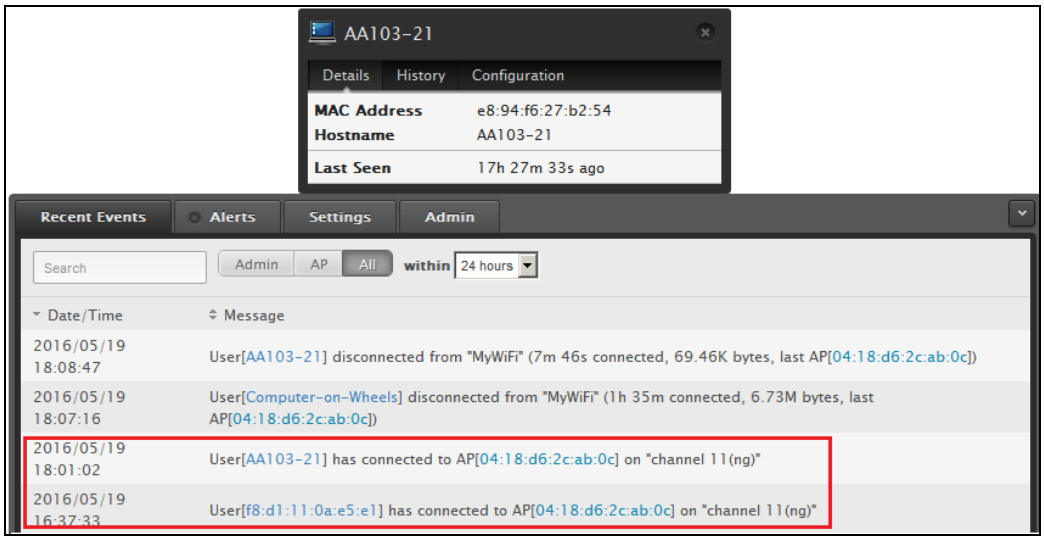


Figure F42: Logs from UniFi Controller during Attack 4

Appendix 5.4: OpenEMR Log

The log from OpenEMR captured the attacker's activities (Figure F43).

Date	Event	User	Certificate User	Group	PatientID	Success	Comments
2016-05-19 15:40:44	login	admin		Default	0	1	success: 172.16.50.3
2016-05-19 15:40:59	view	admin		Default	0	1	3
2016-05-19 15:41:14	patient-record-update	admin		Default	3	1	UPDATE form_encounter SET date = '2016-04-07', onset_date = '', reason = 'BP is very low 116/52.', facility = 'General Hospital Service location', pc_catid = '9', facility_id = '5', billing_facility = '4', sensitivity = 'normal', referral_source = '' WHERE id = '6'
2016-05-19 15:41:14	patient-record-delete	admin		Default	3	1	DELETE FROM issue_encounter WHERE pid = ? AND encounter = ? ('3','14')
2016-05-19 15:41:17	logout	admin		Default	0	1	success
2016-05-19 17:08:49	login	doc007		Default	0	1	success: 172.16.50.151
2016-05-19 18:05:56	login	doc007		Default	0	1	success: 172.16.50.151
2016-05-19 18:08:50	login	doc007		Default	0	1	success: 172.16.50.163
2016-05-19 18:12:45	login	doc007		Default	0	1	success: 172.16.50.163
2016-05-19 18:12:50	view	doc007		Default	0	1	7
2016-05-19 18:12:51	view	doc007		Default	0	1	7
2016-05-19 18:14:12	patient-record-update	doc007		Default	7	1	UPDATE form_encounter SET date = '2016-05-02', onset_date = '', reason = 'John\'s blood glucose reading is 200 mg/dL this evening.', facility = 'General Hospital Service location', pc_catid = '9', facility_id = '5', billing_facility = '4', sensitivity = 'normal', referral_source = '' WHERE id = '13'
2016-05-19 18:14:12	patient-record-delete	doc007		Default	7	1	DELETE FROM issue_encounter WHERE pid = ? AND encounter = ? ('7','27')
2016-05-19 18:14:58	patient-record-update	doc007		Default	7	1	UPDATE form_encounter SET date = '2016-04-28', onset_date = '', reason = 'Blood glucose reading is 20mg/dL today.', facility = 'General Hospital Service location', pc_catid = '9', facility_id = '5', billing_facility = '3', sensitivity = 'normal', referral_source = '' WHERE id = '12'
2016-05-19 18:14:58	patient-record-delete	doc007		Default	7	1	DELETE FROM issue_encounter WHERE pid = ? AND encounter = ? ('7','26')
2016-05-19 18:16:02	logout	doc007		Default	0	1	success
2016-05-19 19:36:20	login	admin		Default	0	1	success: 172.16.50.6

Figure F43: Logs from OpenEMR during Attack 4

Appendix 5.5: XAMPP Logs

After analysing XAMPP logs, the login timestamps of the victim (username: doc007 at 6:08:50:000 PM on 19 May 2016 in Figure F44) and the attacker (6:12:46:000 PM on 19 May 2016 in Figure F45) to Open EMR were found.

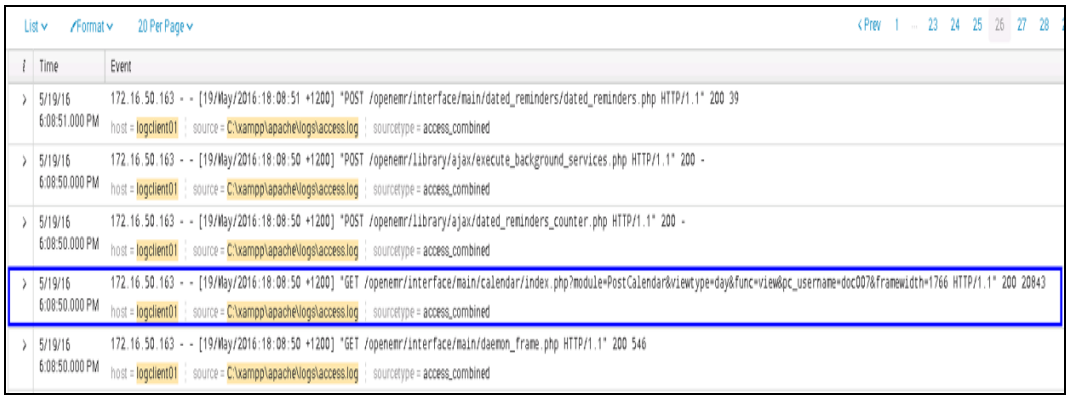


Figure F44: Login timestamp of the victim from XAMPP during Attack 4

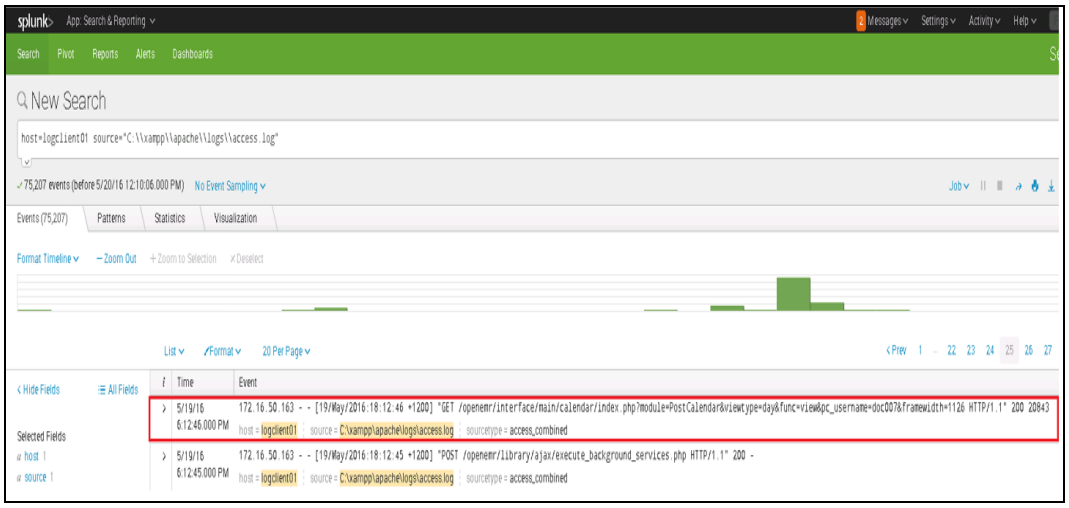


Figure F45: Login timestamp of the attacker from XAMPP during Attack 4

Appendix 5.6: RADIUS Server Logs

RADIUS server captured the login timestamps of the legitimate client (MAC address: 00:08:10:74:b7:dc) and the fake client (MAC address: f8:d1:11:0a:e5:e1) as shown in the Figures F46 and F47, respectively.

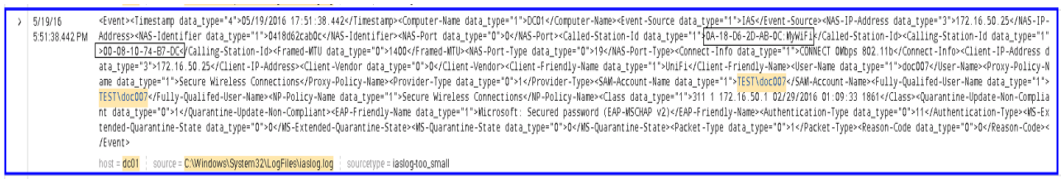


Figure F46: Evidence of the legitimate user's login timestamp from RADIUS

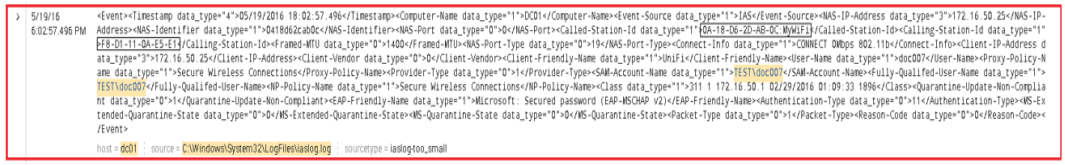


Figure F47: Evidence of the attacker's login timestamp from RADIUS

Appendix 5.7: OSSEC Server Logs

The hash values of the patient database, before and after the attack, were found in OSSEC server logs (Figures F48.a, F48.b, F48.c and F48.d)

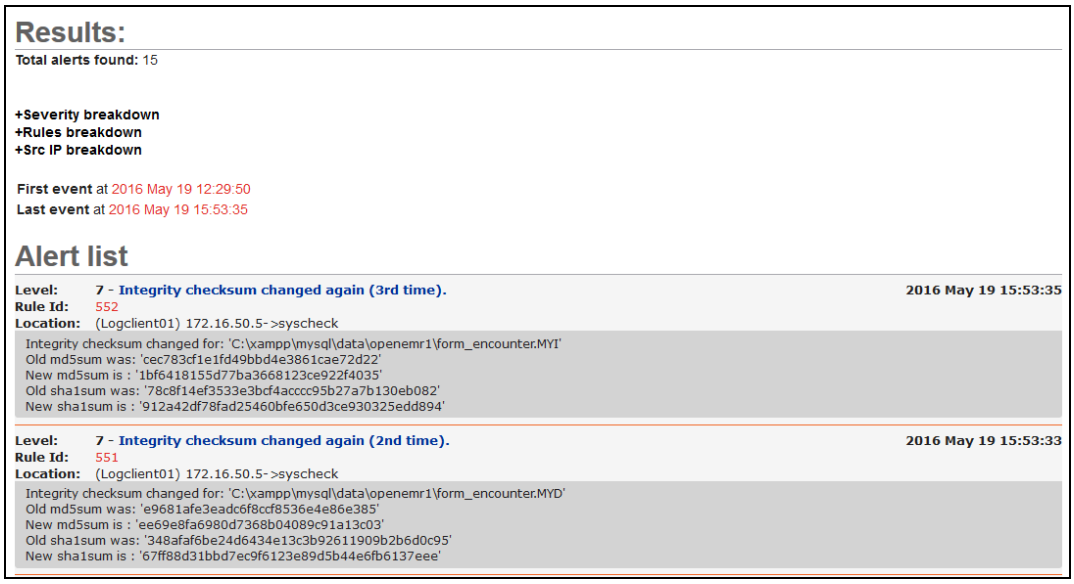


Figure F48.a: Evidence of the hash value changes from OSSEC

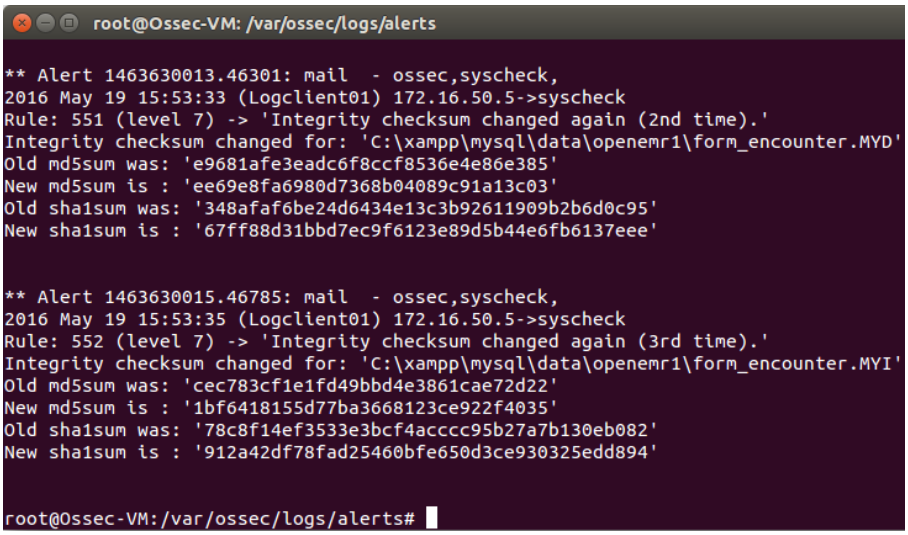


Figure F48.b: Evidence of the hash value changes from OSSEC

Figure F48.c: Evidence of the hash value changes from OSSEC

```
** Alert 1463640354.50049: mail  - ossec,syscheck,
2016 May 19 18:45:54 (Logclient01) 172.16.50.5->syscheck
Rule: 552 (level 7) -> 'Integrity checksum changed again (3rd time).'
Integrity checksum changed for: 'C:\xampp\mysql\data\openemr1\form_encounter.MYD'
Old md5sum was: 'ee69e8fa6980d7368b04089c91a13c03'
New md5sum is : '3b4aac9240b7f513487add122f25f16f'
Old sha1sum was: '67ff88d31bbd7ec9f6123e89d5b44e6fb6137eee'
New sha1sum is : '02d42a8caae921238c05004f770cdcb6162a6229'


root@Ossec-VM:/var/ossec/logs/alerts#
```

Figure F48.d: Evidence of the hash value changes from OSSEC

Appendix 5.8: SolarWinds Server Logs

SolarWinds server also captured the evidence of timestamp when the patient database was changed.

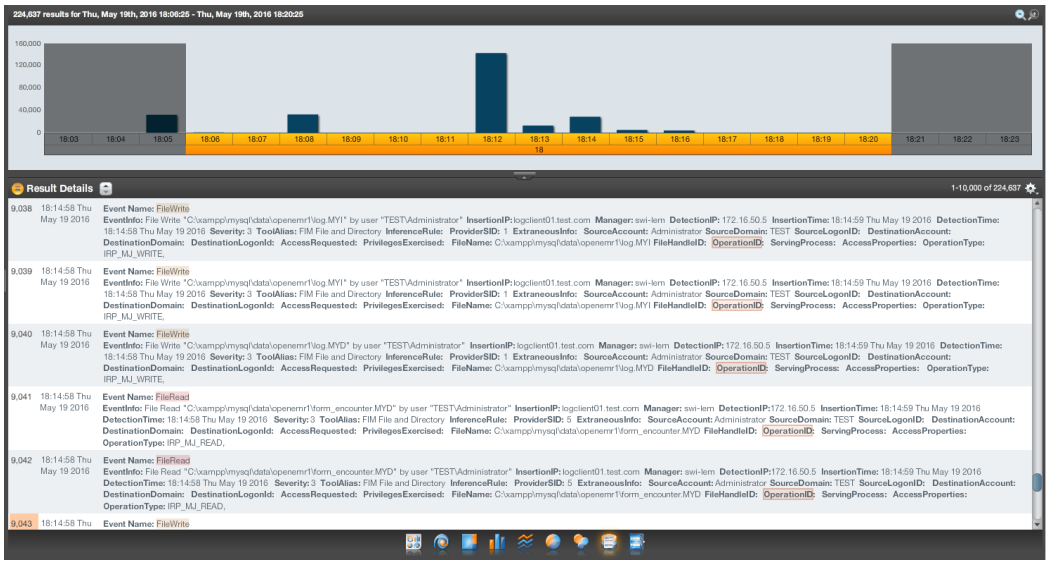


Figure F48.d: Evidence of the patient database changes from SolarWinds

Appendix 5.9: WFserver Logs

The digital evidence of a Fake AP running in the WMedSys was captured by WFserver (see Figure F49.a, F49.b, and F49.c).

```
Thu May 19 18:07:14 2016 CRYPTODROP 0 00:24:6C:2B:50:50 00:24:6C:2B:50:50 00:00:00:00:00:00 00:00:00:00:00:00 Network BSSID
00:24:6C:2B:50:50 changed advertised SSID '' encryption to no encryption when it was previous advertised, an impersonation attack may
be underway
Thu May 19 18:07:24 2016 CRYPTODROP 0 00:24:6C:2B:92:60 00:24:6C:2B:92:60 00:00:00:00:00:00 00:00:00:00:00:00 Network BSSID
00:24:6C:2B:92:60 changed advertised SSID '' encryption to no encryption when it was previous advertised, an impersonation attack may
be underway
Thu May 19 18:07:28 2016 ADHOCCONFLICT 0 00:11:22:33:44:00 00:08:10:74:B7:DC 00:11:22:33:44:00 00:00:00:00:00:00 Network BSSID
00:11:22:33:44:00 advertised as AP network, now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
Thu May 19 18:08:25 2016 CRYPTODROP 0 00:24:6C:2B:92:60 00:24:6C:2B:92:60 00:00:00:00:00:00 00:00:00:00:00:00 Network BSSID
00:24:6C:2B:92:60 changed advertised SSID '' encryption to no encryption when it was previous advertised, an impersonation attack may
be underway
```

Figure F49.a: Evidence of the Fake AP running in WMedSys from WFserver

Kismet-20160519-17-50-19-1.nettxt

```
Network 3: BSSID 00:11:22:33:44:00
 Manuf      : Cimsys
 First      : Thu May 19 18:04:26 2016
 Last       : Thu May 19 18:19:23 2016
 Type       : infrastructure
 BSSID      : 00:11:22:33:44:00
   SSID 1
    Type       : Beacon
    SSID       : "MyWiFi"
    First      : Thu May 19 18:04:26 2016
    Last       : Thu May 19 18:19:23 2016
    Max Rate   : 11.0
    Beacon     : 10
    Packets    : 450
    Encryption : None
   SSID 2
    Type       : Probe Response
    SSID       : "Binatone_1"
    First      : Thu May 19 18:04:48 2016
    Last       : Thu May 19 18:08:37 2016
    Max Rate   : 11.0
    Packets    : 4
    Encryption : None
   SSID 3
    Type       : Probe Response
    SSID       : "Binatone_2"
    First      : Thu May 19 18:05:00 2016
    Last       : Thu May 19 18:08:39 2016
    Max Rate   : 11.0
    Packets    : 9
    Encryption : None
 Channel    : 11
 Frequency  : 2442 - 1 packets, 0.19%
 Frequency  : 2452 - 72 packets, 13.38%
 Frequency  : 2457 - 155 packets, 28.81%
 Frequency  : 2462 - 155 packets, 28.81%
 Frequency  : 2467 - 132 packets, 24.54%
 Frequency  : 2472 - 23 packets, 4.28%
 Max Seen   : 11000
 LLC        : 489
 Data       : 49
 Crypt      : 0
 Fragments  : 0
 Retries    : 0
 Total      : 538
 Datasize   : 8231
 Last BSSTS : 5734784
    Seen By : i2 (drone) 917ca922-1d85-11e6-b71d-b3027e0b1802 538 packets
              Thu May 19 18:19:23 2016
```

Figure F49.b: Evidence of the Fake AP running in WMedSys from WFserver

Mozilla Firefox

file:///hom...19-1.netxml

file:///home/administrator/Kismet-20160519-17-50-1

Search

```
    </wireless-client>
  -<wireless-client number="2" type="fromds" first-time="Thu May 19 18:19:23 2016" last-time="Thu
   May 19 18:19:23 2016">
     <client-mac>00:11:22:33:44:00</client-mac>
     <client-manuf>Cimsys</client-manuf>
     <channel>11</channel>
     <freqmhz>2442 1</freqmhz>
     <freqmhz>2452 70</freqmhz>
     <freqmhz>2457 144</freqmhz>
     <freqmhz>2462 119</freqmhz>
     <freqmhz>2467 107</freqmhz>
     <freqmhz>2472 22</freqmhz>
     <maxseenrate>1000</maxseenrate>
```

Figure F49.c: Evidence of the Fake AP running in WMedSys from WFserver

Moreover, WFserver also captured a fake or an illegitimate client (MAC address: f8:d1:11:0a:e5:e1) associated to the wireless AP (see Figures F50.a and F50.b).

```
Client 11: MAC F8:D1:11:0A:E5:E1
 Manuf      : Tp-LinkT
 First      : Thu May 19 17:52:37 2016
 Last       : Thu May 19 18:19:55 2016
 Type       : Established
 MAC        : F8:D1:11:0A:E5:E1
 Channel    : 0
 Frequency  : 2452 - 8 packets, 6.61%
 Frequency  : 2457 - 11 packets, 9.09%
 Frequency  : 2462 - 89 packets, 73.55%
 Frequency  : 2467 - 13 packets, 10.74%
 Max Seen   : 11000
 Carrier    : IEEE 802.11b+
 Encoding   : PBCC
 LLC        : 0
 Data       : 121
 Crypt      : 78
 Fragments  : 0
 Retries    : 0
 Total      : 121
 Datasize   : 13906
    Seen By : i2 (drone) 917ca922-1d85-11e6-b71d-b3027e0b1802 121 packets
              Thu May 19 18:19:55 2016
```

Figure F50.a: Evidence of a fake client association in WMedSys from WFserver

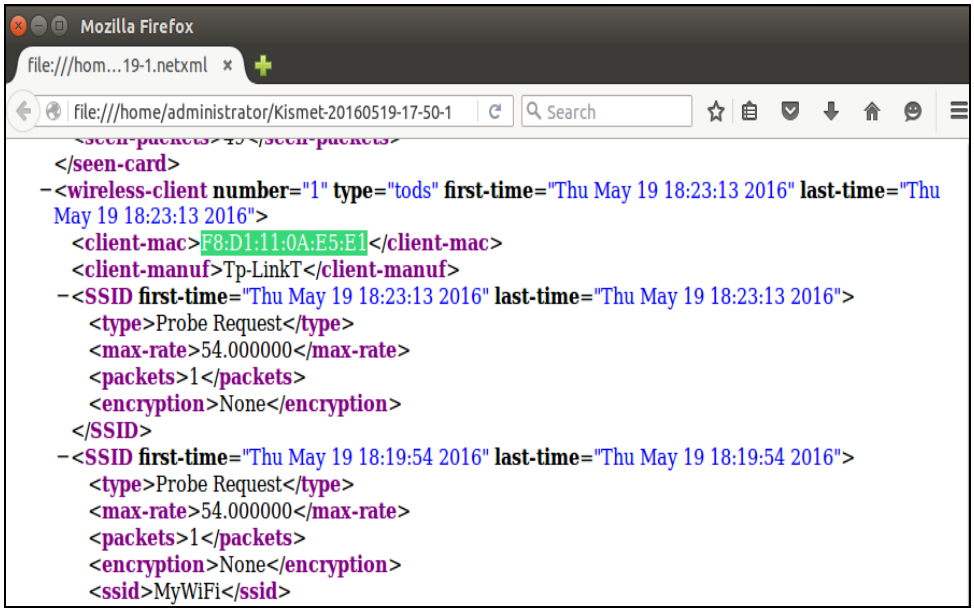


Figure F50.b: Evidence of a fake client association in WMedSys from WFserver

In addition, WFserver also captured all activities of the Fake AP as it was shown on Wireshark (see Figure F51).

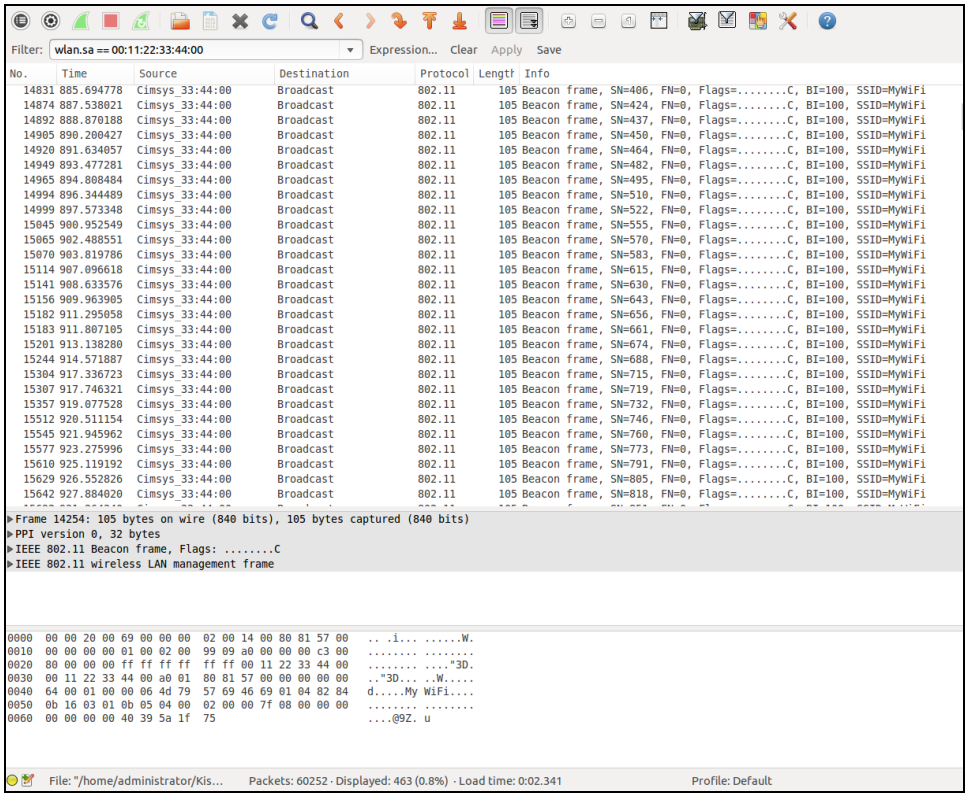


Figure F51: Evidence of activities of the Fake AP in WMedSys from WFserver

Appendix 5.10: Bro-IDS Server Logs

Moreover, the analysis of logs from Bro-IDS server (Figures F52.a and F52.b) validated that the attacker's machine (IP address: 172.16.50.163) was present in the WMedSys and showed the strange UDP packets associated to it.

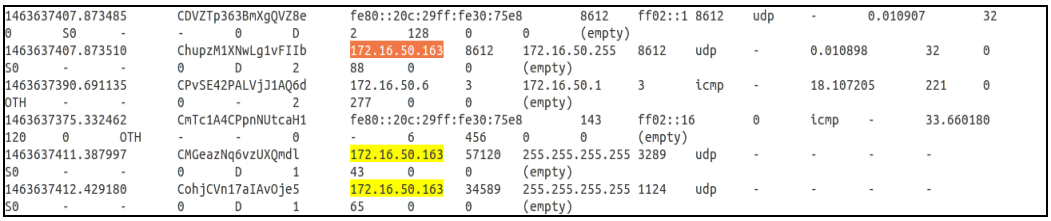


Figure F52.a: Evidence of the attacker's machine in WMedSys from Bro-IDS

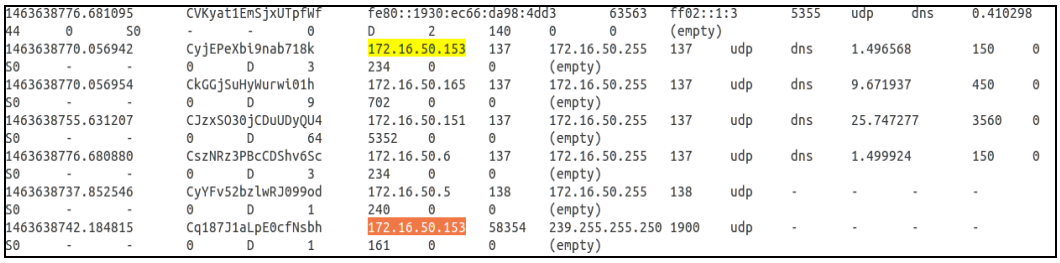


Figure F52.b: Evidence of the attacker's machine in WMedSys from Bro-IDS

The evidence from Bro-IDS also pointed that the DNS spoofing attack was initiated by the attacker (see Figures F53.a and F53.b).

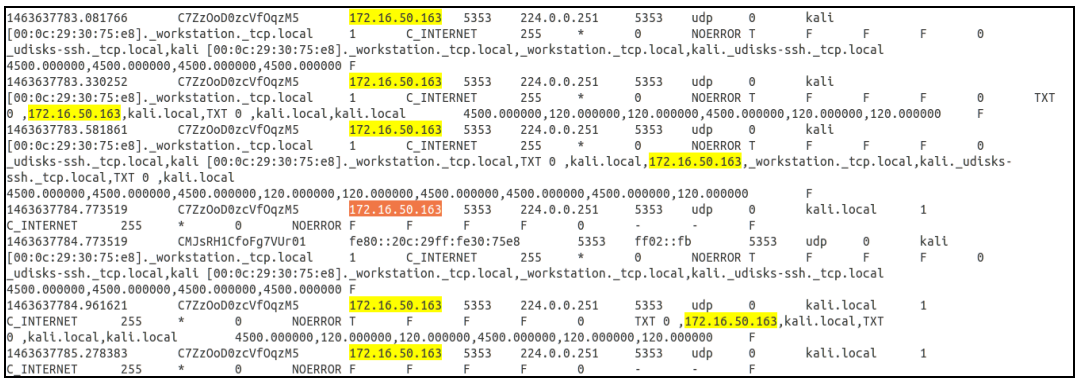


Figure F53.a: Evidence of DNS spoofing attack by the attacker's machine captured by Bro-IDS

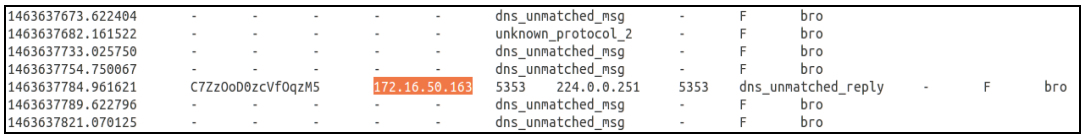


Figure F53.b: Evidence of DNS spoofing attack by the attacker's machine captured by Bro-IDS