2018

Mobile device wardriving tools' comparison: Nuku'alofa as case study

Raymond Lutui

'Osai Tete'imoana

George Maeakafa

DOI: 10.25958/5c5271c16668e

Lutui, R., Tete'imoana, O., & Maeakafa, G. (2018). Mobile device wardriving tools' comparison: Nuku'alofa as case study. In *proceedings of the 16th Australian Information Security Management Conference* (pp. 51-61). Perth, Australia: Edith Cowan University.

MOBILE DEVICE WARDRIVING TOOLS' COMPARISON: NUKU'ALOFA AS CASE STUDY

Raymond Lutui[1], 'Osai Tete'imoana[2], George Maeakafa[2]
[1]Auckland University of Technology, Auckland, New Zealand
[2]Christ's University in Pacific, Kingdom of Tonga
rlutui@aut.ac.nz, oteteimoana@gmail.com, gmaeakafa@yahoo.com

Abstract

This paper describes the justification for a project to assess the security status of wireless networks usage in Nuku'alofa, the CBD of Tonga, By War Driving these suburbs, actual data was gathered to indicate the security status of wireless networks and provide an understanding of the users' level of awareness and attitudes towards wireless security. This paper also takes the opportunity to compare the performance of the War driving tools that this study employed – GMoN, SWardriving, and Wi-Fi Scan. Wireless network communication remains a challenging and critical issue. This study takes an exploratory approach in which it allows the researcher to explore and dig deeper in to the data to find out the true status of wireless network security in Tonga. Not only that, it also allows the researcher to compare the performance of the tools based on the data. The results are very interesting, they indicate that, since the introduction of the fibre optic network, the usage of wireless communication technology grows as well. However, it is evident that wireless network security is still in its early stages. WEP encryption method is still in use, 24.2% with no encryption, and 9.2% did not change their SSID. In terms of tools' performances, it is evident in this study that the SWardriving tool outperforms the GMoN and the Wi-Fi Scan tools

Keywords

Wardriving, Wi-Fi, Wardriving tools, Wireless Network Security, Tools Comparison.

INTRODUCTION

The growth of the communication technologies has changed the way we live and conduct our day to day tasks. Information and Communication Technology (ICT) is one of the most vital traits of every new development (Alshehri & Drew, 2010, p.35). This trend of technological advancements has reached the Kingdom of Tonga. In 2010, Tonga Communications Corporation (TCC) – the country's leading provider of complete end-to-end telephony and Internet services – launched the new mobile-broadband-enabled GSM to replace the previous macro-GSM network (Grealish, 2010, P.1). On the 21st August 2013, the first submarine cable (fibre optic) that connects Tonga to the outside world went live (Matangi Tonga, 2013, P.1).

The Kingdom of Tonga is one of the developing countries in the South Pacific with a population of just over 107 thousand. In 2009, the Government of Tonga has identified Information and Communication Technologies (ICT) as an engine for growth in a national ICT vision and strategy. This focuses on Education, Health, Environment Sustainability, and the Growth of the Industry. The National ICT policy for Tonga consists of six main components - Provision of ICT in Homes and Communities, Education and Skill Development, E- Government, Industry Growth and Economic Development, An enabling technical infrastructure and the ICT related legislation (Ma'u, 2015, p.1). The rapid growth of ICT technologies in Tonga is evident in the literature. In 2010, the Tonga Communications Corporation (TCC) – the country's leading provider of complete end-to-end telephony and Internet services – launched the new mobile-broadband-enabled GSM to replace the previous macro-GSM network. Before the introduction of the fibre optic cable, only 20% across the country uses Internet. At the time of writing this paper, over 75% of the country subscribes for an Internet connection. There are only two Internet Service Providers (ISPs) in Tonga - Tonga Communications Corporation (TCC) and Digicel.

TCC provides hosting and both Wireless and Fixed broadband access while Digicel only provides Wireless access. Jensen and Minges (2017) explained that, the Danden Group provides Internet access via satellite (VSAT) (p.140). Several wireless technologies (WiMAX and 3G) are offered, and TCC provides fixed broadband using ADSL2+

in some areas. An 827km submarine cable connecting Tonga to Fiji was commissioned in August 2013. From Fiji, onward connectivity is provided via the Southern Cross cable to Australia and the United States. The new cable provides an initial capacity of 10 Gbps (ADB, 2018, p.3). Therefore, more places are now available with open wireless hotspot such as pizzerias, hotels, cafes, pubs, and restaurants.

PREVIOUS LITERATURE

Recently, the advancement in the wireless communication technologies, and reduction of cost have allowed for multi-hop wireless networks mainly for monitoring. For instance, wireless technologies such as such as sensors for measurements of plant variables can be transmitted to data centres wirelessly (Zheng et al., 2017, p.139). The 802.11 standards are a group of evolving specifications defined by the institute of electrical and electronic engineers (IEEE). Commonly referred to as Wi-Fi the 802.11 standards define a through-the-air interface between a wireless client and a base station access point or between two or more wireless client. There are many other standards defined by the IEE, such as the 802.3 Ethernet standards (Nisbet, 2012, p.1168).

Table 1: Various wireless standards

Standard	Release Date	Frequency	Maximum Rate	Physical Layer Technology	Technology
802.11	1997	2.4GHz	1 & 2Mbps	DSSS FHSS, IR	N/A
802.11b	1999	2.4GHz	11Mbps	DSSS	N/A
802.11a	1999	5GHz	6 to 54Mbps	OFDM	N/A
802.11g	2003	2.4GHz	54Mbps	DSSS, OFDM	N/A
802.11n	2009	2.4GHz	600Mbps	OFDM	MIMO:4 SPATIAL STREAMS
802.11ac	2014	5GHz	1.3Gbps	OFDM	MIMO, MU-MIMO:8 spatial streams

From among various wireless LAN standards, 802.11ac is more recent, a faster and more scalable version of 802.11n. It operates in the 5-GHz waveband and provides eight channels of 866.7Mbps each with a maximum range of 150 meters or 450 feet. It is backward compatible with 802.11b, 802.11a, 802.11g and 802.11ac products (Bejarano, Knightly & Park, 2013, p.85). The table below provides a brief overview of the currently used IEEE WLAN standards (Sidhu, Singh & Chhabra, 2007, p.45).

Today, Tongan society is networked, ranging from people to objects. Day to day life's so dependent on technology in order to communicate with each other. However, systems that enable us to conduct our day to day tasks are required to be networked (Pesch & Timm-Giel, 2008). As the popularity of wireless applications grew rapidly, wireless network professionals were faced with problems of protecting the privacy and confidentiality of its users. Now, managing wireless LANs should integrate seamlessly into existing enterprise network design and network management principles. At the moment, the technologies for supporting such integration are not highly developed (Vassis et al., 2005, p.21). Security measures were built into the wireless network standards, IEEE 802.11 - for instance, Wired Equivalent Privacy protocol (WEP) and Wi-Fi Protected Access (WPA). Yet, it is now accepted worldwide that wireless networks are more vulnerable than the traditional wired. Some of the problems are due to the fact that the network is wireless, and also based on the type of wireless communication technique supported by 802.11, and also some vulnerabilities are protocol based.

Although there has been tremendous growth and performance success, everything relative to 802.11 WLANs has not been positive. There have been numerous published reports and papers describing attacks on 802.11 wireless networks that exposed organizations to security risks. This subsection will briefly cover the risks to security—i.e., attacks on confidentiality, integrity, and network availability.

Threats to Wireless LAN

Wireless networks are not very expensive to implement and maintain. However, security has hindered network managers in the field from employing the technology (Vacca, 2006, p.4). Encryption was the technology designed to deal with the threat of sniffing, this was included in the development of the Wireless Application Protocol (WAP) released with the Wireless LAN 802.1 lb standard (Gohring, 2005, p.1). Wireless Networks enables anytime and anywhere access for its users. Sniffing is an inherent problem in wireless. Sniffers must have access

to physical parts of the network in order to break in the wired world. However, it is not like that with the Wireless technology, they do not even have to be in the network. Sniffers can be sniffing from a vehicle outside (Xiushuang, Zhankao & Dengke, 2006, p.1390).

Improper installation and configuration of a Wireless LAN devices is one of the main contributors to the problems. For instance:

a) Not hiding the SSID/ESSID
b) Using a very easy to identify network name
c) Lack of control over a connection area (range may be too large)
d) Access Points are not password protected.
e) Failing to apply security controls.

As mentioned earlier, an attack on traditional wired network, the attacker has to be in the perimeter. As for the wireless network, the attacker needs only to be within range of a wireless device. The security requirements for WLANs can be divided into primary goals and secondary goals. Primary goals include Confidentiality, Integrity, Authentication, and Availability. Secondary goals include data freshness, self-organisation or distributed collaboration (Harvey, 2014, p.19). Typical attacks against wired and wireless networks can be divided into passive and active attacks. Passive attacks include monitoring of network traffic and wireless communication channels for information that can be used to execute active attacks (Kisner et al., 2010, p.15). Some of the well-known threats to wireless as listed:

1) Rouge access points
2) DoS/DDoS attacks
3) Attacks on cryptographic safeguards
4) Disrupting the client-access point connection (which is considered preparatory for further attacks)
5) Man-in-the-Middle attack.

Table 2: Cybersecurity attack-vulnerability-damage model (Kisner et al., 2010, p.16).

Attack			**Vulnerability**	**Damage**		
Origin	**Action**	**Target**		**State effect**	**Performance effect**	**Severity**
Local	Probe	Network	Configuration	None	None	None
Remote	Scan	Process	Specification	Availability	Timeliness	Low
	Flood	System	Implementation	Integrity	Precision	Medium
	Authenticate	Data		Confidentiality	Accuracy	High
	Bypass	User				
	Spoof					
	Eavesdrop					
	Misdirect					
	Read/copy					
	Terminate					
	Execute					
	Modify					
	Delete					

Wi-Fi networks are easy to be detected, identified and analysed. There are off the shelf or free download wireless analysis tools available that can be used to do the following:

a) Analysis of packet headers
b) SSIDs are visible
c) MAC addresses can be seen
d) Encryption method can be revealed

e) Signal range/strength can be determined
f) Wi-Fi device vendor's information can be extracted
g) IP addresses can be obtained

Organisations (ISO TMB Working Group, 2008, p.4) in the public and private sectors depend on Information Technology (ISO/IEC, 2005, p.1). Information Systems these days are very complicated (Ross et al., 2008, p.1) and to successfully carry out their missions and business requirements they have to employ IT. An Information Systems can include an office networks, financial and personnel systems to a very specialized system ranging from an industrial control systems, weapons systems, telecommunications systems, and environmental control systems. As a result, Information systems can attract serious threats that will have an impact on the organisation's operations and assets, individuals by exploiting both known and unknown vulnerabilities to compromise the Confidentiality, Integrity, or Availability of the information either in process, stored, or even in transmission. Threats to information systems can include targeted attacks, natural disaster, human errors, and structural failures (Blank & Gallagher, 2012, p.1).

Table 3: Layer based categorisation of possible attacks on identified assets

Assets	**Possible attacks**	**Layers**
Availability	Signal jamming Intentional collision of frames, virtual jamming UDP flood, ICMP flood DoS attacks, DDoS DNS spoofing, TCP SYN flood, de-synchronization	Physical data-link network transport
Data integrity	Mac spoofing session hijacking	Data-link transport
Confidentiality	Replay attack, eavesdropping and man-in-the-middle, mac spoofing, pre-computation and partial matching	Data-link
Software	Worms and viruses	Application
Hardware	Device tampering and physical damage	Physical

It is evident in the literature that the best possible way to identify potential threats to an Information System is to first identify possible attacks based on network assets. Threats/attacks aim towards one or more assets (Myagmar, Lee & Yurcik, 2005, p.3). Table 3 identified known attacks on each identified information assets (Glass, Portmann & Muthukkumarasamy, 2008, p.31) and the attacks are categorised by layer. The layer-wise categorisation of threats on assets help Information System Security Experts in identifying suitable security controls.

As the popularity of wireless applications grew rapidly, wireless network professionals are faced with problems of protecting the privacy and confidentiality of its users. Now, managing wireless LANs should integrate seamlessly into existing enterprise network design and network management principles. At the moment, the technologies for supporting such integration are not highly developed (Reiher et al., 2007, p.7). Security measures were built into the wireless network standards, IEEE 802.11 - for instance, Wired Equivalent Privacy protocol (WEP) and Wi-Fi Protected Access (WPA). Yet, it is now accepted worldwide that wireless networks are more vulnerable than the traditional wired. Some of the problems are due to the fact that the network is wireless, and also based on the type of wireless communication technique supported by 802.11, and also some vulnerabilities are protocol based.

Although there has been tremendous growth and performance success, everything relative to 802.11 WLANs has not been positive. There have been numerous published reports and papers describing attacks on 802.11 wireless networks that exposed organizations to security risks. This subsection will briefly cover the risks to security—i.e., attacks on confidentiality, integrity, and network availability. Known weaknesses of the cryptographic protocols and algorithms have been used to work out tools which enable carrying out the attack. The popular tools are as follows: AirSnort, which enables recovery of the WEP key on the basis of an analysis of the sufficient number of the intercepted packets (e.g. by means of the FMS method – which name derives from the surnames of its authors:

Fluhrer, Mantin, and Shamir), Aircrack (which uses a dictionary attack on WPA but is not limited to it), and WepLab, which uses optimized FMS and Korek's attacks. The Wigle.net site has worked out the list of 1000 most popular WLAN network names in the world, and it was used by the makers of tools for cracking safeguards as the base for creation of special tables (rainbow tables), which facilitated the practice.

FINDINGS & DISCUSSIONS

A systematic guidance of a methodology is highly recommended to maintain the integrity of the findings. Exploratory research is employed in this study as it allows the researcher to gain a deeper understanding of an issue or problem (ISO/IEC, 2004, p.7). Benbasat, Goldstein and Mead (1987) rightly pointed out that, it is an exploratory paper that reveals an important factor in the implementation process. This exploratory study will conclude with suggestions to which opensource tool that it is suitable for such an environment. The design of the study aims to first identify the problem and the motivation of the study based on the literature analysis. When the problem identification is completed then the second task is to define the problem and extract its significance. This involves analysing the existing literature in the body of knowledge; identify the problem, and consulting experts in the field.

The third stage of the study is designed to deal with designing and formulating the main research question and the development of the research design. The fourth stage deals with identifying the best route for the war-drive. This is the first time for a study like this to be conducted in Tonga. As a result, in order to identify the true status of WLAN security implementation in the CBD of Tonga, the war-drive needs to capture both enterprise and personal WLAN data. This philosophy needs to be the main factor in determining the route for the war-drive in this phase. Once the route is determined, then the data collection process will start according as shown in Figure 1.

Once the data collection is finished then the data analysis will begin in phase five. The data analysis phase is designed to identify the true status of WLAN security in the CBD, Nuku'alofa. That is, conduct vendors' analysis, SSID configuration analysis, encryption methods analysis, and so on. The final phase of the study is designed to allow the researcher(s) to employ various scholarly electronic databases to communicate the outcome of the study.

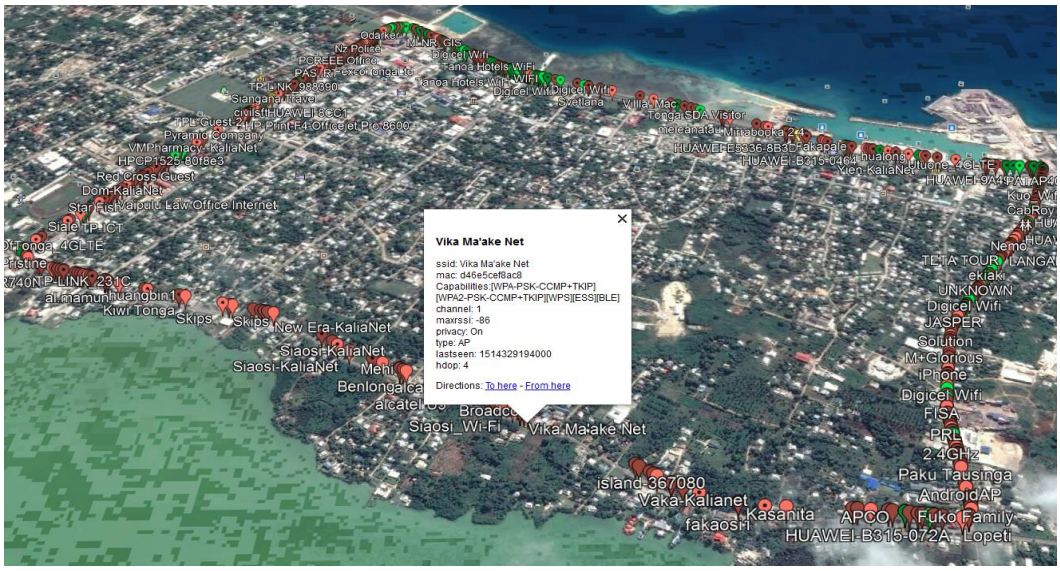

Figure 1: War-Driving route in Nuku'alofa

WLAN is easier to exploit than traditional wired networks. Some people use war-driving to demonstrate how easy it is to compromise or penetrate WLANs (Harley, 2008, p.221). The war driver can easily map the locations of the wireless nodes. To start collecting data, tools for war-drive such as hardware and software need to be considered. Employing of well-known tools such as a laptop with good wireless card and a Wi-Fi signal booster, GPS unit, magnetically mount external antenna for the top of the vehicle and amplifier is recommended. Scanning software such as Kismet, Network Stumbler (NetStumbler), Airbase, and AirCrack however, it is quite hard to find in Tonga. The following sub-sections is designed to introduce the tools employed and discuss the findings.

War-Driving Tools

This study employed three different open-source war-driving tools namely SWardriving, GMoN, and Wi-Fi Scan.

SWardriving, a simple application used for Wardriving anywhere in the world, is a powerful scanner for Wardriving. GPS and Wireless Wi-Fi network scanner collaborates to locate access points Wi-Fi in this application of SWardriving. Then the essential data is saved in a database where it can be exported to a KML, CSV, or GEOJSON and sqlite. It is important to wait for the device to determine the current location through GPS to acquire the necessary data Wireless Wi-Fi network. A file may be created with the information provided from using the SWardriving application. This file is called a Keyhole Markup Language (KML) file, created and opened with Google Earth to pin point the data using map mode. When the Google Earth is opened, the position of the Wi-Fi network will appear as coloured dots. By clicking on each dot, more information is displayed such as signal strength, quality and type of network. Comma Separated Values (CSV) which displays the GPS-Tagging and statistics of the captured WLANs can also be transmitted using SWardriving. For encryption purposes, SWardriving has five different display results such as WEP, WPA, WpaPsk, WPA2, Open and not defined.

The analysis in this study covers the various features of WLAN usage in Nuku'alofa, the capital city of the Tonga Islands. This study also considers well known AP vendors, nature of SSID settings used, WLAN standards used, location, channels and encryption systems used, as well as deployment of network types. SWardriving does not support MAC filtering, therefore MAC filtering was not included in the analyses of the identified 505 Wireless nodes in this study.

Table 4: War-Driving tools and their key features

G-MoN	**Wi-FiScan**	**SWardriving**
Key Features:	**Key Features**	**Key Features**
○ Shows every WLAN tht's in range ○ CSV-Export ○ KML-Export ○ GPS-Tagging of the found WLANs ○ Statistics about your found WLANs ○ Show your position and APs in Map-Mode	○ Shows every WLAN that's in range ○ CSV EXPORT RUN ○ KML EXPORT RUN ○ CSV EXPORT DB ○ KML EXPORT DB ○ BACKUP DATABASE ○ Statistics about your found WLANs ○ Show your position and APs in Map-Mode	○ Shows every WLAN that's in range ○ wifiscan-export.csv ○ wifiscan-export.kml ○ wifiscan-kistmet-export.csv
Views of different encryption modes:	**Views of different encryption modes:**	**Key Features**
○ # WPA2 ○ + WPA ○ - WEP ○ " " Open ○ ? not defined	○ WPA2 ○ WPA ○ WEP ○ [ESS] ○ [IBSS]	○ WPA2 ○ WPA ○ WEP ○ [ESS] ○ [IBSS]
Menu-Buttons:	**Menu-Buttons:**	**Key Features**
○ KML-Export: Exports your results as gmon_wlan_YYYY_MM_DD.kml to the SD-Card. This file you can import in Maps or Google Earth. ○ Daily Export: Exports your daily scanresults to gmon_wlan_export_YYYY_MM_DD.txt. This file is comma separated so you can create your own Statistic-Database ○ Day & Night: Toggle the Day & Night Modus. High contrast and low contrast. ○ Map: Shows your Position on a Googlemap and APs in your environment	○ Uses GPS to estimate locations of observed networks ○ Observations logged to local database to track your networks found ○ Upload and compete on the global WiGLE.net leaderboard ○ Real-time map of networks found, with overlays from entire WiGLE dataset ○ Free, open source, no ads (pull requests welcome at https://github.com/wiglenet/wigle-wifi-wardriving)	○ Export KML files in the SD (for importing into Google Maps/Earth, Wigle.net, ...) ○ Export CSV files in the SD (separated by commas to Excel, OpenOffice/LibreOffice, ...) ○ Export GEOJSON files in the SD (separated by commas. ○ X: Delete ALL data collected. ○ STOP: STOP Scanning

○ Stop Scanning & Exit: Exits G-Mon and stops the backgroundprocess ○ About: About-Information ○ Help: Help	○ Export to CSV files on SD card (comma separated values) ○ Export to KML files on SD card (to import into Google Maps/Earth) ○ Bluetooth GPS support through mock locations Audio and Text-to-Speech alerting and "Mute" option to shut off all sound/speech	○ START: Start Scanning.

When looking at the above table, the three tools detected similar number of devices that uses WEB, WPA, and WPA2 encryption, Unlike Open and Unknown Encryption which they have a big different between them with their number of devices.

- ~ G-MoN tool detect 83 devices while Wi-Fi Scan detect 113 devices and SWardriving identify up to 121 devices were configured open.
- ~ It was identified that 38 devices were marked as unknown with G-MoN tool because it cannot identify the encryption methods used while the other two tools did not pick up any device with Unknown encryption.

Table 5: Encryption methods comparison in %

Encryption	GMoN %	SWardriving %	Wi-Fi Scan %
Open	16.6	24.2	22.6
WEP	1	1	1.2
WPA	39.2	39	39
WPA2	36.6	36.6	37
Unknown	7.6	0	0

- ~ Table 5 shows that there are 39% of wireless devices in the Kingdom that still use WPA Encryption technique. Even though WPA improved security of WEP Encryption, but is now also considered vulnerable to intrusion.
- ~ Over 36% of wireless devices in Nuku'alofa use WPA2, even though it is not perfect, but currently the most secured choice.
- ~ 16.6% of the devices were found by the GMoN tool to be Open meaning, no encryptions were used. At the same time, the Wi-Fi Scan identified 22.6% while the SWardriving tool identified 24.2% of the detected devices to be online with no encryption methods employed.
- ~ 7.6% of the devices were marked with Unknown encryption by the GMoN tool meaning, the tool cannot identify the encryption technique used. The SWardriving and the Wi-Fi Scan tool detected 0%.
- ~ Both the GMoN and the SWardriving identified 1% and the Wi-Fi Scan tool identified 1.2% of the detected devices that still uses WEP encryption method.

Based on the analysis results shown in Table 5, the results for all the three chosen tools showed some very interesting numbers. The SWardriving tools managed to identified 7.6% more devices than the GMoN tool, and 1.6% more than the Wi-Fi Scan tool that did not used any encryption method. All three tools basically detected and yielded very similar numbers when talking about the three commonly used encryption methods. Based on the results shown in Table 5, only the GMoN tool that was not able to detect the encryption status of 7.6% devices.

Following in Table 6, the results from the analysis of the devices' SSID from the three chosen tools.

Table 6: SSID analysis comparison

SSID	GMoN %	SWardriving %	Wi-Fi Scan %
Change	88.4	84	83.2
Default	9.2	8.6	9.2
Unknown	0.2	4.4	5.8
Other Devices	3.4	4.2	3

- It is quite interesting to see that the GMoN tool identified 88.4% of the detected devices that their SSIDs have been changed from the default. The SWardriving tool identified 84% while the Wi-Fi Scan tool only identified 83.2%.
- The GMoN and the Wi-Fi Scan tools both identified 9.2% of the detected wireless devices that still used the default SSIDs that came with either from the ISPs or the Vendors.
- The Wi-Fi Scan tool was having difficulty identifying the status of 5.8% of the devices while the SWardriving tool stuck with 4.4% of the devices and the GMoN tool only struggles with 0.2% of the devices detected.
- One of the interesting results showed in Table 6 is that all of the tools employed in this study detected and identified some devices that were not a wireless hotspot however in fact, they were identified as wireless printers. The SWardriving tools identified the most at 4.2% while the GMoN tool identified 3.4% and 3% by the Wi-Fi Scan tool.

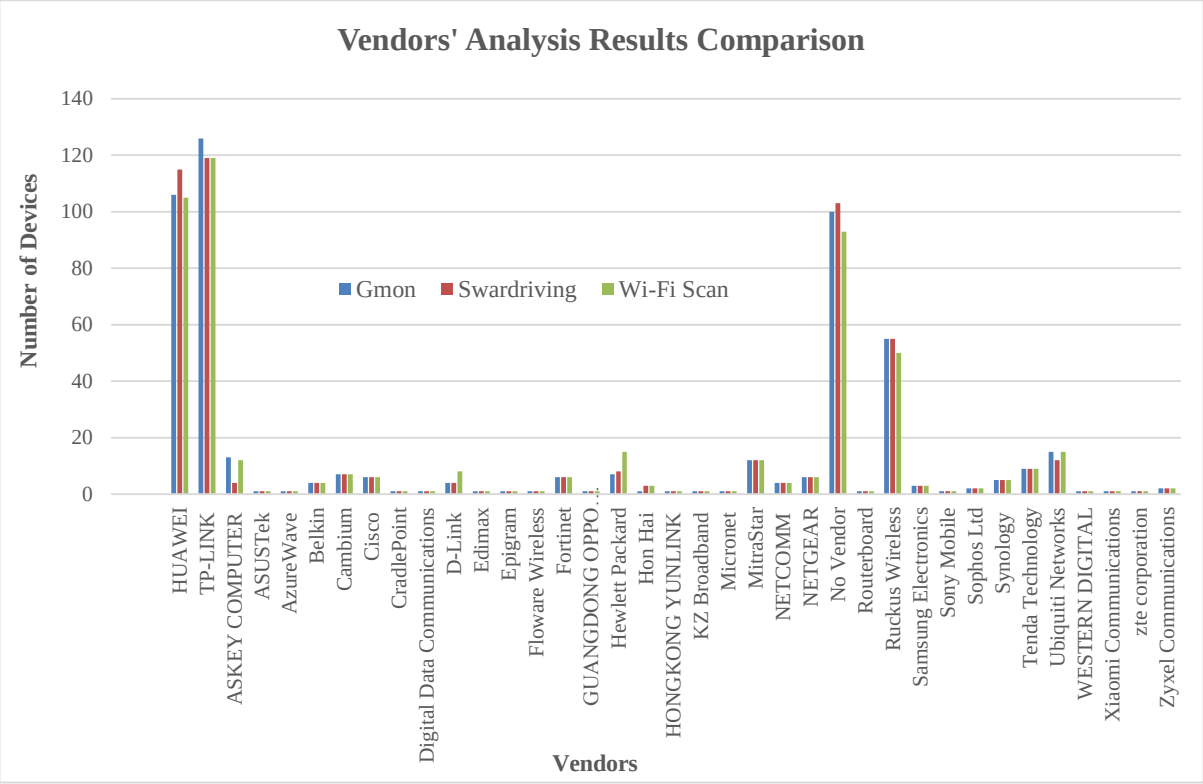

Figure 2: Vendors' analysis results comparison

36 vendors were identified out of the total of 500 wireless nodes detected in this war-drive study. Figure 2 illustrates the total results of the vendor's analysis whereas Table 7 shows a summary of the most popular vendors in the market today. As it illustrated in Figure 2, TP-Link seems to be the most used wireless device in Tonga at 25.2% as identified by the GMoN tool. Both SWardriving and Wi-Fi Scan identified 23.8% used TP-Link. The second most used device in Tonga is the Huawei devices at 23% identified by the SWardriving tool while the GMoN tool identified 21.2% and the Wi-Fi Scan identified 21% used Huawei devices.

Table 7: Vendors' analysis results comparison

Vendors	GMoN	SWardriving	Wi-Fi Scan
HUAWEI	21.2%	23%	21%
TP-LINK	25.2%	23.8%	23.8%
Cisco	1.2%	1.2%	1.2%
D-Link	0.8%	0.8%	1.6%
NETGEAR	1.2%	1.2%	1.2%
Ruckus Wireless	11%	11%	10%
Tenda Technology	1.8%	1.8%	1.8%
Ubiquiti Networks	3%	2.4%	3%
Xiaomi Communications	0.2%	0.2%	0.2%
ZTE Corporation	0.2%	0.2%	0.2%
Zyxel Communications	0.4%	0.4%	0.4%
No Vendor	20%	20.6%	18.6%

According to Table 7, a well-known vendor in the world market today such as Cisco and Netgear, all tools only identified that only 1.2% of Tonga used devices from these two well-known vendors. D-Link came up at 0.8% according to GMoN and SWardriving while Wi-Fi Scan tool identified 1.6%. It is also evident in this study the growth in the usages of devices from vendors such as Ruckus Wireless. Both the GMoN and the SWardriving tools identified 11% while the Wi-Fi Scan tools showed 10% in terms of the usages of devices from the Ruckus Wireless. All tools identified a 1.8% of the devices were from the Tenda Technology while 0.2% were from the Xiaomi Communications. 0.2% were identified came from the popular ZTE Corporation and 0.4% from the Zyxel Communications.

The last row in Table 7 showed that SWardriving identified 20.6% as no vendor, 20% identified by GMoN and 18.6% identified by Wi-Fi Scan. The process employed by this study to identify the vendors of the detected devices was by taking their MAC addresses and put it through https://macvendors.com/. The first three bytes of the MAC address is taken and the vendor's information is extracted. This means that the macvendors.com website cannot extract the vendor's information from the MAC address.

CONCLUSION

This paper conducted a study to analyse the status WLAN deployment growth and its security status in Nuku'alofa. At the same time, evaluate the performance of the three tools employed in this study. As a result, this study concluded that the status of wireless network growth increased considerably over the past five years since the deployment of the fibre optic network. It is also evident in the study that WLAN security is still in its early stages. WEP encryption method is still in use, 9.2% were detected by both the GMoN and the Wi-Fi Scan tools that they did not change their SSID. 88.4% of the devices were identified by the GMoN tool that their SSID were changed. However, 5.8% were identified by the Wi-Fi Scan tool as unknown meaning the tool cannot extract information regarding its SSID. In terms the encryption methods, the SWardriving tool identified 24.2% left their encryption not configured, 39% have their encryption configured to use the WPA method and 36.6% to use the WPA2 method. In terms of tools' performances, it is evident in this study that the SWardriving tool performs the best. The SWardriving tool has demonstrated consistency, yielding data that can be trusted to base well informed decision on. This study should be repeated after two years to get a better view of the status of WLAN security in the CBD of Tonga, there is still a lot of room for improvements.

REFERENCES

ADB. (2018). Tonga, Key Indicators. Retrieved September 17, 2018, from https://data.adb.org/dataset/tonga-key-indicators

Alshehri, M., & Drew, S. (2010). E-Government Fundamentals, *Proceedings of the IADIS International Conference ICT, Society and Human Beings* (pp. 34-42). Freiburg: MCCSIS.

Bejarano, O., Knightly, E. W., & Park, M. (2013). IEEE 802.11 ac: from channelization to multi-user MIMO. *IEEE Communications Magazine, 51*(10), 84-90.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS quarterly*, 369-386.

Blank, R. M., & Gallagher, P. D. (2012). Special Publication 800-30 Guide for Conducting Risk Assessments. *NIST Special Publication 800-30 Revision 1, 1*(1), 1-95.

Glass, S., Portmann, M., & Muthukkumarasamy, V. (2008). Securing wireless mesh networks. *IEEE Internet Computing* (4), 30-36.

Gohring, N. (2005). Motion Sickness. *eWeek*.

Grealish, A. (2010). *Altobridge wireless network goes live in tonga*. Retrieved July 25, 2017, from https://www.realwire.com/releases/Altobridge-Wireless-Network-goes-Live-in-Tonga

Harley, D. (2008). Chapter 6 - WarDriving and Wireless Penetration Testing with OS X. In *OS X Exploits and Defense* (pp. 219-249). Burlington: Syngress.

Harvey, M. G. (2014). Wireless Threats and Key Management Issues [Harvey2014]. In *Wireless Next Generation Networks: A Virtue-Based Trust Model* (pp. 13-30). Cham: Springer International.

ISO/IEC. (2004). ISO/IEC International Standard - Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. *ISO/IEC 8802-11, Second edition: 2005/Amendment 6 2006: IEEE STD 802.11i-2004 (Amendment to IEEE Std 802.11-1999)*, c1-178. doi:10.1109/IEEESTD.2004.311922

ISO/IEC. (2005). Information technology–Security techniques–Information security management systems–Requirements. *ISO/IEC FDIS 27001:2005(E), 1*(1), 1-42.

ISO TMB Working Group (2008). Risk management — Vocabulary. *ISO/IEC CD 2 Guide73, 1*(1), 1-17.

Jensen, M., & Minges, M. (2017). Ensuring Sustainable Connectivity in Small Island Developing States. *Internet Society: A Global Review of Internet Infrastructure Issues, 1*(1), 140.

Kisner, R. A., Manges, W. W., MacIntyre, L. P., Nutaro, J. J., Munro, J., Ewing, P. D., Howlader, M., Kuruganti, P.T., Wallace, R. M., Olama, M. M. (2010). Cybersecurity through real-time distributed control systems. *Oak Ridge National Laboratory, Technical Report ORNL/TM-2010/30*.

Matangi Tonga. (2013). *Tonga's high-speed internet goes live august 21*. Retrieved July 25, 2017, from http://matangitonga.to/2013/08/14/tonga%E2%80%99s-high-speed-internet-goes-live-august-21

Ma'u, P. (2015). E-Government in Tonga'. *Asia-Pacific Regional Forum on e-Government, 1*(1), 1-19.

Myagmar, S., Lee, A. J., & Yurcik, W. (2005). Threat modeling as a basis for security requirements. In *Symposium conducted at the meeting of the Symposium on requirements engineering for information security (SREIS)* (pp.1-8). Citeseer.

Nisbet, A. (2012). A tale of four cities: Wireless security and growth in New Zealand. *Proceedings of the 2012 International Conference on Computing, Networking and Communications (ICNC)* (pp. 1167-1171). Maui, HI: IEEE.

Pesch, D., Rea, S., & Timm-Giel, A. (2008). Embedded Wireless Networking: Principles, Protocols, and Standards. In *Ambient Intelligence with Microsystems: Augmented Materials and Smart Objects* (pp. 157-184). Boston, MA: Springer US.

Reiher, P., Makki, S. K., Pissinou, N., Makki, K., Burmester, M., Le Van, T., & Ghosh, T. (2007). Research Directions in Security and Privacy for Mobile and Wireless Networks. In *Mobile and Wireless Network Security and Privacy* (pp. 1-22): Springer.

Ross, R. S., Johnson, L. A., Katzke, S. W., Toth, P. R., Stoneburner, G., & Rogers, G. (2008). *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*.

Sidhu, B., Singh, H., & Chhabra, A. (2007). Emerging wireless standards-wifi, zigbee and wimax. *World Academy of Science, Engineering and Technology, 25*(2007), 308-313.

Vacca, J. R. (2006). Wireless Network Security Fundamentals [Vacca2006]. In *Guide to Wireless Network Security* (pp. 3-55). Boston, MA:

Vassis, D., Kormentzas, G., Rouskas, A., & Maglogiannis, I. (2005). The IEEE 802.11 g standard for high data rate WLANs. *IEEE Network, 19*(3), 21-26.

Xiushuang, Y., Zhankao, W., & Dengke, Z. (2006). Sniffing threat and practices in IPv6 networks [journal article]. *Wuhan University Journal of Natural Sciences, 11*(5), 1389-1393.

Zheng, M., Liang, W., Yu, H., & Xiao, Y. (2017). Performance Analysis of the Industrial Wireless Networks Standard: WIA-PA. *Mobile Networks and Applications, 22*(1).