

An Investigation into the Privacy and Security Risks of Smart Toys in New Zealand

Nicole Girvan

A thesis submitted to the Faculty of Design and Creative Technologies Auckland University of Technology

In partial fulfilment of the requirements for the degree of
Master of Information Security and Digital Forensics

School of Engineering, Computer and Mathematical Sciences

Auckland, New Zealand, 20 February 2020

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.

A handwritten signature in black ink that reads "Nicole Girvan". The signature is written in a cursive style with a long, sweeping underline.

Nicole Girvan

20 February 2020

Acknowledgements

I wish to thank my research supervisor, Dr Alastair Nisbet, for providing essential support and feedback during the process of completing this study. Additional thanks go to my friends and colleagues, Dr Lopez and Mr Antony, who answered numerous questions and gave advice and encouragement along the way. Finally, thanks to my beautiful son, Ellis, who sacrificed weekends with mommy for me to complete this work.

Abstract

Smart toys are a growing portion of the children's toy market. They offer a unique and personalised play experience via the use of onboard sensors, internet connectivity, and innovative technology. International research has shown that the smart toy environment can be insecure and vulnerable to cyberattacks and can place children at risk. Smart toy security and privacy must be understood to protect children; however, to date, the literature has not addressed this in the New Zealand context.

To address this gap in the literature, this study investigates whether smart toys pose any security or privacy risks to New Zealand users. It asks, what common security and privacy impacting vulnerabilities are found in smart toys currently available for purchase by New Zealanders? Furthermore, what levels of privacy and security concern and awareness do New Zealand parents and guardians have regarding smart toy use?

An anonymous online survey targeting New Zealand parents/guardians was designed. A total of 394 respondents answered 32 questions to determine their levels of concern and awareness around the privacy and security of smart toys. A security testing methodology was also used to assess a collection of smart toys to determine if they contained security or privacy vulnerabilities.

Analysis of survey responses showed a high average level of concern of New Zealand parents/guardians ($M = 8.26$, $SD = 1.7$) around the security and privacy risks of using smart toys. The survey also revealed a low overall level of awareness regarding security and privacy risks when using smart toys, with participants answering an average of 14.5 out of a possible 30 ($SD = 5.66$) questions accurately.

Analysis of the results from the physical security testing of a selection of smart toys showed insufficient authentication weaknesses, including unauthenticated Wi-Fi connections, unauthenticated Bluetooth pairing, and weak or no password use. Insecure data transfer was demonstrated, with some toys using no encryption for communication. Insufficient privacy protection weaknesses including the unreasonable collection of personally identifiable information, a lack of parental control mechanisms, and the use of non-random device identifiers, were also present.

Based on these results, it can be concluded that smart toys pose security and privacy risks to New Zealand users, and that greater focus should be placed on educating parents and guardians about the potential risks these products pose and how to mitigate them. Smart toy manufacturers and legislators should additionally consider addressing the high levels of concern seen regarding these issues by focusing on safer smart toy design and strengthening existing privacy legislation for children's products.

Table of Contents

Declaration	ii
Acknowledgements	iii
Abstract	iv
List of Figures.....	vii
List of Tables	ix
List of Abbreviations	x
Chapter 1: Introduction.....	1
1.1 Background and Motivation.....	1
1.2 Research Approach and Findings.....	3
1.3 Thesis Structure	3
Chapter 2: Literature Review	5
2.1 Introduction.....	5
2.2 The IoT	5
2.2.1 Overview	5
2.2.2 IoT Architecture	8
2.2.3 IoT Technologies.....	10
2.3 Securing the IoT	13
2.3.1 Unique Challenges to Privacy and Security in the IoT Environment	15
2.3.2 The Smart Home Environment.....	22
2.4 Smart Toy Security and Privacy.....	23
2.4.1 Smart Toys	23
2.4.2 Security Incidents.....	24
2.4.3 Smart Toy Security and Privacy Challenges.....	26
2.5 Awareness and Risk	31
2.6 Conclusion.....	33
Chapter 3: Research Design and Methodology	36
3.1 Introduction.....	36
3.2 Research Questions.....	36
3.3 Research Approach	37
3.4 Survey Design	38
3.4.1 Approach and Mode	38
3.4.2 Sample	39
3.4.3 Questionnaire Design.....	39
3.4.4 Measures.....	40
3.4.5 Scoring	42
3.4.6 Reliability	42
3.4.7 Validity Pre-Testing	42
3.4.8 Pilot Survey	43
3.4.9 Data Collection	43
3.4.10 Data Preparation and Analysis.....	43

3.4.11	Ethics.....	44
3.5	Smart Toy Security Testing Design	44
3.5.1	Smart Toy Environment and Attack Surface.....	45
3.5.2	Test Strategy	46
3.5.3	Test Environment and Tools	50
3.5.4	Test Case Plan and Measurement.....	53
3.5.5	Validity and Reliability	59
3.6	Conclusion.....	59
Chapter 4:	Findings.....	60
4.1	Introduction.....	60
4.2	Survey Findings	60
4.2.1	Completion Rate and Exploratory Data Analysis	60
4.2.2	Summary of Findings	60
4.3	Smart Toy Security Testing Findings	69
4.3.1	Vulnerability Area 1 – Insufficient Authentication.....	70
4.3.2	Vulnerability Area 2 – Insecure Data Transfer	84
4.3.3	Vulnerability Area 3 – Insufficient Privacy Protection.....	87
4.3.4	Exclusions	93
4.3.5	Summary of Physical Test Findings.....	94
4.4	Conclusion.....	95
Chapter 5:	Discussion	96
5.1	Introduction.....	96
5.2	Research Sub-Questions	96
5.2.1	Sub-Question 1	96
5.2.2	Sub-Question 2	97
5.2.3	Hypothesis.....	102
5.2.4	Sub-Question 3	102
5.3	Main Research Question.....	104
5.4	Additional Discussion	105
5.5	Strengthening User Privacy and Security in the Smart Toy Environment	106
5.6	Conclusion.....	109
Chapter 6:	Conclusion.....	110
6.1	Summary of Research	110
6.2	Research Methods and Limitations.....	111
6.3	Recommendations and Contributions	112
6.4	Future Research	113
6.5	Conclusion.....	113
References	115
Appendix A:	Survey Participant Invitation and Information Notices.....	130
Appendix B:	Survey Questionnaire	133
Appendix C:	Pre-Test Technical Consultation and Pilot/Target Audience Feedback.....	141
Appendix D:	Smart Toy Descriptions	144

List of Figures

Figure 2.1. IoT architectural layers. Adapted from “Review: Internet of Things security: A survey”, by F. A. Alaba, M. Othman, I .T. Hashem, & F. Alobaiti, 2017, Journal of Network and Computer Applications, 88, pp.10–28. Copyright (2017) by Elsevier. Adapted with permission from Elsevier.	8
Figure 3.1. The survey research process adapted from Groves (2009).	38
Figure 3.2. An example of a survey question.....	41
Figure 3.3. An example of a survey question asked to measure awareness	42
Figure 3.4. The security testing process. Adapted from Testing Guide 4.0 by OWASP, (2014b). CC BY-SA 3.0.	45
Figure 3.5. The smart toy attack surface.....	46
Figure 4.1. Highest level of education as reported by the participants	61
Figure 4.2. Average level of participant concern around the security and privacy risks of using smart toys	62
Figure 4.3. Percentage of correct answers received for questions in dimension 1 around participants knowledge of smart toy technical capabilities	64
Figure 4.4. Percentage of correct answers received for questions in dimension 2 around participants knowledge of smart toy security and privacy risks	65
Figure 4.5. Overall average level of participant knowledge seen across all dimensions by the highest level of education completed.....	68
Figure 4.6. Average level of participant awareness in each knowledge dimension.....	69
Figure 4.7. The BLE pairing process	71
Figure 4.8. The BLE protocol stack. Reprinted from multihop real-time communication over BLE industrial wireless mesh networks by L. Leonardi, 2018, IEEE Access, 4 (1).	72
Figure 4.9. The Adafruit BluefruitV2 BLE sniffer and the Ubertooth1	73
Figure 4.10. Kismet display of Furby Connect device name and MAC address details	74
Figure 4.11. The Ubertooth1 while capturing the traffic for the R2-D2 Droid.....	75
Figure 4.12. The Bluefruit Wireshark interface actively capturing live R2-D2 Droid broadcasting packets.	76
Figure 4.13. Pairing response packet from Furby Connect (Slave) to smartphone (Master) captured using the BluefruitV2.	77
Figure 4.14. Pairing response packet generated from the R2-D2 Droid (Slave) to smartphone (Master) and captured using the Ubertooth1	78
Figure 4.15. The successful capture of pairing packets required for CrackLE decryption	79
Figure 4.16. Successful cracking of the Furby Connect encryption key using CrackLE	79
Figure 4.17. Numeric comparison pairing between a Kurio Watch 2.0 and Kurio Watch Messenger	80
Figure 4.18. Identification of LAP of Kurio Watch	80
Figure 4.19. Kurio Watch user manual page showing factory-set password to access emergency details	81
Figure 4.20. Identification of the Air Hogs FPV Race Car open network.....	82
Figure 4.21. Toy Mail Talkie Unicorn authentication and communication establishment packets.....	83
Figure 4.22. WPA handshake captured by passively eavesdropping the communication between Toy Mail Talkie Unicorn and the smartphone application	83
Figure 4.23. Successful cracking of WPA2 personal wi-fi network passkey.....	84
Figure 4.24. Toy Mail Talkie Unicorn password reset function	84
Figure 4.25. Encrypted Toy Mail Talkie Unicorn application data viewed in Wireshark	85
Figure 4.26. Air Hog High Speed Race Car unencrypted data frame as viewed in Wireshark	86
Figure 4.27. Kurio Watch encrypted data packet captured and viewed in Wireshark	87
Figure 4.28. Kurio Watch setup process	88
Figure 4.29. Furby Connect pairing packet showing the exchange of an IRK.....	92
Figure 4.30. R2-D2 Droid pairing response packet exchange within Wireshark	93

Figure 4.31. Kurio Watch set up process using username to create the device identifier 93

List of Tables

Table 3.1. In-scope areas of vulnerability with related attacks, attack surfaces, and impacts of an attack.....	49
Table 3.2. Selected smart toys and their characteristics	50
Table 3.3. Security test description, measurement criteria, and test process for each area of vulnerability in scope.....	55
Table 4.1. Participant demographics – Gender	61
Table 4.2. Summary of findings in vulnerability area 1 – insufficient authentication	71
Table 4.3. Summary of findings in vulnerability area 2 – Insecure data transfer	85
Table 4.4. Summary of findings in vulnerability area 3 – Insufficient privacy protection	88
Table 4.5. PII requested by smart toy and companion applications during set up and use	89
Table 4.6. Permissions requested by the toys companion applications during set up and use.....	90
Table 4.7. Summary of physical test findings for each smart toy	94

List of Abbreviations

AES	Advanced Encryption Standard
ANOVA	Analysis of variance
BLE	Bluetooth Low Energy
CoAP	Constrained Application Protocol
DDoS	Distributed denial-of-service
DoS	Denial-of-service
DTLS	Datagram transport layer security
ECDH	Elliptic curve Diffie–Hellman
EU	European Union
FBI	Federal Bureau of Investigation
FPV	First Person View
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
IDS	Intrusion detection systems
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IRK	Identity resolution key
KGC	Key generation centre
LAP	Lower address part
LLN	Low-power and lossy networks
LoWPAN	Low-power wireless personal area network
LTE	Long-Term Evolution
LTK	Long-term key
MAC	Message authentication codes
MITM	Man-in-the-middle
NFC	Near-field communication
NIST	National Institute of Standards and Technology
OPLS	Online Privacy Literacy Scale
OS	Operating systems
OSSTMM	Open Source Security Testing Methodology Manual
OWASP	Open Web Application Security Project

PII	Personally identifiable information
PSK	Pre-shared key
RBAC	Role-based access control
RF	Radio frequency
RFID	Radio frequency identification
SOA	Service oriented architecture
STK	Short term key
TCP	Transmission Control Protocol
TK	Temporary key
TLS	Transport Layer Security
WSN	Wireless sensor networks

Chapter 1: Introduction

1.1 Background and Motivation

Smart toys are a growing phenomenon that bridge physical and online play environments through the use of internet connectivity and a variety of onboard sensors that capture, process, and respond to user input. New technology features found in smart toys such as voice recognition, motion detection, and location awareness enhance the play experience by enabling the toys to be more interactive than traditional toys. Internet connectivity also allows the smart toys to generate and deliver personalised content to create unique play experiences. Many smart toys interact with a dedicated mobile companion application via Wi-Fi or Bluetooth to provide real-time game feedback and download regular new content (Pickering, 2017).

Smart toys are proving popular with consumers and the industry is experiencing explosive growth, with forecasters believing the market will grow by 28% between 2020 and 2025. Fuelling this growth is the continual development of new technologies such as machine learning and artificial intelligence, the use of cloud data processing and storage, and a greater awareness that technology can provide unique learning opportunities (Mordor Intelligence, 2020).

Smart toys are a subset of the greater trend of connecting all consumer devices to the internet coined the Internet of Things (IoT). As such, smart toys currently suffer from many of the same challenges that the IoT faces. Standards and protocols for secure operation are immature, and at times, inconsistent. Additionally, manufacturers face technical challenges when attempting to design and deliver secure IoT consumer products, such as the inability to use traditional security mechanisms due to the resource constraints inherent in smaller, cheaper devices (Lindqvist & Neumann, 2017).

Recent discoveries of privacy and security impacting vulnerabilities in smart toys overseas have resulted in various organisations warning the public to be cautious when using them. One smart toy has been banned from use in Germany due to its covert surveillance abilities (BBC, 2017b), and others have been labelled dangerous due to the ease in which a hacker can take control of the toys to steal data, present objectionable content, or spy on their users (Tung, 2017).

In recent years, smart toy companies have also suffered large-scale data breaches, exposing children's personal information and potentially putting them at risk from crimes such as identity theft (Federal Trade Commission [FTC], 2018). This current situation has led to growing international concern around how smart toys companies use the data these toys collect and whether children's security and privacy is adequately protected.

Whilst there is a large body of research describing the security and privacy issues faced in the general IoT environment, investigations around the security and privacy risks of smart toy use are in their infancy. North America currently dominates the smart toy market; however, the Asia-Pacific region is expected to be the fastest-growing sales region for these products in the next five years (Mordor Intelligence, 2020). Despite this projected growth in the region, no research

has yet been conducted in the New Zealand market to uncover whether the dangers seen in overseas products are found here.

If insecure smart toy products are currently available for purchase by New Zealanders, the security and privacy of New Zealand children may be at risk from attacks such as those seen internationally. These attacks could lead to personal data loss or misuse, denial of access, location stalking, and device hijacking. Determining whether smart toys pose any risk in New Zealand could assist in deciding whether the growing international concern applies to the New Zealand context, and whether any steps need to be taken by either the industry or New Zealand consumers to enhance the safety of these products.

Many smart toys look similar to traditional plush toys and the technology embedded within them is very new. Because of this, many New Zealand parents and guardians may be unaware of the abilities the toys have and any issues surrounding their use. Technology literacy is an important influencing factor of digital safety (Tomczyk, 2019). Therefore, understanding whether New Zealand parents and guardians have sufficient knowledge of the potential risks these products pose and how they can be used safely, could contribute to the limited body of knowledge that exists in this area to date. This understanding could also indicate whether developing training or awareness strategies to combat any risk is necessary.

Personal motivation for investigating this area comes from being a parent to a wildly curious toddler and the inherent protective instinct to keep him safe from harm. Parent coffee group conversations often focus on the somewhat bewildering pace of technological change faced today, whereby two-year-olds instinctively navigate smartphones and demand internet entertainment. Personal observation has led to my suspicion that many parents and guardians are concerned about the welfare of their children in a fully connected world; however, lack the detailed knowledge and tools to fully determine whether their concern is justified, what the risks might be to their children, and how they might prevent them.

Ensuring the security and privacy of smart toys is imperative, as they are used primarily by vulnerable members of our society who must be protected from any future risks the rapidly changing online landscape holds. Therefore, the objective of this research is to investigate various factors that may glean insights into the privacy and security situation of smart toys in New Zealand, and determine whether they pose any risk to New Zealand users.

This study examines how concerned New Zealand parents and guardians are about smart toy privacy and security, and measures the current level of awareness they have around these issues. It also inspects a range of smart toys available for purchase by New Zealand parents and guardians for technical vulnerabilities, and determines whether they pose any security or privacy risks.

The primary research question and supporting sub-questions this study aims to answer are as follows:

Question 1. Do smart toys pose a security or privacy risk to users in New Zealand?

Sub-question 1. What level of privacy and security concern do New Zealand parents and guardians have regarding smart toy use?

Sub-question 2. What level of privacy and security awareness do New Zealand parents and guardians have regarding smart toy use?

Sub-question 3. What common security and privacy impacting vulnerabilities are found in smart toys currently available for purchase by New Zealanders?

Further, a hypothesis to analyse the relationship between smart toy privacy and security levels of concern, and smart toy privacy and security levels of awareness is proposed.

Hypothesis 1. A higher level of participant concern around smart toy privacy and security risks, will correlate to a higher level of participant awareness around these risks.

1.2 Research Approach and Findings

To answer these research questions, two appropriate and effective methodologies were derived and are presented in Chapter 3. Each method focused on deriving empirical data for analysis and review.

Firstly, an anonymous online survey was developed to gain data concerning New Zealand parent's and guardian's level of concern and awareness of smart toy risks. The first section of the survey was designed to identify current levels of concern around the privacy and security risks of smart toys, and the results demonstrated very high levels of concern from all participants around both security and privacy risks.

The survey then measured levels of awareness around smart toy security and privacy using questions in five areas of knowledge, including smart toy technical capabilities, smart toy security and privacy risks, smart toy company data procedures, data protection and privacy law, and personal protection strategies. The results from this section of the survey found that awareness levels overall were low.

Secondly, several smart toys were physically evaluated to determine if they used sufficient security and privacy controls to mitigate any common risks. A repeatable security testing methodology was used to investigate three potential technical areas of vulnerability in the toys, including insufficient authentication, insecure transport, and insufficient privacy protection. The research proved that vulnerabilities in each of these areas could be found in smart toys available for purchase by New Zealanders.

1.3 Thesis Structure

The thesis consists of six chapters. This chapter introduced the thesis topic and provided some background information on the origin of the topic and the current state of research in this area. The motivation for conducting this study was outlined and the importance of this research was

emphasised. The chapter then presented the methodology used in this study and the high-level findings obtained.

Chapter 2 provides a literature review covering four main areas: the IoT, IoT security, smart toy security and privacy, and user awareness and risk. This chapter begins by outlining the evolving IoT, including new technologies being developed for use within the IoT and the various architectural models proposed to describe the environment.

A review of security within the IoT then highlights that traditional security aims such as confidentiality, integrity, and availability are still primary concerns; however, there are many new challenges identified that make satisfying these goals difficult. Areas of challenge identified in the literature and elaborated on include heterogeneity, trust management, resource constraints, encryption, authentication and access control, device management, scale, and standardisation. Smart toy security and privacy research studies that outline recent security incidents, including data breaches and the discovery of specific smart toy vulnerabilities, highlight the current risks in this space. Literature is presented that describes both the security and privacy challenges faced by smart toy manufacturers and the progressive technology proposed to address those challenges.

Chapter 2 concludes with a review of various literature that relates user awareness to levels of technology risk. The literature review revealed gaps in the current body of knowledge, including a lack of New Zealand focused investigation and a limited array of studies specifically targeting smart toys.

Chapter 3 identifies the main research question and sub-questions this study aims to answer to address the gaps in the current body of knowledge. This chapter then describes the two approaches selected for this research and the process of derivation from similar studies and relevant industry methodologies.

Chapter 4 presents the findings obtained from executing both research methods. Firstly, the results from the online survey conducted are described, starting with demographic findings and followed by the findings around participant level of concern and participant level of awareness of smart toy security and privacy issues. This is followed by the findings from the physical testing of a selection of smart toys. The findings in each of the three areas of vulnerability tested are presented.

Chapter 5 analyses the findings from Chapter 4 and relates them to the main issues described in the literature review to answer the research questions posed by this study. This chapter also describes the implications of the findings, along with recommendations for improving the security and privacy of the smart toy environment.

Chapter 6 concludes by summarising the findings and providing an overview of possible future research areas, which, if undertaken, could further advance the overall knowledge of smart toy security and privacy.

Chapter 2: Literature Review

2.1 Introduction

Many recent studies highlight the importance of understanding the impact that the pervasive connectivity of the IoT has on our daily lives (Kliarsky, 2017; Rivas, 2017). Smart toy use is one aspect of the IoT where this impact, particularly in the areas of security and privacy, becomes especially important to understand, as smart toys are primarily used by children who may not have the ability to protect themselves in this environment (Tang & Hung, 2017).

This chapter reviews the relevant literature available on smart toys and the broader IoT environment they operate within. The objectives of this review are to outline the current understanding of smart toy privacy and security, and identify any gaps in the existing body of knowledge that warrant investigation. The critical issues faced in providing a secure and private experience for smart toy users which led to the formation of the main research questions for this thesis are also presented.

The review consists of five main sections. Section 2.2 discusses the general IoT environment focusing on current literature that describes the architecture of the IoT and outlines the new technologies found in this environment. Section 2.3 discusses the security goals and the challenges seen when attempting to secure devices in the IoT, and also includes literature that investigates the smart home environment where IoT consumer products such as smart toys are found.

Section 2.4 focuses specifically on research pertaining to smart toys. This section describes the current understanding of these products, relevant security incidents faced by the smart toy industry, and the known privacy and security challenges apparent in smart toys. Recent research into possible solutions to the challenges faced in this area is then discussed.

Section 2.5 considers literature relating to user awareness and technology risk, and finally, Section 2.5 concludes the literature review.

2.2 The IoT

2.2.1 Overview

Due to its relative infancy and broad scope, no single agreed definition exists for the IoT. Misra, Maheswaran, and Hashmi (2017) chose to define it as “a paradigm that considers pervasive presence in the environment of various things, that through wireless and wired connections are able to interact and cooperate with other connected things to create seamless communication and contextual services, and reach common goals” (p. 6). The Oxford Dictionary, however, defines it more simply as “the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data” (“Internet of Things”, 2019). Bassi, Europe, and Horn (2008) describe it as “a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols” (p.6). However, current literature highlights that the use of standard protocols remains a challenge today (Laplante, Voas, &

Laplante, 2016; Nguyen, Laurent, & Oualha, 2015; Raza, Seitz, Sitenkov, & Selander, 2016). Despite the number and varied content of IoT definitions, the definitions generally include the idea of diverse systems—devices or “things” interoperating, and the concept of connecting and communicating with other available devices within range.

The things that make up the IoT can be divided into four categories. The first comprises personal computers, servers, switches, routers, and other traditional information technology equipment. The second comprises of supervisory control and data acquisition systems, medical machinery, and other operational technology. The third includes smartphones and tablets, and the fourth contains single-use consumer devices such as fridges, automobiles, and toys (Stout & Urias, 2016). The devices in each category may have sensors that monitor and collect numerous types of data from their environments, and connect and communicate with each other and the internet at any time (Alaba, Othman, Hashem, & Alotaibi, 2017).

For businesses, there are vast benefits of adopting IoT technology, such as improved performance, enhanced customer experience, and accelerated growth. IoT devices can aid companies in reducing risk by enabling new ways of working, such as protecting inventory and equipment in large and remote areas using combined technologies such as radio frequency identification (RFID) and wireless sensor networks. IoT technology is already implemented in a wide variety of industries such as transport, health, agriculture, and infrastructure, and it is estimated that businesses which extensively implement IoT technology will be 10% more profitable by 2025 compared to those who do not (Tankard, 2015).

For the consumer, the IoT allows daily life to become more connected with consumer goods such as home appliances, wearables, toys, physical locks, and video surveillance. These consumer goods are distinguished by their ability to communicate through the internet via smartphones and other mobile devices. Example benefits of this smart connectivity include connected medical devices allowing at-risk patients to more effectively manage their health, and smart energy meters in the home allowing consumers to be more energy conscious (FTC, 2015).

IoT development has been fuelled by technical innovation in areas such as wireless sensors and nanotechnology-based architectures. Many researchers anticipate explosive growth in the IoT and point to research by Gartner, who predicts that the number of connected devices will reach 50 billion by 2020 (Gartner, 2013). This predicted growth will lead to IoT architectures handling the interactions of billions of objects, and as attacks against IoT devices and systems may be responsible for more than 25% of the total identified enterprise attacks, each of these interactions will need to be secure (Roman, Zhou, & Lopez, 2013).

The vast and varied application of the IoT is driving more pervasive connectivity and opening our daily lives to potential new threats. Many common and previously simple devices now contain computing capability, and are used by consumers who may have little knowledge around the risks these new functionalities can bring into their home environments (Rivas, 2017). This new threat exposure, combined with the predicted explosive growth, increases the importance of understanding the inherent threats and risks of the IoT (Kliarsky, 2017).

The FTC identifies three potential security risks to consumers from the use of the IoT: the unauthorised access and misuse of personal information, the facilitation of attacks on other systems, and risks to personal safety. Connected devices may collect, store, and transmit vast amounts of personal data, and as highlighted by the FTC, the IoT generates potential privacy risks from the long-term collection of personal data such as an individual's habits, health, financial account numbers, and geolocation. Data collection is of concern if the data is then misused in future decision-making processes such as in employment, insurance, or finance suitability (FTC, 2015).

The risk of a compromised IoT device facilitating attacks on other systems is now also a reality, and a new area of literature has started investigating the use of IoT devices in botnets. Kambourakis, Kolias, and Stavrou (2017) describe how poorly protected IoT devices have become "low hanging fruit" for hackers who harness their large numbers to conduct powerful denial-of-service (DoS) attacks, spam, and fraud. They reviewed the success of using IoT devices in botnets by focusing on a recent attack called "Mirai", which managed to take remote control of half a million IoT devices and disable hundreds of high-profile websites such as Twitter and Netflix for hours. Their research uncovers why the IoT provides such a fertile ground for hackers; however, does not talk in detail about solutions. Bertino and Islam (2017) take this discussion one step further by exploring solutions, and conclude that preventing botnet infections through techniques such as antivirus software, intrusion prevention systems, and firewalls is the best defence. Both researchers agree, however, that this is challenging in a world of poorly configured IoT devices and that threats will only increase in complexity over time.

Security of the IoT is also heavily related to the safety of the individual. Interference in an IoT network, whether malicious or not, can cause serious harm by interrupting the operation of devices such as pacemakers and cars. In the home, data shared between smart devices may contain information relevant to a user's safety—such as whether their front door is locked. When unprotected, devices such as televisions, cameras, and baby monitors can send data such as captured audio and video streams over the internet and threaten user safety. Therefore, securing these devices and the confidentiality of this data is paramount (Rivas, 2017).

The problems with IoT device security have been demonstrated by many researchers. In one IoT study by Hewlett Packard, 70% of the devices tested by Hewlett Packard were found to be "vulnerable to attack" (Hewlett Packard Enterprise, 2014) and many consumer goods have also been found to be susceptible. Research has shown that implantable medical devices such as pacemakers and insulin pumps can be remotely hacked and tampered with (Tankard, 2015), and successful attacks have also been conducted against numerous IoT consumer devices including the My Friend Cayla doll, LG refrigerator, Nest, Belkin Smart Plug, smart light bulbs and smart televisions (Stout & Urias, 2016).

However, securing these devices can be challenging, as many IoT devices have power, memory, computation, and storage constraints that make traditional security mechanisms unsuitable. The countermeasures used against cyberthreats today may be ineffective or inefficient for the IoT because of the limited available computing power, many interconnected

devices, and varied communication protocols and hardware being used (Rivas, 2017). New solutions are required to resolve the inherent security and privacy challenges the IoT faces. However, IoT research remains in its infancy. No standards for secure design or implementation are universally agreed, and many proposed solutions to the challenges faced by a rapidly expanding IoT are still untested (Liu, Yang, Zhang, & Chen, 2015).

2.2.2 IoT Architecture

As yet, there is no single established and agreed IoT reference architecture. Various researchers and organisations have proposed models, with the simplest and most commonly referenced being the three-layered model as shown in Figure 2.1 (Alaba et al., 2017; Pallavi & Smruti, 2017; Radovan, Golub, & Daimler, 2017; Stout & Urias, 2016).

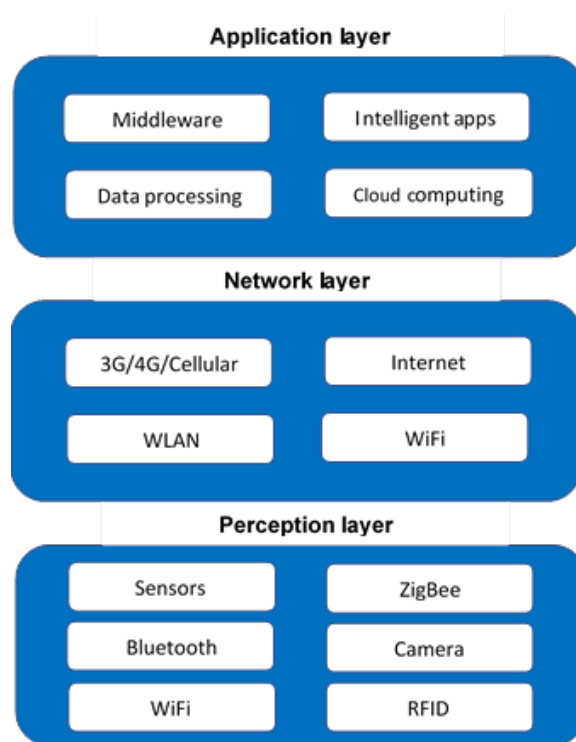


Figure 2.1. IoT architectural layers. Adapted from “Review: Internet of Things security: A survey”, by F. A. Alaba, M. Othman, I. T. Hashem, & F. Alobaiti, 2017, *Journal of Network and Computer Applications*, 88, pp.10–28. Copyright (2017) by Elsevier. Adapted with permission from Elsevier.

The three-layered model may be described as follows:

The perception layer includes devices or things that capture information including dynamic data from the surrounding environment. As the devices at this level are vulnerable to a variety of attacks, the physical protection of any device, as well as authentication and data provenance, are security considerations. For example, sensor nodes suffer from DoS, jamming, and Sybil attacks. Radio frequency identification tags are vulnerable to DoS, repudiation, eavesdropping, counterfeiting, and spoofing attacks. ZigBee is susceptible to packet manipulation, hacking, Killer Bee and key exchange vulnerabilities; and Bluetooth suffers from threats such as DoS, bluesnarfing, bluejacking, and eavesdropping. This layer is most often connected to the network layer via wireless technology (Alaba et al., 2017).

The network layer performs data transmission and includes functions such as device addressing, packet forwarding, and routing and security protocols. It also acts as the communication layer between devices in the perception layer and any cloud storage. Attacks at this level may include man-in-the-middle (MITM), DoS, or distributed denial-of-service (DDoS) attacks, traditional network security threats, counterfeiting, and IPv6 application vulnerabilities. Security at this layer consists of a wide variety of rapidly evolving standards and technologies (Radovan et al., 2017).

The application layer involves data analysis, processing, and presentation. These activities may occur in locations such as in the cloud or on a smartphone application. Security considerations at this level include authentication challenges, access control, and information disclosure (Stout & Urias, 2016).

Whilst the most commonly used model, the three-layered architecture is criticised for its simplicity. Researchers such as Sethi and Sarangi (2017) believe this model is not detailed enough to base IoT research on, and suggest alternatives such as a five-tier architecture. A five-tier architecture contains the three standard layers seen above, and adds a layer for processing that encompasses middleware and a layer for the business that encompasses management functions. A five-tier architecture is also supported by Shahid and Aneja (2017); however, in this case, the network layer is called the data exchange layer and performs data transmission, and a fourth layer called the information integration layer purports to clean and transform the data collected for use by the application layer.

Another architectural model that utilises five layers is service oriented architecture (SOA). As software developers are moving towards using service oriented programming for the interaction of heterogeneous devices, an effective SOA method for the IoT is being explored in the literature. Kumar, Mouli, and Kumar (2017) conducted a survey on research papers that utilised some form of SOA architecture in the IoT, and determined that while most examples provided better efficiency of service, they all lacked robust security features. This is likely due to the high resource consumption that security services demand and that IoT devices lack. This research did not propose a solution for the resolution of this issue and remains an open and active area of research.

Another recent trend is to describe the IoT in terms of a fog or edge architecture. Proponents of this type of architecture believe the traditional view does not support the unique volume and connectivity needs of the IoT, and an edge model that supports more pre-processing of data in edge devices is necessary (Green, 2004). Whilst a distributed architecture such as the fog model allows IoT applications to have greater response times and a higher quality of service, challenges remain with its implementation, particularly in the area of resource management amongst the nodes or devices (Lin et al., 2017). Security and privacy issues are also still a significant challenge in the fog or edge IoT environment. Lin et al. (2017) created a comprehensive survey of these security challenges, and described threats and identifying possible mitigations at each architectural layer; however, the difficulties with deploying the suggested security mechanisms into the complex IoT environment were not discussed.

Ray (2016) conducted a survey attempting to consolidate recent research focused on various IoT-oriented architectures, and concluded there was a diverse array of domain-centric architectures proposed. Ray (2006) also found that these architectures are in danger of becoming silos, which will prevent the overarching goal of interoperability which is key to the success of the IoT moving forward. By categorising the research in domains, Ray (2006) naturally highlighted the differences in the proposed models, but did not discuss the potential areas of interoperability, which if conducted, may have offered different insights. In response to a similar concern that vertical and isolated solutions have emerged in the IoT architectural space, The European Lighthouse Integrated Project (IoT-A) developed an IoT reference model, architecture, and set of fundamental building blocks intended to lay the foundation for a ubiquitous IoT (Bauer et al., 2013). Whilst heralded a success by its supporters, the numerous versions of IoT architectures still being proposed and described in literature today demonstrate the wide-ranging scope of the IoT concept. This makes defining a single reference architectural model challenging, and suggests that there is still some way to go before the idea of a standard description is accepted.

2.2.3 IoT Technologies

The IoT is powered by a wide range of technologies that must work collaboratively across varied environments which are often geographically diverse, prompting the importance of robust, secure, and reliable communication.

Communication technologies used within the IoT include well-known technologies such as wireless fidelity (Wi-Fi), Long-Term Evolution (LTE), and second, third, and fourth generation (2G/3G/4G) cellular technology. Applications that require high data rate transfer over long ranges can use these existing standard networks; however, this covers little of the IoT environment. More commonly, IoT networks differ from traditional networks, in that IoT devices are deployed on low-power and lossy networks (LLN) which have constraints such as low processing power, energy, and memory. This means that satisfying security and privacy requirements in the IoT environment requires the development of new protocols and standards to manage the unique challenges (Radovan et al., 2017).

IoT devices generally communicate using either a radio frequency (RF) signal or via an internet gateway, and can connect to the internet either through the Internet Protocol (IP) stack or via non-IP communication channels; however, each method has challenges to overcome. The traditional IP stack is complex and resource-hungry which does not suit most IoT devices. Non-IP communication channels such as Bluetooth, RFID, and near-field communication (NFC) are limited in their range. All RF protocols are also vulnerable to signal interception (Alaba et al., 2017). These challenges have prompted researchers to modify, adapt, and develop new protocols for secure communication, and some of the leading technologies now used in the IoT and the challenges they face are outlined next.

2.2.3.1 IEEE 802.15.4

Various protocols are currently used in the IoT environment to obtain communication security, and at the physical layer, many WSNs use IEEE 802.15.4. Created by the Institute of Electrical and Electronics Engineers (IEEE) and maintained by the IEEE 802.15 working group, IEEE 802.15.4 is a technical standard for low-rate wireless personal area networks that provide security services such as data confidentiality, data authenticity, and protection against replay. However, threats against this protocol exist, such as unencrypted ACK frames, NULL security, and no timed frame counters (Alaba et al., 2017).

2.2.3.2 ZigBee

ZigBee is a protocol that is based on the IEEE 802.15.4 standard. It is robust, highly secure, scalable, and works at 2.4GHz requiring low data rates of 250Kbps within a 100m range.

It satisfies the low-power RF communication requirements of IoT devices using a wireless mesh technology, but is only suitable for short-term communication (Radovan et al., 2017).

2.2.3.3 Z-Wave

Z-Wave is similar to ZigBee in that it supports short-term communication at low cost and with low energy and reliability. While it is a simpler architecture to implement than ZigBee, it is severely limited in the number of nodes it can include in the network (Lin et al., 2017).

2.2.3.4 6LoWPAN

6LoWPan refers to IPv6 low-power wireless personal area networks. Designed by the Internet Engineering Task Force (IETF), it can use multiple frequency bands across multiple platforms and allows almost every connected device to have a unique IP address. It is an IP which allows small devices with limited processing power (such as those commonly found in the IoT), the ability to transmit wirelessly, and its advantages include easier connectivity with legacy architectures, low-power needs, and ad-hoc self-organisation. 6LoWPAN networks must connect to the internet via a gateway containing protocol translation support between IPv4 and IPv6 to communicate with all other IP-based devices on the internet (Radovan et al., 2017).

2.2.3.5 Datagram transport layer security (DTLS)

Transport Layer Security (TLS) protocol is the recommended choice in many IETF security standards to provide communications security over a network; however, it is not suitable for resource-constrained environments that do not operate over Transmission Control Protocol (TCP) such as the IoT. DTLS, which is an implementation of TLS over UDP, has been proposed as its replacement for these circumstances, and has now been widely adopted in the IoT (Nguyen et al., 2015). Challenges arise, however, when using DTLS in an IoT network, as DTLS requires the key establishment process to succeed which is usually achieved via the use of X.509 certificates and a public key infrastructure. Unfortunately, many IoT devices are too resource-constrained to support this key establishment method, leaving only non-scalable

options such as the use of pre-shared keys, which is unmanageable in many vast IoT implementations (Raza et al., 2016).

2.2.3.6 Constrained Application Protocol (CoAP)

In the application layer of an IoT environment, CoAP is used as the messaging protocol for communication rather than HTTP (Hypertext Transport Protocol) as HTTP is too complicated. Constrained Application Protocol modifies some HTTP functions to enable IoT device interaction but relies upon DTLS for its security. Therefore, a secure implementation is dependent on resolving any DTLS issues (Sethi & Sarangi, 2017).

2.2.3.7 Bluetooth Low Energy

Bluetooth Low Energy (BLE) originated in the Bluetooth version 4.0 core specification and was designed especially for small chunks of data. Working at 2.4GHz, it conserves energy by using small bursts of RF communication within a range of 50–150 metres at 1Mbps. Bluetooth Low Energy technology uses adaptive frequency hopping technology, enabling it to transmit reliably even in ‘noisy’ RF environments such as those found in the home and industrial settings (Townsend, Akiba, & Davidson, 2014).

After recognising that initial (now referred to as legacy) BLE standards had security concerns, subsequent versions such as Bluetooth 4.2 introduced new security models including BLE Secure Connection Only mode. Bluetooth Low Energy Secure Connection Only mode uses a Federal Information Processing Standard (FIPS)-compliant elliptic-curve Diffie–Hellman (ECDH) algorithm for key generation and a new pairing procedure for key exchange (Townsend et al., 2014).

Whilst ideal for IoT devices that have severe resource constraints, Kliarsky (2017) highlights that when trying to implement security mechanisms such as intrusion detection in an IoT network, using new RF communication protocols such as BLE can present additional challenges as they often require specialised tools that are still developing and immature.

2.2.3.8 Wireless Sensor Networks

Wireless sensor networks (WSN) are groups of independent nodes that communicate wirelessly over limited bandwidth and frequency, and the IoT often integrates them with RFID in systems such as food tracking and healthcare (El Mouaatamid, Lahmer, & Belkasmi, 2016). Whilst a key component in the IoT environment, there are numerous known challenges when trying to secure WSNs. For example, along with being susceptible to standard wireless security attacks, they are additionally unable to deal with traditional cryptographic mechanisms due to severe resource constraints, including low processing power and limited memory. Sharma, Bala, and Verma (2012) presented an overview of proposed cryptographic schemes for use in WSNs, and described and compared known symmetric, asymmetric, and hybrid models. No single method was suggested as ideal, and applying the appropriate method for each network remains a challenge.

2.2.3.9 *Radio Frequency Identification*

Radio frequency identification allows data to be stored and retrieved remotely using tags or transponders and readers or transceivers. Tags attached to IoT objects hold data that a reader then gathers via two-way radio transmission, enabling the tracking of individual objects. Used as a contactless method for identifying and tracking objects in the IoT, it has benefits such as small size, low cost, and durability; however, is only applicable for short-range use as it supports data transfer via radio signals (Lin et al., 2017).

2.2.3.10 *Near-Field Communication*

Near-field communication is a short-range wireless communication technology based on RFID and allows two NFC-enabled devices to transfer data over a minimal distance. Often used in smartphones, it allows two-way communication and can be used to secure transactions such as payments. As proximity is a requirement for data transfer, it is limited in its application (Sethi & Sarangi, 2017).

2.2.3.11 *Wi-Fi HaLow (IEEE 802.11ah) and IEEE 802.11ax*

Based on the IEEE 802.11ah standard, Wi-Fi HaLow is a relatively new low-power variant of Wi-Fi that has the advantage of not only consuming less power, but also operating over a greater range than traditional Wi-Fi making it suitable for the IoT. Operating in the 900Mhz frequency means it is slower than traditional Wi-Fi, but can penetrate objects that block 2.4GHz and 5GHz. This makes it useful in IoT scenarios where devices are beyond traditional Wi-Fi reach. Wi-Fi HaLow, however, is still subject to interference and uptake has been slow in the IoT world. This slow uptake is due to the need for special access points and many countries not assigning it a spectrum. IEEE 802.11ax is even newer and may become more popular as it delivers some of the same benefits as Wi-Fi HaLow such as low-power and complexity. IEEE 802.11ax does not require unique access points as it still operates on standard Wi-Fi frequencies. However, it does not have as long a range, and it remains to be seen which technology proves more popular long-term (Chasker, 2017).

2.3 Securing the IoT

There is an abundance of literature discussing security in the IoT. Many authors agree that as with traditional information technology security, security in the IoT may be defined as the provision of various basic security services including confidentiality, integrity, authentication, non-repudiation, authorisation, availability, and privacy (El Mouaatamid et al., 2016; Misra et al., 2017; Radovan et al., 2017).

Confidentiality ensures that data can only be accessed and understood by authorised users while in transmission or at rest. Man-in-the-middle attacks seek to breach confidentiality by capturing, transmitting, and sometimes altering data transmitted between legitimate network devices. The wireless communication channels of many IoT networks are vulnerable to this kind of attack. Encryption techniques may assist in hindering MITM attacks by protecting parts of the

data stream; however, implementing traditional encryption in an IoT environment can be challenging (El Mouaatamid et al., 2016).

Integrity assures that system and information resources are accurate, consistent, and trustworthy over their lifecycle and that data cannot be accessed, modified, or changed in transit or at rest by unauthorised entities (Misra et al., 2017). Attacks against data integrity are increasing in the IoT environment and can include message alteration and fabrication. The use of hash functions and digital signatures are one line of defence against this kind of attack (Yaqoob et al., 2017).

Authentication services ensure that data, communications, and transactions are genuine and that all parties are whom they claim to be. Authentication controls are essential in the IoT environment, as weak or no authentication can allow unauthorised access to data and possibly allow a malicious attacker to change or alter a device function and endanger individual safety. Attacks against authentication in the IoT include impersonation where an attacker pretends to be an authorised user, and the Sybil attack where an attacker may use many different identities simultaneously (Misra et al., 2017).

Non-repudiation is strongly linked to authentication and identity management, and seeks to prove an entity's participation in a specific data exchange and allow traceability of unique actions. Traditional non-repudiation techniques include the use of digital certificates with a certificate authority. A lack of non-repudiation controls and strong auditing functions can allow the malicious manipulation of actions or data in the system (El Mouaatamid et al., 2016).

Authorisation is the process of allowing someone to do or have something and ensures that entities can only perform functions that they are authorised to do. Insufficient authorisation can include a lack of role-based access controls which may lead to data loss, theft, or corruption (Open Web Application Security Project [OWASP], 2014a).

Availability aims to ensure that data and resources are always available to authorised users. Attacks against availability in the IoT include traditional attacks such as DoS, DDoS, buffer overflow and flood attacks. Jamming attacks, where a communication channel is blocked by introducing noise are also a significant threat to IoT networks. IoT networks often consist of small nodes with limited resources that prevent the use of traditional anti-jamming methods (El Mouaatamid et al., 2016).

Privacy is similar to confidentiality, in that the aim is to ensure private information is not leaked or stolen, but also includes the concepts of data inference and unauthorised use of data. Privacy is of great concern in the IoT environment, and a threat to privacy may involve the exposure of sensitive data to unauthorised entities or the inference of personal information from the gathering of data over time (Misra et al., 2017). As many IoT devices communicate primarily via a wireless connection to the internet, they are vulnerable to attacks against privacy such as eavesdropping, skimming, replay, and traffic analysis (Yaqoob et al., 2017).

2.3.1 Unique Challenges to Privacy and Security in the IoT Environment

Recognised as currently one of the most important advancements in the information technology arena, the new technology and paradigm of the IoT brings a set of unique challenges for addressing network security and privacy. Characteristics such as its heterogeneity, resource constraints, scale, and environment, along with the challenges of privacy, standardisation, and user awareness are discussed in the following sections.

2.3.1.1 *Heterogeneity*

A vital benefit of the IoT is its versatility and applicability in a wide range of environments. This versatility is due in large part to IoT systems containing a wide range of heterogeneous devices and technologies, and often an IoT network will contain a combination of both low resource devices and very powerful devices. For example, in a smart home, power usage sensors that can only conduct simple actions may connect and communicate with smart TVs that perform complicated computations (Sha, Wei, Yang, Wang, & Shi, 2018).

The heterogenic nature of the IoT means that a wide range of operating systems (OS) and communication technologies must interoperate making traditional security solutions often inapplicable. Many resource-constrained devices cannot use traditional IP-based security solutions such as IPsec, SSL, and SSH, and solutions that may work for one OS such as Android, may not work for Windows-based devices in the same network. This diversity leads to differing levels of security throughout the IoT, and the least secure device determining the overall network security (Sha et al., 2018).

2.3.1.2 *Trust Management*

An area made additionally challenging due to the heterogenic nature of the IoT is that of trust management. The concept of trust is an idea that combines aspects such as confidence, dependability, reliability, and integrity of an entity, and the management of trust is essential in any network to promote user acceptance (Yan, Zhang, & Vasilakos, 2014). Whilst required for interoperability, establishing trust is challenging in the IoT environment, where many heterogeneous networks connect via the internet and interaction occurs between devices with differing security standards and trust criteria (Yaqoob et al., 2017).

In addition to the characteristic of heterogeneity, managing trust is complicated in the IoT by factors such as the high mobility of devices, identity challenges, and temporary relationships formed between devices. Peer-to-peer or ad-hoc networks typically struggle with the issue of trust and are also commonly used in the IoT, and therefore this challenge is inherited (Sha et al., 2018).

The importance of trust management in the IoT is recognised within the literature. Yan et al. (2014) surveyed over 35 articles discussing trust management in the IoT and proposed a set of trust management goals including reliable data collection, user privacy protection, system security, data communication and transmission trust, and identity trust. They also proposed a research framework for further work. Sha et al. (2018) highlighted an end-to-end security

architecture that supports trust management in the IoT by utilising new protocols such as 6LoWPAN to allow end devices to manage security. Sato, Kanai, Tanimoto, and Kobayashi (2016) additionally suggested managing trust in an “area”, rather than establishing trust for an individual device. An area could contain the devices, the network that connects them, and the control and data service clouds.

Each of the authors cited describe unique ways to approach trust management in the IoT; however, each system still poses open challenges that need resolving before widespread use in the IoT landscape is possible. As highlighted by Sicari, Rizzardi, Grieco, and Coen-Porisini (2015), judging the success of the proposed methods is also difficult, as many approaches to trust management, including those mentioned, do not include evaluation methodologies or metrics.

2.3.1.3 Resource Constraints

To achieve speed to market and low cost, many IoT devices are built with extremely limited capabilities and contain constraints such as low computational ability, limited power, and restricted memory. As traditional security solutions often cannot work within these constraints, the range of available security mechanisms for use in the IoT is narrower than that of a traditional network (Sha et al., 2018). These device constraints create specific challenges in the IoT in areas such as encryption, key distribution and management; authentication and access control; and device management. These constraints are discussed in the following sections.

2.3.1.4 Encryption and Key Distribution/Management Challenges

Encryption is essential to securing the confidentiality of most wireless communications; however, many IoT devices are unable to utilise existing secure encryption protocols and standards as the devices are not powerful enough. Most IoT devices cannot use traditional asymmetric encryption algorithms due to their limited computational capabilities, and many others such as basic sensors cannot even support symmetric algorithms such as Advanced Encryption Standard (AES) or Data Encryption Standard (Misra et al., 2017). The IoT requires encryption mechanisms that are less resource-intensive and faster, but which offer the same level of security as traditional trusted methods. However, research to develop secure, lightweight encryption, decryption, and digital signature schemes is seen to be in its infancy (Yaqoob et al., 2017).

Most lightweight cryptographic solutions are based on symmetric-key cryptography, and require the sharing of symmetric keys to all devices which is troublesome to implement. Nguyen et al. (2015) studied various key pre-distribution schemes required for using symmetric cryptography in the IoT, and concluded that whilst they require low computational complexity, they have many disadvantages including low scalability, vulnerability against node attacks, and high communication complexity. Attempting to solve some of these challenges, Raza et al. (2016) proposed a key management architecture using symmetric keys called Scalable Security with Symmetric Keys (S3K), that enables the use of DTLS with either pre-shared symmetric keys or raw public keys established during the DTLS handshake. Scalable Security with Symmetric Keys

promises flexibility and scalable key establishment in a resource-constrained environment, but is still in the proof of concept phase.

An alternative to symmetric cryptography is public key cryptography. However, not all smart devices have public keys that come with a digital certificate for authenticity, and asymmetric key schemes generally require a lot of computational capability and energy. Key distribution and management are also challenging, as traditional schemes such as the Diffie–Hellman algorithm and the use of a trusted certificate authority rely upon resource-hungry asymmetric algorithms. This leads to IoT devices using pre-shared key mode (PSK) or raw public key mode, which both require the pre-provisioning of keys on each object making them unscalable models that are not ideal for the IoT (Yaqoob et al., 2017).

Despite the challenges of using asymmetric mechanisms, there is still research being conducted to make them applicable to the IoT environment, and if successful, they could offer scalability, high resilience against node capture, and require low memory resources. Salami, Baek, Salah, and Damiani (2016) believe elliptic curve cryptography could provide a solution to the implementation of asymmetric cryptography in the IoT, as it has small key sizes and requires limited computational and memory resources. They proposed a lightweight encryption scheme based on identity that also requires no public certificates which goes some way towards resolving key management challenges; however, remains theoretical at this stage. Identity-based cryptography schemes such as this, whereby the key is kept in escrow by a key generation centre (KGC), have also been shown to be prone to key-escrow attacks which can compromise the KGC and impersonate an authorised user (Nguyen et al., 2015).

Finally, attempts to secure data at rest or in transit by using traditional protocol-based encryption mechanisms may be insufficient to protect the IoT where end-points are susceptible to modification. Additionally, numerous older or substandard IoT devices still lack any encryption capabilities at all, despite standards bodies starting to require this for interoperability (Stout & Urias, 2016).

2.3.1.5 Authentication, Access Control and Intrusion Detection

When verifying IoT data, the identity of the sending device and the integrity of the data must be sound; however, authentication mechanisms are often limited by the resource constraints of the devices. Often IoT devices do not support strong authentication standards such as 802.1X (Liu, 2015), and most IoT devices can only handle symmetric based authentication at best—ruling out secure traditional authentication mechanisms such as digital signature-based schemes. The use of Kerberos, a network authentication protocol utilised by Microsoft Windows, is also not suitable for most IoT environments as it works on IP-based protocols and does not scale easily to suit the vast scope of IoT networks (Sha et al., 2018).

Alrababah, Al-Shammari, and Alsuh (2017) surveyed available lightweight authentication protocols that are suitable for use in the IoT, finding that most protect against attacks such as masquerading, replay, and forgery by using techniques such as message authentication codes (MAC) hashes, timestamps, or asymmetric encryption. No single technique discussed can be

applied to all circumstances, and many of the stronger methods surveyed are unsuitable for the most resource-constrained networks. This suggests that brand new standardised solutions are still required.

The resource constraints of IoT devices also means that using security mechanisms such as access control and intrusion detection systems is challenging, as these solutions often require more computational power than is available. In the IoT environment, information such as the granularity of access and the location of the requester becomes essential to include in access control policies; however, the significant resource constraints of the devices prohibit the use of a complex access control mechanism (Roman et al., 2013). Traditional solutions such as role-based access control (RBAC) protocols require vast policy libraries that cannot be stored in the memory of IoT devices. Gusmeroli, Piccione, and Rotondi (2013) describe that both attribute-based access controls and RBAC mechanisms are ineffective for the scale of the IoT, are not suitable for a consumer scenario, and struggle to satisfy the critical principle of least privilege. Building on earlier research, they proposed a capability-based access control system that uses a “capability” or token of authority, that when held by a process, grants the ability to interact in specific ways. This system is more suitable for a consumer environment; however, it still relies upon X.509 certificates which limits its use to IoT devices powerful enough to handle RSA encryption. This solution would need extending to use alternative standards such as elliptical curve cryptography (ECC) if it was to be suitable for the entire IoT environment.

In the IoT, intrusion detection may be required in a traditional IP network or a low-power wireless personal area network (LoWPAN). In a traditional TCP/IP environment, there are many resources available for intrusion detection systems (IDS); however, deploying IDS in the IoT is often constrained by RF limitations and distance (Alaba et al., 2017). The LoWPAN RF communication protocols found in the IoT such as BLE can also require specialised tools that are still developing and are immature. For example, in a survey of 18 intrusion detection research papers, Zarpelão, Miani, Kawakani, and de Alvarenga (2017) found that most papers proposed new IoT IDS solutions for 6LoWPANs; however, solutions have not yet been explored for other IoT technologies such as BLE or Z-Wave leaving a significant gap.

2.3.1.6 Device Management

Traditional computing devices and networks have rich interfaces to manage them. However, IoT devices often do not have the ability for rich (if any) user interaction due to their inherent resource constraints and design features. Many do not have any space for a keyboard or screen, and these limitations can make the configuration of devices difficult. In the consumer market, additional challenges can arise as a result of these limitations when attempting to provide consumers with information and choice around data collection, security, and privacy policies (FTC, 2015).

Solutions such as using voice to input data where traditional mechanisms such as keyboards are impossible have been proposed in the literature, and voice control technologies are becoming a new normal in some IoT consumer goods. However, in response to strong concerns

around the use of captured voice data from smart devices, California recently introduced a statute regulating the collection and use of voice data from smart televisions. The introduction of this regulation suggests that there are still many privacy concerns and risks with devices that record and process voice conversations, and using this solution would bring another set of challenges that are yet to be overcome (Silvestro & Black, 2016).

Other suggestions made by the FTC include introducing privacy options and configuration choices at the point of sale or affixing Quick Response codes on devices. However, these solutions are limited in their applicability, and it is acknowledged that giving end-users easily configurable privacy and security settings may be impossible for all IoT devices (FTC, 2015). One additional new solution to this problem without having to replace or upgrade the capability of legacy IoT devices uses Blockchain Connected Gateways as mediators between the IoT device and the user. This research, while promising, does not appear to have been tested in a commercial setting (Cha, Tsai, Peng, Huang, & Hsu, 2017).

The resource constraints inherent in many IoT devices also mean they are often impossible to update, and applying security patches to any discovered vulnerability is impossible. Other IoT devices circumvent this constraint by allowing automatic updates to occur remotely over the internet, but this is not ideal, as communication channels may be insecure and end-users may be unaware of the activity (Lindqvist & Neumann, 2017). The lack of secure update mechanisms and rich user interfaces to manage devices means that satisfying privacy and security requirements remains an ongoing issue for the IoT.

2.3.1.7 Scale and Environment

The large scale of the IoT also contributes to the unique security challenges it faces. Interaction between billions of devices can increase the cost of any security deployment, and many connected devices increase the available attack surface. One compromised device can open the door for a malicious intruder into an entire network (Sha et al., 2018).

Physical protection of devices also becomes more challenging in the IoT construct due to the large number and distributed nature of these devices. Risk of unauthorised access via an available USB port is higher than in some traditional networks, as many IoT devices reside in public areas (Yaqoob et al., 2017).

Additionally, consumer IoT devices are often located in personal living spaces such as bedrooms, bathrooms, cars, and even attached to the human body. This uniquely personal environment brings security and privacy risks to the foreground of the discussion.

2.3.1.8 Privacy

The vast amount of personal data being collected by IoT devices in all aspects of our lives has introduced unique privacy risks. Research by Sha, Alatrash, and Wang (2017), found that IoT devices such as utility meters can reveal personal habits such as when and how often a person takes a shower and when they are at home. The ubiquitous nature of IoT devices also creates new challenges around preserving location privacy and preventing personal information

inference. IoT data exchanges may be observed, allowing personal data that an individual may wish to remain private such their location, to be inferred (El Mouaatamid et al., 2016).

There has been much research on data inference in social networks, and while this is not a new issue, the increase in personal and rich metadata contributed by the IoT has escalated the risk of inference attacks. In research by Sun and Tay (2017), the privacy in an IoT network is categorised into “data privacy” which refers to the protection of raw data from a single node, and “inference privacy” which refers to preventing a central processing centre from making any unauthorised statistical inferences. Sun and Tay (2017) proposed a solution for maintaining both kinds of privacy by studying various privacy metrics in the literature and implementing a nonparametric optimisation framework. This framework places the responsibility for ensuring unauthorised inference does not occur on the network provider or supplier. In contrast to this, Torre, Adorni, Koceva, and Sanchez (2016) presented the concept of an adaptive inference discovery service. This service assists user-driven data management by supporting a user to identify risks and configure data sharing permissions via a personal data manager. Researchers have proposed multiple additional privacy enabling technologies such as those mentioned; however, commercial adoption of these solutions remains low (Geneiatakis et al., 2017).

Many IoT services are based upon extensive data mining and analysis, which by its very nature intrudes upon user privacy. Finding a balance between providing advanced personalised and contextually aware services, while preserving privacy, remains an open discussion area for the IoT (Yan et al., 2014). Sha et al. (2018) discussed how satisfying both privacy and security needs in the IoT could be a challenge as these ideas are often in conflict. For example, to achieve strong privacy, functions such as identity need to be weak and the tracing of information limited; whereas effective security mechanisms such as authentication and firewalls demand strong identity management and full audit capability. As yet, solutions for achieving this balance have not been widely addressed by the research community.

2.3.1.9 Standardisation

The lack of a comprehensive and proven security model, including agreed standards, is a crucial challenge facing the adoption and acceptance of the IoT; however, achieving standardisation is proving difficult (Misra et al., 2017). The different devices, OS, and hardware that the IoT contains and the varied implementations of the architecture pose a challenge. For example, some IoT environments utilise machine-to-machine communication and never extend data beyond the local area network, whereas others rely on cloud processing and storage. Each environment requires different technologies and protocols (Stout & Urias, 2016).

Additionally, the fast development and growth of new IoT devices mean that standards for these technologies do not always exist, or if implemented, are not always well tested. This is of most concern in the consumer market where cheaper devices are created quickly for home use (Radovan et al., 2017).

The development of standard protocols for security and communication is necessary to ensure trust in the IoT, to limit the amount of protocol translation occurring between traditional networks

and IoT networks, to avoid the use of protocols that are not suited for resource-constrained devices, and to ensure safe interoperability. Efforts to standardise security protocols in the IoT have begun by organisations such as The Open Mobile Alliance who are looking at machine-to-machine management, and the IETF who are investigating the use of DTLS and authentication and authorisation in resource-constrained environments such as the IoT. These efforts have a long way to go before current challenges are resolved and consistency is achieved (Raza et al., 2016).

Although many standards are evolving for the IoT environment, including device, communication, network, and application standards, the work to ensure that these standards are interoperable is only just beginning. The National Institute of Standards and Technology (NIST) have recently released *Special Publication (SP) 800-183* that could go some way towards helping the various current, evolving, and future standards for the IoT to interoperate. It defines the core activities of an IoT network as sensing, communication, and computation, and describes a set of primitives and elements that make up the IoT system (NIST, 2016). Lindqvist and Neumann (2017) believe that the IoT will become a highly contentious space if governments, standards bodies, and manufacturers do not actively coordinate their efforts to resolve the outstanding issues around privacy and security. The consistent use of the NIST basic definitions may begin the process of standardising IoT language and facilitate the blending of existing standards to support this coordinated effort.

Whilst not a standardisation body, OWASP is another organisation that has recognised the need for a collaborative approach to securing the IoT, and leads a specific online IoT project intended to support consumers, developers, and manufacturers to use and create secure IoT systems. Regular publication of a “top 10 things to avoid” list highlights the current and most prevalent security issues faced by the IoT (OWASP, 2014a).

Security models and protocols for developing IoT devices are not the only areas where standardisation is required to ensure security. The testing of these products and environments should also be conducted in a standardised and repeatable fashion as part of a full development lifecycle to build secure systems (OWASP, 2014b). Several organisations, including the OWASP, recognise this and have developed security testing guides, methodologies, and frameworks to assist manufacturers and researchers in consistently evaluating the security of products.

The OWASP Testing Guide aims to promote a defined and consistent approach to testing web applications. It defines a testing framework that utilises tools and techniques for inclusion at all stages in the systems development lifecycle (SDLC). At a high level, it conducts testing in two phases: Phase 1 is a passive mode, whereby the primary task is information gathering; and Phase 2 is an active mode, whereby tests in 11 subcategories such as authentication testing and cryptography are performed (OWASP, 2014b). It details how to test for controls in these subcategories and identifies possible testing tools. As this guide focuses on web application testing, it does not cover all aspects of IoT device controls and therefore cannot be considered a full methodology for IoT security testing.

The Open Source Security Testing Methodology Manual (OSSTMM) is another proposed de facto standard for security testing that may be adopted by IoT developers (Institute for Security and Open Methodologies, 2009). This method defines the scope of testing into three parts: the communications security channel, the physical security channel, and the spectrum security channel. It is then broken down into much more granular areas and describes a large set of test actions. This methodology focuses heavily on communication analysis and data flow, and whilst comprehensive, it is not easy to follow and does not provide ample support for the creation of detailed test plans (Prandini & Ramilli, 2010). Using this methodology would require an IoT developer to be very experienced in order to create IoT device and system-specific procedures from this generic material, and cover a wide range of possible scenarios in the complex heterogenic IoT environment.

The NIST has also released both a security testing methodology (NIST, 2014), and a technical guide to information security testing and assessment (Scarfone, Cody, Souppaya, & Orebaugh, 2008). These methodologies and guides are technology-neutral and quite broad in scope—making them adaptable for use in the IoT. The NIST describes that the use of several methodologies may be necessary to achieve specific outcomes for any given scenario (NIST, 2014) however, highlight the lack of a single security testing methodology suitable for obtaining consistent, repeatable results across the IoT development landscape.

Each of the individual security and privacy challenges faced in the IoT environment discussed in Section 2.3.1 such as heterogeneity, resource constraints, weak encryption, authentication, access control mechanisms, and a lack of standardisation, require research to develop new solutions for the IoT to succeed and thrive.

2.3.2 The Smart Home Environment

One growing area of application for IoT technology is within the home. Referred to as either the “smart home” or “connected home”, these living spaces utilise a range of networked devices to deliver various digital services. The smart home brings everyday “things” such as refrigerators, televisions, and toasters online. Sensors and networking capabilities are used within the smart home to collect and share large amounts of personal data, and enable the delivery of context-aware, customised, and highly personalised services (McAfee, 2016).

Balancing the traditional security goals of confidentiality, integrity, and availability with functional goals such as the delivery of tailored, context-aware services in a smart home is proving a challenge. There are many examples in the literature of smart home security breaches, that when combined, show an immediate need for new solutions to the potential security and privacy vulnerabilities inherent in this environment.

Fox-Brewster (2015) described seven baby monitors that were compromised using simple hacking techniques; Munro (2016) provided detailed instructions on how a commercial Wi-Fi kettle can be hacked allowing further access into a home Wi-Fi network; and Michele and Karpow (2014) conducted a proof of concept attack against a Samsung smart television, showing how additional smart features contained within home devices increase the possible

attack surface. Chothia and de Ruiter (2016) suggest that the security quality of consumer off-the-shelf IoT devices, such as those contained in a smart home, is so poor that they should be used in the classroom as learning opportunities for penetration testing. They proposed and successfully tested a cybersecurity education course outline based on this premise.

In addition to device vulnerability, risks in the smart home network can be found due to a lack of user awareness and technical skill. In the smart home, users are expected to manage a vast number of devices from multiple vendors. The scale of this network can be similar to that of a medium company. Home users, however, do not have the assistance of security tools such as those found in an enterprise environment; furthermore, they may not have the knowledge, skill or additional support to manage all of these devices thoroughly (Rafferty, Farkhund, & Hung, 2017).

Home users can also lack awareness around the capabilities of the connected devices as they appear similar to traditional home appliances. Users have also been seen to have higher levels of trust in everyday items such as home appliances, and may not fully understand the consequences if their security is breached (Canonical, 2017).

This increasingly complex smart environment is where the popular IoT consumer product, the smart toy, is often found.

2.4 Smart Toy Security and Privacy

2.4.1 Smart Toys

Various definitions are used to describe smart toys. Some authors differentiate between smart toys and connected toys, and define a smart toy as a toy containing embedded electronics that adapt to user actions and process data from sensors, and a connected toy as a toy that can connect to internet systems and other devices to enable data collection, processing, or sharing (Alonso et al., 2016). Other authors such as Tang and Hung (2017) focus on the use of networking to enhance the functionality of a traditional toy in their definitions.

For this research, a smart toy is defined as a physical toy that can connect to the internet and other devices for data collection, processing, and sharing, and may contain embedded electronics to process data from a variety of sensors. Examples of smart toys include Mattel's smart doll "Hello Barbie" which uses interactive voice response to communicate with the user and connects to the internet via Wi-Fi to transmit the recorded conversations; CogniToys Dino which connects to a backend database allowing it to listen and answer to questions by voice; and Furby Connect which connects to the internet exclusively through a Bluetooth connection using an associated smartphone or tablet application (Alonso et al., 2016; Taylor & Michael, 2016).

A smart toy often contains many of the same technologies found in any other commercial IoT devices, such as wireless connectivity (often IEEE 802.11 Wi-Fi or Bluetooth); cloud-based data collection, storage, and analysis; an edge node containing sensors; and a human interface. Some smart toys even include elements of artificial intelligence. They utilise technology such as

GPS, cameras, microphones, video recorders, and various other sensors to gather valuable context data to provide specific and relevant content to the user (Pickering, 2017).

The merging of the internet and toys defines a subset of the IoT coined “The Internet of Toys”, and it is an area that is fast gaining in popularity. The smart toy market was estimated to be worth 5 billion US dollars globally in 2017 and is set to increase, with Juniper Research (2018) forecasting that smart toy sales will reach \$15.5 billion in hardware and application content revenues by 2022.

This growth in the popularity and use of smart toys is leading to concerns around the lack of security features built into the toys and the risk of security and privacy threats they bring. As the users of smart toys are generally vulnerable children, the privacy and security requirements of these devices are considered even more critical than other IoT devices (Tang & Hung, 2017).

2.4.2 Security Incidents

An increasing amount of research is being conducted on smart toy security, and this has resulted in security vulnerabilities reported in several smart toys. The My Friend Cayla doll sold by Genesis Toys is one example of a product that has been controversial, with hackers demonstrating they could make the doll quote foul language instead of her usual conversation (Taylor & Michael, 2016). As the doll does not require authentication when pairing with other devices, any device within a 50-foot range can access the doll's microphone and voice control functions. The United Kingdom's National Cyber Security Centre also recently demonstrated how the hacked doll could then be used to unlock a voice-controlled smart lock within the home (Mills, 2017).

Research conducted in Germany on toys including the My Friend Cayla doll and i-Que robot reviewed the type and method of data transmission used by the toys, and investigated whether an unauthorised user could connect to the toys and obtain data. They found that by using free applications from the Google play store, both the My Friend Cayla doll and the i-QUE robot could be used as recording devices and conduct two-way communications (Forbrukerradet, 2016). As a result of such research, The Federal Network Agency (Bundesnetzagentur) in Germany concluded that the My Friend Cayla doll amounted to a “concealed transmitting device” which are illegal in Germany. Regulators have encouraged parents to destroy the dolls, as selling or buying a banned surveillance system can lead to a jail sentence of up to two years (BBC, 2017b).

Denning, Matuszek, Koscher, Smith, and Kohn (2009) found that two children's robots (Wowwee Robosapien V2 and Erector Spykee) transmitted plain text login credentials and did not encrypt transmitted video files, thus leaving the devices open to eavesdropping and/or manipulation. The researchers then demonstrated various scenarios where these vulnerabilities could be used for malicious purposes. More recently, an investigation into the Furby Connect toy has found multiple security issues such as poor Bluetooth security and insecure firmware updates (Tung, 2017).

The companies associated with smart toy technologies have also been found to be susceptible to attacks. In 2017, hackers accessed the database of Spiral Toys, the company that produces

the talking smart toys called CloudPets. The compromised CloudPets' database contained email addresses, passwords, and voice recordings from children. This information was held for ransom by cybercriminals attempting to extort money from the victims. The breach affected more than 800,000 people (BBC, 2017a).

The children's toy company, VTech, also suffered a high-profile data breach in 2015 involving the leaking of over 6 million database records containing children's names, genders, birthdates, photographs, and chat logs associated with parents addresses, passwords, and secret question information (Taylor & Michael, 2016). Subsequently, in the first case of its kind involving children's privacy and smart toys, the company settled charges brought against them by the FTC who alleged the company collected personal information from children without consent. It also accused VTech of not securing the data it had collected with reasonable steps, such as implementing IDS or taking sufficient measures to protect data transmitted and stored by the company. In addition to the above-noted lack of security measures, it is alleged that while VTech claimed in its privacy policy to encrypt all captured data, it did not (FTC, 2018).

In November, 2015, a United Kingdom consumer watchdog requested that any smart toys with proven privacy or security issues be either made secure or removed from sale. Included in this list were the i-Que Intelligent Robot, My Friend Cayla, Toy-Fi Teddy and CloudPets (Tung, 2017). In 2019, an online search showed that many retailers were still selling the toys; however, Amazon, Target and Walmart have finally responded to the concerns and recently removed CloudPets from their shelves.

Alonso et al. (2016) researched a variety of smart toys to identify their connection methods and consent processes. They identified the following steps that companies could take to safeguard data: conduct independent security audits; become involved in a bug bounty programme; determine when local vs remote processing and third-party sharing is appropriate and mitigate risks for the selected approach; implement strong encryption standards (HTTPS/TLS); do not use hardcoded or default passwords; prevent unauthorised firmware updates; and keep up to date with industry norms for device updating and sharing of risk information. These points provide a starting point from which companies can progress further to ensure security is built into their products.

The toy industry has been prompted by recent events to start considering these topics and have responded in various ways. ToyTalk, a producer of Hello Barbie, a connected doll which has been the subject of much controversy due to its ability to record, transmit, and store online conversations held with a child, have implemented one of the suggestions from the above research by developing a bug bounty programme to discover security flaws in their products. Mahmoud (2018) however points out in his study that the doll still contains known vulnerabilities such as broadcasting open hotspots and enabling unauthorised pairing, despite ToyTalk being aware of these design issues.

Even after large-scale data breaches, some toy companies still fail to strengthen their security. For example, VTech revised their terms and conditions of its user agreement by shifting more

responsibility for data leaks onto parents, rather than increasing the security of the product after its major data breach in 2015. The limitation of liability agreement now states: “You acknowledge and agree that any information you send or receive during your use of the site may not be secure and may be intercepted or later acquired by unauthorised parties” (VTech, 2015, para. 17).

This summarised research into the vulnerabilities of smart toys, combined with recent significant data breaches and a lack of adequate response from impacted toy companies, suggests that securing the privacy and security of smart toys may not be straightforward.

2.4.3 Smart Toy Security and Privacy Challenges

Early research into smart toys found many privacy and security related issues. As these toys are part of the broader IoT environment, many of the same challenges exist when trying to secure them for safe consumer use, such as resource constraints and lack of standardised protocols. However, as smart toys are used primarily by children, specific privacy and security challenges around securing children’s data, implementing parental control mechanisms, and gaining informed consent are additionally heightened to protect some of society’s most vulnerable.

2.4.3.1 *Data Privacy*

One area of concern for consumers is that of data privacy. As children represent a profitable portion of the consumer market, corporate researchers like to collect both usage and personal data to conduct targeted marketing campaigns. Technical advances in voice recognition and other sensing technologies have allowed smart toys to evolve to collect, share, and process a vast array of information that may be used to profile a child and enable this form of marketing. Data privacy can, however, become a concern if marketers use the information collected for undisclosed or unwelcome purposes (Tang & Hung, 2017).

Additionally, sensitive data gleaned such as location information, videos, pictures, and names may also present an opportunity for child exploitation. The Federal Bureau of Investigation (FBI) has been monitoring child safety and smart toys for some time. Toys that include microphones with the ability to record and collect conversations (including personal information about a child or family which may then be combined with information gleaned from the internet such as user account details) have led to them expressing concerns around both privacy and physical safety (FBI, 2017).

Research into the risks of using general IoT devices is a growing field, with many studies looking at identifying and mitigating the security risks of these products. Rafferty, Hung, et al. (2017) used threat modelling to identify privacy risks associated with the use of dynamic smart home devices such as smart toys. They used Microsoft’s STRIDE model and OWASP’s list of IoT attack surface areas to identify privacy threats. The research identified device-specific threats such as firmware extraction and malicious updates; web interface threats such as weak or default passwords, cross-site scripting, and SQL injection; and communication threats such as interception and eavesdropping. Whilst not specific to smart toys, the research results apply to the smart toy device.

Whilst Rafferty, Hung, et al.'s (2017) research focused on demonstrating a framework for identifying privacy threats, Butler, Huang, Roesner, and Cakmak (2015) attempt to resolve privacy threats by investigating the privacy-utility trade-off in remotely teleoperated robots. The researchers reduced the quality of visual information captured and transmitted by a home robot in an attempt to preserve the end user's privacy while not reducing the robot's performance. The study found that sacrificing a small amount of utility could significantly improve privacy, and is a demonstration of how solutions to the privacy challenges faced in an IoT world can be found.

Another privacy risk associated with the use of smart devices is identity fraud or theft. Opportunities exist for child identity fraud if enough personally identifiable information (PII) is gathered from the interception of devices such as smart toys. A report released in 2018 by Javelin Strategy and Research, states that over one million children were victims of identity fraud in 2017 and that children's identity theft is growing. Children's data is worth more on the black market than adults, and as such, is in high demand, suggesting that targeted attacks on children's data will continue to grow (Mahmoud, Hossen, Barakat, Mannan, & Youssef, 2017).

Specific research on the data privacy risks of smart toys is more limited than that of general IoT device research. However, Mahmoud (2018) researched several smart toys to expose any potential PII leakage and any weak security measures. Techniques such as network traffic and Bluetooth analysis, code analysis, and smartphone app reverse engineering were used to assess the PII collected and transmitted by the smart toys, including PII transmitted to third parties such as advertising and analytic services. Mahmoud's (2018) study found that the smart toys collected excessive unique identifiers and sent data to unauthorised entities highlighting the ongoing privacy and security risks inherent in these toys. However, as this research was conducted on a minimal array of toys, further research would be required to conclude that large privacy and or security threats exist for consumers.

2.4.3.2 Regulation/Legislation

Mechanisms exist to protect children's data and include the Children's Online Privacy Protection Act of 1998 (COPPA). COPPA provides strong legal protection over children's data, including enforcing requirements to obtain verifiable parental consent, to provide notice, minimise data collection, and maintain reasonable data protection processes. COPPA applies to all modern toys that connect to the internet. However, it is unclear at this time whether it applies to toys that employ non-internet forms of communication such as short-range communication via Bluetooth, ZigBee, or Z-Wave technologies (Alonso et al., 2016). No literature was found that investigated the specific security and privacy risks of IoT devices utilising these new technologies, and this area could present a new opportunity for research.

Moini (2017) discussed the legal gaps within children's privacy legislation, highlighting that current COPPA legislation does not enforce mandatory reporting of suspicious speech or video found by any company collecting this data. As such, suspected child abuse or neglect that may be disclosed by a child talking to their doll may be ignored. Additionally, children over 13 years old may still be considered vulnerable; however, are not covered by legislation such as COPPA.

Jones and Meurer (2016) questioned whether even stronger safeguards and standards should apply to products marketed for children, in particular, around the areas of data collection, storage, and sharing. They stressed that because of the intimate nature of the information that can be shared by children interacting with toys, stronger data sharing regulations should be warranted. Voicing similar concerns, more than 18 privacy groups filed privacy-related complaints with the EU (European Union) and the FTC concerning smart toys in 2016 (Kshetri & Voas, 2018).

The American toy industry via the Toy Industry Association has raised concerns that if children's data is controlled or regulated too heavily, companies may no longer be able to innovate and supply customised experiences. Imposing tight restrictions may mean they cannot collect the data required to improve the content and personalise their toy offerings (Tang & Hung, 2017). In New Zealand, the toy industry has regulations in place for toy safety; however, these regulations do not specifically cover privacy issues in the context of smart toys (Commerce Commission New Zealand, n.d.) and as this as a new issue for retailers, they primarily use self-regulation, knowledge, and judgement to determine whether a toy will be sold locally (S. Holdsworth, personal communication, May 15, 2018).

In New Zealand, the New Zealand Privacy Act 1993 covers legislation around the collection of data and "controls how 'agencies' collect, use, disclose, store and give access to personal information" (Office of the Privacy Commissioner, 2013, para. 1). The Act outlines a set of 12 information privacy principles to be followed, which is similar in approach to comparative European data protection laws (Office of the Privacy Commissioner, 2013). The Act applies to any information about an identifiable living individual (Office of the Privacy Commissioner, 2013), and therefore encompasses any data collected from or about a child. However, there are no specific or additional safeguards specified for children's data.

Whether the Act protects a New Zealand consumer from possible unlawful or insecure data practices, may depend on whether the company is considered to be an agency that is "operating in New Zealand". If an overseas company had little relationship with New Zealand, it is unlikely the Act would apply to that company, and any toy purchased from such a source would not have to comply with New Zealand legislation (Office of the Privacy Commissioner, personal communication, October 25, 2018). As many consumer products, including smart toys, are now purchased online from a store or manufacturer located in any part of the world, consumers should be made aware of this risk.

The EU General Data Protection Regulation (GDPR) has been introduced to strengthen data protection laws in the EU in response to concerns that vulnerable consumers such as children need to be protected. It strengthens requirements in areas such as "request for consent", which it states must be given in an intelligible and easily accessible form, with a clear purpose for data processing identified (European Commission, n.d.). Stronger legislative requirements such as these around clear identification of data usage have prompted research to be undertaken in the areas of privacy policies and parental consent and controls.

2.4.3.3 Privacy Policy Research

Many smart toy privacy policies outline their information usage and disclosure practices; however, these policies are often not easily located, read, or understood (Tang & Hung, 2017). When conducting a survey on children's web applications, the FTC found that only around 45% of the applications contained direct links to privacy policies (Cohen & Yeung, 2015). Alonso et al. (2016) pointed out that companies often only post privacy policies on their websites, where parents who set up a toy and interact with it over a smartphone or tablet application may never see it.

In response to concerns that existing mechanisms to present online privacy policies to consumers have been ineffective, Kelley, Bresee, Cranor, and Reeder (2009) developed a privacy label that uses visual representation techniques similar to those on nutrition labels to show how a company collects, uses, and shares any personal information. Kelley et al. (2009) found that users could find important privacy information faster using this label, and therefore had a better experience when using the website. This early research was limited to website policies, and did not discuss mobile applications or IoT devices where information display has now become commonplace.

After identifying that there was no comprehensive framework available that focuses on the evaluation of smart toys privacy policies, Mahmoud et al. (2017) developed a set of 17 privacy-sensitive criteria in five categories for evaluating privacy policies. They used the criteria to assess several smart toys and found weaknesses around PII collection, web tracking, and data storage locations. Although this study presented clear results for each toy based upon the criteria measured, it did not indicate to readers the level of privacy risk posed by any toy that did not meet or only partially met the suggested criteria in any area. All of the analysis was static, so further work is required to physically test whether these toys behave as suggested by their policies.

2.4.3.4 Parental Consent/Control Research

The constantly evolving threats that children may be exposed to when online has generated interest in developing parental control software tools. These tools can allow guardians to restrict the amount of content a child can provide to a smart toy, control access to inappropriate content, and be informed regarding how a child interacts with the technology. Examples of current parental control interfaces include Hello Barbie's "Safety and privacy settings" which requests a parent's consent for using the toy through the associated mobile application, and the Jibo "Privacy statement" which informs the user of privacy details related to using the toy in order to request consent and permission (Rafferty, Hung, et al., 2017).

The existing parental control interfaces described are very limited in functionality. Despite the European Union Safer Internet Programme (n.d.) describing usability as a core consideration in the development of these interfaces, research has highlighted that where these interfaces have been implemented to date, they can be difficult to use and offer limited options for setting privacy preferences (De Lima Salgado, Agostini do Amaral, Castro, & De Mattos Forte, 2017). This

research concluded that parental control solutions are essential for smart toys, and suggests developers consider existing standard usability requirements when designing an interface, focus on user-centred design techniques, and evaluate effectiveness throughout the development process. In addition to this, the research highlighted that unresearched new technologies may be required to conduct user-centred design successfully in the smart toy context.

A study by Fuentes, Quimbiulco, Galárraga, and Garcia-Dorado (2015) evaluated current parental control software, and found all the software included in the study rated poorly in terms of its ease to configure. They concluded that this difficulty, combined with a general lack of awareness about the availability of parental control tools, meant they were not frequently used.

Research focusing on solving the current problems faced in this space is just beginning, with Rafferty, Hung et al. (2017) aiming to provide a standard model for protecting children's data and setting consent in the smart toy paradigm. Their research describes a conceptual model for privacy rules, where legal guardians own all of the collected data about their child and provide consent for sharing through configurable access rules. The model is demonstrated using two smart toys—Sphero and Tek Recon. The research proposed a moderately complex access control framework based on creating privacy policy rules. It relies on the parent to create, name, provide descriptions, and set an expiry date for the privacy rules. The proposal offers much greater data control for the parent; however, it would require user testing to ensure ease of use which is not addressed in the study. Additionally, no discussion is provided around whether resource-constrained smart toys would manage a complex access control mechanism such as this.

Some researchers see parental control and monitoring functions as essential elements for any connected toy. In a survey conducted by McReynolds et al. (2017), all respondents believed that parental control is necessary; however, monitoring children's play by means such as voice recording has raised ethical concerns. Researchers such as Taylor and Michael (2016) and Jones and Meurer (2016) both highlighted the ethical issues around adult interference in children's play. They challenged the notion that parents should listen to the private recordings made of their child's interactions with a toy, and believed such behaviour is an invasion of privacy which could damage relationships.

McReynolds et al. (2017) found that children were generally unaware that what they said to their toy may be heard by anyone else, and research has shown that the anthropomorphic design of many smart toys can result in children divulging much personal information to these toys as they unconsciously trust them (Rafferty, Hung et al., 2015). McReynolds et al. (2017) additionally found that children are mostly unaware that the toy they are playing with might record what they say.

The studies outlined reinforce the necessity of protecting and educating children when they are exposed to toys of this nature, but additionally highlight the complex and sensitive nature of the topic that makes a "one size fits all" solution unrealistic.

2.4.3.5 *Additional Smart Toy Risks*

Additional risks inherent in smart toys include their constant connectivity, mobility, and large attack surface. The constant connectivity of some smart toys to the internet increases privacy and security risks not found in traditional toys, as they may capture information from the surrounding environment without users being aware. Jodka (2017) suggests solutions to enable more safety, such as including features such as “wake words”, whereby a device does not begin recording until a specific word or phrase is spoken. The importance of allowing the user to review any recordings and delete them permanently from all storage locations and enabling “mass purge” features is also emphasised.

Smart toys are an example of dynamic IoT devices that are mobile, and therefore may physically move beyond a home network. This mobility increases the risk of the toys suffering an external attack, either by connecting to insecure external networks or by physically tampering (Rafferty, Farkhund, et al., 2017). When smart toys are found in settings such as classrooms and hospitals, additional challenges also appear, such as a primary guardian not being present at the time of the initial toy set up to grant consent for use. The portability of toys and the frequency with which they are shared also leads to scenarios such as friends bringing over their connected toy for use with another child. A parent may not have permitted their child to play with a toy, or may be unaware of the functionality of a toy a playmate has (Alonso et al. 2016).

Finally, as described by Pickering (2017), the hardening of every element on the Internet of Toys chain is essential for adequate security. Smart toys, however, can have an enormous potential attack surface that includes the devices, companion applications, remote hosts, and all communication between these entities. This makes security a complex challenge.

While some of the toys included in the literature reviewed in this chapter are available locally, others are not. Specific investigations into smart toys available in the New Zealand context have not been found, and as the range of toys available to a consumer vary both over time and between countries, in order to apply any conclusions about smart toy risks in New Zealand a study that includes toys available locally must be undertaken.

2.5 Awareness and Risk

The idea that the user is the weakest link in any security chain is well documented in the literature, and it is thought that poor and risky security behaviours can be linked to the extent of a user’s information security awareness (Öğütçü, Testik, & Chouseinoglou, 2016). Surveys have shown that users of smart devices such as smartphones are often inadequately prepared to make security decisions (Mylonas, Kastania, & Gritzalis, 2013), and the ubiquitous nature of the IoT introduces a new set of risks that may not be fully understood by consumers.

Many consumers may not have even heard of the term IoT, let alone understand the security and privacy threats the new technology brings. For example, a consumer may think it does not matter if a hacker knows the content of their fridge. If, however, the same access allows the

hacker to see the fridge has not been opened in days, indicating that the owner is possibly away, the threat becomes more apparent (Liu, 2015).

Additionally, as many consumers have limited technical knowledge, manufacturers try to provide an excellent customer experience by offering simple installation and set-up processes. Security controls and requirements that would introduce complexity to these processes have therefore often been overlooked in IoT devices. This lack of strong device security, combined with a lack of awareness of data usage policies, security and privacy policies, and device capabilities, could lead to the compromise of user privacy and security due to unsafe user practices and the incorrect set up of devices (Lindqvist & Neumann, 2017).

Literature about successful methods to increase user awareness and education around privacy and security in the IoT is limited. There are also varied opinions around whether increasing user privacy and security awareness is effective and therefore necessary. Dibrov (2017) believes that whilst conducting security awareness programmes is prudent, they should not be relied upon, and points to a report by security provider PhishMe that showed 80% of people who had completed security awareness training were still susceptible to a phishing attack. He believes IoT security issues should no longer be deemed as user interaction problems, but device and system interaction problems, and that only advancing intelligent security technology will combat the growing risks that the IoT brings.

In contrast to reducing reliance on user awareness and good security hygiene, Miedema (2018) posed that users should be co-stewards of the internet arena, and therefore must be held to account if they fail to protect their information systems and devices. Miedema (2018) describes the increased risk of DDoS attacks that the IoT brings, and highlights the role individuals play when they fail to protect their devices, allowing them to be conscripted into botnet armies. The outcome of this allows botnet armies to conduct devastating attacks on critical infrastructure, commerce, and government. Increasing user awareness by way of widespread user awareness campaigns is seen as a critical first step in this scenario to encourage the notion of co-stewardship and decrease the growing security risk from the IoT.

Whilst no specific studies have been found that investigate user awareness and smart toy risks, a body of literature has grown that investigates information security awareness, digital literacy, and the relationship of these to online behaviour that may be used as a base to understand this area and perform further research.

Park (2011) conducted a study examining the relationship between a user's level of privacy knowledge and the control of their personal information online. Park (2011) hypothesised that higher levels of knowledge would lead to more active data control and his results supported this hypothesis, but also found an overall low level of user awareness. Whilst earlier studies had used a single variable to represent "user knowledge", he expanded this and used three dimensions to measure the concept of knowledge; familiarity with technical aspects; awareness of standard institutional practices; and understanding of privacy policies. These additional dimensions added robustness to his results.

Trepte et al. (2015) expanded on studies such as that conducted by Park (2011), and developed a full scale to measure online privacy knowledge using a total of five dimensions. The scale is based on an extensive literature review and rather than using a Likert scale, they suggested true/false or multi-choice questions to measure actual knowledge rather than perceived knowledge. The positive contributions of this research include the ability to tailor the measurement tool to new environments while maintaining the basis of a consistent measurement tool. Limitations of the work include its generalisation as it does not focus on any single technology and its age. Technology and the knowledge required to use it safely continuously evolve, hence the need to review any scale that uses questions that are more than a couple of years for applicability to the current environment.

In the IoT space, Udoh and Alkharashi (2016) focused on investigating the awareness that American students have around the privacy risks of using a smartwatch, and the impact that awareness has on their behaviour. The study found that most students were unaware of the full capabilities of their device, and many did not engage in any privacy-enhancing behaviour. The study used a non-probability convenience sample and qualitative interviews to assess awareness. Limitations included the sample size, as only 10 students were interviewed. Additionally, the researchers noted that participants seemed to change their views as the interviews progressed, and more information about the risks of smartphones was revealed to them. This shows how the influence of the interviewer and information given to the participant during the research can have a direct impact on the results. It is unclear in the literature how factors of this research, such as the information that was given to the participants during the interviews, was controlled, and therefore the results of this study could not be seen to be representative of any other group.

Early internet research that found a significant correlation between a user's awareness of privacy protection strategies and their security and privacy behaviours (Donmeyer & Cross, 2003) confirmed the importance of measuring user awareness when examining and assessing technology risks. Therefore, to examine whether smart toys pose any security or privacy risk in New Zealand, an investigation into the awareness levels of New Zealand parents/guardians is warranted.

2.6 Conclusion

The literature reviewed has provided an overview of research undertaken in the IoT area and uncovered a growing body of material focused on general IoT security and privacy. However, it has also revealed gaps in our understanding, and highlights that limited investigation has been conducted in specific areas of the IoT such as the security and privacy issues and risks of devices such as smart toys.

Section 2.2 focused on an overview of the IoT. The definition of the IoT was described, and the origins of its explosive growth discussed. The benefits for both business and the consumer, along with the potential new security and privacy threats that the additional level of daily and pervasive connectivity the IoT supports, was highlighted. Research into architectural reference

models for the IoT was then explored and revealed disparate models being proposed that may lead to interoperability problems for the IoT if a common language is not universally agreed.

The differences between an IoT network and a traditional network were discussed, such as the IoTs use of LLN and the resource constraints that an IoT network faces that traditional networks do not, such as low memory, energy, and processing power. These constraints have driven research into the development of new technologies, protocols, and standards which are essential for the efficient operation of the IoT. The literature review also revealed that whilst many new technologies such as BLE and ZigBee have been developed, many support tools are still developing and immature.

Section 2.3 investigated securing the IoT. The literature review found that most authors agreed that securing the IoT is vital for its success and basic security goals such as confidentiality, integrity, authentication, non-repudiation, availability and privacy still apply. However, it is clear from the research studied that some of the unique characteristics of the IoT, such as its heterogeneity, resource constraints, scale, and environment mean that new challenges are being faced when attempting to address security and privacy in these networks.

Open research challenges were found to exist in areas such as secure trust management, encryption, authentication, access control, device management, and privacy in the IoT. Research into the development of new techniques, such as lightweight encryption schemes, lightweight authentication protocols, and access control systems that require less computational power to operate were investigated. However, the review found that research conducted so far does not cover all new IoT technologies or environments, or address many known security and privacy challenges.

Standardisation in the IoT was covered next. It was found that the fast development of new IoT devices and technologies have outpaced the development of agreed security standards in the IoT which are still evolving. Devices available on the consumer market have been recognised as being insecure, and efforts have started to standardise security protocols used in the IoT.

Literature focusing on the smart home was reviewed, which demonstrated multiple examples of security and privacy vulnerabilities inherent in IoT devices in the home such as televisions and baby monitors.

Section 2.4 focused specifically on smart toy security and privacy. The characteristics of smart toys were investigated, and a definition of a smart toy for this research was provided. The concern around the growing threat of security and privacy issues surrounding IoT toys was outlined, which led to a review of security incidents involving these devices.

Research into smart toy security was reviewed next. Whilst it was found that there is not an extensive body of research undertaken in this area, several international research studies were discussed that revealed multiple vulnerabilities in specific smart toys available on the consumer market. The results of these initial research studies indicate that smart toy security is an area warranting further investigation.

Recent large-scale data breaches were then reviewed, with the literature revealing that toy companies that collect and store children's data, have been, and still are, susceptible to hacking and data leaks, which places children's privacy at risk. Researchers have begun to outline the steps companies can take to safeguard data, but the literature notes that not all companies have followed this advice.

Studies that discussed the specific challenges involved in smart toy security and privacy were covered next. Data privacy was identified through the review as an area of growing concern; however, limited research on data privacy and smart toys has been undertaken to date. An initial study found that the collection of PII by some smart toys was excessive, but this is a gap that requires more research to be conducted to conclude whether a genuine threat exists to users. Regulation and legislation that aims to protect children's data were reviewed, with international regulations found to be tightening in response to recent research in this area. The New Zealand context was discussed, highlighting that this is still a new and emerging area of concern here.

The literature review next looked at privacy policy and parental control research, and found a growing body of research into solutions to overcome the challenges of providing consent and information mechanisms in resource-constrained and lightweight devices such as smart toys. The ethical considerations around parental control mechanisms were explored, and the sensitive and complex nature of this topic uncovered.

Additional risks including the constant connectivity, mobility, and large attack surface of smart toys were then discussed. This highlighted a lack of research in these areas. No specific investigation into the security and privacy risks of smart toys available in New Zealand was found, and therefore, the risks to New Zealand consumers are as yet undetermined by the currently available literature.

Finally, Section 2.4 reviewed the link between user awareness and risk. Research that concluded that user awareness is directly linked to online user behaviour, and therefore the level of risk in an online environment, was discussed. No specific literature studying smart toys and user awareness was found, and therefore this gap will be addressed in this study.

Chapter 3 focuses on the identification of a research approach to investigate whether there are any security or privacy risks involved with the use of smart toys in New Zealand. An appropriate method to research the level of user awareness around potential smart toy security and privacy risks, along with a method to uncover any potential vulnerabilities in the smart toys available to New Zealand parents will be formed.

Chapter 3: Research Design and Methodology

3.1 Introduction

The purpose of this chapter is to identify an appropriate methodology for researching the security and privacy risks of smart toys in New Zealand. The literature review in Chapter 2 identified many technical, legal, and practical issues around the security and privacy of IoT devices. These issues, along with gaps identified in the current body of research, have been used to derive, articulate, and justify the research questions and sub-questions outlined in Section 3.2. It has been determined that two separate methodological approaches are required to answer these questions effectively. The chosen methodologies for each part of the research are discussed in Sections 3.4 and 3.5

Section 3.3 describes the survey method and the process that was undertaken to develop the instrument. Validity and reliability of the tool is discussed and the approach to data collection and analysis outlined. The ethical approval required to conduct this research is presented.

Section 3.4 describes the testing process undertaken for the second research component. The smart toy environment is outlined, and the objectives, scope and approach for the investigation and testing of the smart toys are described.

3.2 Research Questions

The literature review presented in Chapter 2 demonstrated that smart toys available for purchase overseas contained security vulnerabilities that may impact the safety and privacy of consumers, and that there is an increasing level of concern amongst consumers around these issues (Tang & Hung, 2017). No similar research studies have been conducted for the New Zealand context, and this research aims to address this gap by investigating current levels of concern and awareness of New Zealand parents/guardians around the risks of smart toy use. Furthermore, several smart toys available for purchase by New Zealand consumers are examined to determine what potential security and privacy vulnerabilities they possess.

The main question that this research will seek to answer is as follows:

Question 1 (Q1). Do smart toys pose a security or privacy risk to users in New Zealand?

It is recognised that the companies designing and producing smart toys have sometimes failed to implement high levels of security and privacy standards in their products, leading to known vulnerabilities (New Zealand IoT Alliance, 2017). Previous research has also found a positive correlation between a lack of user awareness and a failure to implement protective mechanisms when using online technology. This is thought to increase the potential security and privacy risks of connected devices (Donmeyer & Cross, 2003).

Therefore, as security and privacy risks can be inherent in both the design of a product and be heightened by user awareness and subsequent behaviour, both elements are investigated to answer the main research question.

The following sub-questions were formulated to address the issues outlined previously:

Sub-question 1 (SQ1). What level of privacy and security concern do New Zealand parents and guardians have regarding smart toy use?

Sub-question 2 (SQ2). What level of privacy and security awareness do New Zealand parents and guardians have regarding smart toy use?

Sub-question 3 (SQ3). What common security and privacy impacting vulnerabilities are found in smart toys currently available for purchase by New Zealanders?

The literature review in Chapter 2 indicated a rising level of concern from international smart toy consumers around security and privacy risks. In order to explore the relationship between privacy and security concern and privacy and security awareness, the following hypothesis has been generated:

Hypothesis 1 (H1). A higher level of participant concern around smart toy privacy and security risks, will correlate to a higher level of participant awareness around these risks.

3.3 Research Approach

The outcome of investigations into each sub-question will determine the answer to the main research question. Two separate approaches were identified as most appropriate for gathering the required data to answer these sub-questions. Both approaches can be categorised as descriptive research; the aim of which is to describe the current state of a target variable within a specific group (Thomas, 2003). Both approaches also use an empirical method as they are data-based and seek to reach conclusions that are verified by quantitative, measurable data (Salkind, 2010).

Firstly, a survey method is described that is used to collect data to answer SQ1 and SQ2. A survey systematically gathers data from a subset of individuals to describe the characteristics of a population (Scheuren, 2005). As this study attempts to determine the characteristics of concern and awareness amongst a subset of the New Zealand parent/guardian population, a survey method was chosen as a suitable approach.

The high-level survey research process undertaken is outlined in Figure 3.1:

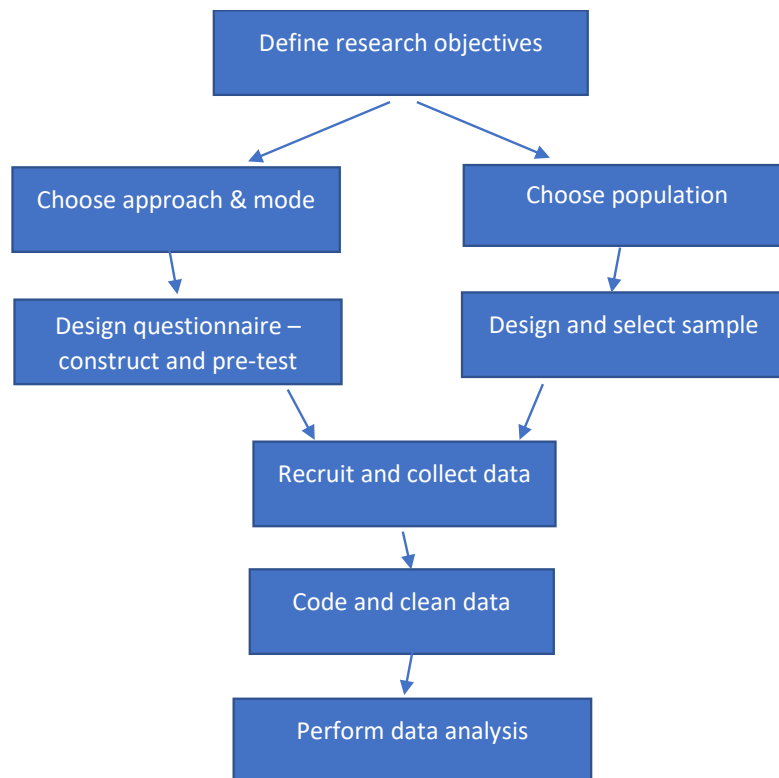


Figure 3.1. The survey research process adapted from Groves (2009).

Secondly, a standards-based security testing methodology was adapted to collect the data required to answer SQ3. Following this methodology, several smart toys were systematically evaluated in a controlled environment to determine if the toys utilised basic security controls. The results of this evaluation can indicate any potential security and privacy vulnerabilities the toys may have.

3.4 Survey Design

A cross-sectional survey was undertaken to answer SQ1 and SQ2. The objective of the survey was to collect qualitative and quantitative data for analysis to obtain both the level of concern and level of awareness of New Zealand parents/guardians around smart toy privacy and security risks.

3.4.1 Approach and Mode

The survey was conducted as an online questionnaire where the anonymity of the respondents was assured. The survey contained a total of 36 questions using a combination of true/false and ordinal scale response options. SurveyMonkey was used to deliver the online questionnaire because of its clear navigation and layout.

A convenience sample of volunteers was gained by advertising the research at relevant locations including Plunket offices, parent and child playgroups, parenting Facebook groups, sports clubs, and willing schools across New Zealand. These locations were chosen to recruit volunteers who were representative of the area of interest and most likely to have the required knowledge. For example, Plunket offices were used to gain volunteer participants that were parents/guardians

of children under five years old, as most New Zealand children have several Plunket visits before the age of five. Sports clubs and schools were used to recruit participants that were parents/guardians of children over the age of five as they are more likely to be involved in a sport or enrolled in school.

All potential participants were directed to the online SurveyMonkey questionnaire and invited to complete the survey. A copy of the information and invitation notices is in Appendix A. These notices remained in place until the survey closed.

To ensure anonymity, no PII was collected and IP address and email address tracking were disabled.

3.4.2 Sample

A non-probability sample of adults was used that met the following criteria:

- Must reside in New Zealand
- Must be a parent or guardian of a child (the legal definition of a child in New Zealand is any human under the age of 18 and was used for this study).

The target audience of New Zealand parents/guardians was determined using the most recent national census as a total population of 908,127 (StatsNZ, 2013). As such, a statistically significant sample size was calculated to be 385 respondents to reach an industry-standard confidence level of 95% and a margin of error of 5% using the following formula:

$$\frac{\frac{z^2 \times p(1-p)}{e^2}}{1 + \left(\frac{z^2 \times p(1-p)}{e^2 N} \right)}$$

Where z (confidence level represented as a z-score) = 1.96, N (population size) = 908,127, e (margin of error represented as a decimal) = 5%.

3.4.3 Questionnaire Design

The questionnaire was designed to measure the concepts of both concern and awareness of smart toy privacy and security risks, after conducting a thorough literature review and holding a consultation with industry experts.

The first section of the survey collected demographic data that was used to categorise the respondents by their level of highest education and gender. Where possible, the format for these questions was standardised as per the StatsNZ website categories (StatsNZ, 2013) as this format would allow the findings to be compared to other standardised studies if required.

The second section of the survey required the respondents to answer two questions on whether security and privacy was a concern for them when their children used smart toys. These

questions were derived from similar research measuring levels of concern around social networking sites (Al Johani, 2016).

The third section of the survey asked participants a series of questions that aimed to measure their level of awareness around smart toy security and privacy. A foundation of research literature exists that conceptualises online privacy awareness and knowledge in order to successfully measure these ideas (Donmeyer & Cross, 2003; Hong & Thong, 2013; Park, 2011; Trepte et al., 2015). There are also existing scales that measure general information security awareness (Parsons et al., 2017); however, to date, no instrument has been explicitly tailored for measuring smart toy privacy and security awareness. Additionally, no existing instrument could be found that measured IoT device privacy and security awareness in a New Zealand context. Survey instruments used in the research discussed in the literature review were therefore examined for their applicability to this study.

As a result of this examination, The Online Privacy Literacy Scale (OPLS) (Trepte et al., 2015) was chosen to be adapted and used as the core measurement framework for this part of the survey. The OPLS was selected as it most closely reflected the concept of awareness that this research aimed to measure, by encompassing knowledge dimensions relevant to smart toy security and privacy. Additionally, the OPLS was designed to be modified for use in environments beyond its initial application, making the adaption of it for a New Zealand context more reliable.

The original OPLS, however, was only designed to measure general online security and privacy awareness. As using specific technologies such as smart toys requires specific knowledge, the questions were adapted to ensure the accurate measurement of smart toy privacy and security awareness. Suitable content for new questions was derived from a review of existing literature and similar research studies.

The final survey questions encompassed input from sources such as the OWASP Top 10 Guidance series (OWASP, 2014a), The New Zealand Privacy Commissioner Privacy Principles (Office of the Privacy Commissioner, 2013), and previous research studies covered in the literature review such as Park (2011) and Parsons et al. (2017). International law questions were substituted for questions on New Zealand privacy law with guidance from the Privacy Commission. As the OPLS was several years old, questions on more modern technology were also included.

A copy of the questionnaire can be found in Appendix B.

3.4.4 Measures

The concept of *security and privacy concern* was defined as a combination of both concern around the potential security risks of using smart toys, and concern around the potential privacy risks of using smart toys.

Two Likert scale items were asked to determine the level of security and privacy concern. There were five possible response categories which ranged from 'Strongly agree' to 'Strongly disagree'.

Figure 3.3 shows one example of these items.

1. I am concerned about the privacy risks of using smart toys (*such as my personal information being stolen or misused*).

☐ Strongly agree

☐ Disagree

☐ Agree

☐ Strongly disagree

☐ Neither agree nor disagree

Figure 3.2. An example of a survey question

In order to measure *security and privacy concern*, a Likert scale consisting of the sum of all Likert item responses was used.

Security and privacy awareness was defined as factual knowledge relating to security and privacy. Factual knowledge refers to users' knowledge about the technical aspects of smart toys, potential security and privacy risks, applicable laws, protection strategies, and institutional practices.

Security and privacy awareness was measured using five knowledge dimensions as follows:

1. Knowledge of the technical capabilities of smart toys

This dimension included questions regarding the standard features of smart toys sold to consumers today. For example, whether a smart toy can use GPS for location tracking.

2. Knowledge of common potential smart toy security and privacy risks or vulnerabilities

This dimension included six questions regarding knowledge of the most common IoT device vulnerabilities as recorded in the literature, such as the ability to allow a user to select weak passwords.

3. Knowledge of the data procedures of smart toy and affiliate companies

This dimension included six questions regarding knowledge of smart toy company policies and procedures around data use. For example, company data retention strategies and data use declaration practices such as privacy statements.

4. Knowledge of data protection and privacy laws/legal aspects in New Zealand

This dimension included six questions regarding applicable privacy legislation in New Zealand, such as *The Privacy Act* (1993).

5. Knowledge of security and privacy protection strategies

This dimension included six questions derived from OWASP consumer security guidance regarding common protection strategies, such as enabling encryption and changing default passwords.

An example of a question used to measure awareness in the survey is shown in Figure 3.4:

1. Some smart toy mobile applications can track your location even if you haven't launched them.

☐ True

☐ False

☐ Don't Know

Figure 3.3. An example of a survey question asked to measure awareness

3.4.5 Scoring

Responses from the items measuring the level of concern were scored as follows: 1 = Strongly disagree, 2 = Disagree, 3 = Neither agree nor disagree, 4 = Agree, and 5 = Strongly agree. As described by Harwell and Gatti (2001), ordinal scale variables are commonly treated as interval scale data for statistical analysis. Additionally, as the benefit of handling ordinal scale data in this manner has been seen in previous research (Knapp, 1990), an equal distance between item response categories was assumed in this study and all Likert item responses that measured the level of concern were summed and handled as interval scale data.

Responses from the questions measuring the level of awareness were scored 1 for a correct answer and 0 for an incorrect or "Don't know" answer. Scores from all six questions in each dimension were summed to determine knowledge levels in that dimension. An overall awareness level was determined by summing the scores in all dimensions to indicate the overall level of participant smart toy security and privacy awareness.

3.4.6 Reliability

Reliability refers to how well surveys measure what they should (Gaur & Gaur, 2009). As this study used multi-item scales to measure a participant's level of concern and level of awareness around smart toy security and privacy risks, the reliability of these scales was evaluated. Cronbach's alpha testing was used to ensure the internal consistency of the scale items. Cronbach's alpha scores for level of concern and level of awareness were .86 and .92, respectively, indicating that the scales used in this study had acceptable internal consistency.

3.4.7 Validity Pre-Testing

As modifying an existing instrument can impact validity, a consultation pre-test was conducted to determine the content and construct validity of the proposed survey questions. A sample of 10 information technology experts participated in the pre-test. This sample consisted of industry professionals, New Zealand Privacy Commission representatives, and postgraduate students

researching information security. Pre-tests of this nature analyse individual items in a scale for suitability and identify items that should be retained for further testing (Howard, 2018).

An item-ranking approach was taken, whereby participants were given construct definitions and asked to evaluate the extent that the item represented the construct using a response scale consisting of “Clearly representative”, “Somewhat representative” and “Not representative”.

A total score was determined for each item and the highest scoring items were retained for use in the pilot survey. Additional feedback was also considered when selecting the final set of questions and led to the following modifications:

- Questions that involved highly specialised technical jargon were removed.
- Questions that were related to the smart toys’ wider environment rather than being specific to the smart toy were removed.
- Unclear questions were reworded.
- Questions that may have ambiguous answers (particularly in the legal section) were reworded to comply with the interpretation of New Zealand legislation.

3.4.8 Pilot Survey

A pilot survey was undertaken with a subset of the target population before full distribution to ensure the questionnaire was clear, straightforward, and unambiguous. SurveyMonkey offers a preview and test mode that allows distribution of a link to the survey to gain comments and feedback, and this was used to conduct the pilot. Feedback from the pilot was incorporated into the final instrument, and included suggestions such as adding examples to clarify terms such as “security risk” and “privacy risk”, and general feedback on font size and layout.

A summary of all feedback collected via the pre-test consultation and the pilot can be found in Appendix C.

3.4.9 Data Collection

The survey was available online for three months for all eligible participants to complete at a convenient time. The data from the survey was collected and stored online as per the SurveyMonkey privacy policy (SurveyMonkey, 2018) until the survey closed. After the survey closed, the data was downloaded to the researcher’s computer for analysis and removed permanently from SurveyMonkey.

3.4.10 Data Preparation and Analysis

Firstly, exploratory data analysis was undertaken on the survey data. This process can provide insights into the underlying structure of the data (Salkind, 2010). Anomalies such as data outliers and unexpected patterns discovered during this process were resolved by data cleaning and processing.

Once the data set was ready, data analysis tools supplied by SurveyMonkey were used to filter and categorise variables. To derive further findings from the data, descriptive statistical analyses were performed using SPSS V26. SPSS was chosen for the data analysis stage due to its straightforward and user-friendly interface. Calculations such as frequencies and means were used to analyse the scale data. Independent *t*-tests and one-way analysis of variance (ANOVA) were used to compare means, and further statistical methods such as Pearson correlations were used to determine any relationships between the variables measured.

3.4.11 Ethics

The survey obtained ethical approval by the AUT Ethics Committee prior to its use (Ethics Application Number 19/27). The survey was anonymous, did not require the respondent to enter any personal information, and participation was completely voluntary. No incentives to participate were given. Data was not shared with any third party, and no data contained any identifying characteristics.

3.5 Smart Toy Security Testing Design

To answer SQ3 and determine what common security and privacy impacting vulnerabilities can be found in smart toys available for purchase by New Zealanders, a physical security testing approach was undertaken. A set of smart toys were systematically assessed against a set of common vulnerabilities known to potentially impact user privacy or safety, to determine if these vulnerabilities were present.

Security testing is a structured process whereby experiments are conducted to determine one or more characteristics of a given object to reveal vulnerabilities in a system. It usually focuses on the verification of common security controls such as authentication, authorisation, confidentiality, integrity, and availability (Scarfone et al., 2008). As the objective of SQ3 was to determine whether any common security vulnerabilities could be found in smart toys, a basic security test methodology was selected as the most appropriate approach for this study.

Renowned security testing literature previously described in Chapter 2 was used to derive the security test methodology. This literature included the NIST Technical Guide to Information Security Testing and Assessment (Scarfone et al., 2008), the Institute for Security and Open Methodologies (ISECOM) OSSTMM (ISECOM, 2009), and the OWASP Testing Guide (OWASP, 2014b).

Each of these frameworks provides generic processes, techniques, and tools to conduct security testing and are designed to be adapted for use in many environments. However, none of these frameworks or methods fully supports IoT testing. The OWASP Testing Guide focuses on web application testing which has features that overlap the IoT environment. The resources within the OWASP Testing Guide were therefore found to most closely align with the scope of testing required for this research, and was chosen as the framework to base the security testing approach for this study on.

The OWASP Testing Guide describes a process for testing at all stages of the SDLC. This research focused on testing operational IoT devices after deployment, and therefore any testing options relevant to product design and development were removed from the process. High-level process steps that were consistent with security testing an IoT device in production were included.

The derived high-level security testing process used in this research is outlined in Figure 3.4.

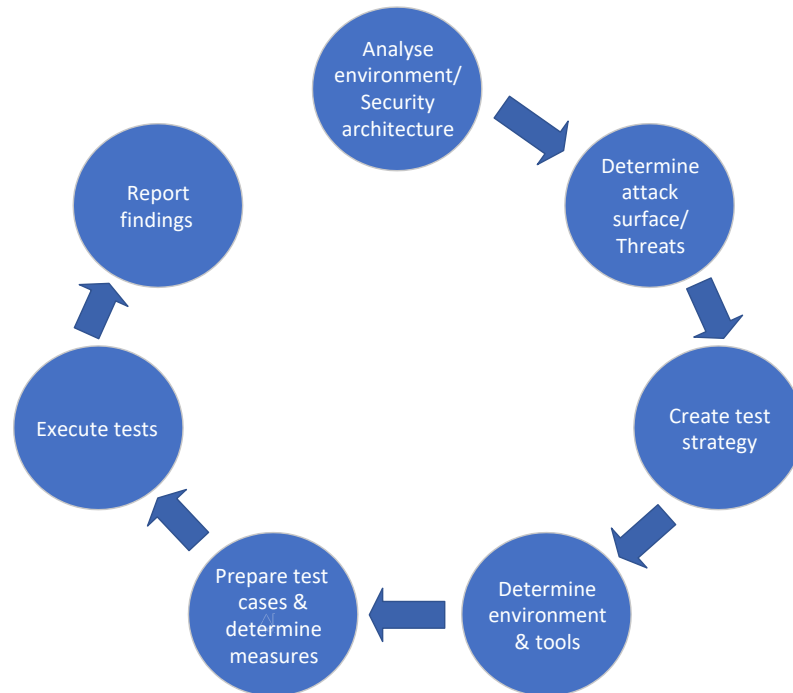


Figure 3.4. The security testing process. Adapted from Testing Guide 4.0 by OWASP, (2014b). CC BY-SA 3.0.

3.5.1 Smart Toy Environment and Attack Surface

As discussed in Chapter 2, the potential attack surface of smart toys (as with many IoT devices) can be large and varied. It includes the physical smart toy, any mobile companion application it interacts with, and any web or additional remote hosts. Additionally, it includes all communication between each of these elements. Each of these interaction points presents an opportunity for vulnerabilities to be found and exploited. Figure 3.5 portrays this environment.

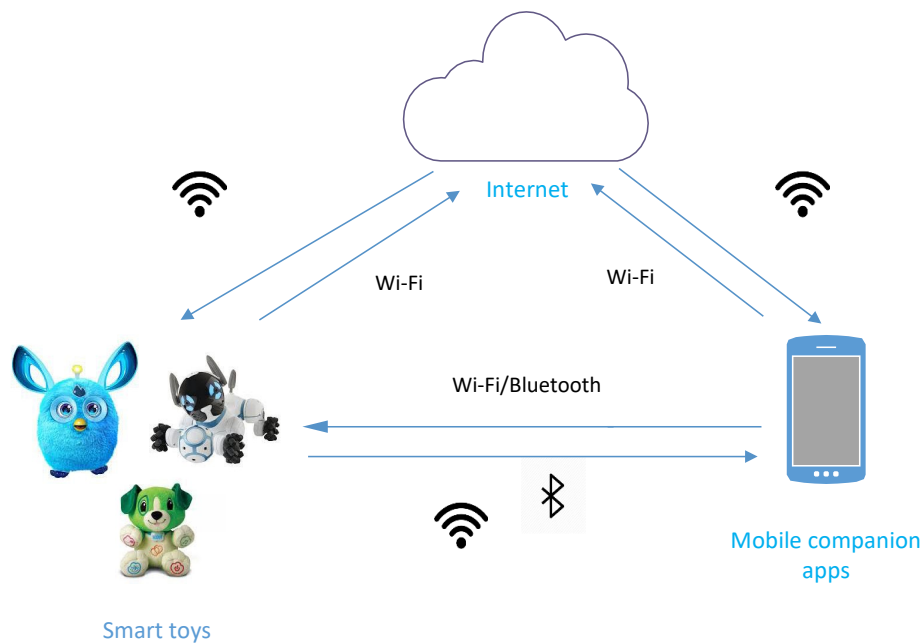


Figure 3.5. The smart toy attack surface

Most smart toys are designed to interact with a mobile companion application, and many include online user accounts to access additional features from related websites. Connection to the internet is often utilised to download content and updates and upload data collected from the toy. The most common communication technologies used are Wi-Fi (802.11) and Bluetooth or BLE (Mahmoud, 2018).

3.5.2 Test Strategy

The high-level objective of the research was to determine *what common security and privacy impacting vulnerabilities are found in smart toys available for purchase by New Zealanders?* Systematic testing of a group of smart toys was undertaken to meet this objective, and verify whether basic security controls that would mitigate the vulnerabilities in scope were operational in the smart toys.

There are many ways in which IoT devices or applications can be vulnerable due to their vast potential attack surfaces and the varied technologies and environments they utilise (OWASP, 2014b). Therefore, it was not feasible to test all areas of the attack surface noted in Figure 3.5 for weaknesses. Attacks are increasingly sophisticated with new vulnerabilities and methods for security breaches discovered daily. Zero-day vulnerabilities, or undiscovered weaknesses such as unpatched software flaws a vendor is unaware of, are one example of why testing for all vulnerabilities is infeasible, as all potential vulnerabilities are not known (Ciampa, 2018). Additionally, the attack surface of the IoT includes areas that are not accessible for examination, such as the security of cloud-based data storage solutions used to store data collected from smart toys, and the vendor or third-party back end APIs.

Therefore, this research defined its scope as:

In scope

- Only common, known IoT vulnerabilities
- Only vulnerabilities that could be investigated using industry-standard tools without a high level of specialised penetration testing knowledge
- Smart toys, devices and applications tested were limited to those outlined in Section 3.5.3

Out of scope

- Any vulnerabilities associated with web and remote hosts beyond user-web account initiation
- Vulnerabilities or security controls that required advanced penetration testing knowledge or rare or proprietary tools

For this research, common vulnerabilities were defined as known vulnerabilities (not obscure or zero-day) which are widely prevalent in IoT systems today. The OWASP Top 10 IoT issues list was consulted to determine the subset of in-scope vulnerabilities. The Top 10 List outlines the most common vulnerabilities and issues impacting IoT devices today (OWASP, 2018). The literature review in Chapter 2 also identified some key common areas of security and privacy weakness found in smart toys overseas, including insecure Bluetooth implementations, insufficient communication encryption, and inadequate privacy policies and parental control mechanisms (Kshetri & Voas, 2018; Mills, 2017; Tung, 2017).

Vulnerability areas on the OWASP Top 10 List that were most relevant for the smart toy environment and that had been seen in previous research of smart toys overseas were included in scope. The resulting vulnerability areas for testing were as follows:

1. Insufficient authentication
2. Insecure data transfer
3. Insufficient privacy protection

Insufficient authentication was defined for this study as the use of weak or easily crackable passwords, the use of well-known factory default or hardcoded passwords that cannot be changed, a lack of account lockout mechanisms, the use of insecure account recovery mechanisms, and the lack of authentication controls. Previous research has shown that smart toys with insufficient authentication vulnerabilities are at risk from unauthorised users who may access the toy and tamper with its features (Taylor & Michael, 2016).

Insecure data transfer was defined as the lack of transport encryption or the use of weak encryption for data transfer. Internationally, smart toys have been found to transfer data

insecurely by not implementing encryption, exposing them to the risk of eavesdropping and data manipulation (Forbrukerradet, 2016).

Numerous studies such as Alonso et al. (2016), Kshetri and Voas (2018), and Mahmoud (2018) have highlighted the risks children are exposed to if sufficient privacy protection controls are not implemented within smart toys. These risks include identity fraud, identity theft, spying, and location tracking. Insufficient privacy protection was therefore defined for this study as the collection of excessive PII or sensitive information, the lack of a comprehensive privacy policy, or the lack of an explicit declaration of data use and data retention policy. Additionally, a lack of parental controls for data removal was considered within this area.

For the purposes of this study, PII is any information that could identify an individual. In the smart toy environment, this could include data such as name, address, gender, email, images, phone numbers, interests, birthdays, payment information, demographic details, location coordinates, and unique device identifiers (Fox & Hoy, 2019). For this research, excessive PII is determined to be any information over and above an email address required to create user accounts and communicate important information to.

The existence of any of these vulnerability areas in the smart toy environment may open the possibility of a user suffering a cyber-attack that breaches their privacy and or safety. Table 3.1 outlines various known cyberattacks for each area of vulnerability explored and the possible impacts.

Table 3.1. In-scope areas of vulnerability with related attacks, attack surfaces, and impacts of an attack

Vulnerability area	Possible attacks	Applicable attack surface	Possible impact
1. Insufficient authentication	<ul style="list-style-type: none"> - Brute force password/passkey hacking - Account enumeration - Unauthorised access 	<ul style="list-style-type: none"> - Smart toy device interface - The mobile companion application interface - Web host interface 	<ul style="list-style-type: none"> - Personal data loss, modification, or corruption - Denial of access - Fraudulent use of user account or personal information
2. Insecure data transfer	<ul style="list-style-type: none"> - Data monitoring and MITM attacks whereby communication data is interrupted, stolen, or spoofed - Packet injection whereby objectionable material is inserted into a communication 	<ul style="list-style-type: none"> - Communication between a smart toy and the web host - Communication between a smart toy and a mobile device 	<ul style="list-style-type: none"> - Breach of privacy - Personal data loss - Full device compromise
3. Insufficient privacy protection	<ul style="list-style-type: none"> - The use of multiple other attack vectors such as insufficient authentication or lack of encryption to view and obtain personal data 	<ul style="list-style-type: none"> - Smart toy set up - Web account establishment - Mobile companion application account establishment 	<ul style="list-style-type: none"> - Information loss due to theft - Information misuse (due to it being sold to unauthorised parties or used for purposes outside of the smart toy agreed scope)

Note. Adapted from OWASP Internet of Things Project Top 10, (2018). CC BY-SA 3.0.

3.5.3 Test Environment and Tools

3.5.3.1 Toy Selection

The smart toys used in this research were selected to represent the wider market, and therefore targeted a range of age groups from younger children through to older children. Only one smart toy was found for this study that marketed to the youngest children, that is, those under three. This may be due to additional regulation, such as rules restricting small parts that exist for any toys intended for use by children under three years of age (CPSC, n.d.). The toys chosen contain functionality representative of smart toys in general, such as wireless communication (Wi-Fi or Bluetooth) and sensors such as microphones and cameras. The toys were all easily found and obtained either locally or internationally via an online search or by in-store browsing in New Zealand.

Smart toys that had undergone previous security testing in international studies were not excluded if they were available to New Zealand consumers, as it was deemed essential to investigate whether vulnerabilities seen in these toys still existed in the toys sold today. Additionally, the scope of testing may have differed between this study and previous studies. A detailed description of each smart toy chosen for this study, including any previous research conducted on the toy can be found in Appendix D.

The smart toys included in this research and the characteristics that led to their inclusion are outlined in Table 3.2.

Table 3.2. Selected smart toys and their characteristics

Smart toy	Target age group					Communication technology			Onboard sensors & AI				Companion application	
	<3 years	3–5 years	6–8 years	9–12 years	>12 years	Wi-Fi	Bluetooth	BLE	Microphone	Camera	GPS	Speech recognition	Android	iOS
Furby Connect		X	X	X				X	X	X	X		X	X
Toymail Talkie		X	X			X			X			X	X	X

Smart toy	Target age group					Communication technology			Onboard sensors & AI				Companion application	
R2-D2 Droid			X	X	X			X		X	X		X	X
Air Hogs FPV High Speed Race Car			X	X	X	X				X	X		X	
Kurio Smart Watch			X	X	X		X		X	X	X		X	
Toy-Fi Teddy	X	X				X			X			X	X	X
StarLily Unicorn			X	X					X		X		X	X
CogniToys Dino		X	X	X		X				X	X	X		X

3.5.3.2 Test Methods

Security objectives can be validated using different testing methods such as code analysis which looks at source code to highlight any security flaws; threat modelling, which focuses on identifying design flaws; and penetration testing which identifies vulnerabilities while in operation (OWASP, 2014b). Additionally, security tests can be classified as “black box” tests where the tester has no knowledge of the target system; “grey box” tests where the tester has some knowledge of the target; or “white box” tests where testers have full access to all code and architecture documentation (Poston, 2019). No single testing or experimentation technique would suffice for effectively investigating each area in scope for this research; however, the techniques that were identified as most suitable for this scope and were therefore utilised for this research were as follows:

- Manual review: Static testing conducted by analysing publicly available documentation

- Penetration testing: Running the smart toy environment to find security vulnerabilities. In this scenario, it was primarily conducted as a black box test as the researcher knew very little about the internal operations of the device or application being tested.

3.5.3.3 *Hardware/Environment Set Up*

The test environment was set up to support the physical toy testing required for this research as follows.

A laptop hosting the Kali Linux OS was used as the primary investigation laptop. This laptop hosted much of the software required for monitoring (sometimes referred to as “sniffing”) and analysing the traffic communicated between the smart toys and their companion applications. Kali Linux, a Debian-based Linux distribution, was selected for this research as it is an open-source OS specifically created to support security testing and penetration (Offensive Security, 2019).

A laptop hosting Windows 10 was used to replicate a home user PC for user account registration on applicable smart toy websites. Windows 10 had more than 75% of the desktop computer market in New Zealand when this research was conducted (StatCounter, 2019a).

The smart toy mobile companion applications were investigated using a Samsung A10 smartphone using Android OS version 9.0. Android version 9.0 was the most commonly used mobile OS in New Zealand at the time this investigation was conducted, and was therefore the most suitable choice (StatCounter, 2019b).

Capturing the communication between the smart toys and any mobile companion application required the use of hardware designed to monitor and capture Wi-Fi and Bluetooth data packets traversing between the devices. As the smart toys selected for testing utilised a variety of communication technologies including Bluetooth Classic, BLE and Wi-Fi, a variety of hardware devices and their accompanying software were required.

Previous research into BLE security including Saundarajan (2017) and Cusack, Antony, Ward and Mody (2017), indicated varying levels of success with BLE sniffing hardware. An analysis of these studies concluded that no single device had performed without challenges, and it was therefore decided that several BLE sniffers would be used to provide the best chance of capturing the level of detail required to determine the smart toy’s Bluetooth security. The BLE sniffers implemented in this method were as follows:

- Ubertooth 1.0 is a fully open source Bluetooth test tool. It was selected for sniffing the BLE traffic between the smart toys and any mobile companion application. It has been used in previous research to capture ongoing conversations between two BLE devices successfully. Ubertooth 1.0 allows data packets captured to be saved as PCAP files for later examination.
- The Bluefruit LE Sniffer nRF51822 from Adafruit was the second BLE sniffer chosen. This device passively captures data exchanges between two BLE devices and pushes

the data into Wireshark where packet-level descriptors enable simple interpretation of the BLE traffic.

- A Cambridge Silicon Radio USB 4.0 dongle was also chosen for its ability to be automatically detected in Kismet.

A TP-LINK TL-WN722N Wi-Fi dongle was used to capture the 802.11 Wi-Fi traffic. This dongle was chosen for its ability to operate in monitor mode and as is recommended for use with Kali Linux.

3.5.3.4 *Software Tools*

For network analysis, Wireshark was utilised to view and decrypt where necessary the network traffic communicated between the smart toys and any companion application. Wireshark is a widely used network protocol analyser and was chosen for its ability to inspect a wide range of protocols, including those used in smart toy communication such as BLE and 802.11 (Wireshark, n.d.). The packets captured using Wireshark were then analysed to observe the pairing and TLS communication practices of the smart toys.

In addition to Wireshark, Kismet was used to detect and view both Bluetooth and wireless traffic. Kismet is an 802.11 open source wireless network monitoring tool and was chosen as it comes as part of the Kali Linux distribution and purports to support the Ubertooth 1.0 as a plug-in with a graphical user interface (Kismet, 2019).

BLE Scanner was also used to investigate the security of the Bluetooth connections between the smart toys and their mobile companion applications. BLE Scanner was chosen as it is an easily obtained and free tool that can be downloaded from the Google Play Store and used with limited expertise. It has a simple display that shows clearly whether the Bluetooth MAC address used by a device is persistent or dynamically changing, and what services the device has exposed.

CrackLE was chosen to be used for its ability to decrypt BLE packets if the prerequisite pairing data is successfully captured. CrackLE works by exploiting a flaw in the BLE pairing mechanism that leaves all communications vulnerable to decryption by passive eavesdropping. It achieves this by brute-forcing the temporary key (TK) used in the pairing modes supported by many IoT BLE devices. Once it has the TK, it can then derive the long-term key (LTK) used to encrypt all subsequent traffic.

Finally, the Aircrack-ng suite of wireless network assessment tools was used within Kali Linux to analyse the Wi-Fi communication of the smart toys. Aircrack-ng is a set of proven open source command-line tools that come pre-installed in many Kali Linux distributions.

3.5.4 Test Case Plan and Measurement

Whilst many standards are still evolving for the IoT, the literature review in Chapter 2 identified that some industry-recognised security standards and guidelines have been published by organisations such as the NIST and the OWASP that apply to smart toy security.

To determine the specific tests to be run and the measurement criteria to be used in each area of vulnerability in scope, a variety of these applicable industry standards were consulted. These included the OWASP Testing Guide (OWASP, 2014b), the NIST Guide to Bluetooth Security (NIST, 2017b), and the NIST Digital Identity Guidelines (NIST, 2017a).

To test for insufficient authentication, the OWASP Testing Guide was initially consulted to identify appropriate general authentication controls and standards for measurement. The criteria for measuring authentication and password strength and length were obtained from the OWASP Testing Guide and the NIST Digital Identity Guidelines. Criteria for measuring Bluetooth and 802.11 Wi-Fi authentication were derived from the NIST Guide to Bluetooth Security and the Wi-Fi Alliance, respectively.

The specific tests and criteria for examining transport encryption vulnerabilities were derived from the OWASP Testing Guide and the NIST Guide to Bluetooth Security. Privacy protection controls and measurement criteria were derived from the OWASP Testing Guide and previous privacy research from Mahmoud et al. (2017).

Each measurement criterion specified reflected recommended levels of security that should be implemented according to relevant industry standards.

3.5.4.1 Scoring

Where a test result met the measurement criteria for that control, the result was recorded as “Meets criteria”. Where a test result did not meet the measurement criteria, the result was recorded as “Does not meet criteria”. If a result indicated partial satisfaction of the criteria, it was recorded as “Partially meets criteria”. Where the measurement criteria for any control could not be tested or validated, the result of the test was recorded as “Unknown”. Not all measurements were applicable for every smart toy, and if a control was not applicable to that device, it was noted as such.

The higher the overall number of “Does not meet criteria” results obtained by a device in any area of vulnerability, the higher the degree of risk the device represented due to fewer security controls being validated.

A description of all tests run and the measurement criteria used for each category can be seen in Table 3.3.

Table 3.3. Security test description, measurement criteria, and test process for each area of vulnerability in scope

Vulnerability area 1: Insufficient authentication		
Basic controls to be tested	Measurement criteria	Tests/Test process
Use of a strong authentication procedure for communication establishment	<ul style="list-style-type: none"> - Bluetooth and BLE devices must pair using AES-CMAC and P-256 elliptic curve (security mode 1, level 3) or LE Secure Connections or security mode 2, level 3 - Wi-Fi (802.11) devices must connect using a secure WPA-PSK or WPA2-PSK authentication protocol 	<p>IA1: Pair/connect smart toy to mobile interface and capture communication traffic</p> <p>IA2: Pair/connect smart toy to the web interface and capture communication traffic</p> <p>IA3: Conduct manual review of public information repositories for associated information</p>
Use of a strong password for authentication	<ul style="list-style-type: none"> - A password is always required for pairing/connection - The minimum password length is to be at least eight characters - Passwords cannot contain the username - Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols 	<p>IB1: Complete initial set up of smart toy and associated user account on mobile interface</p> <p>IB2: Complete initial set up of smart toy and associated user account on the web interface</p> <p>IB3: Connect/login to smart toy and any associated user account on mobile interface</p> <p>IB4: Connect/login to smart toy and any associated user account on the web interface</p> <p>IB5: Conduct manual review of public information repositories for associated information</p>
Use of a secure password recovery mechanism	<ul style="list-style-type: none"> - Valid user account information cannot be determined using password recovery mechanisms - The application responds with an identical error message and length to different incorrect login attempts - Password recovery mechanism message does not reveal if a username is valid or not - Returned page title does not reveal if a username is valid or not 	<p>ID1: Enter invalid username in the web application</p> <p>ID2: Enter an invalid password in the web application</p> <p>ID3: Attempt to recover password using an incorrect username</p> <p>ID4: Attempt to recover password using a valid username</p>

Option to change default username and password	<ul style="list-style-type: none"> - Default username and password, if exists, must be changed during initial setup 	<p>IE1: Complete initial set up of smart toy</p> <p>IE2: Complete initial set up of mobile interface user account</p> <p>IE3: Complete initial set up of smart toy and associated user account on the web interface</p> <p>IE4: Conduct manual search of public repositories for default username/password credentials for device and applications</p>
Use of secure account lockout mechanism	<ul style="list-style-type: none"> - A user account is locked out after 3–5 failed login attempts - User account does not automatically unlock after a pre-determined amount of time 	<p>IF1: Attempt to login to web user account with invalid credentials 3 times before logging in with correct credentials</p> <p>IF2: Repeat the above test using 4 attempts, then 5 attempts until the account is locked out</p> <p>IF3: 5 minutes after account lockout attempt to login with correct credentials</p> <p>IF4: 10 minutes after account lockout attempt to login with correct credentials</p>
Vulnerability area 2: Insecure data transfer		
Basic controls to be tested	Measurement criteria	Tests/Test process
Communication is encrypted	<ul style="list-style-type: none"> - All data is encrypted in transport - No data is transmitted as plain text and no human-readable data can be seen. 	<p>IDA1: Pair/connect the smart toy to mobile interface and capture communication traffic</p> <p>IDA2: Pair/connect the smart toy to the web interface and capture communication traffic</p> <p>IDA3: Use smart toy with a mobile application and capture communication traffic</p> <p>IDA4: Use smart toy with a web interface and capture communication traffic</p>

Secure encryption protocols are used for all communication:	<ul style="list-style-type: none"> - Standard industry-recognised secure protocols are used during data transport (e.g., SSL, TLS) 	<p>IDB1: Pair/connect the smart toy to mobile interface and capture communication traffic for analysis</p> <p>IDB2: Pair/connect the smart toy to the web interface and capture communication traffic for analysis</p> <p>IDB3: Use smart toy with a mobile application and capture communication traffic for analysis</p> <p>IDB4: Use smart toy with a web interface and capture communication traffic for analysis</p>
Vulnerability area 3: Insufficient privacy protection		
Basic controls to be tested	Test criteria	Test process
Reasonable PII collection	<ul style="list-style-type: none"> - Personal data collected is limited to an email address only 	<p>IPA1: Document all data collected during smart toy set up</p> <p>IPA2: Document all data collected during mobile application account set up</p> <p>IPA3: Document all data collected during web interface account set up</p>
Comprehensive privacy policy	<ul style="list-style-type: none"> - A smart toy/device specific privacy policy must be available rather than a generic privacy policy - Where applicable, companion application, website, application store page contains a link to the smart toy privacy policy - Privacy policy contains the date of last update and method to communicate updates to users - Data types collected are identified in the policy - Data retention periods are specified in the policy - Data use outlined in the policy - Location of any data storage is stated in the policy 	<p>IPC1: Review app store for privacy policy</p> <p>IPC2: Review web site for privacy policy</p> <p>IPC3: Review mobile companion application for privacy policy</p> <p>IPC4: Review of privacy policy details</p> <p>IPC5: Conduct manual review of public information repositories for associated information</p>
Privacy support mechanisms	<ul style="list-style-type: none"> - Dedicated support service is available to address privacy concerns with the smart toy or companion app such as a dedicated web page or email contact 	<p>IPD1: Conduct manual review of public information repositories for associated information</p>

Acceptable parental control mechanisms	<ul style="list-style-type: none"> - Parents/guardians can permanently delete any information collected by a smart toy or associated application 	<p>IPE1: Review mobile app interface for data deletion options</p> <p>IPE2: Review web interface for data deletion options</p> <p>IPE3: Review physical toy interface for data deletion options</p> <p>IPE4: Conduct manual review of public information repositories for associated information</p>
Use of random unique identifying device identifier (MAC)	<ul style="list-style-type: none"> - Static MAC or device addresses are not used during a communication session - No PII is visible in the device identifier 	<p>IPF1: Pair/connect the smart toy to mobile interface and capture communication traffic</p> <p>IPF2: Repeat pair/connection process to observe device identification changes</p>

Note: Basic controls adapted from OWASP (2014b). Measurement criteria for Bluetooth authentication from NIST (2017b) and Wi-Fi authentication from Wi-Fi Alliance (n.d.). Measurement criteria for privacy protection controls adapted from Mahmoud et al. (2017). Criteria for all other controls adapted from OWASP (2014b).

3.5.5 Validity and Reliability

The method was derived predominantly through the review of current industry-standard methods and previous similar research to ensure validity. Sundararajan (2017) and Rafferty, Farkhund, et al. (2017) successfully demonstrated the feasibility of capturing data transmitted by IoT devices, and analysing for details around their security implementations by using the devices and software proposed in this study. While most previous research focused on other types of IoT devices, each tool selected for use in this method was previously used to obtain successful results. Mahmoud et al. (2017) showed in their research that the use of a clear set of criteria could be used to evaluate the privacy practices of smart toys. To ensure validity, this research design used a clear set of privacy criteria inspired both by previous research outlined in Chapter 2 on privacy concerns within the IoT, and by the privacy framework outlined by Mahmoud et al. (2017).

Each test performed in this method was executed multiple times to confirm the reliability of the approach, and all the results gleaned from the use of the method outlined in this chapter can be replicated with the use of similar devices and software.

3.6 Conclusion

Chapter 3 presented the proposed research methodologies to be undertaken in this study. The chapter outlined the main research question, sub-questions, and hypothesis posed. The methodology design, data collection, and analysis approach were discussed. Chapter 4 reports the findings obtained from the online survey and the physical security testing methods.

Chapter 4: Findings

4.1 Introduction

Chapter 3 established a research methodology for investigating the security and privacy of smart toys in New Zealand. The main research question and sub-questions were formed based on the review of relevant literature undertaken in Chapter 2, that identified potential security and privacy risks around smart toys, and a lack of understanding of these issues in the New Zealand context.

This chapter presents the findings obtained from the investigations into smart toy privacy and security in New Zealand. Section 4.2 discusses the results of the online survey conducted to determine levels of concern and awareness amongst New Zealand parents/guardians regarding smart toy privacy and security. Section 4.3 presents the findings from the physical security testing of a group of smart toys.

4.2 Survey Findings

This section presents the findings from the survey questions and begins with a description of the completion rate and initial data cleaning. A summary of the main findings is presented in a graphical and narrative format. These findings include the outcomes of statistical analyses performed on the data to identify any relationships and trends within the data set that may allow for further understanding of the findings and help answer the research questions.

4.2.1 Completion Rate and Exploratory Data Analysis

The survey was available online and open for participation by eligible New Zealand parents/guardians from February, 2019 to April, 2019. Over this period, a total of 428 responses were collected containing 394 completed responses, leading to a completion rate of 92%.

During the exploratory data analysis phase, incomplete responses were removed to avoid using a data set containing missing values for analysis that may skew the findings. A total of 394 completed responses was deemed sufficient to meet the previously calculated target of a representative sample of 385, and therefore, a representative sample of 394 completed responses was used for analysis.

4.2.2 Summary of Findings

This section presents a summary of the findings from the survey questions beginning with the qualification and demographic questions. The findings from survey questions that addressed the level of smart toy privacy and security concern of New Zealand parents/guardians are presented next. This is followed by the findings from the five knowledge dimensions that measured the level of smart toy privacy and security awareness of New Zealand parents/guardians. Finally, the results of the statistical analyses to discover relationships between the main variables is presented. These results are used to investigate the hypothesis that respondents who show a higher level of concern will have a corresponding higher level of awareness around smart toy security and privacy risks.

4.2.2.1 Qualifying Questions

Two questions were asked at the beginning of the survey. These questions were designed to disqualify anyone who was not eligible to complete the survey. As a result of the responses to these questions, five participants were disqualified as they did not reside in New Zealand, and a further 15 were disqualified as they were not the parent or guardian of a child.

4.2.2.2 Demographic Information

Two questions were asked in order to gather demographic information about the respondents. This information was then used in later analysis to identify any differences between the demographic groups and their levels of smart toy privacy and security concern and awareness.

As can be seen in Table 4.1, a higher percentage of females responded to the survey than males, and no participants identified as being gender diverse.

Table 4.1. Participant demographics – Gender

<i>Gender</i>	<i>Response (%)</i>	<i>Response (N = 394)</i>
<i>Male</i>	39.09	154
<i>Female</i>	60.91	240
<i>Gender diverse</i>	0.00	0

Participants were then asked to identify their level of highest education completed. Figure 4.1 shows a relatively even distribution of respondents across all levels of education, with the highest response rate (28.17%, $n = 111$) coming from those who had completed a university degree qualification.

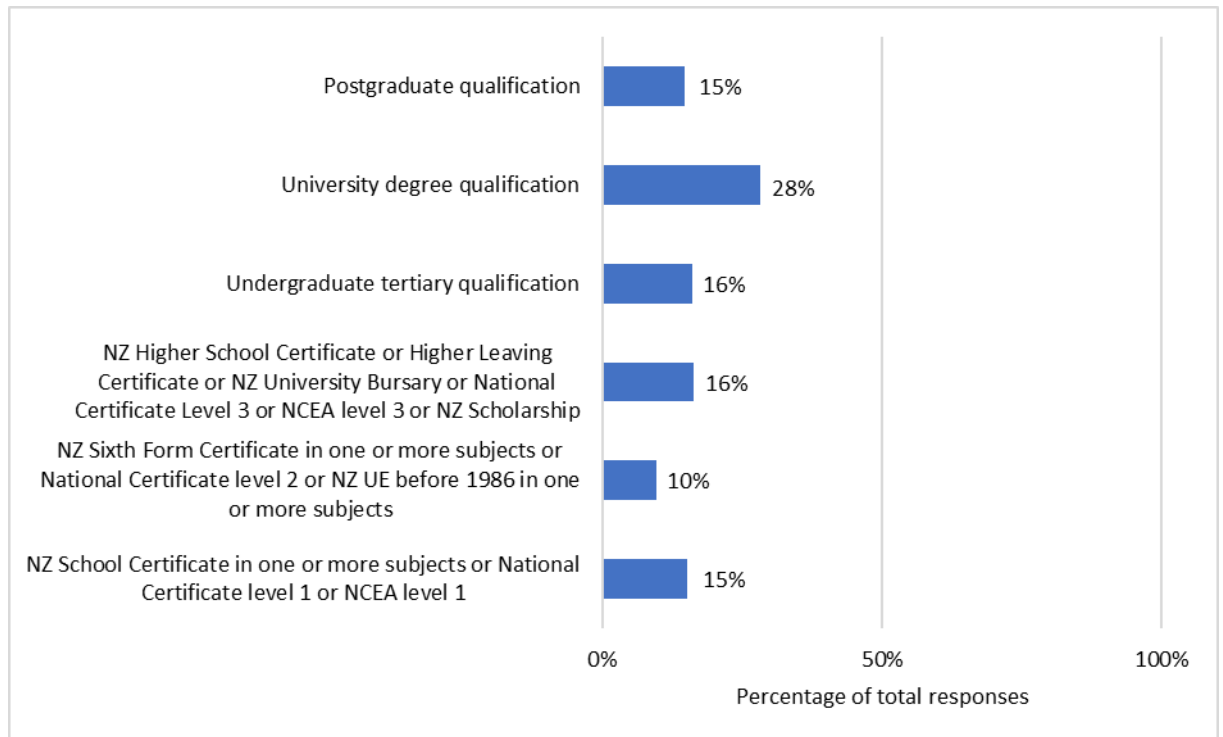


Figure 4.1. Highest level of education as reported by the participants

4.2.2.3 Level of Concern

A primary goal of this research was to determine the current levels of concern that New Zealand parents/guardians have around smart toy security and privacy risks. This section presents the findings from this investigation. The questions in this section of the survey aimed to gain insight into whether participants were concerned about the security risks or the privacy risks of smart toy use.

The participants were asked two questions around concern:

1. I am concerned about the security risks of using smart toys (such as a stranger taking control of my device)
2. I am concerned about the privacy risks of using smart toys (such as my personal information being stolen or misused)

As shown in Figure 4.2, the findings from question one indicated a high average level of concern ($M = 4.14$, $SD = 0.93$) from the participants around the security risks of using smart toys. Similarly, the participants' responses showed a high average level of concern ($M = 4.13$, $SD = 0.88$) around the privacy risks of using smart toys.

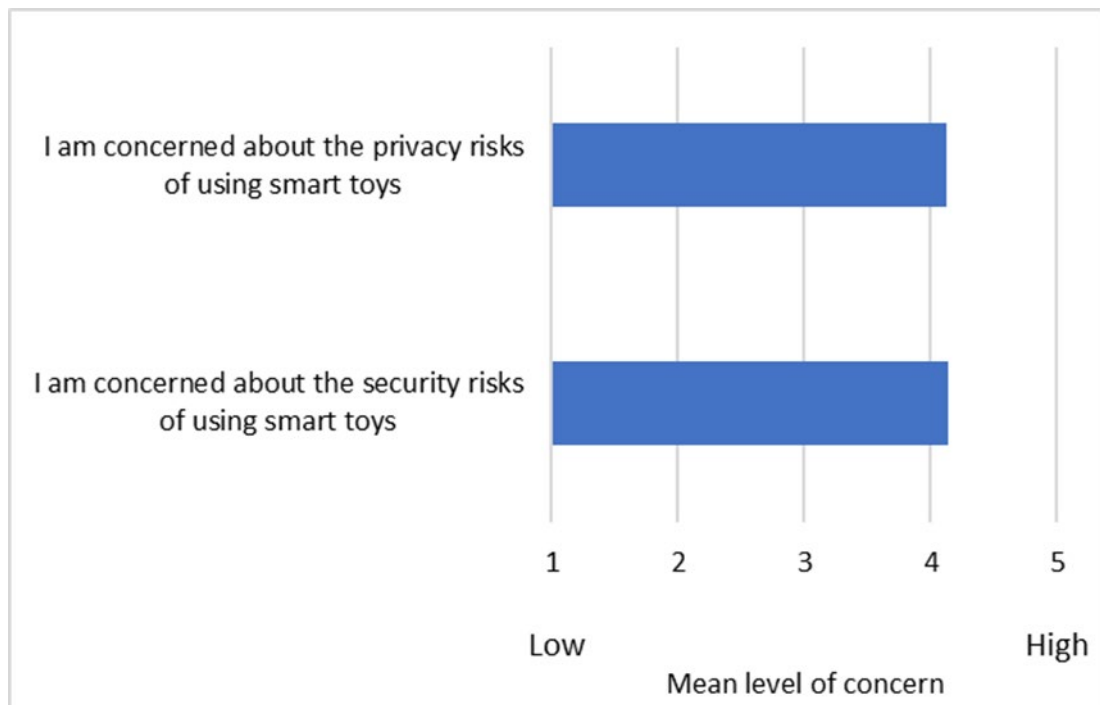


Figure 4.2. Average level of participant concern around the security and privacy risks of using smart toys

Overall Participant Level of Concern

Findings from both questions were summed to determine the overall level of concern around the security and privacy risks of using smart toys. The results found a high average level of concern from the respondents ($M = 8.26$, $SD = 1.70$) regarding smart toy security and privacy risks.

An independent *t*-test found that the level of concern measured from the male respondents ($M = 8.34$, $SD = 1.72$) was not significantly different to those of the female respondents ($M = 8.23$; $SD = 1.70$): $t(392) = .628$; $p = .53$, Cohen's $d = 0.06$.

Similarly, a one-way ANOVA indicated there were no significant differences in the participants' level of concern in respect to their level of education ($F(5, 388) = 1.73$, $p = .13$).

4.2.2.4 Level of Awareness

As the literature review in Chapter 2 described, levels of security and privacy risk can be associated with levels of user awareness (Öğütçü et al., 2016). Therefore, the next section of the survey consisted of 30 questions that aimed to gain insights into the level of smart toy security and privacy awareness that New Zealand parents/guardians have. These questions measured factual knowledge in five different knowledge dimensions. Each dimension consisted of six questions and required the participant to select a response of "True", "False", or "Don't know".

Dimension 1 – Knowledge of Smart Toy Technical Capabilities

The first dimension was designed to measure a participant's knowledge of the technical capabilities of smart toys. Having strong knowledge of what a smart toy can do, may allow a user to mitigate any risks specific to these capabilities. For example, knowing that a smart toy may contain a microphone would allow the user the choice to moderate their conversations whilst the toy was in use.

Summary of Findings

When responding to the questions around smart toy technical capabilities, the majority of participants correctly identified that a smart toy can be equipped with a microphone or camera (83%, $n = 328$) and most were also aware that smart toys use Wi-Fi or Bluetooth to transmit data to other devices (82%, $n = 322$).

However, as seen in Figure 4.3, awareness was much poorer in relation to internet connectivity and the use of sensors. Just over half of the participants (59%, $n = 231$) were aware that smart toys may use sensors to determine who is playing with them, and only 50% ($n = 199$) of participants knew that a smart toy may remain connected to the internet even when not switched on.

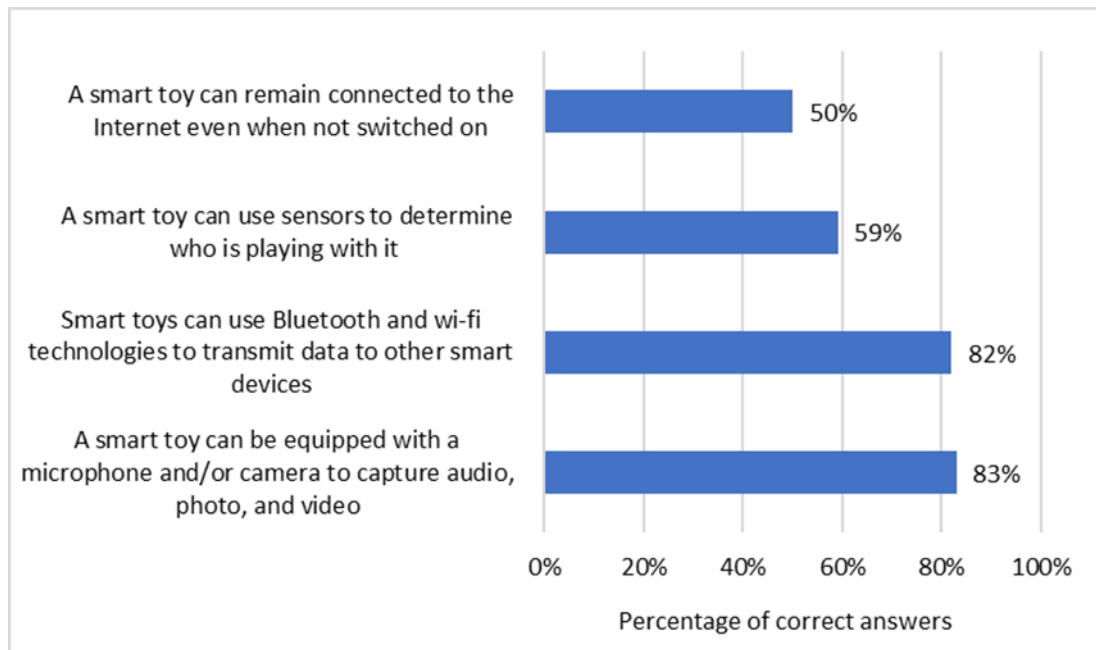


Figure 4.3. Percentage of correct answers received for questions in dimension 1 around participants knowledge of smart toy technical capabilities

Overall in this dimension, the participants answered an average of 3.9 out of 6 questions correctly ($SD = 1.7$), indicating a moderate level of awareness around smart toy technical capabilities.

An independent t -test showed that males ($M = 4.3$, $SD = 1.5$) had a significantly higher level of awareness in this dimension than females ($M = 3.6$, $SD = 1.76$): $t(362) = 4.169$; $p < 0.01$, Cohen's $d = 0.42$, a small effect.

A one-way ANOVA test with Tukey post hoc tests also determined that on average, participants with higher levels of education such as a postgraduate qualifications answered more questions correctly ($M = 4.50$, $SD = 1.23$), than those with lower levels of education such as New Zealand School Certificate ($M = 3.21$, $SD = 1.97$), thereby demonstrating a higher level of awareness around the technical capabilities of smart toys ($F(5, 388) = 4.62$, $p < .001$, $\eta_p^2 = .06$).

Dimension 2 – Knowledge of Potential Smart Toy Security and Privacy Risks

Research has shown that smart toys can contain vulnerabilities which may expose a user to security and privacy risks (Mills, 2017). Knowledge of these vulnerabilities and potential risks could allow the use of relevant protection strategies, and therefore, the second dimension was designed to measure a participant's knowledge of potential smart toy security and privacy risks and vulnerabilities.

Summary of Findings

The findings from these questions indicate a gap in knowledge around smart toy risks and vulnerabilities. For each question in this dimension, between 20% ($n = 83$) and 41% ($n = 162$) of participants selected "Don't know" as their response.

Additionally, as shown in Figure 4.4, some of the common risks associated with using smart toys were not well known, with less than half (44%, $n = 183$) of the respondents being aware that smart toy content can be intercepted and changed, and only 13% ($n = 51$) of respondents being aware that not all smart toys can receive security updates.

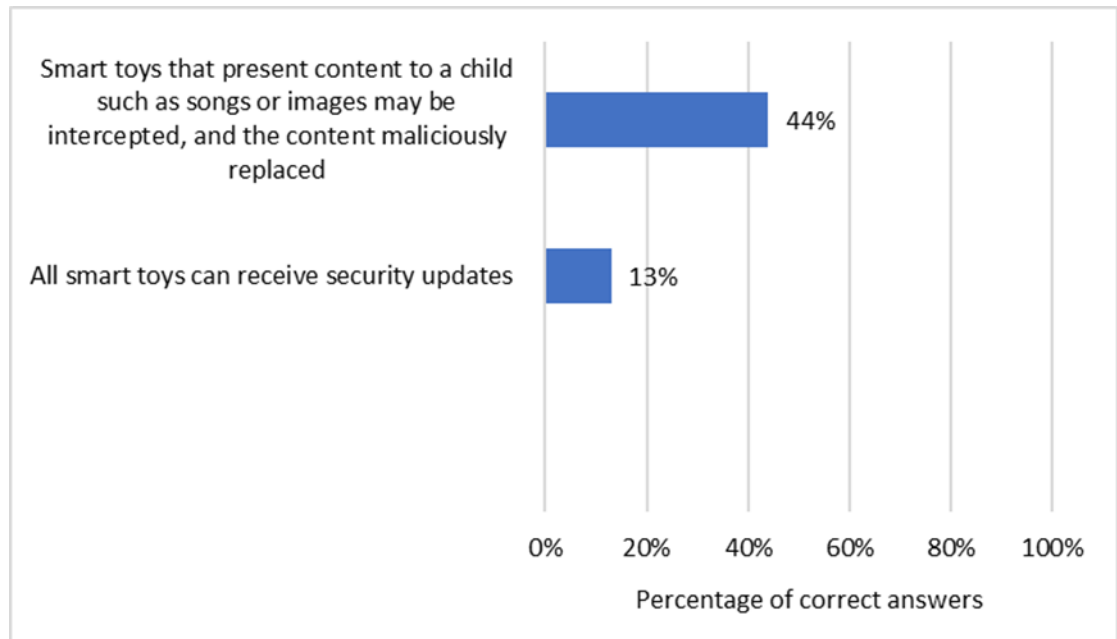


Figure 4.4. Percentage of correct answers received for questions in dimension 2 around participants knowledge of smart toy security and privacy risks

Overall, the participants answered an average of 3 out of 6 questions correctly ($SD = 1.76$) around potential smart toy security and privacy risks and vulnerabilities.

An independent t -test showed that the level of awareness measured from the male responses in this dimension ($M = 3.5$, $SD = 1.5$) was significantly higher than the level of awareness measured from the female responses ($M = 2.6$, $SD = 1.78$): $t(352) = 5.236$; $p < .001$ (two-tailed). Cohen's $d = 0.53$, a medium effect.

Additionally, results from conducting an ANOVA with Tukey post hoc analysis indicated that on average, the number of questions answered correctly was significantly higher for participants holding a university degree ($M = 3.61$, $SD = 1.70$) than those with lower levels of education such as a New Zealand School Certificate ($M = 2.42$, $SD = 1.89$) or Sixth Form certificate ($M = 2.21$, $SD = 1.70$) ($F(5, 388) = 6.30$, $p < .001$, $\eta_p^2 = .08$).

Dimension 3 – Knowledge of the Data Procedures Used by Smart Toy Companies

The third dimension was designed to measure a participant's knowledge of the data procedures used by smart toy and affiliate companies. This included knowledge around how a smart toy company may use a consumer's personal information.

Summary of Findings

Whilst 42% ($n = 166$) of participants were aware that a smart toy company could send their child's data abroad, an equal percentage of participants (42%, $n = 164$) did not know if this was

true. This demonstrated a lack of understanding of how smart toy companies may handle data. Despite many well-known toy companies being located offshore, the remaining 16% ($n = 64$) of respondents believed their child's data could not be sent overseas.

Just over half (54%, $n = 213$) of the participants were aware that a smart toy company might sell their data to third-party organisations, and 66% ($n = 262$) believed a smart toy company might store any personal data they collect for an indefinite duration.

The overall results for this dimension indicate a low level of knowledge around the data procedures of smart toy companies and their affiliates. On average, participants only answered 2.4 questions out of 6 ($SD = 1.75$) correctly in this area. Additionally, over one-third (34%, $n = 803$) of the total responses received from the participants in this dimension was "Don't know". This indicates a significant gap in participants' knowledge regarding smart toy company data procedures.

An independent t -test for this dimension showed a small but still significant difference in the results between genders, with males answering an average of 2.8 questions correctly and females an average of 2.1. ($M = 2.8$, $SD = 1.69$): $t(392) = 3.930$; $p < .001$. Cohen's $d = 0.41$, a small effect.

An ANOVA test concluded that the effect of level of education on the level of awareness in this dimension was significant ($F(5, 388) = 4.02$, $p = .001$, $\eta_p^2 = .05$). Tukey post hoc analysis indicated that participants who had a higher level of education such as a postgraduate qualification answered more questions correctly ($M = 2.91$, $SD = 1.65$) than participants with a lower level of education such as New Zealand Sixth Form Certificate ($M = 1.66$, $SD = 1.40$).

Dimension 4 – Knowledge of Data Protection, Privacy Laws, and Legal Aspects

The fourth dimension was designed to measure a participant's knowledge of data protection, privacy laws, and relevant New Zealand legislation. An awareness of the protection afforded a consumer under New Zealand law could enable them to make more educated judgements regarding sharing their data and maintaining their privacy when using smart toys.

Summary of Findings

Although New Zealand law is only applicable to companies seen to be operating within New Zealand, over 50% ($n = 211$) of participants incorrectly believed that the New Zealand Privacy Act 1993 would stop all international toy companies from misusing their data. In addition to this, almost half of the participants (49%, $n = 192$) believed that all smart toys purchased online must comply with the New Zealand Privacy Act 1993. These results demonstrated a lack of awareness around the jurisdictional issues that arise in an increasingly international marketplace, where a purchaser may reside in one country and the manufacturer and sales agent may reside in another and therefore operate under a different set of privacy legislation.

Over half of the participants (56%, $n = 221$) also incorrectly believed that all smart toy companies operating in New Zealand were legally obligated to tell you if your data has been breached, despite this legislation not being in place in New Zealand at the time of this survey.

The overall results for this dimension indicated a lack of understanding around the privacy protections afforded by New Zealand law. On average, respondents answered only 1.3 out of 6 questions correctly ($SD = 1.13$).

When the responses for all questions in this category were summed, it was found that 43% ($n = 1,021$) of the total responses received were incorrect. This suggests a belief by the participants that New Zealand legislation will protect the data privacy of smart toy consumers more than it is currently designed to do. The “Don’t know” category received 35% ($n = 827$) of the total responses for this dimension, leaving the percentage of accurate responses for dimension 4 at less than a quarter overall (22%).

In this dimension there was no significant difference in the level of knowledge between male and female respondents, with both genders answering a similarly low average number of questions correctly ($M = 1.3$, $SD = 1.19$): $t(392) = .029$; $p = 0.97$. Cohen’s $d = 0.00$.

Analysis of variance testing also concluded that the participants’ level of education had no significant effect on the level of awareness in this dimension ($F(5, 388) = 1.36$, $p > .05$). All participants showed a low level of knowledge around data protection and privacy laws and legal aspects.

Dimension 5 – Knowledge of Security and Privacy Protection Strategies

The fifth and final dimension was designed to measure a participant’s knowledge of security and privacy protection strategies, and therefore, whether they had the required knowledge to protect themselves from smart toy risks.

Summary of Findings

The responses in this dimension showed that the participants did have knowledge of privacy protection strategies, with the majority of participants accurately identifying that they should disable Bluetooth when not in use (77%, $n = 302$), to not use easy to remember details in their passwords (72%, $n = 171$), and limit the information they disclose to toy companies (81%, $n = 319$) to protect their privacy.

However, despite a good level of knowledge around general privacy protection strategies, when responding to questions related more specifically to protection strategies for newer smart toy technology, the overall percentage of “Don’t know” responses was high. For example, when responding to questions such as whether to disable remote viewing, 34% ($n = 134$) selected “Don’t know”, and when asked about the impact of disabling default location tracking, 38% ($n = 181$) chose a “Don’t know” response.

When compared to the other four dimensions, participants demonstrated the highest overall level of knowledge for this dimension, correctly answering an average of 3.9 questions out of 6 ($SD = 1.51$) about personal protection strategies.

Once again, an independent t -test showed a significant difference between the mean results of male and female participants in this dimension. The level of awareness measured from males

($M = 4.1$, $SD = 1.51$) was significantly higher than the level of awareness measured from females ($M = 3.7$, $SD = 1.51$): $t(392) = 1.974$; $p = 0.049$ (two-tailed). Cohen's $d = 0.23$, a small effect.

Analysis of variance testing with additional Tukey post hoc tests found once again that awareness levels regarding personal protection strategies were higher in participants with higher levels of education ($F(5, 388) = 5.49$, $p < .00$, $\eta_p^2 = .07$). Participants with postgraduate qualifications answered an average of 4.6 questions correctly ($SD = 0.99$), whilst those with New Zealand School Certificate only answered an average of 3.4 ($SD = 1.8$) questions correctly regarding personal protection strategies.

Overall Participant Awareness Level of Smart Toy Privacy and Security Risks

The total number of accurate responses across all five dimensions measured were summed to determine the participants' overall awareness levels regarding smart toy security and privacy risks. The average number of questions that were accurately answered by the participants in this section was 14.5 out of a possible 30 ($SD = 5.66$).

Male participants showed significantly higher levels of overall knowledge than females ($M = 16.1$, $SD = 4.9$) $F = 13.5$; $SD = 5.9$: $t(392) = 4.567$; $p < .001$. Cohen's $d = 0.48$, a small effect). As can be seen in Figure 4.5, participants with a higher level of education such as those with a university degree or postgraduate qualification showed significantly higher levels of awareness overall than participants whose highest level of education was lower such as New Zealand School Certificate or Sixth Form Certificate ($F(5, 388) = 6.99$, $p < .001$, $\eta_p^2 = .08$).

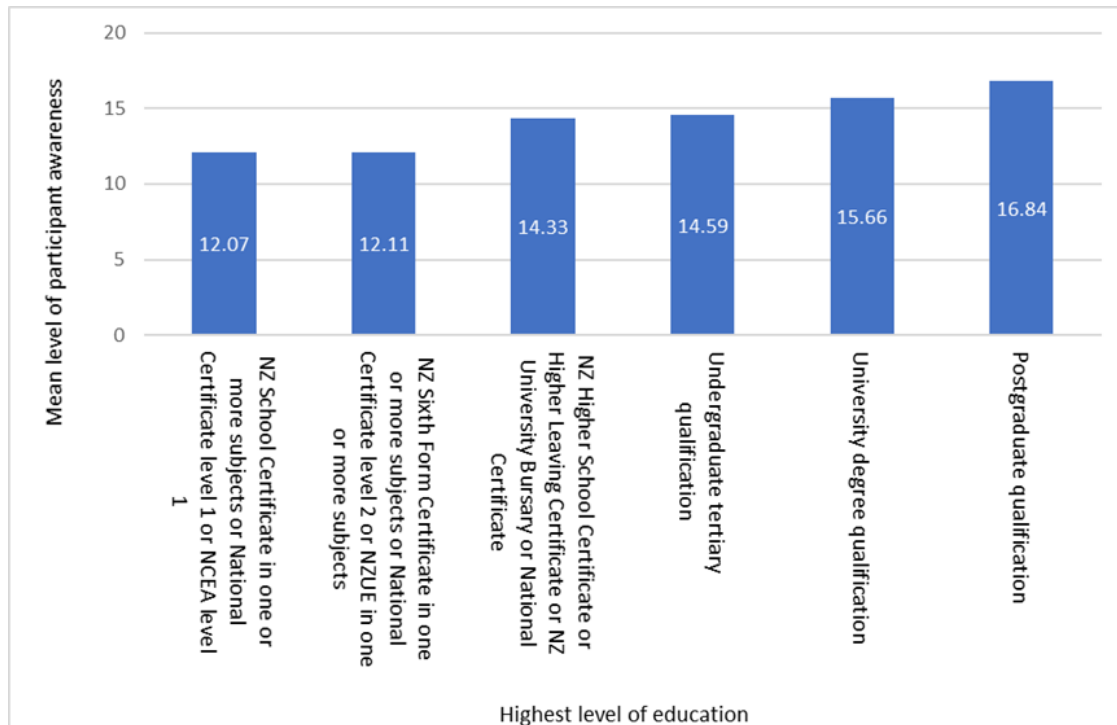


Figure 4.5. Overall average level of participant knowledge seen across all dimensions by the highest level of education completed

As seen in Figure 4.6, knowledge in areas such as the technical capabilities of smart toys and personal protection strategies was much higher than the level of knowledge demonstrated

around company data procedures and the legal aspects of privacy protection. This highlighted specific areas where focused education may lift overall awareness levels.

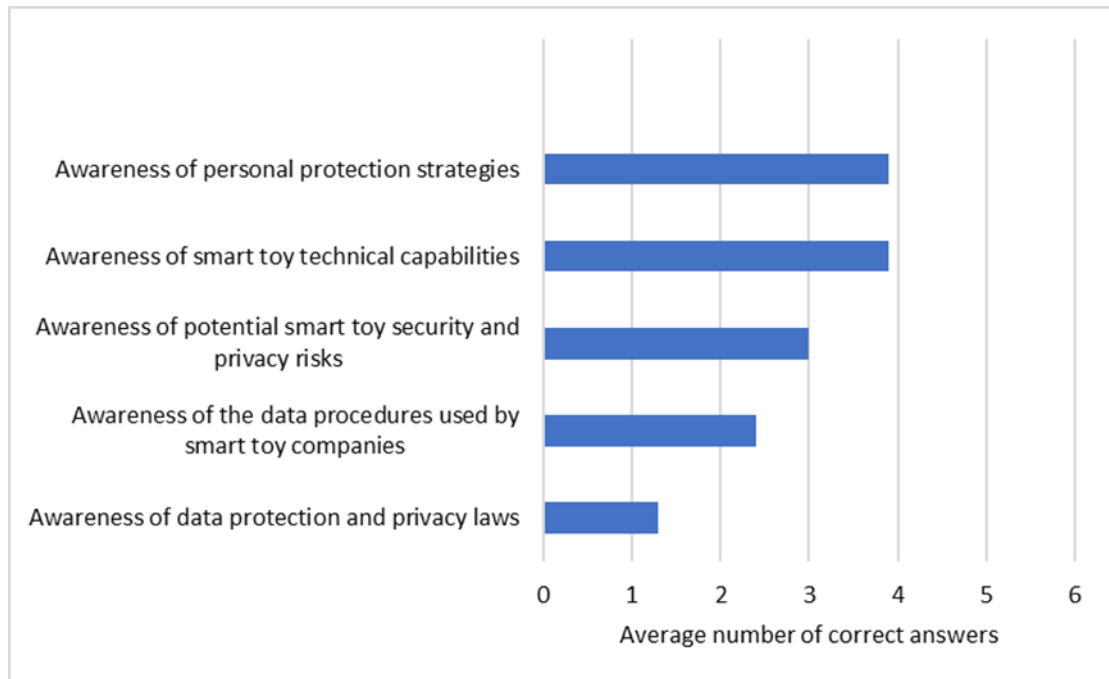


Figure 4.6. Average level of participant awareness in each knowledge dimension

In conclusion, the overall low average of accurately answered questions in this survey suggests a low overall level of awareness regarding the security and privacy risks when using smart toys.

4.2.2.5 Hypothesis Testing

In Chapter 3 it was hypothesised that a higher level of concern around the security and privacy risks of using smart toys would correlate to higher levels of awareness regarding these risks.

A Pearson correlation was conducted to determine whether a correlation existed between a participant's level of concern and their level of awareness around these risks. The results of this statistical analysis found that as hypothesised, there was a small, but significant, positive correlation between the participants level of concern and their level of awareness ($r = 0.17$, $n = 394$; $p < .01$). This indicated that those participants with higher levels of concern around smart toy privacy and security risks also had higher levels of knowledge around the privacy and security risks of using smart toys.

4.3 Smart Toy Security Testing Findings

This section presents the findings obtained from the physical security testing undertaken on a sample of smart toys. Section 4.3.1 describes the results from evaluating the smart toys for security controls in the first area of vulnerability in scope - insufficient authentication. Section 4.3.2 outlines the findings for the second area in scope - insecure transport, and finally, Section 4.3.3 describes the findings from assessing the smart toys security controls in the area of privacy

protection. Test exclusions are presented in Section 4.3.4 and an overall summary of all findings is provided in Section 4.3.5.

4.3.1 Vulnerability Area 1 – Insufficient Authentication

Authentication involves securely verifying who is at the other end of any communication link. It usually involves some form of authentication procedure to establish trust between two devices before communication begins.

Several techniques were used to investigate the authentication security of smart toys. A review was undertaken of any publicly available documentation available about the authentication process used by each toy. This review provided initial clues as to the technologies utilised by each toy, and directed the method to be used for further investigation.

For smart toy to mobile application communication authentication, the connection process was performed repeatedly and reviewed. This involved passively sniffing the connection event, capturing the packets involved in this process, and inspecting them using a packet analysis tool.

For testing user account authentication of a web or mobile application associated with the smart toy, various processes in the user account lifecycle were recreated and evaluated for security controls.

A summary of the overall findings for this vulnerability area can be seen in Table 4.2.

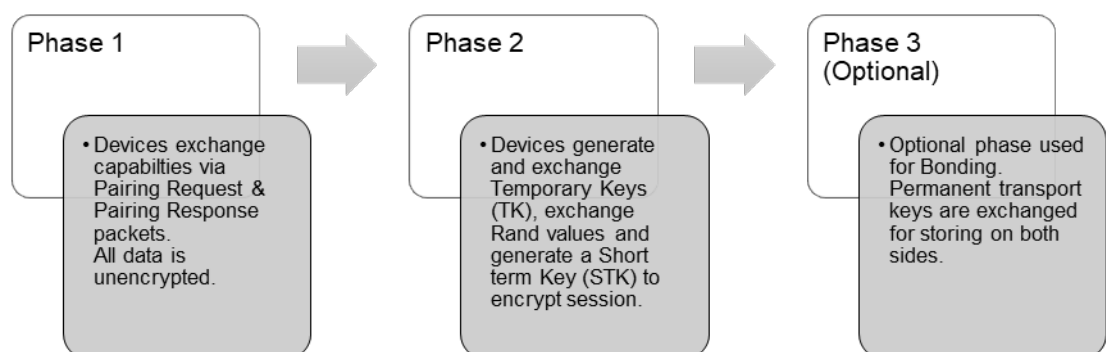
Table 4.2. Summary of findings in vulnerability area 1 – Insufficient authentication

Smart toy	<i>Use of strong authentication procedure</i>	<i>Use of strong password</i>	<i>Use of secure password recovery</i>	<i>Option to change the default password</i>	<i>Secure account lockout</i>
<i>Furby Connect</i>	N	N/A	N/A	N/A	N/A
<i>Toy Mail Talkie Unicorn</i>	M	M	M	N/A	N
<i>R2-D2 Droid</i>	N	N/A	N/A	N/A	N/A
<i>Kurio Smart Watch</i>	U	N	N/A	N/A	N/A
<i>Air Hogs FPV High Speed Race Car</i>	N	N/A	N/A	N/A	N/A

Note: M = Meets control, N = Did not meet control, P = Partially meets control, U = Unknown, N/A = Not applicable.

Static analysis of the smart toys found that Furby Connect and the R2-D2 Droid utilised BLE to establish a connection and communicate with their respective companion mobile applications. A review of available documentation, however, did not reveal what, if any, security mechanisms were utilised by each toy for authentication. This lack of documentation meant it was necessary to investigate the process at the packet level, and also highlighted how difficult it is for a parent/guardian to determine the security level of any toy purchased.

Authentication in Bluetooth is usually achieved by a security procedure called pairing. Pairing involves an exchange of Security Manager Protocol packets between the two devices to generate a short term key (STK) on both sides. This key is then used to encrypt the link. As displayed in Figure 4.7, the pairing process may optionally continue to a further procedure called “bonding”, which generates and exchanges permanent security keys for data encryption (Bluetooth SIG, 2019).

**Figure 4.7.** The BLE pairing process

Bluetooth SIG (2019) describes four pairing procedures for generating an STK, with each providing different levels of security:

1. Numeric comparison: In this method, both devices display an identical six-digit value which the user is asked to compare and if they are the same, agree to connect. In LE Legacy Pairing, this method offers no protection against passive eavesdropping and MITM attacks. In standard Bluetooth pairing, this method provides some protection from MITM attacks.
2. Just works: In this pairing method, the STK is generated using a known TK (often zero) and communicated in plain text on both sides. This method offers no protection against passive eavesdropping or MITM attacks.
3. Passkey display: One device displays a randomly generated number which must be entered on the other device to pair. This method offers protection against MITM attacks.
4. Out of band: In this method additional pairing data is transferred via a method other than BLE such as NFC. This method offers protection against MITM attacks.

BLE devices determine the pairing method they will use in a communication session by sharing Attribute Protocol (ATT) values at layer 4 in the Bluetooth protocol stack, as seen in Figure 4.8.

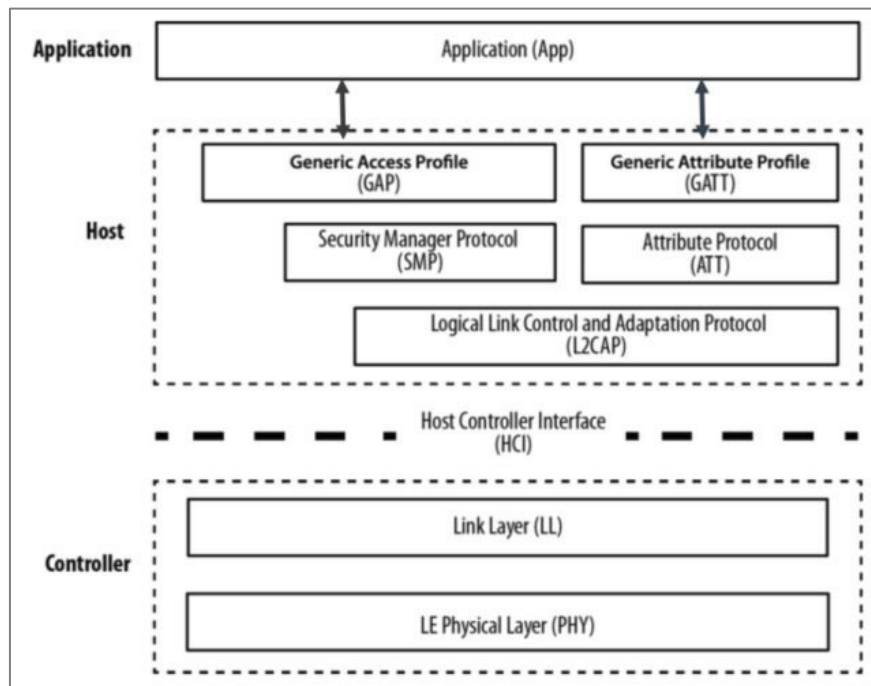


Figure 4.8. The BLE protocol stack. Reprinted from multihop real-time communication over BLE industrial wireless mesh networks by L. Leonardi, 2018, IEEE Access, 4 (1).

Neither of the smart toys using BLE in this study had user input ability, and the pairing instructions given for these toys did not involve utilising NFC or any other method for data transfer. It was therefore determined by initial inspection that they used the “just works” method for pairing. To confirm this method, packet inspection was required.

In addition to a pairing method, a Bluetooth connection also operates in one of two possible security modes. The security mode used is determined as part of the pairing process. There are also three possible BLE security levels as follows:

Security mode 1 – Security is enforced via encryption

- Level 1: No security, the link is not encrypted.
- Level 2: Unauthenticated encryption is used. Encryption standard used is AES-CMAC.
- Level 3 or Secure Connections Only mode: Authenticated encryption is used via ECDH public key cryptography.

Security mode 2 – The use of data signing enforces security

- Level 1: Unauthenticated data signing is used.
- Level 2: Authenticated data signing is used (Townsend et al., 2014).

To confirm that the pairing method used by Furby Connect and the R2-D2 Droid was “just works” and to determine the security mode and level implemented for authentication, it was necessary to review the pairing process at the packet level. This pairing communication was captured using both the Adafruit BluefruitV2 sniffer and the Ubertooth1. Figure 4.9 shows the Adafruit BluefruitV2 (left) and the Ubertooth1 (right) devices used.

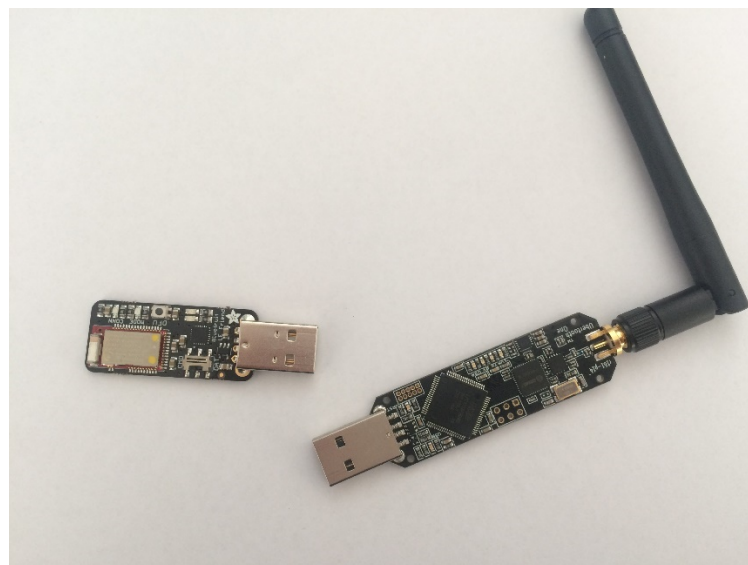


Figure 4.9. The Adafruit BluefruitV2 BLE sniffer and the Ubertooth1

Every Bluetooth device has an address that uniquely identifies itself to other Bluetooth devices called the Bluetooth device address (BD_ADDR). Two types of device addresses may be used as follows:

- A public device address which is a fixed, factory-programmed device address that is registered with the IEEE registration authority and never changes.

- A random device address which is either dynamically generated at runtime or pre-programmed on the device (Townsend et al., 2014).

In order to follow a connection and capture the packets communicated only by the target device, it was first necessary to find the unique BD_ADDR for each smart toy.

Each of the sniffing tools detected many Bluetooth devices when scanning Bluetooth advertising spectrum channels 37, 38, and 39. This spectrum noise made identifying the correct BD_ADDR for each smart toy a challenge. It was determined that the Kismet user interface most clearly outlined the device name and linked this with the BD_ADDR (MAC) as shown in Figure 4.10, and Kismet was therefore subsequently used to determine all smart toy BD_ADDRs.

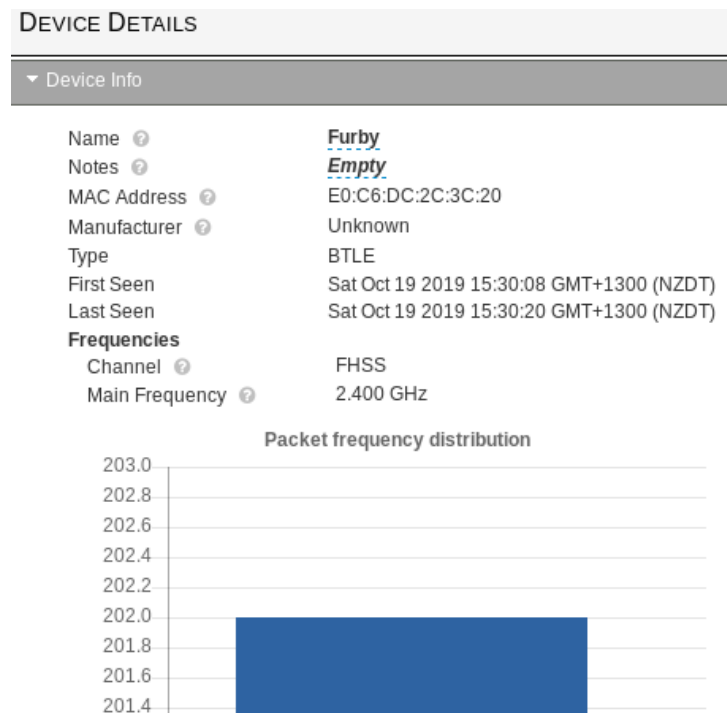


Figure 4.10. Kismet display of Furby Connect device name and MAC address details

The BD_ADDR was then used to limit the packets monitored by the sniffer to just those sent to and from the target smart toy. The Ubertooth1 seen in Figure 4.11 was initially used to sniff the connection and pairing process of each toy. After attempting the pairing process 10 times with the first smart toy, it was determined that using channel 38 captured the most traffic, and future packet capture attempts were thereafter limited using the following commands:

Ubertooth -btle -t eo:c6:dc:2c:3c:20 (-t used to limit the target BD_ADDR to the smart toy, in this case, Furby Connect)

Ubertooth -btle -f -A 38 -r FileName01.pcap (-f used to follow the connection through the channels, -A to set the Ubertooth1 to monitor advertising channel 38 and -r to save the output)

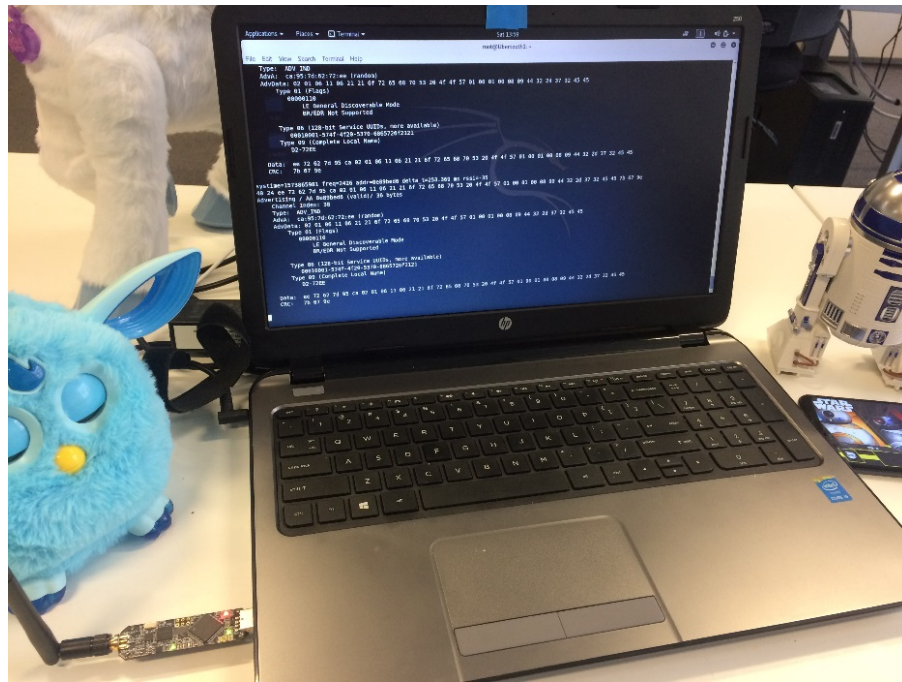


Figure 4.11. The Ubertooth1 while capturing the traffic for the R2-D2 Droid.

Due to the channel hopping nature of Bluetooth, the Ubertooth1 did not always manage to capture all of the packets involved in each exchange, and could not always successfully follow the conversation through the channels. It was therefore necessary to capture the pairing process of each smart toy another 10 times using the Ubertooth1 to obtain sufficient data to view the full pairing and communication practices of the smart toy and smartphone.

Whilst the Ubertooth1 successfully followed a BLE exchange, the output into Wireshark appeared limited and this made the packet details challenging to interpret. The process of capturing the pairing of each smart toy was then repeated using the Adafruit BluefruitV2 sniffer as this purported to give additional supporting information within Wireshark. Figure 4.12 shows the BluefruitV2 actively capturing live communication.

After selecting the nRF Sniffer (COM4) as the interface to be monitored, the Bluefruit Wireshark plug-in allowed the device and channel to be selected in the toolbar, as seen in Figure 4.12.

When used during LE Legacy Pairing, MITM protection enables an authenticated STK generation process. However, as can be seen in Figure 4.13, there is no MITM protection required for Furby Connect, and therefore the key generation process is unauthenticated.

No.	Time	Source	Destination	Protocol	Info
31.849780		Slave...	Master_0x33847436	SMP	Rcvd Pairing Response: AuthReq: Bonding
31.896264		Maste...	Slave_0x33847436	SMP	Sent Pairing Confirm

<ul style="list-style-type: none"> Frame 3963: 37 bytes on wire (296 bits), 37 bytes captured (296 bits) on interface 0 Nordic BLE Sniffer Bluetooth Low Energy Link Layer <ul style="list-style-type: none"> Access Address: 0x33847436 [Master Address: 6d:86:ce:ef:1b:5d (6d:86:ce:ef:1b:5d)] [Slave Address: e0:c6:dc:2c:3c:20 (e0:c6:dc:2c:3c:20)] Data Header: 0x0b06 <ul style="list-style-type: none"> [L2CAP Index: 2] CRC: 0xcdcf373 Bluetooth L2CAP Protocol Bluetooth Security Manager Protocol <ul style="list-style-type: none"> Opcode: Pairing Response (0x02) IO Capability: No Input, No Output (0x03) OOB Data Flags: OOB Auth. Data Not Present (0x00) AuthReq: 0x01, Bonding Flags: Bonding <ul style="list-style-type: none"> 000. = Reserved: 0x0 ...0 = Keypress Flag: False 0... = Secure Connection Flag: False0.. = MITM Flag: False01 = Bonding Flags: Bonding (0x1) Max Encryption Key Size: 16 Initiator Key Distribution: 0x02, Id Key (IRK) <ul style="list-style-type: none"> 0000 = Reserved: 0x0 0... = Link Key: False0.. = Signature Key (CSRK): False1. = Id Key (IRK): True0 = Encryption Key (LTK): False Responder Key Distribution: 0x03, Id Key (IRK), Encryption Key (LTK) <ul style="list-style-type: none"> 0000 = Reserved: 0x0 0... = Link Key: False0.. = Signature Key (CSRK): False1. = Id Key (IRK): True1 = Encryption Key (LTK): True
--

Figure 4.13. Pairing response packet from Furby Connect (Slave) to smartphone (Master) captured using the BluefruitV2.

From the data collected and analysed during the pairing process, it was concluded that Furby Connect used just works, LE Legacy Security Mode 1, Level 2, unauthenticated pairing.

When analysing the pairing packets details from the R2-D2 Droid, it was also found that the toy did not use an authenticated pairing process and paired using just works, LE Legacy Pairing, Security Mode 1, Level 2, unauthenticated. Figure 4.14 shows an R2-D2 Droid pairing response packet captured using the Ubertooth1.

The only difference observed in the pairing options between Furby Connect and the R2-D2 Droid was that Furby Connect alone enabled bonding to occur. This can be seen by the enabled bonding flag in Figure 4.13. When bonding is used, a LTK is generated, and the devices can remain paired even during a reboot or when sleep mode is activated.

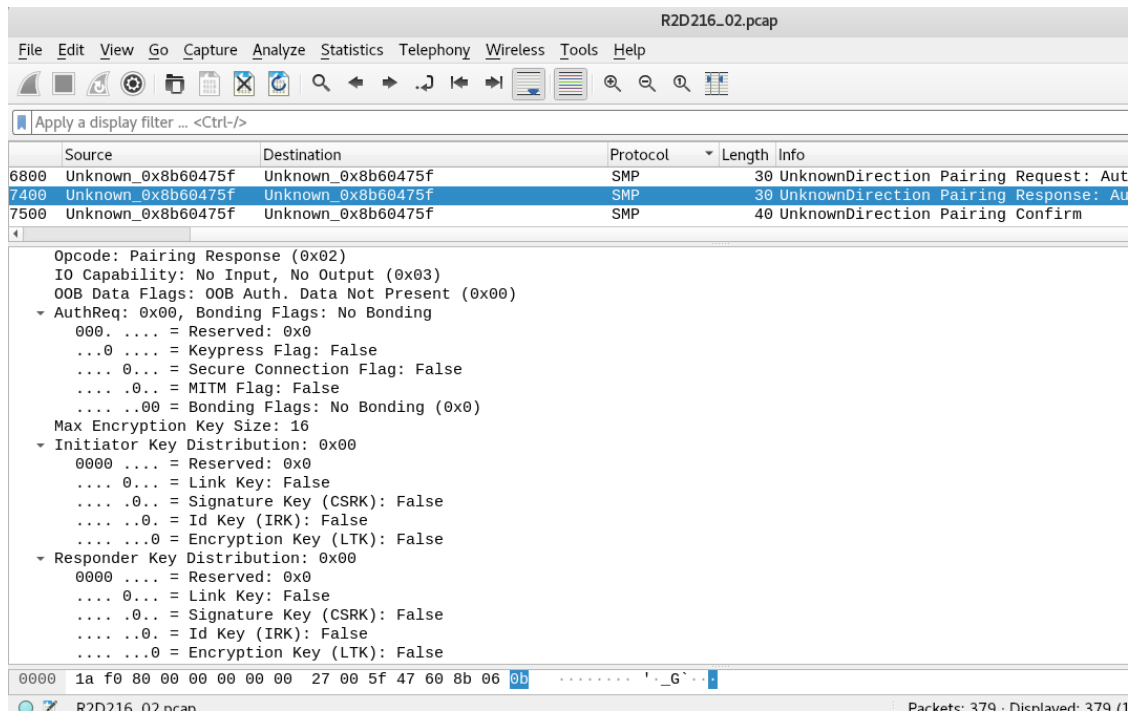
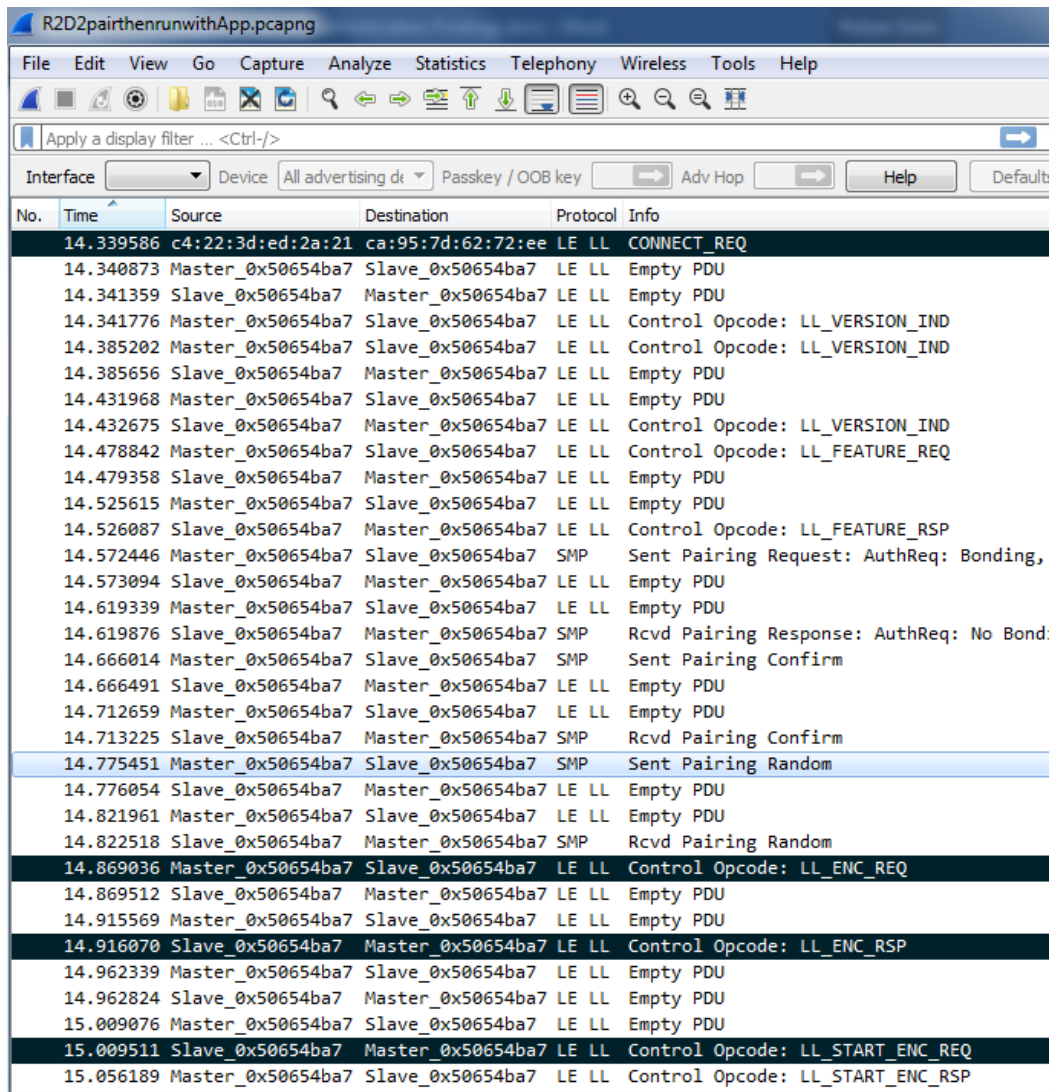


Figure 4.14. Pairing response packet generated from the R2-D2 Droid (Slave) to smartphone (Master) and captured using the Ubertooth1

Just works and LE Legacy Pairing does not protect from a passive eavesdropper. As this pairing method uses a known value for the TK (often zero), it is a simple process to capture the pairing information and crack the STK using CrackLE; a custom-built command-line tool for cracking BLE.

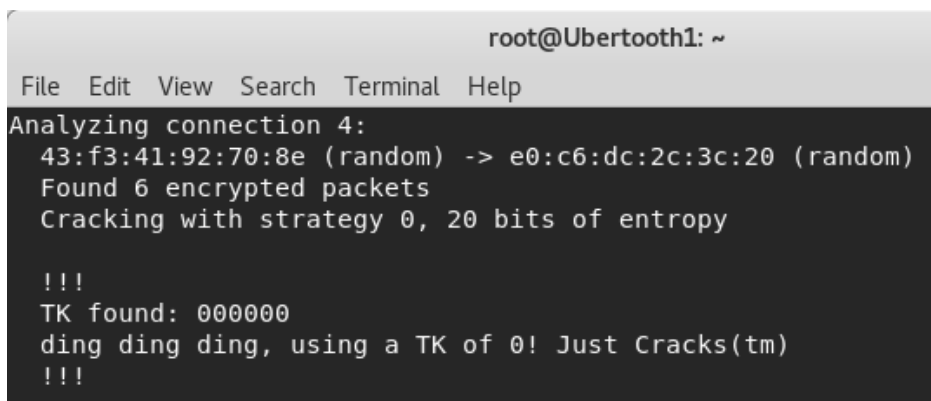
If the following packets are captured: CONNECT_REQ, LL_ENC_REQ, LL_ENC_RSP, LL_START_ENC_REQ using passive eavesdropping of the pairing process, the CrackLE tool can be used to find the STK and LTK. Figure 4.15 shows the successful capture of the R2-D2 Droid smart toy packets as determined above, and Figure 4.16 shows CrackLE successfully cracking the key.



The image shows a Wireshark packet capture titled "R2D2pairthenrunwithApp.pcapng". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar with various icons, and a display filter set to "Apply a display filter ... <Ctrl-/>". Below the toolbar, there are fields for "Interface", "Device" (set to "All advertising de..."), "Passkey / OOB key", "Adv Hop", and "Help". The main packet list table is as follows:

No.	Time	Source	Destination	Protocol	Info
14.339586	c4:22:3d:ed:2a:21	ca:95:7d:62:72:ee	LE LL	CONNECT_REQ	
14.340873	Master_0x50654ba7	Slave_0x50654ba7	LE LL	Empty PDU	
14.341359	Slave_0x50654ba7	Master_0x50654ba7	LE LL	Empty PDU	
14.341776	Master_0x50654ba7	Slave_0x50654ba7	LE LL	Control Opcode: LL_VERSION_IND	
14.385202	Master_0x50654ba7	Slave_0x50654ba7	LE LL	Control Opcode: LL_VERSION_IND	
14.385656	Slave_0x50654ba7	Master_0x50654ba7	LE LL	Empty PDU	
14.431968	Master_0x50654ba7	Slave_0x50654ba7	LE LL	Empty PDU	
14.432675	Slave_0x50654ba7	Master_0x50654ba7	LE LL	Control Opcode: LL_VERSION_IND	
14.478842	Master_0x50654ba7	Slave_0x50654ba7	LE LL	Control Opcode: LL_FEATURE_REQ	
14.479358	Slave_0x50654ba7	Master_0x50654ba7	LE LL	Empty PDU	
14.525615	Master_0x50654ba7	Slave_0x50654ba7	LE LL	Empty PDU	
14.526087	Slave_0x50654ba7	Master_0x50654ba7	LE LL	Control Opcode: LL_FEATURE_RSP	
14.572446	Master_0x50654ba7	Slave_0x50654ba7	SMP	Sent Pairing Request: AuthReq: Bonding,	
14.573094	Slave_0x50654ba7	Master_0x50654ba7	LE LL	Empty PDU	
14.619339	Master_0x50654ba7	Slave_0x50654ba7	LE LL	Empty PDU	
14.619876	Slave_0x50654ba7	Master_0x50654ba7	SMP	Rcvd Pairing Response: AuthReq: No Bond,	
14.666014	Master_0x50654ba7	Slave_0x50654ba7	SMP	Sent Pairing Confirm	
14.666491	Slave_0x50654ba7	Master_0x50654ba7	LE LL	Empty PDU	
14.712659	Master_0x50654ba7	Slave_0x50654ba7	LE LL	Empty PDU	
14.713225	Slave_0x50654ba7	Master_0x50654ba7	SMP	Rcvd Pairing Confirm	
14.775451	Master_0x50654ba7	Slave_0x50654ba7	SMP	Sent Pairing Random	
14.776054	Slave_0x50654ba7	Master_0x50654ba7	LE LL	Empty PDU	
14.821961	Master_0x50654ba7	Slave_0x50654ba7	LE LL	Empty PDU	
14.822518	Slave_0x50654ba7	Master_0x50654ba7	SMP	Rcvd Pairing Random	
14.869036	Master_0x50654ba7	Slave_0x50654ba7	LE LL	Control Opcode: LL_ENC_REQ	
14.869512	Slave_0x50654ba7	Master_0x50654ba7	LE LL	Empty PDU	
14.915569	Master_0x50654ba7	Slave_0x50654ba7	LE LL	Empty PDU	
14.916070	Slave_0x50654ba7	Master_0x50654ba7	LE LL	Control Opcode: LL_ENC_RSP	
14.962339	Master_0x50654ba7	Slave_0x50654ba7	LE LL	Empty PDU	
14.962824	Slave_0x50654ba7	Master_0x50654ba7	LE LL	Empty PDU	
15.009076	Master_0x50654ba7	Slave_0x50654ba7	LE LL	Empty PDU	
15.009511	Slave_0x50654ba7	Master_0x50654ba7	LE LL	Control Opcode: LL_START_ENC_REQ	
15.056189	Master_0x50654ba7	Slave_0x50654ba7	LE LL	Control Opcode: LL_START_ENC_RSP	

Figure 4.15. The successful capture of pairing packets required for CrackLE decryption



```

root@Ubertooh1: ~
File Edit View Search Terminal Help
Analyzing connection 4:
 43:f3:41:92:70:8e (random) -> e0:c6:dc:2c:3c:20 (random)
Found 6 encrypted packets
Cracking with strategy 0, 20 bits of entropy

!!!
TK found: 000000
ding ding ding, using a TK of 0! Just Cracks(tm)
!!!

```

Figure 4.16. Successful cracking of the Furby Connect encryption key using CrackLE

Due to the pairing method and security level implemented in these toys, neither Furby Connect nor the R2-D2 Droid met the control requirements to be protected from insufficient authentication vulnerabilities.

The only smart toy chosen for testing that used Bluetooth Classic to communicate was the Kurio Watch 2.0. A documentation review identified that the Kurio Watch used Bluetooth version 3.0, which offers the same pairing methods as described earlier.

By performing the pairing process between the smartphone Kurio Messenger application and the Kurio Watch, it was found that the Kurio Watch used a numeric comparison pairing method. In numeric comparison, a six-digit number is displayed on each device and the user is required to confirm they are the same in order to pair. This process can be seen in Figure 4.17.

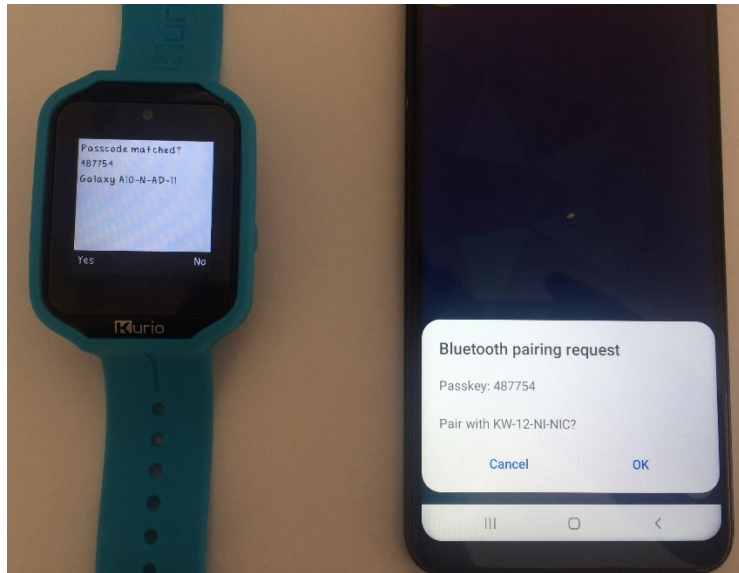


Figure 4.17. Numeric comparison pairing between a Kurio Watch 2.0 and Kurio Watch Messenger

The numeric comparison method of pairing provides some protection from a MITM attack. The Bluetooth specification notes that with a six-digit numeric comparison, there is a 1 in 1,000,000 chance of a MITM attack being successful (Bluetooth SIG, 2019).

The Ubertooth1 was used to capture the pairing and communication at packet level between the devices, in order to confirm the Bluetooth security mode and level implemented on the watch. To successfully capture Bluetooth Classic traffic, the lower address part (LAP) of BD_ADDR must be determined. As can be seen in Figure 4.18, the Ubertooth1 identified the Kurio Watch LAP as LAP = 1d6261 using the command *ubertooth -rx*.

```
root@Ubertooth1: ~
File Edit View Search Terminal Help
^Croot@Ubertooth1:~# ubertooth-rx
systemtime=1574306796 ch=78 LAP=1d6261 err=0 clkn=4779 clk_offset=4627 s=-56 n=-55
snr=-1
systemtime=1574306796 ch=31 LAP=1d6261 err=2 clkn=4907 clk_offset=4633 s=-52 n=-55
snr=3
systemtime=1574306797 ch=33 LAP=1d6261 err=0 clkn=5555 clk_offset=4652 s=-53 n=-55
snr=2
systemtime=1574306797 ch=73 LAP=1d6261 err=1 clkn=8235 clk_offset=4745 s=-59 n=-55
```

Figure 4.18. Identification of LAP of Kurio Watch

Entering the LAP of the Kurio Watch into the Ubertooth1 command line enabled the discovery of the upper address part. After this discovery process, the Ubertooth1 detected packets only from this piconet.

Despite pairing with the smartphone application a total of 20 times, the Ubertooth1 was unable to capture any identifiable pairing traffic between the watch and the phone. It is possible this was as a result of the Kurio Watch operating in Secure Connection Only mode, or that the Ubertooth1 could not successfully follow the device through the spectrum hopping sequence to capture the pairing packets. The Bluetooth authentication security level was therefore unable to be determined for this device.

The Kurio Watch did not meet the control criteria of *use of strong passwords* to protect against insufficient authentication vulnerabilities. No authentication mechanism was required to access the physical watch storage itself. The Kurio Watch stores a child's PII, including "in case of emergency" information on the device, which includes sensitive contact and medical details. This is the only area of the watch that requires a password to be entered before accessing the contents; however, the password is a factory default four-digit pin that is publicly available in the information brochure as seen in Figure 4.19. At no stage in the Kurio Watch set up process does the device prompt or allow the user to change this password. This means that anyone who has seen the Kurio Watch information brochure can access this information and have the means to access and change the stored PII.

Mute	Activate / Deactivate the volume
Incoming call	Select the Phone ringtone (when the KURIO Watch is paired to a smartphone by Bluetooth®). MP3 sounds loaded on the internal memory of the KURIO Watch (not on the Micro SD card) can be us
Alarm	Select the Alarm ringtone
ICE details	Edit the Emergency details. A password is required to access this parental area. Password is 1248

Figure 4.19. Kurio Watch user manual page showing factory-set password to access emergency details

Two of the smart toys were found to use Wi-Fi rather than Bluetooth for communication, namely the Air Hogs FPV High Speed Race Car and Toy Mail Talkie Unicorn. To investigate whether these toys used secure authentication methods, the Wi-Fi communication packets between the smart toys and their companion mobile applications were captured using a TP-LINK TL-WN722N Wi-Fi dongle and the Aircrack-ng suite of command-line Wi-Fi network security assessment tools from Kali Linux.

The dongle was first placed in monitor mode to find and review the available Wi-Fi networks. As can be seen in Figure 4.20, the Air Hogs FPV High Speed Race Car BSSID was found immediately on channel 1, and the race car network identified as "Open", meaning it was using no security protocols for authentication or encryption.

```

root@Ubertooth1: ~
File Edit View Search Terminal Help

CH 14 ][ Elapsed: 0 s ][ 2019-11-23 14:15

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
EC:3D:FD:1D:C4:16 -47      6         0  0  1  54e.  OPN             AH_RACE_CAR_1dc416
04:DA:D2:4F:30:02 -50      2         0  0  1  54e.  WPA2 CCMP  MGT  eduroam
04:DA:D2:4F:30:00 -51      3         0  0  1  54e.  WPA2 CCMP  PSK  AUT-Test
04:DA:D2:4F:30:01 -51      2         0  0  1  54e.  WPA2 CCMP  MGT  AUTwifi

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
(not associated) F8:34:41:20:A4:F9 -82    0 - 1    0      2

```

Figure 4.20. Identification of the Air Hogs FPV Race Car open network

To confirm no authentication was required to join this network, the race car was paired with the smartphone companion application. No password was required to join this network and no other authentication procedures were required. Therefore, the Air Hogs FPV High Speed Race Car did not meet the control requirements to be secure against insufficient authentication vulnerabilities.

The other smart toy using Wi-Fi for communication was the Toy Mail Talkie Unicorn. Rather than operate over an open network like the Air Hogs FPV Race Car, it was found that the Toy Mail Talkie Unicorn utilised the home Wi-Fi network for authentication and communication between the toy and the smartphone companion application. A personal Wi-Fi network with WPA2 encryption was used to connect the Toy Mail Talkie Unicorn and capture the communication packets for investigation in Wireshark. WPA2-personal uses a PSK of between 8 and 63 ASCII characters for authentication. A four-way handshake is then performed between the devices to confirm security protocols and generate encryption keys for further communication. The communication between the Toy Mail Talkie Unicorn and the smartphone companion application was captured, and as seen in Figure 4.21, analysis of the packets in Wireshark confirmed the use of TLS 1.2. It also showed the completion of the four-way handshake to establish communication.

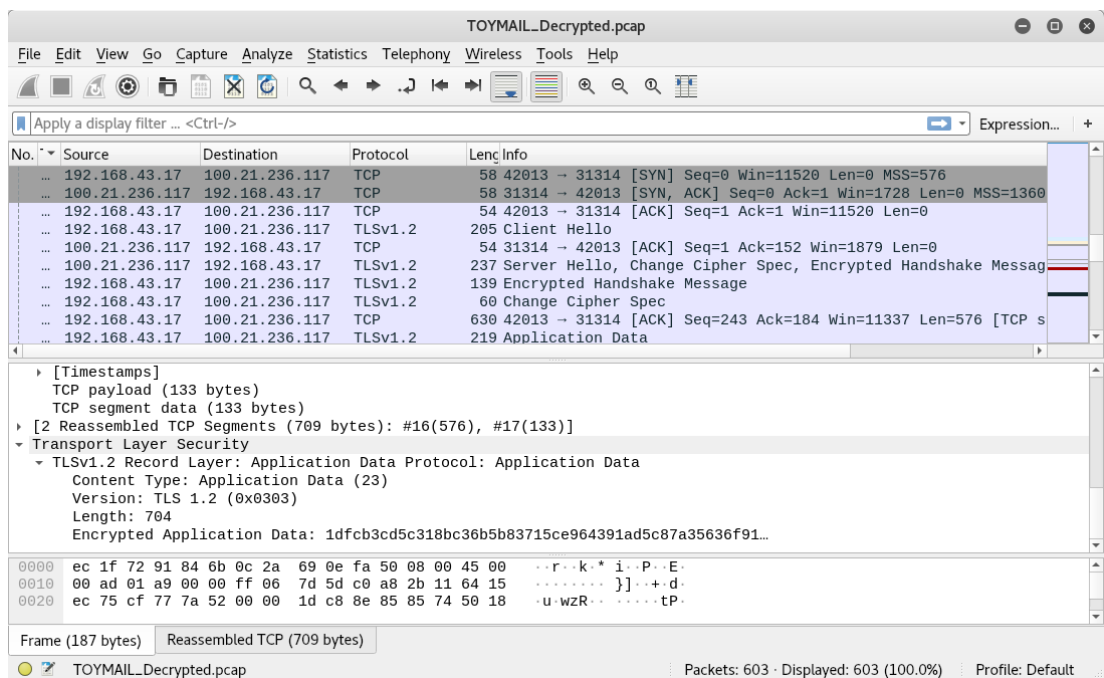


Figure 4.21. Toy Mail Talkie Unicorn authentication and communication establishment packets

As demonstrated in Figure 4.21, the Toy Mail Talkie Unicorn met the requirements to satisfy secure Wi-Fi authentication control criteria and avoid insufficient authentication vulnerabilities.

Despite using a secure authentication method, the Toy Mail Talkie Unicorn is only as secure as the home user's network. Whilst secure if implemented robustly, a WPA2 personal network (when established with a dictionary word password of only eight characters) can be easily cracked. The test WPA2 Wi-Fi network used in this investigation was configured using a passkey of "password", which was the fourth most breached password in 2019 (National Cyber Security Centre, 2019).

The Aircrack-ng suite of command-line tools was used to capture the authentication communication between the Toy Mail Talkie Unicorn and the smartphone application. As can be seen in Figure 4.22, the WPA handshake was captured in these packets.

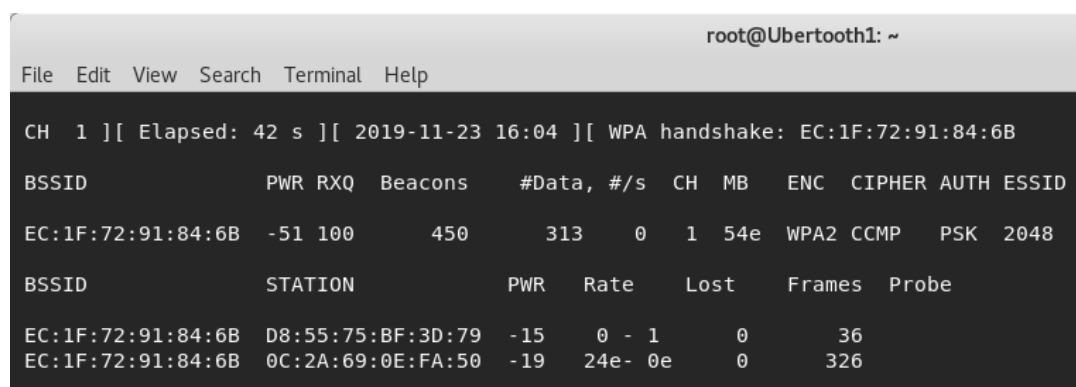


Figure 4.22. WPA handshake captured by passively eavesdropping the communication between Toy Mail Talkie Unicorn and the smartphone application

Once the WPA handshake was successfully captured, the command-line tool took seconds to determine the passkey as seen in Figure 4.23. Once this passkey is known, the network is no longer secure.

```

root@Ubertooth1: ~
File Edit View Search Terminal Help

Aircrack-ng 1.2 rc4

[00:00:00] 4/7120716 keys tested (250.41 k/s)

Time left: 7 hours, 54 minutes, 42 seconds      0.00%

KEY FOUND! [ password ]

Master Key   : 32 28 26 4C C8 E1 B2 66 5C 6E 4B 82 F7 7D 52 D0
               E3 7E FB 34 69 C1 69 22 C6 AC ED 3C 21 39 10 74


Transient Key : 59 84 DE 24 6F AD 1D DF E3 E8 A3 20 66 9D 7A 83
               0F 54 17 2F 1B 3C BA 89 D7 EB 81 70 A9 59 CE F3
               21 CE B4 23 29 C1 51 EB E3 04 75 01 84 60 3A FA
               6A 38 33 3B 4E DB 05 C6 26 78 50 86 29 1D E1 DE

EAPOL HMAC   : ED 7C 84 C1 31 28 B3 AD 91 EB 95 3E 43 F1 AC 72
root@Ubertooth1:~#

```

Figure 4.23. Successful cracking of WPA2 personal Wi-Fi network passkey

The Toy Mail Talkie Unicorn was the only smart toy tested that required the user to set up an account on the mobile companion application before the toy could be used. The Toy Mail Talkie Unicorn user account contains confidential details about each child using the toy. The Toy Mail Talkie Unicorn account satisfied the authentication control *use of a secure password*, requiring a minimum 8-digit password using numbers and special characters as seen in Figure 4.24. It also satisfied the control *use of secure password recovery mechanism*. It did not, however, satisfy the control *use of secure account lockout mechanism* as it did not lock the account after 30 failed login attempts. No account lockout allows the account to be vulnerable to a brute force password attack.



Reset your password:

Password must be at least 8 characters long and contain a letter, a number and a special character

Figure 4.24. Toy Mail Talkie Unicorn password reset function

4.3.2 Vulnerability Area 2 – Insecure Data Transfer

Securely transferring data across any network, including Wi-Fi, Bluetooth, and ethernet, involves using encryption to prevent against the possibility of data alteration or theft (El Mouaatamid et

al., 2016). To assess whether the smart toys in this study used secure data transfer methods, an analysis of data transfer between the smart toys and their companion applications was performed to look for any unencrypted data sent and any encryption standards used.

A summary of the overall findings for this vulnerability area can be seen in Table 4.3.

Table 4.3. Summary of findings in vulnerability area 2 – Insecure data transfer

Smart toy	Communication is encrypted	Secure encryption protocols used for all communication
<i>Furby Connect</i>	P	N
<i>Toy Mail Talkie Unicorn</i>	M	M
<i>R2-D2 Droid</i>	P	N
<i>Kurio Watch</i>	M	U
<i>Air Hogs FPV High Speed Race Car</i>	N	N

Note: M = Meets control, N = Did not meet control, P = Partially meets control, U = Unknown, N/A = Not applicable.

The Toy Mail Talkie Unicorn met all of the control criteria to protect against *insecure data transfer* vulnerabilities. No unencrypted data was observed in any of the packets captured for inspection, and as can be seen in Figure 4.25, all data transmitted and received by this toy was encrypted using TLS 1.2.

No.	Source	Destination	Protocol	Length	Info
...	192.168.43.17	100.21.236.117	TCP	58	42013 → 31314 [SYN] Seq=0 Win=11520 Len=0 MSS=576
...	100.21.236.117	192.168.43.17	TCP	58	31314 → 42013 [SYN, ACK] Seq=0 Ack=1 Win=1728 Len=0
...	192.168.43.17	100.21.236.117	TCP	54	42013 → 31314 [ACK] Seq=1 Ack=1 Win=11520 Len=0
...	192.168.43.17	100.21.236.117	TLSv1.2	205	Client Hello
...	100.21.236.117	192.168.43.17	TCP	54	31314 → 42013 [ACK] Seq=1 Ack=152 Win=1879 Len=0
...	100.21.236.117	192.168.43.17	TLSv1.2	237	Server Hello, Change Cipher Spec, Encrypted Handshake
...	192.168.43.17	100.21.236.117	TLSv1.2	139	Encrypted Handshake Message
...	192.168.43.17	100.21.236.117	TLSv1.2	60	Change Cipher Spec
...	192.168.43.17	100.21.236.117	TCP	630	42013 → 31314 [ACK] Seq=243 Ack=184 Win=11337 Len=576
...	192.168.43.17	100.21.236.117	TLSv1.2	219	Application Data

<ul style="list-style-type: none"> ▶ [Timestamps] TCP payload (133 bytes) TCP segment data (133 bytes) ▶ [2 Reassembled TCP Segments (709 bytes): #16(576), #17(133)] ▼ Transport Layer Security <ul style="list-style-type: none"> ▼ TLSv1.2 Record Layer: Application Data Protocol: Application Data <ul style="list-style-type: none"> Content Type: Application Data (23) Version: TLS 1.2 (0x0303) Length: 704 Encrypted Application Data: 1dfcb3cd5c318bc36b5b83715ce964391ad5c87a35636f91...
--

Figure 4.25. Encrypted Toy Mail Talkie Unicorn application data viewed in Wireshark

In contrast, the controls in this area of vulnerability were not met by the Air Hogs High Speed Race Car, which used no encryption at all to transmit images and video files over Wi-Fi. The race car captures and saves photographs and real-time video from its onboard camera, and anyone intercepting this unencrypted data stream could potentially recreate the layout of the house where the toy was being used, and identify the child using the toy by viewing these images. Figure 4.26 shows an unprotected (unencrypted) data frame captured during the race car operation.

40	0.394300		SamsungE_91:84:6b (... 802.11	10	Clear-to-send, Flags=
41	0.394324	192.179.132.107	192.179.8.1	TCP	74 33606 → 6320 [ACK] Se
42	0.394300	ec:3d:fd:1d:c4:16 (... SamsungE_91:84:6b (... 802.11		28	802.11 Block Ack, Fla
43	0.433212	192.179.8.1	192.179.132.107	UDP	215 8989 → 51315 Len=153
44	0.433239		ec:3d:fd:1d:c4:16 (... 802.11	10	Acknowledgement, Flag

[Coloring Rule String: tcp]

- IEEE 802.11 QoS Data, Flags:T
 - Type/Subtype: QoS Data (0x0028)
 - Frame Control Field: 0x8801
 -00 = Version: 0
 - 10.. = Type: Data frame (2)
 - 1000 = Subtype: 8
 - Flags: 0x01
 -01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x01)
 -0.. = More Fragments: This is the last fragment
 - 0... = Retry: Frame is not being retransmitted
 - ...0 = PWR MGT: STA will stay up
 - ..0. = More Data: No data buffered
 - .0.. = Protected flag: Data is not protected
 - 0... = Order flag: Not strictly ordered
 - .000 0000 0011 0000 = Duration: 48 microseconds
 - Receiver address: ec:3d:fd:1d:c4:16 (ec:3d:fd:1d:c4:16)
 - Destination address: ec:3d:fd:1d:c4:16 (ec:3d:fd:1d:c4:16)
 - Transmitter address: SamsungE_91:84:6b (ec:1f:72:91:84:6b)
 - Source address: SamsungE_91:84:6b (ec:1f:72:91:84:6b)
 - BSS Id: ec:3d:fd:1d:c4:16 (ec:3d:fd:1d:c4:16)
 - STA address: SamsungE_91:84:6b (ec:1f:72:91:84:6b)
 - 0000 = Fragment number: 0
 - 0010 1101 1011 = Sequence number: 731
 - Qos Control: 0x0000
 - 0000 = TID: 0
 - [....000 = Priority: Best Effort (Best Effort) (0)]
 - 0... = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
 -00. = Ack Policy: Normal Ack (0x0000)

Figure 4.26. Air Hogs FPV High Speed Race Car unencrypted data frame as viewed in Wireshark

The Kurio Watch met the control *use of encryption* as the Ubertooth1 was unable to capture any data sent in the clear. Due to the difficulty in capturing and following the pairing packets between the watch and its companion application, the nature of the encryption used was undetermined. Figure 4.27 shows encrypted Kurio Watch data captured by Ubertooth1 and examined in Wireshark.

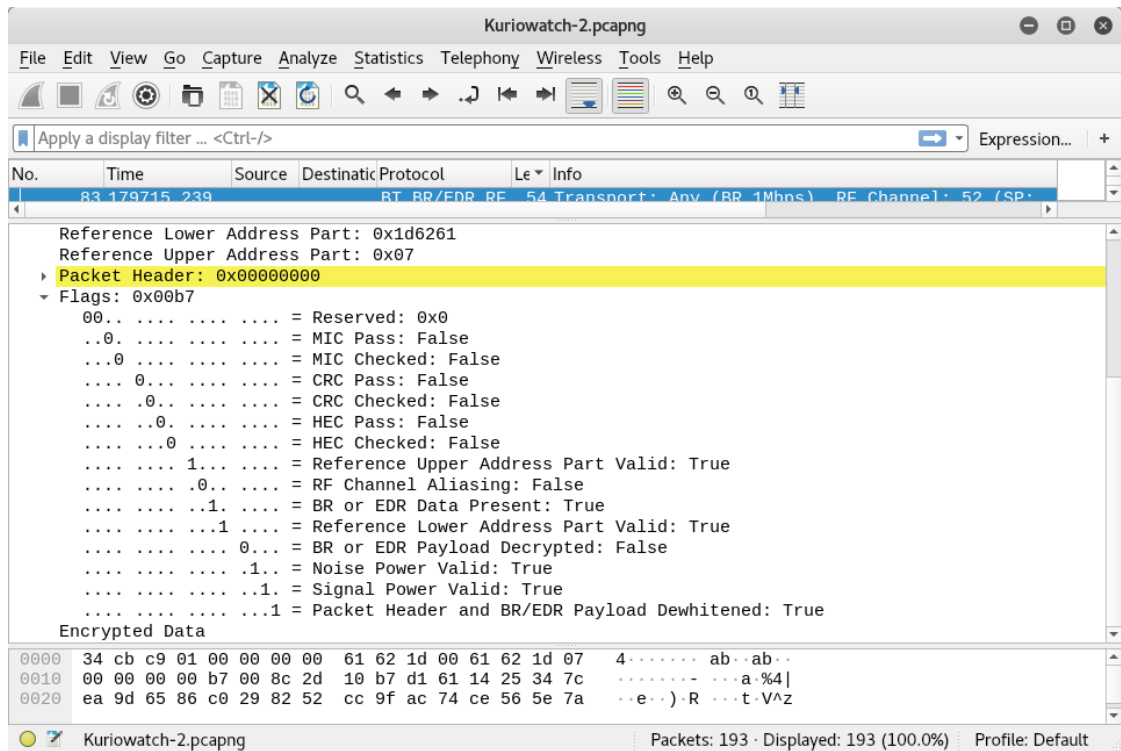


Figure 4.27. Kurio Watch encrypted data packet captured and viewed in Wireshark

Furby Connect and the R2-D2 Droid both partially met the control requirements in this area. When data packets exchanged by each of these toys were viewed in Wireshark, both encrypted and unencrypted data packets were observed. As found when observing the authentication and pairing packets of these toys, both used LE Legacy Security Mode 1, Level 2 which can encrypt data for confidentiality using AES-CCM, a secure encryption protocol. However, confirmation of this protocol use could not be obtained.

4.3.3 Vulnerability Area 3 – Insufficient Privacy Protection

To determine whether the smart toys implemented the controls required for adequate privacy protection, a full review of each of the toys set up and operational processes was undertaken. Privacy policies were obtained wherever possible and examined for comprehensiveness against the test criteria, and all data and permissions requested by the smart toy and the companion application were recorded.

A summary of the overall findings for this vulnerability area can be seen in Table 4.4.

Table 4.4. Summary of findings in vulnerability area 3 – Insufficient privacy protection

Smart toy	<i>Reasonable PII collection</i>	<i>Comprehensive privacy policy</i>	<i>Privacy support mechanisms</i>	<i>Acceptable parental control mechanisms</i>	<i>Use of random unique device identifier</i>
<i>Furby Connect</i>	P	P	M	N	P
<i>Toy Mail Talkie Unicorn</i>	N	P	M	N	U
<i>R2-D2 Droid</i>	P	P	M	N	N
<i>Kurio Watch</i>	N	P	M	N	N
<i>Air Hogs FPV High Speed Race Car</i>	M	P	M	N	U

Note: M = Meets control, N = Did not meet control, P = Partially meets control, U = Unknown, N/A = Not applicable.

The control criteria for *reasonable PII collection* was only fully met by one toy—the Air Hogs FPV High Speed Race Car. The race car required no user account to be established, and no personal data was requested during set up or use of the toy. The Kurio Watch and the Toy Mail Talkie Unicorn did not meet the control criteria, as both toys requested numerous types of PII during setup. The Kurio Watch requested first and last names, birthday, and even a child’s favourite colour during the setup process as seen in Figure 4.28. There was no option to skip this input and still operate the watch. The watch then requested additional optional information such as blood type, allergies, emergency contacts and insurance details.

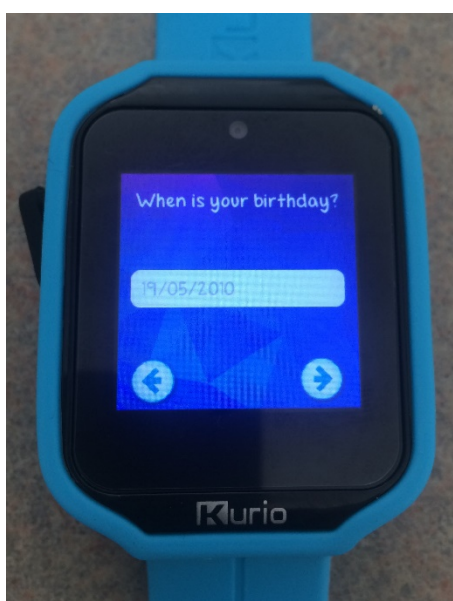


Figure 4.28. Kurio Watch setup process

The Toy Mail Talkie Unicorn also did not meet this control as it collected both parent and child information during set up of the account. It requested details such as names, birthdates, location, and photographs from the user.

Furby Connect partially met the control criteria for *reasonable PII collection*, as although no personal details were requested during the initial set up of the toy and the companion application, in order to view the privacy policy from within the application the user's birthdate had to be entered. The Furby Connect World App also collected additional user data such as payment details in order to make purchases from the within the application.

The R2-D2 Droid also partially met this control. The application requested the user enter their age during the setup process, and did not allow set up to continue if this was not completed. If the age entered was over 13, an optional email address was then requested. This is explained in the privacy policy as a required step to ensure the details of younger children are not collected; however, as an email address is not required for the operation of the toy it seems unnecessary.

A full list of information requested by the smart toys and their companion applications can be seen in Table 4.5. Permissions requested by the toys companion applications can be seen in Table 4.6.

Table 4.5. PII requested by smart toy and companion applications during set up and use

	<i>Parent name</i>	<i>Child name</i>	<i>Physical address</i>	<i>Email address</i>	<i>Phone number</i>	<i>Country</i>	<i>Childs photo</i>	<i>Voice recording</i>	<i>Birthday/Age</i>	<i>Interests</i>	<i>Payment details</i>	<i>Additional contact Information</i>
<i>Furby Connect</i>	Y		Y	Y	Y	Y			Y		Y	
<i>R2-D2 Droid</i>				Y					Y			
<i>Kurio Watch</i>		Y							Y	Y		Y
<i>Air Hogs FPV High Speed Race Car</i>												
<i>Toy Mail Talkie Unicorn</i>	Y	Y					Y	Y	Y			

Table 4.6. Permissions requested by the toys companion applications during set up and use

	<i>Photos, media, files, and storage</i>	<i>Contacts</i>	<i>Bluetooth settings</i>	<i>Take pictures</i>	<i>Microphone</i>	<i>Record video</i>	<i>Device location</i>	<i>Record audio</i>	<i>Call history</i>
<i>Furby Connect</i>	Y		Y				Y		
<i>R2-D2 Droid</i>	Y		Y		Y		Y	Y	
<i>Kurio Watch</i>	Y	Y			Y		Y	Y	Y
<i>Air Hogs High Speed FPV Race Car</i>	Y			Y		Y	Y		
<i>Toy Mail Talkie Unicorn</i>	Y	Y		Y	Y		Y	Y	

All of the smart toys tested partially met the control criteria for *comprehensive privacy policy*. The R2-D2 Droid, Furby Connect, and the Toy Mail Talkie Unicorn all had privacy policies written explicitly for the toy, whereas the Kurio Watch and the Air Hogs High Speed FPV Race Car only linked to generic company privacy policies with no specific references to the toy being tested.

Privacy policy links were available for Furby Connect, Toy Mail Talkie Unicorn and the Air Hogs High Speed FPV Race Car from within the companion applications, from the application stores, and from the toys' websites. The R2-D2 Droid did not have a toy-specific privacy policy available from the website; however, this toy required the user to accept both the privacy policy and the terms of use before opening and accessing the companion application. The Kurio Watch generic company privacy policy was available from the application store and the website; however, there was no link within the companion application itself.

All of the toys assessed displayed the last updated date in their privacy policies. It was observed, however, that the Kurio Watch policy had not been updated since July, 2013, which did not seem recent enough considering the considerable changes in privacy legislation seen globally in the previous five years. All of the toys except the Toy Mail Talkie Unicorn also described the method with which changes to their policies would be communicated to users.

Each of the privacy policies described the data types collected and their use by the various companies. None of the toys however adequately outlined data retention periods. Only Furby Connect and Toy Mail Talkie Unicorn referred to data retention in their privacy policies, and neither were specific as to how long they would retain data collected. Toy Mail Talkie Unicorn specified that data is kept as long as the user is a Toy Mail customer, but does not explain how they define who a customer is. Hasbro (Furby Connect) stated it would retain the data collected as long as it deems necessary.

The Toy Mail Talkie Unicorn and Air Hogs FPV Race Car privacy policies both partially identified data storage location by stating that their data is stored both inside and outside the United States. Neither the Kurio Watch nor the R2-D2 Droid policy addressed where user data was stored. The Furby Connect policy met this criterion by stating that data is stored within the United States. It goes on to state, however, that other storage locations are not ruled out in the future.

All of the smart toys met the control criteria for *privacy support mechanisms*. Each toy tested provided a dedicated email contact address to address privacy concerns with both the Furby Connect and the Toy Mail Talkie Unicorn companies taking the additional step of engaging a third-party organisation to complete this service.

In contrast to the above, none of the smart toys tested met the control requirements for *acceptable parental control mechanisms*. These findings back up previous research seen in the literature review that concluded that parental controls for use in IoT devices are not well designed or widely implemented to date (De Lima Salgado et al., 2017). None of the toys tested allowed a parent to delete data collected and stored by the physical toy. For example, there is no way to delete voice messages stored locally on the Toy Mail Talkie Unicorn, and parents must send a request to the company to delete any PII held on their servers.

The Kurio Watch may be returned to factory settings, effectively removing any data collected, and the companion application deleted from the user's smartphone. A parent or guardian may also request the company suspend from collecting any further data; however, the deletion of any data collected and held by the company to date is not addressed in the Kurio Watch policies.

The Furby Connect, Air Hogs FPV High Speed Race Car, and R2-D2 Droid privacy policies each stated that they will delete personal information held upon request. However, Hasbro (Furby Connect) and Sphero (R2-D2 Droid) also stated that they will complete this only to the extent that they are required to do so by applicable law. These statements emphasise the reliance that consumers of these products have on legislation for privacy protection.

The ability to physically track the location of a child is a privacy concern that has been expressed in recent years by the FBI (FBI, 2017). All portable devices, including smart toys that operate over Wi-Fi or Bluetooth, have a unique 48-bit identifier called a MAC or Bluetooth MAC address. This address is used to identify the source and destination of communication frames (Townsend et al., 2014) and is synonymous with the smart toy, and therefore, potentially the child using the toy. Physically identifying and tracking a child becomes possible if the toy uses a static MAC address or if the unique identifier broadcast during communication consists of the user's PII.

MAC address randomisation and BLE privacy features prevent this scenario by replacing fixed addresses with random values that change over a fixed time interval (Townsend et al., 2014). To test the smart toys and determine whether they used random unique device identifiers, the toys broadcast packets were captured and observed over several days, both before pairing with another device, and after being paired with a trusted device.

Furby Connect only partially met the criteria *use of random unique device identifier* as the toy advertised using the same MAC address (e0:c6:dc:2c:3c:20) every time the toy was unpaired, allowing for easy detection. Investigation of the pairing packets captured in Wireshark however also showed that the toy could implement the LE privacy feature once paired. The exchange of an identity resolution key (IRK) during the pairing process, as seen in Figure 4.29, allowed the Furby Connect to create and resolve random MAC addresses for subsequent use while paired.

Interface	COM4	Device	"Furby" -64 dBm e0:c6:dc:2c:3c:20 random	Passkey / OOB key	
No.	Time	Source	Destination	Protocol	Length Info
11540	159.026600	Master_0x5065756d	Slave_0x5065756d	LE LL	26 Empty PDU
11541	159.088061	Master_0x5065756d	Slave_0x5065756d	LE LL	26 Empty PDU
11542	159.088605	Slave_0x5065756d	Master_0x5065756d	SMP	41 Rcvd Master Identification
11543	159.088978	Master_0x5065756d	Slave_0x5065756d	LE LL	26 Empty PDU
11544	159.089430	Slave_0x5065756d	Master_0x5065756d	SMP	47 Rcvd Identity Information
11545	159.089803	Master_0x5065756d	Slave_0x5065756d	LE LL	26 Empty PDU

Frame 11544: 47 bytes on wire (376 bits), 47 bytes captured (376 bits) on interface 0

Nordic BLE Sniffer

Board: 4

Header Version: 1, Packet counter: 13048

Length of packet: 10

Flags: 0x3d

- ...1 = CRC: OK
- ...0. = Direction: Slave -> Master
- ...1.. = Encrypted: Yes
- ...1... = MIC: OK
- .011 ... = PHY: Reserved (3)
- 0... = RFU: 0

Channel: 22

RSSI (dBm): -81

Event counter: 18

Delta time (µs end to start): 181

[Delta time (µs start to start): 181]

Bluetooth Low Energy Link Layer

Access Address: 0x5065756d

[Master Address: c4:22:3d:ed:2a:21 (c4:22:3d:ed:2a:21)]

[Slave Address: e0:c6:dc:2c:3c:20 (e0:c6:dc:2c:3c:20)]

Data Header: 0x151a

- ...10 = LLID: Start of an L2CAP message or a complete L2CAP message with no fragmentation (0x2)
- ...0.. = Next Expected Sequence Number: 0
- ...1... = Sequence Number: 1 [OK]
- ...1 = More Data: True
- 000. = RFU: 0

Length: 21

[L2CAP Index: 193]

CRC: 0x5a5638

Bluetooth L2CAP Protocol

Length: 17

CID: Security Manager Protocol (0x0006)

Bluetooth Security Manager Protocol

Opcode: Identity Information (0x08)

Identity Resolving Key: e05a53ba8f3a0587d94683ea87a67def

Figure 4.29. Furby Connect pairing packet showing the exchange of an IRK

The R2-D2 Droid however, did not meet the criteria for this control. The toy broadcast the same MAC address throughout the study, and an inspection of the pairing packet exchange within Wireshark, as shown in Figure 4.30, showed no generation of an IRK for enabling LE privacy functions.

179	14.619339	Master_0x50654ba7	Slave_0x50654ba7	LE LL	26 Empty PDU
180	14.619876	Slave_0x50654ba7	Master_0x50654ba7	SMP	37 Rcvd Pairing Response: AuthReq: No Bonding Initiator Key(s): <none> Responder Key(s): <none>
181	14.666014	Master_0x50654ba7	Slave_0x50654ba7	SMP	47 Sent Pairing Confirm
182	14.666491	Slave_0x50654ba7	Master_0x50654ba7	LE LL	26 Empty PDU
<pre> Delta time (µs end to start): 150 [Delta time (µs start to start): 230] Bluetooth Low Energy Link Layer Access Address: 0x50654ba7 [Master Address: c4:22:3d:ed:2a:21 (c4:22:3d:ed:2a:21)] [Slave Address: ca:95:7d:62:72:ee (ca:95:7d:62:72:ee)] Data Header: 0x0b06 [L2CAP Index: 1] CRC: 0x7adc4d Bluetooth L2CAP Protocol Length: 7 CID: Security Manager Protocol (0x0006) Bluetooth Security Manager Protocol Opcode: Pairing Response (0x02) IO Capability: No Input, No Output (0x03) OOB Data Flags: OOB Auth. Data Not Present (0x00) AuthReq: 0x00, Bonding Flags: No Bonding 0000 = Reserved: 0x0 0... = Keypress Flag: False 0... = Secure Connection Flag: False 0... = MITH Flag: False 0000 = Bonding Flags: No Bonding (0x0) Max Encryption Key Size: 16 Initiator Key Distribution: 0x00 0000 = Reserved: 0x0 0... = Link Key: False 0... = Signature Key (CSRK): False 0... = Id Key (IRK): False 0... = Encryption Key (LTK): False Responder Key Distribution: 0x00 0000 = Reserved: 0x0 0... = Link Key: False 0... = Signature Key (CSRK): False 0... = Id Key (IRK): False 0... = Encryption Key (LTK): False </pre>					

Figure 4.30. R2-D2 Droid pairing response packet exchange within Wireshark

The Kurio Watch also did not meet the criteria for this control. After completing the process of setting up, detecting, and pairing with the watch, it was apparent that the watch used user-inputted information, i.e., username, to create its unique identifier. As seen in the series of images in Figure 4.31, the watch requested the user to input their name along with many other personal details such as medical information as part of the setup process. The username “NIC” was entered during testing and was subsequently used by the watch as its advertising name when broadcasting its presence to other devices.

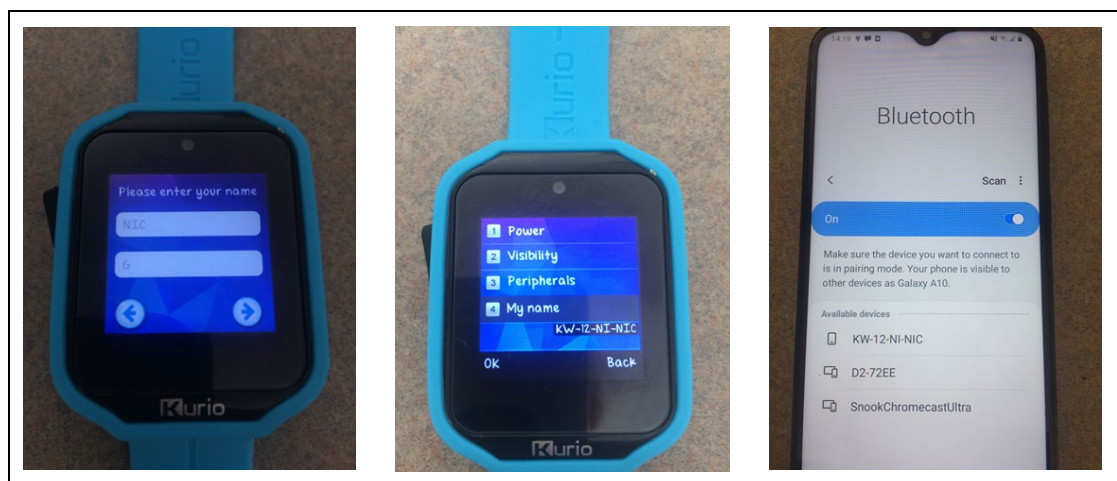


Figure 4.31. Kurio Watch set up process using username to create the device identifier

The use of a child’s name to publicly broadcast a device, such as seen here, potentially allows an individual child to be identified and tracked.

4.3.4 Exclusions

Three toys that were outlined in the method were unable to be tested for a variety of reasons. Star Lily Unicorn could not be paired with its companion application using the smartphone model used for testing. It only supports a limited range of smartphones and versions of iOS and Android

OS, which are now outdated. The company has no plans to add support for any more modern OS or devices, despite the unicorn still being available for sale online from many international retailers. Without the ability to pair with a companion application, the unicorn is essentially a standard plush toy with no smart features.

Between defining the method for this research and starting the physical toy testing, CogniToys, the company who produce the Dino appear to have gone out of business. Despite the application still being available from the Google Play Store at the time of this research, it was unable to be used, and the backend server appears to have been decommissioned. An email to the support address failed to deliver and was returned. This has unsurprisingly upset many consumers who purchased the CogniToys Dino, which continues to be sold online by some retailers.

The Toy-Fi Teddy mobile companion app was also withdrawn from the Google Play Store before the physical testing was completed, with no official comment explaining why.

Each of these scenarios raises questions around the ability for toy companies to provide ongoing support for smart toys and their companion applications. The inability to maintain adequate support, including providing essential security updates for the toy's firmware and the companion applications, may leave customers exposed to future vulnerabilities. It is also unclear what happens to the PII previously collected by companies such as CogniToys who then fail to remain in business.

4.3.5 Summary of Physical Test Findings

In summary, none of the smart toys tested met all of the security control criteria to prevent vulnerabilities in all three areas in scope. The Air Hogs FPV High Speed Race Car was the only toy that did not collect excessive PII; however, it met the least number of overall controls. The Toy Mail Talkie Unicorn met the most security controls, showing sufficient protection in the areas of authentication and data transfer. It failed to meet the criteria necessary to protect privacy, however, by not implementing any parental data control mechanisms and collecting unnecessary PII. Whenever a smart toy does not fully meet the controls specified, there remains some element of potential security or privacy risk for the user.

Table 4.7 summarises the overall result for each smart toy.

Table 4.7. Summary of physical test findings for each smart toy

Smart toy	<i>Insufficient authentication controls</i>	<i>Insecure data transfer controls</i>	<i>Insufficient privacy protection controls</i>
Furby Connect	Does not meet	Partially meets	Partially meets
Toy Mail Talkie Unicorn	Meets	Meets	Partially meets
R2-D2 Droid	Does not meet	Partially Meets	Partially meets
Kurio Watch	Does not meet	Unknown	Partially meets
Air Hogs FPV High Speed Race Car	Does not meet	Does not meet	Partially meets

4.4 Conclusion

Chapter 4 has reported the findings of both an online survey of New Zealand parents and guardians determining levels of concern and awareness around smart toy security and privacy, and the physical testing of a group of smart toys determining vulnerabilities in the toys.

The survey has confirmed that high levels of concern and low levels of awareness exist around smart toy security and privacy. The physical security testing has demonstrated that weaknesses in all three vulnerability areas tested exist in smart toys in New Zealand. Chapter 5 will further discuss these findings, linking them to the literature review and using the results to answer the main research question and sub-questions posed by this study.

Chapter 5: Discussion

5.1 Introduction

Chapter 4 presented the findings from the survey and the physical security testing of a group of smart toys. These findings were obtained using methods derived from a review of similar studies and industry-standard methodologies and are presented in Chapter 3.

The aim of Chapter 5 is to provide an analysis of the findings presented in Chapter 4, and discuss their relationship to the issues of smart toy security and privacy outlined in the literature review. The main research question and sub-questions introduced in Chapter 3 are answered using these findings.

This chapter consists of four sections. Section 5.2 answers the research sub-questions and hypothesis posed in Chapter 3, and discusses whether the findings reflect, advance, or contradict previous relevant research presented in the literature review. Section 5.3 answers the main research question, thereby satisfying the overall aim of this study. Additional discussion of key findings from this study is presented in Section 5.4. Finally, based on all findings, Section 5.5 presents recommendations for strengthening user privacy and security in the smart toy environment.

5.2 Research Sub-Questions

Three sub-questions were posed in Chapter 3 to assist in answering the main research question. The following sections answer each of these sub-questions.

5.2.1 Sub-Question 1

SQ1. What level of privacy and security concern do New Zealand parents and guardians have regarding smart toy use?

Answer:

The findings show that New Zealand parents and guardians have a high level of concern around both the privacy and the security risks of smart toy use.

Discussion:

The results from this study support the literature findings discussed in Chapter 2 that concluded international concern was growing in this area (Tang & Hung, 2017). This high level of global concern suggests that manufacturers of smart toys should consider placing more attention on this area, and focus on addressing the security and privacy concerns that parents are expressing.

The literature review found smart toy companies have been slow to respond to privacy concerns, with many privacy policies reportedly hard to read, and residing in unhelpful locations (Alonso et al., 2016; Tang & Hung, 2017). Evidence from the physical testing phase of this research, however, shows that this situation has improved. All toys tested had dedicated support functions

to address customer privacy concerns, and most had easy to locate privacy policies available in multiple locations. Addressing privacy concerns from parents and guardians demonstrates that smart toy companies are starting to recognise the importance of children's privacy issues.

Security concerns, however, have not been similarly addressed by the smart toy industry. The literature review described companies shifting more responsibility for security onto the customer (Kshetri & Voas, 2018), and failing to remedy known security vulnerabilities (Mahmoud, 2018). This lack of response to security concerns was backed up by the results of this study, which found a lack of security controls implemented on many of the toys tested, as seen in Section 4.3. Additionally, only limited public information was available about the specific technical security measures implemented in the toys assessed. This absence of comprehensive information also demonstrates a lack of responsiveness by smart toy companies to user concern in this area.

Failing to fully address the demonstrable user concern around security and privacy risks may ultimately lead to a lack of trust in the industry by New Zealand parents and guardians. Each toy tested in this study requested permissions for multiple types of user data and mobile device access, as seen in Section 4.3.3. Most of this data is currently used for product improvement and therefore, ultimately to increase customer satisfaction, the number of smart toys sold, and the subsequent profit for the companies producing them. The toy industry has expressed concern around stronger regulation of children's data leading to an inability to improve their products (Tang & Hung, 2017). Should security concerns remain unaddressed by these companies, New Zealand parents and guardians may become unwilling to share data and start to demand the stronger regulation that smart toy companies wish to avoid.

The high levels of concern shown by participants in this study are unlikely to reduce until the smart toy industry has addressed security and privacy concerns adequately, and demonstrated a track record of smart toy safety. As the literature review described several recent security issues and data breaches, the conditions required to reduce this concern still seem some way off.

5.2.2 Sub-Question 2

SQ2. What level of privacy and security awareness do New Zealand parents and guardians have regarding smart toy use?

Answer:

The findings show that New Zealand parents and guardians have a low level of awareness regarding the privacy and security risks of smart toy use.

Discussion:

Awareness was measured in five areas, as follows:

Knowledge of the Technical Capabilities of Smart Toys

The findings of this study indicate that parents and guardians know less about some smart toy capabilities, such as pervasive internet connectivity and the use of sensors than others, such as speaker and camera functionality. This may be because these features are not immediately apparent to the eye, and work in the background of a play session without the need for any user control. Unawareness of these features, however, may expose users to a higher risk of suffering a privacy or security breach as they may not take protective measures to prevent this occurring.

For example, the findings seen in Section 4.3.3 show that security controls developed to prevent the physical location tracking of a child are not evident in all smart toys. Lack of physical security controls combined with a lack of user awareness around the ability for a toy to have location tracking capability, leads to an enhanced risk of a child being tracked without the knowledge of their parent or guardian.

Understanding a smart toy's technical capabilities is additionally complicated, as smart toy manufacturers often avoid technical jargon when promoting their products. The link between a smart toy's advertised features, such as "Easy connectivity" or "Interactive games", and the underlying technical capabilities that enable these features such as GPS and Bluetooth Smart, may not be apparent to the general consumer. Highlighting the risks associated with some of these underlying capabilities is one area that is important for end-users to remain safe, but where responsibility remains unclear.

Knowledge of Common Potential Smart Toy Security and Privacy Risks and Vulnerabilities

The findings in Section 4.2.2.4 indicated a gap in knowledge around potential smart toy security risks and vulnerabilities. Without an understanding of the current vulnerabilities found in these toys, a parent or guardian may believe they are safer than they actually are. Conversely, understanding that a smart toy cannot receive security updates could allow a user to make an informed decision on how long they keep a toy operational. Much like the knowledge that meat is only safe to eat within a set time, the awareness that a smart toy is protected against known malware for a limited period only could help a user to understand and mitigate any risks the use of this product may pose.

Another vulnerability that was not widely understood by New Zealand parents and guardians was the ability for smart toy content to be intercepted and changed. Both the literature review in Chapter 2 and the physical test findings in Section 4.3.1 confirmed that this vulnerability exists in smart toys available to New Zealanders. The use of unauthenticated Bluetooth pairing, insecure Wi-Fi networks, and unencrypted data transmission, as demonstrated in the results of this study, allow for the possibility of valid smart toy content to be replaced with objectionable material. Low awareness of this risk by users may mean that smart toy manufacturers continue to use technology susceptible to this, as they receive no demands for change. Education on the vulnerabilities that may exist in the smart toy environment may assist parents and guardians protect themselves, and give them the knowledge to advocate for stronger technical security controls in these products.

Knowledge of the Data Procedures Used by Smart Toy and Affiliate Companies

The results in Section 4.2.2.1 show that many New Zealand parents and guardians are unaware of where smart toy companies store the data they collect, and in particular, that this data can be sent and stored offshore. This issue appears to be compounded by the findings from the physical toy testing phase of this study, which show that smart toy privacy policies do not always disclose this information.

Whilst many countries are tightening their data privacy laws, the literature review highlighted how different jurisdictions could currently have very different privacy legislation (Moini, 2017). It is therefore essential for a user to know where their data is stored to understand the laws that apply to its use. The results from this study prove that this is not always possible due to the lack of information shared by smart toy companies. This situation should be addressed to allow customers to be fully informed of what they agree to when they use a smart toy and share children's data.

Research indicates that technology product manufacturers are one of the heaviest users of the cloud (Zachary, 2019). The use of cloud-based data storage, however, may complicate the ability for any smart toy companies to achieve data location transparency. By its inherent design, multi-tenanted virtual storage allows data to be hosted and backed up across multiple locations, adding to the challenge of knowing exactly where data is held at any one time. While this form of storage makes economic sense for many companies, it is not the only available option. Companies using cloud storage need to ensure that cloud service providers are adapting to satisfy new data regulations such as the GDPR and provide enough specific details regarding where data resides. Ensuring the location of sensitive data such as children's PII is fully known, is key to providing further transparency to parents and guardians about where their data is held and fixing this current gap.

Overall, the results of this study indicated that the understanding of how smart toy companies use the data they collect is low. This low awareness is apparent, despite findings from the physical inspection of the toys showing that all smart toy privacy policies declared the types of data collected and how it would be used. These results suggest that the information within privacy policies is either not read or understood by users, and that new and more effective ways of informing and educating parents and guardians, beyond the use of written policies, needs to be investigated.

One toy tested in this study (the R2-D2 Droid), forced the user to read and accept their privacy policy before allowing any access to the mobile companion application. This compulsory step during the set up procedure could be a design other smart toy companies could adopt to emphasise the importance of reading this information. However, the R2-D2 Droid privacy policy itself was still a traditional, wordy, text-only document. This form of communication may not appeal to all users or be an effective way to convey privacy information as it assumes a reasonable level of written literacy which all users may not possess.

A low level of awareness of how data is used could ultimately lead to unwelcomed surprises if parents give uninformed consent for companies to use their child's data, and it is subsequently sold or used for purposes beyond the original intent. For example, a child's future application for health insurance or finance may potentially be negatively impacted if data such as medical information is shared to a third party without their knowledge. As smart toys become more prevalent in society, the opportunities for the misuse of children's data will increase. Therefore, it becomes imperative to fully understand the data procedures used by companies handling children's data to avoid future hurt.

Knowledge of Data Protection and Privacy Law/Legal Aspects in New Zealand

The results of this study seen in Section 4.2.2.4 found a deficient level of understanding and awareness around data protection and privacy law by New Zealand parents and guardians. Of concern is the perceived belief that current New Zealand legislation will protect a user's data from all misuse by international toy companies.

This misperception is unhelpful, as the physical test findings in Section 4.3.3 also showed that some smart toy companies only agree to delete personal information held to the extent with which they are required to by law. If New Zealand parents and guardians believe that legislation protects them more than it does, and toy companies only comply with customer requests if they are legally bound to do so, a New Zealand user may find themselves unable to exercise the amount of control they would like or expect to have over their data once it has been shared.

Overestimating the level of protection that New Zealand legislation gives also means parents and guardians may not pay close attention to stated data privacy policies, incorrectly believing they do not need to worry about how smart toy companies handle their child's data.

Reform of New Zealand's *Privacy Act* is proposed in 2020, which would strengthen the current privacy law by introducing more regulations, including increased cross-border data protection (Office of the Privacy Commissioner, n.d.). The findings of this study support the need for these legislative changes, as they may go some way to aligning the current legislation with the expectations of the law seen by parents and guardians in this study. The proposed changes are yet to be approved or actioned, therefore New Zealand parents and guardians continue to make decisions in this area without adequate knowledge. Should the changes be passed into law, this could be a good opportunity to publicise and educate New Zealanders around what New Zealand privacy legislation covers and what it does not, and thereby reduce any misperceptions currently held.

Knowledge of Security and Privacy Protection Strategies

New Zealand parents and guardians showed a high level of awareness around security and privacy protection strategies, particularly in areas of older and familiar areas of technology risk such as password selection. Protection strategies for newer technology features such as the location tracking feature now commonly seen in smart toys was lacking. These results suggest that knowledge and awareness of how to mitigate risk grow the longer a technology is in use.

With the fast rate of technological advancement and the potential safety consequences of not implementing protection strategies for technology used by children, this learning curve must be accelerated. Society as a whole shares the responsibility to protect its vulnerable members and therefore, to educate parents and guardians on how to protect their families from the risks involved with using smart toys. New methods to highlight evolving technology risks and potential protection strategies need exploring.

Male Versus Female Awareness of Smart Toy Security and Privacy Risks

Overall this study has highlighted that males have a greater knowledge of smart toy security and privacy risks than females. Whilst exact numbers are unknown, most literature agrees that women are responsible for a higher percentage of all household and consumer purchasing than men (Bloomberg, 2018). Along with often being the primary caregivers of children in society, this suggests it is New Zealand women who may ultimately decide whether to purchase a smart toy for a child. The lower level of awareness demonstrated in this study by females around the risks of these products, could mean those without enough knowledge of how smart toys can be safely used are purchasing the majority of these toys in New Zealand. This may subsequently increase the overall risk to children from these products. An investigation into why such a difference in knowledge was seen between genders in this study may allow new education strategies to be formed to close this gap and reduce the risk it currently presents to families.

Level of Education and Smart Toy Security and Privacy Risk Awareness

This study found that on average, the higher the level of education a parent or guardian held, the higher the level of awareness they had around privacy and security risks. These results give an insight into how New Zealand could lower the risk these products potentially pose in the community by clearly identifying where education on privacy and security issues would be most beneficial.

All New Zealand households have equal rights to purchase technology, and therefore all households should have equal opportunity to understand any risks their purchases may present. Users with lower levels of education may have less ability to comprehend the currently available privacy policies, once again highlighting the need for alternative education methods.

While parents and guardians are ultimately responsible for the safety and wellbeing of any child in their care, more diverse communication methods around technology risk may also assist in informing children themselves around the implications of using these products. The literature review suggested children are often unaware of how smart toys can monitor them (McReynolds

et al., 2017), and therefore arming children with more knowledge around their toys seems sensible so that they can adjust their behaviours in response to this information.

Strategies to increase the knowledge of privacy and security risks in smart toys, outside of formal education, perhaps using methods such as video demonstrations or graphical systems, should therefore be investigated to lift the awareness of both adults with a lower level of formal education and the children that use these smart toys.

5.2.3 Hypothesis

H1. A higher level of participant concern around smart toy privacy and security risks will correlate to a higher level of participant awareness around these risks.

Answer:

The results confirm a positive correlation between the level of concern and the level of awareness.

Discussion:

Whilst the findings from this study confirmed that greater concern over privacy and security risks was seen in those with higher levels of knowledge or awareness around these risks, the correlation was small. This correlation suggests that increasing levels of knowledge may lead to increased levels of concern; however, the survey results showed that high levels of concern of the potential risks of smart toys could also exist without high levels of awareness. Further research is required to fully understand this tenuous relationship and determine how one factor may influence the other either positively or negatively.

5.2.4 Sub-Question 3

SQ3. What common security and privacy impacting vulnerabilities are found in smart toys currently available for purchase by New Zealanders?

Answer:

1. Insufficient authentication vulnerabilities including unauthenticated Bluetooth pairing, unauthenticated Wi-Fi connections, insufficiently strong passwords, and insecure account lockout mechanisms were found.
2. Insecure data transfer vulnerabilities, including no use of encryption for communication were found.
3. Insufficient privacy protection vulnerabilities including unreasonable PII collection, non-comprehensive privacy policy, no acceptable parental control mechanisms, and no use of a random device identifier were found.

Discussion:

Security vulnerabilities were assessed in three areas as follows.

Insufficient Authentication

The results of this study reflect previous international research that demonstrated smart toys use insecure Bluetooth or Wi-Fi implementations. Additionally, this study found weaknesses in passwords used and password lockout mechanisms.

While the literature review discussed the difficulty in securing IoT devices such as smart toys (Sha et al., 2018), it also highlighted advances made in some areas that allow the implementation of additional security (Townsend et al., 2014). All of the insufficient authentication vulnerabilities found in this study are known, and many are seen in previous research outlined in Chapter 2. This is concerning as it highlights that smart toy companies are not responding or adding security functions to their products, despite being made aware that the vulnerabilities exist.

Insufficient authentication may allow unauthorised access to the smart toy network and data. If unauthorised access is gained, negative impacts could include data loss, manipulation, or theft. Inappropriate data could also be inserted into the communication stream, or the user could lose control of the smart toy altogether.

Two of the smart toys studied were found to use BLE with legacy pairing methods that do not allow authentication to occur. Subsequent Bluetooth releases have introduced Secure Connection Only modes and alternative pairing methods that allow the implementation of full authentication. Smart toy companies must find a way to incorporate these new standards into their toys to respond to consumer concern and mitigate these risks.

One smart toy studied used an open Wi-Fi network with no security measures. The dangers of open Wi-Fi networks are well documented (Bencie, 2017; Dolly, 2018), and their use can only suggest that smart toy manufacturers are still not sufficiently considering security and privacy risks when designing their toys. These findings support literature that suggests manufacturers are placing too much emphasis on ease of use and keeping development costs low, instead of implementing security and privacy features on smart toys, ultimately endangering the end-users of these products, namely children.

Insecure Data Transfer

The findings in this area showed a mixed but ultimately more positive outlook than results seen in the previous research discussed in Chapter 2.

The literature review highlighted many issues and challenges involved in implementing secure encryption protocols within the IoT environment (El Mouaatamid et al., 2016). Some of the smart toys evaluated in this study have found ways to use traditional secure network encryption protocols such as TLS over the home Wi-Fi network. These results show it is feasible to design smart toys that fulfil secure data transfer needs.

While additional steps may be required in the set up process to join a secure network, the level of parental concern around safety shown in this study suggests customers would be willing to sacrifice some usability for a more secure product overall. Smart toy manufacturers could

consider using robust security practices as a marketing tool to offset any perceived inconvenience from the addition of these security steps.

Insufficient Privacy Protection

The findings in this area were very mixed and seem to demonstrate that smart toy companies are responding to increasing privacy concern by implementing robust privacy protection practices in some areas, while ignoring other perhaps more challenging areas altogether.

The ability for parents and guardians to have control over the data a smart toy collects and stores is one area that appears to have made little progress. The literature review highlighted the necessity of parental controls, but also the ethical questions that remain unanswered in this area, such as what level of monitoring of child's play by parents is appropriate (Jones & Meurer, 2016). These unresolved ethical dilemmas may have hampered the progress of implementing technical parental controls, and further research to clarify this space may prompt the development of these necessary features for smart toys.

Without parental controls available on these toys, a parent or guardian has limited ways in which they can protect their child from any potential data misuse. None of the toys studied in this research implemented robust parental control mechanisms, leading to scenarios such as stored audio files being unable to be deleted from toys, and PII residing in mobile applications beyond its use. Any data that is stored unnecessarily presents additional opportunities for data theft or modification that could easily be avoided by its erasure. Providing mechanisms by which a parent or guardian can monitor and delete captured data would ultimately reduce the attack surface of these toys.

5.3 Main Research Question

The overall aim of this study was to answer the following main research question:

Q1. Do smart toys pose a security or privacy risk to users in New Zealand?

Answer:

Yes, smart toys pose some security and privacy risks to New Zealand users.

Discussion:

The combination of low levels of smart toy security and privacy awareness seen in this study, and the physical testing results that demonstrate security and privacy vulnerabilities exist in some smart toys available for purchase, lead to the possibility of New Zealanders having their security or privacy negatively impacted by using smart toys.

The level of risk this poses, however, varies greatly depending on the choice of individual smart toy and how it is used. Some smart toys pose less risk than others, either by implementing stronger physical controls or by not collecting and using PII. Smart toys that require authentication, use secure transport mechanisms, and refrain from collecting excessive personal information, leave little opportunity for a privacy or security issue to occur and therefore could

be deemed lower-risk items. In contrast, those that do not implement any physical control mechanisms and collect and handle PII are vulnerable to a variety of privacy and security attacks, and present many opportunities for user exploitation.

How a smart toy is used and whether a parent or guardian implements protective mechanisms in the wider environment may also influence the level of risk presented by a smart toy. Some smart toys offer the user a choice as to how much PII they collect. While refusing to hand over PII may mean some functions of a smart toy are unavailable, it is a decision that is worth considering carefully. The more information about a child that is presented in an online environment, the more opportunity there is for privacy and security breaches to occur. Using more personal protective mechanisms when operating a smart toy may decrease the opportunity for a vulnerability to be exploited, and therefore lower the overall risk of these products. As long as awareness levels remain low and smart toys contain common vulnerabilities, they will continue to pose security and privacy risks to New Zealand users.

5.4 Additional Discussion

Smart toys can use a wide range of technology implemented in various ways, and all smart toys tested in this study operated quite differently. This variety, combined with a lack of written information, made discovering the security controls, protocols, and levels used in each smart toy a challenge. There currently appears to be no simple way for a parent or guardian to determine the technical security implemented on a toy, even if they have the underlying understanding of the technology used.

More information needs to be readily available to assess the security and privacy of these products both for the general consumer, perhaps displayed in a graphical style such as a traffic light rating, and in more detail for anyone with technical knowledge wishing to understand the device. The findings demonstrate that written privacy policies, which sit somewhere between these two levels of detail, do not seem to be as effective as they could be; yet these are what most companies rely upon for conveying information to the consumer.

This study also found that methods for investigating new technology, such as that seen in smart toys, are lacking. With no clear, standardised measurement system or guidelines for assessing these products, both the manufacturers and consumers must piece together information from varied sources and rely upon common sense to determine the level of security and privacy controls that should be in place. The physical testing results of this study showed that this process is ineffective, as each manufacturer has a very different interpretation of suitable levels of security and privacy controls. Standardisation is one area where organisations such as the NIST, in conjunction with industry regulatory bodies, could play a stronger role moving forward and positively contribute to the IoT environment by creating clear security and privacy measurement guidelines.

5.5 Strengthening User Privacy and Security in the Smart Toy Environment

There is a broad scope for the smart toy environment to become more secure if manufacturers and standards and regulatory bodies completed some of the actions outlined in the previous sections. This includes ensuring the toys are built using secure technical controls, strengthening data regulation, introducing standards for testing devices, and investigating new methods for communicating security information. However, there is still an onus on parents and guardians to take care of their children's security and privacy, and various methods available to do so. Whilst children are seen to become competent technology users from a young age (Nikken & Schols, 2015), the role of the parent or guardian to protect, teach, and be gatekeepers of children's technology use is vital.

There are many recommended techniques for staying safe in the digital world, and although this study showed that most users are aware of these techniques, the sheer volume of information and often conflicting advice published in this area can be confusing (Reeder, Ion, & Consolvo, 2017). Narrowing down the advice to specific areas and prioritising actions may encourage more implementation of these techniques. The physical test results from this study suggest some key areas where immediately implementing personal protections during pre-purchase, setup, and operation of a smart toy would help protect user security and privacy.

Careful selection of a smart toy before purchase to ensure the introduction of safer products into the home is one step a parent or guardian can take. Firstly, considering how recently the toy was released on the market, could assist in determining whether the smart toy uses the most up to date security protocols. Two of the smart toys assessed in this study had been on the market for three years and utilised older less secure Bluetooth implementations. Smart toys designed and released more recently may take the opportunity to implement the latest standards. In addition to this, several smart toys and their companion applications that were initially chosen for this study were found to be no longer supported by the manufacturer, rendering them potentially unsafe as could not receive security updates. Consideration should be given as to whether a company has a proven track record of ongoing support for their products, and communicating clearly with customers around when and how a product decommission might occur.

Researching whether any security or privacy testing has been completed on the toy, or whether any concerns have been raised in media about the product or company that produces it, may also uncover any potential issues before purchase. Awareness of the potential security and privacy issues in these products is heightening globally. The literature review discussed several known security breaches suffered by smart toy companies (BBC, 2017a) and identified some smart toys deemed unsafe internationally that should be avoided by purchasers (Forbrukerradet, 2016; Mills, 2017). Additionally, all of the security and privacy issues seen in the findings of this study are known vulnerabilities, and many have been seen and reported in IoT device studies previously. Therefore, there is some information, albeit still limited, currently available to the

public around security and privacy concerns in specific smart toys that can be used to assist decision-making when purchasing a smart toy.

Implementing protection measures during set up of the smart toy and throughout the areas of the smart toy environment under user control is also recommended to help protect user security and privacy. This study showed that some smart toys utilise the home Wi-Fi network for communication, confirming it is an area that should be prioritised when implementing security mechanisms. A recent study by Douvres and Choi (2019) however, found that many home Wi-Fi networks are still insecure. Parents and guardians should secure smart toy wireless transmissions by ensuring that their home Wi-Fi network is protected. This study demonstrated that insecure Wi-Fi networks with weak passwords could be easily cracked, and therefore changing the default password on the home Wi-Fi router and selecting a unique, secure password is vital. Another step to further secure the home network is ensuring the use of strong encryption. WPA2 is the most recent and effective encryption protocol for home networks, and updating the home router to one that supports and uses this protocol is recommended (CERTNZ, 2020).

Further protective mechanisms for securing a home Wi-Fi network include changing the name of the home wireless network from the default set by the manufacturer to assist in preventing network intrusions. As this SSID information is broadcast, it is also important not to use any identifying information in the name to keep the network anonymous (CERTNZ, 2020). Ensuring the home router firewall is switched on and that all the software used is updated should also be confirmed before smart toy use.

As shown in this study, many smart toys also use a form of Bluetooth for communication. Therefore, along with the home Wi-Fi network, this area is one that should be prioritised in regards to using personal protective mechanisms to enhance security. The findings of this study demonstrated that the Bluetooth implementation used by some smart toys does not require a user to authenticate, thereby allowing anyone within the appropriate vicinity to connect remotely to the smart toy device and access the network. The risk of this occurring can be reduced simply by turning Bluetooth off when not in use.

Another method of Bluetooth pairing seen in the findings of this study was the numeric comparison method. To avoid unauthorised access of any smart toy utilising this pairing method, a user should not enter link keys or PINs into their devices if unexpectedly asked to do so.

The findings also demonstrated how smart toys connected to Bluetooth send advertising beacons regularly, allowing location tracking to occur in many cases. Once again, ensuring Bluetooth is turned off when not in use so that a smart toy is not connected continuously to the internet can protect against this risk.

Another basic security hygiene task that can be undertaken prior to using and whilst using a smart toy, is applying software or firmware updates as soon as available both to the smart toy and any companion application. Keeping systems up to date is one of the most mentioned pieces

of security advice given to users (Reeder et al., 2017) and should be followed wherever possible. Unfortunately, as demonstrated in the literature review, many smart toys as yet do not offer firmware updates, so focusing on mobile companion application updates and general antivirus software updates in the wider smart toy network must be the priority for parents and guardians at this time.

All of the smart toys tested in this study required internet access of some kind to operate, and recognising and understanding that smart toys are often another medium for a child to access the internet is essential. This will enable parents and guardians to understand the risk they present and enable them to moderate how a smart toy is used. There are various ways to moderate a child's technology use, and additional advice on how to keep children safe online that also applies to the smart toy environment is readily available to parents and guardians via organisations such as NetSafe and CERTNZ.

Practical safety strategies that could be considered by parents and guardians include limiting smart toy use outside of the home. Using a smart toy on an open public network such as at the local library or mall should be discouraged, as parents and guardians cannot ensure the security of these networks. As seen in the findings of this study, it is simple to read all data transmitted by a smart toy operating on an open network which could ultimately lead to a privacy breach.

Parents and guardians might also consider only allowing the use of a smart toy in a supervised environment such as a shared living area, rather than the child's bedroom, so that any potential unsafe behaviour can be addressed quickly. Another successful method commonly seen is to co-use the smart toy together (Nikken & Schols, 2015). Co-use gives the opportunity for the parent or guardian not only to monitor how the toy is being used, but to teach the child of the risks these toys may present along the way. Age-appropriate education for any child using smart toys makes sense, as ultimately it is their data and actions that may be exploited.

Research has shown that young people with learning disabilities report a lack of education on technology safety, and additionally, those with learning difficulties are less likely to complete formal education ("Many young people with SEN have not been taught about staying safe online", 2014). The findings from this study also clearly demonstrate that users with lower levels of formal education have less awareness in all areas of smart toy privacy and security knowledge, placing them at higher risk. It is thought that parents who are less technologically savvy may find it more challenging to install appropriate safety mechanisms on smart toys, or discuss the risks critically with their children as compared to more technology literate guardians (Nikken & Schols, 2015). It is therefore imperative that this gap in education is closed for young people, and that all parents and guardians educate themselves on the issues surrounding smart toy use.

Finally, if data privacy is a concern, then parents and guardians should limit the amount of information given to the smart toy, particularly about their child. Reading the privacy policies and terms of use stated by any smart toy purchased is the first step in understanding the risks involved with sharing data with the smart toy and making informed choices.

5.6 Conclusion

Chapter 5 presented a discussion of the findings first presented in Chapter 4, and the main research question and sub-questions posed by this study were answered. The results demonstrated a high level of concern and a low level of awareness around smart toy security and privacy. Vulnerabilities were also seen in the smart toys tested in this study, and it was concluded that smart toys do pose a risk to New Zealand users. This chapter discussed actions the wider industry could take that would enhance the security and privacy of smart toys, and lower this risk, such as implementing more technical security controls into smart toys, developing standard testing methodologies, implementing stronger data regulations, and researching inclusive communication methods for conveying security and privacy information. Finally, the chapter suggests immediate ways in which parents and guardians can better protect themselves and their children in the smart toy environment.

Chapter 6: Conclusion

Chapter 1 introduced the research topic of smart toy privacy and security, outlined the thesis structure, and discussed the motivation behind conducting this study. The literature review presented in Chapter 2 then described the challenges involved with securing IoT devices, and demonstrated valid concerns that user security and privacy are being impacted internationally by new IoT products such as smart toys.

The concerns and issues described in Chapter 2 led to the formation of the research questions for this study focusing on smart toy security and privacy risks to New Zealand users. Similar research studies and industry-standard frameworks were used to develop a suitable methodology for investigating the research questions. Chapter 3 describes the online survey method and the physical security testing approach that was used for this study.

The findings derived from following these methods were presented in Chapter 4. These findings demonstrated vulnerabilities present in the smart toys tested, and high levels of concern around this issue from New Zealand parents and guardians. Chapter 5 analysed and discussed the findings further to link them back to the literature review, and importantly, answer the main research question and sub-questions posed by the study. Some recommendations for how parents and guardians can enhance their security and privacy in the smart toy environment were additionally presented.

This chapter concludes the thesis by summarising the research, highlighting its contributions to the broader area of smart toy security and privacy, and providing suggestions for further research.

6.1 Summary of Research

This research aimed to investigate whether the use of smart toys poses any privacy and security risks to New Zealanders. It targeted New Zealand parents and guardians to study both their levels of concern and their levels of awareness and knowledge of smart toy risks. Additionally, smart toys available for purchase in New Zealand were tested to determine whether they contained vulnerabilities that may impact the privacy and security of New Zealand users.

The smart toys studied demonstrated weaknesses in authentication practices, with some using old, less secure Bluetooth protocols, and others operating over open networks. A lack of secure encryption was also seen in some of the toys tested. Security features in the smart toys did not seem to be prioritised, supporting the literature review, which suggested manufacturers are placing more emphasis on creating cheaper, user-friendly toys, over secure toys. The smart toys tested also collected excessive PII, had no transparency of data storage, and did not implement parental controls suggesting that smart toy manufacturers need to consider privacy concerns more carefully when developing these products.

The smart toy vulnerabilities found in this study contribute to a greater awareness of the potential implications of poor smart toy security design. Smart toys designed without the privacy and

security of their users in mind are more susceptible to known cyberattacks such as unauthorised access, eavesdropping, and device manipulation. Each vulnerability found increases the risk of New Zealand children suffering harm from these toys.

Overall, the awareness New Zealand parents and guardians have of smart toy technical capabilities or features and the risks that these features bring is very low. These low awareness levels contribute to raising the level of risk these products pose, as user knowledge is required to implement protective strategies while using smart toys. Females and participants with lower levels of formal education displayed significantly lower levels of awareness around smart toy risks, placing this population at an even greater danger than most of suffering a privacy or security breach while using smart toys.

Finally, this study highlighted a gap in New Zealanders' understandings of both the data handling practices of smart toy companies and the legal protection afforded them in regards to smart toy security and privacy. Current New Zealand Privacy Act 1993 legislation falls short of the expectations that New Zealand parents and guardians expressed in this research in regards to securing their data from misuse by these companies. If this misalignment continues, New Zealand users will remain at risk of sharing their personal information without awareness of how companies may use data. Furthermore, they may not have the recourse under the law they believe they do to address any subsequent issues encountered.

6.2 Research Methods and Limitations

The use of an anonymous online survey method to obtain data investigating New Zealand parents and guardians levels of concern and awareness of smart toy risks was successful. Response rates to online surveys are generally low (Andres, 2017); however, this limitation was partially mitigated by ensuring the questionnaire was brief and did not require a substantial investment of time from participants. Advertising the survey in a variety of locations such as sports clubs and Plunket groups effectively gained the required number of participants to make this study significant.

Online survey response may also be influenced by age, education, income levels, ethnicity, and internet availability (Andres, 2017). Therefore, full coverage of the target population can be reduced by only offering the survey in a single online mode. However, as the target population of this study was known to have a high internet use rate at over 80% (Statista, 2018), the mode was considered appropriate, and the results demonstrated sufficient population coverage.

Additionally, the use of non-probability sampling for this survey meant that sampling error could not be calculated statistically. In a research project of this size, however, a probability sample is unfeasible to obtain.

To physically test the security controls on a selection of smart toys, a security testing methodology was derived from relevant industry methodologies and similar studies. The tests undertaken in this study were performed in a controlled laboratory environment to ensure any future researchers could replicate this study. An artificial setting is limited, in that it may not

account for any human errors that could occur during smart toy set up and use in a standard home environment. The test environment may also not reflect the full variability of home environments that exist today. This limitation was mitigated however, by setting up the test environment to reflect a typical home use scenario.

A limited number of tests were conducted to identify common vulnerabilities existing in a selection of wirelessly connected smart toys. Failing to find a vulnerability within these tests however, does not exclude the possibility of a more complex vulnerability existing. The scope of each test undertaken was therefore clearly defined to confirm areas covered in this study and support future research. A limited number of smart toys were also included in scope for testing. The toys tested were selected for their variety of technology and target audiences, and were therefore a reasonable representation of the full smart toy market.

The security testing method involved selecting appropriate hardware and software tools to perform a successful investigation. There are a limited number of tools available that effectively perform security testing of IoT devices due to IoT technologies, such as BLE, being relatively new. In particular, capturing Bluetooth traffic for investigation can be challenging due to the need to avoid collisions with other protocols, such as Wi-Fi operating on the same 2.4GHz spectrum. A Bluetooth device such as a smart toy may change transmission frequency many times each second making it difficult for a monitoring device to follow. This limitation was mitigated in this research design by using multiple industry tools to capture the Bluetooth communication, and in most cases, this proved a successful technique to gain results in this study.

6.3 Recommendations and Contributions

This study has shed light on the current smart toy security and privacy situation in New Zealand that was previously unexplored. It has confirmed that the vulnerabilities found and documented overseas also exist in toys in New Zealand. Recognising that negative security and privacy impacts are possible when using smart toys in New Zealand, highlights the importance of generating greater awareness of these issues. Advocating for stronger legislation to protect children and more methods to educate New Zealand parents and guardians is vital. This research has also shown that targeting education and awareness programmes to females and those with lower levels of formal education has the potential to positively influence the overall awareness levels around these risks in New Zealand.

The smart toy industry should consider the implementation of minimum basic security controls wherever possible in devices destined for use by children. More focus on incorporating and marketing security and privacy controls, above offering lower prices and additional features in smart toys, may help to ensure the protection of children and their data. The use of more modern BLE standards such as BLE 4.2 rather than 4.0 and reducing any unnecessary PII collected are two examples of simple design decisions that could be implemented to reduce the level of risk these toys present currently.

This research highlights a gap in New Zealand consumer awareness around smart toy security and privacy risks, and also highlights the overconfidence consumers place in both

manufacturers to provide secure products, and regulation to provide full legal protection. In addition to advocating for stronger regulation and more securely designed products, New Zealand parents and guardians can endeavour to educate themselves on the technologies embedded in smart toys, and proactively take steps to mitigate the risks of using them. Protective mechanisms that do not rely upon outside input, such as selecting strong passwords for user accounts, securing the home Wi-Fi network with up to date protocols, disabling Bluetooth when not in use, and being aware of the information a child is sharing with a smart toy and how the smart toy will use this data, should all be considered as they will lower the risk of any security and privacy impacts when using smart toys.

6.4 Future Research

There are several potential further research areas that if undertaken, could further advance overall knowledge around smart toy privacy and security in New Zealand. This study looked at secure authentication, transport and privacy; however, there are other dimensions of vulnerability that could be assessed in the attack surface of smart toys such as their firmware, security updates, and cloud-based storage. A study of these additional potential areas of vulnerability could build upon this research, and identify further protective mechanisms available for enhancing smart toy privacy and security.

It was clear from this study that current methods to inform and educate users on smart toy security and privacy issues, such as privacy policies, are not fully effective. Therefore, research to determine alternative methods for communicating this knowledge and increasing levels of awareness in the user community is recommended. Using the findings from this study that indicate some population groups currently have less knowledge about these issues than others, and focusing on investigating how awareness programmes could effectively target women and those with lower levels of formal education is a recommendation. Whilst this study confirmed a hypothesis that greater levels of smart toy privacy and security concern correlate to greater levels of smart toy awareness, further analysis of this relationship is also required to determine any impact that one may have on the other.

This study found that even for the technologically savvy user, determining the levels of security implemented in a smart toy is challenging. Further research to investigate how the transparency of this information could be increased and the security levels in a device more easily assessed both for the research community and the general user population, may enhance the ease of which future knowledge in the area of smart toy privacy and security is gained.

6.5 Conclusion

Smart toys are a flourishing consumer product in the IoT that use innovative technology to deliver novel and personalised play experiences to children. This research reported potential vulnerabilities in these products that may impact the privacy and security of New Zealand users. This study also demonstrated that while New Zealand parents and guardians are concerned

about these issues, their knowledge of the risks these products present, and how to manage these risks, is low.

The significance of this research is in revealing the potential harm that could be suffered by New Zealanders using smart toys without adequate awareness of the security and privacy risks they currently pose. Mitigating any future risk to New Zealand children from smart toy use may involve the combined effort of manufacturers prioritising and designing more secure products, legislation tightening to protect children's data further, and parents and guardians raising their awareness levels around the technology risks and corresponding safety strategies relevant to smart toys.

References

- Al Johani, M. (2016). *Personal information disclosure and privacy in social networking sites* (Master's thesis, Auckland University of Technology, Auckland, New Zealand).
Retrieved from <http://hdl.handle.net/10292/10320>
- Alaba, F. A., Othman, M., Hashem, I. T., & Alotaibi, F. (2017). Review: Internet of Things security: A survey. *Journal of Network and Computer Applications*, 88, 10–28.
<https://doi.org/10.1016/j.jnca.2017.04.002>
- Alonso, C., Gray, S., Morris, E., Hanley, J., Anderson, S., Jiang, H., & Tabatabai, E. (2016). Kids & the connected home: Privacy in the age of connected dolls, talking dinosaurs, and battling robots. Retrieved from <https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf>
- Alrababah, D., Al-Shammari, E., & Alsuh, A. (2017). A survey: Authentication protocols for wireless sensor network in the Internet of Things; Keys and attacks. *International Conference on New Trends in Computing Sciences (ICTCS)*, 270.
<https://doi.org/10.1109/ICTCS.2017.34>
- Andres, L. (2017). *Designing and doing survey research*.
<https://doi.org/10.4135/9781526402202>.
- Bassi, A., Europe, H., & Horn, G. (2008, September). *Internet of Things in 2020: A roadmap for the future*. Paper presented at the meeting of Information Society and Media, European Commission. Retrieved from
http://old.sztaki.hu/~pbakonyi/bme/keg/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v3.pdf
- Bauer, M., Boussard, M., Bui, N., Carrez, F., Jardak C., De Loof, J., ... Salinas, A. (2013). *Internet of Things – Architecture IoT-A Deliverable D1.5 – Final architectural reference model for the IoT v3.0*. Retrieved from <https://www.researchgate.net/>
- BBC. (2017a, February 28). Children's messages in CloudPets data breach. *BBC News*.
Retrieved from <https://www.bbc.com>
- BBC. (2017b, February 17). German parents told to destroy Cayla dolls over hacking fears. *BBC News*. Retrieved from <https://www.bbc.com>

- Bencie, L. (2017, May 3). Why you really need to stop using public Wi-Fi. *Harvard Business Review*. Retrieved from <https://hbr.org>
- Bertino, E., & Islam, N. (2017). Botnets and Internet of Things security. *Computer*, 50(2), 76–79. <https://doi.org/10.1109/MC.2017.62>
- Bloomberg. (2018, January 11). Top 10 things everyone should know about women consumers. *Bloomberg*. Retrieved from <https://www.bloomberg.com>
- Bluetooth SIG. (2019). *Bluetooth core specification V 5.1*. Retrieved from <https://www.bluetooth.com/specifications/bluetooth-core-specification>
- Butler, D., Huang, J., Roesner, F., & Cakmak, M. (2015). The privacy-utility trade-off for remotely teleoperated robots. *HRI '15: Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction*, 27–34. <https://doi.org/10.1145/2696454.269484>
- Canonical. (2017). *Taking charge of the IoT's security vulnerabilities*. Retrieved from <https://pages.ubuntu.com/rs/066-EOV-335/images/loTSecurityWhitepaper-FinalReport.pdf>
- CERTNZ. (2020). Secure your home network. Retrieved January 1, 2020, from <https://www.cert.govt.nz/individuals/guides/stepping-up-your-cyber-security/secure-your-home-network/>
- Ciampa, M. (2018). *Security+ guide to network security fundamentals*. Boston, MA: Cengage.
- Cha, S., Tsai, T., Peng, W., Huang, T., & Hsu, T. (2017). Privacy-aware and blockchain connected gateways for users to access legacy IoT devices. *2017 IEEE 6th Global Conference on Consumer Electronics, GCCE 2017*, 1, 1–3. <https://doi.org/10.1109/GCCE.2017.8229327>
- Chasker, H. (2017, June 22). For IoT over WiFi, 802.11ax is the new HaLow. *Network Computing*. Retrieved from <https://www.networkcomputing.com>
- Chothia, T., & de Ruiter, J. (2016, August). *Learning from others' mistakes: Penetration testing IoT devices in the classroom*. Paper presented at the 2016 USENIX Workshop on Advances in Security Education, Texas. Retrieved from <https://www.usenix.org/system/files/conference/ase16/ase16-paper-chothia.pdf>

- Cohen, K., & Yeung, C. (2015). *Kids' apps disclosures revisited*. Retrieved September 21, 2018, from <https://www.ftc.gov/news-events/blogs/business-blog/2015/09/kids-apps-disclosures-revisited>
- Commerce Commission New Zealand. (n.d.). Children's toys. Retrieved November 20, 2018, from <https://comcom.govt.nz/business/your-obligations-as-a-business/product-safety-standards/childrens-toys>
- Condon, C. (2019). *How to hack your Furby Connect – A beginner's guide*. Retrieved June 10, 2019, from <https://medium.com/@chloecondon/how-to-hack-your-furby-connect-a-beginners-guide-d4337c458296>
- CPSC. (n.d.). Small parts for toys and children's products business guidance. Retrieved December 1, 2019, from <https://www.cpsc.gov/Business--Manufacturing/Business-Education/Business-Guidance/Small-Parts-for-Toys-and-Childrens-Products>
- Cusack, B., Antony, B., Ward, G., Mody, S. (2017). Assessment of security vulnerabilities in wearable devices. *The Proceedings of 15th Australian Information Security Management Conference*, 42–48. <https://doi.org/10.4225/75/5a84e6c295b44>
- De Lima Salgado, A., Agostini do Amaral, L., Castro, P., & De Mattos Forte, R. P. (2017). Designing for parental control: Enriching usability and accessibility in the context of smart toys. In J. K. T Tang & P. C .K Hung (Eds.), *Computing in smart toys* (pp. 103–125). https://doi.org/10.1007/978-3-319-62072-5_7
- Denning, T., Matuszek, C., Koscher, K., Smith, J., & Kohno, T. (2009). A spotlight on security and privacy risks with future household robots: Attacks and lessons. *Proceedings of the 11th International Conference on Ubiquitous computing*, 105–114. <https://doi.org/10.1145/1630000.1620564>
- Dibrov, Y. (2017). The Internet of Things is going to change everything about cybersecurity. *Harvard Business Review Digital Articles*, 2–5. Retrieved from: <https://hbr.org/>
- Dolly, J. (2018). Why you should never, ever connect to public WiFi. Retrieved January 10, 2020, from <https://www.csoonline.com/article/3246984/why-you-should-never-ever-connect-to-public-wifi.html>

- Donmeyer, C. J., & Cross, B. L. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness and use of privacy protection strategies. *Journal of Interactive Marketing*, 17(2), 34–51.
<https://doi.org/10.1002/dir.10053>
- Douvres, N. A., & Choi, Y. B. (2019). Protecting house and home. *Proceedings for the Northeast Region Decision Sciences Institute (NEDSI)*, 433–447. Retrieved from <http://www.nedsi.org>
- El Mouaatamid, O., Lahmer, M., & Belkasmi, M. (2016). Internet of Things security: Layered classification of attacks and possible countermeasures. *Electronic Journal of Information Technology*, 9. Retrieved from <http://www.revue-eti.net>
- European Commission (n.d.). 2018 reform of EU data protection rules. Retrieved November 10, 2018, from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- European Union Safer Internet Programme. (n.d.). *Benchmarking of parental control tools for the online protection of children*. Retrieved October 21, 2018, from <https://sipbench.eu/index.cfm/secid.15/secid2.17>
- Federal Bureau of Investigation. (2017). *Consumer notice: Internet-connected toys could present privacy and contact concerns for children*. Retrieved October 31, 2017, from <https://www.ic3.gov/media/2017/170717.aspx>
- Federal Trade Commission. (1998). *Children's Online Privacy Protection Act of 1998*. Retrieved November 15, 2019, from <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>
- Federal Trade Commission. (2015). Internet of Things: Privacy and security in a connected world. *Journal of Current Issues in Media & Telecommunications*, 7(2), 155–188.
- Federal Trade Commission. (2018, January 8). *Electronic toy maker VTech settles FTC allegations that it violated children's privacy law and the FTC Act*. Retrieved August 20, 2018, from <https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated>
- Forbrukerradet. (2016). *Investigation of privacy and security issues with smart toys*. Retrieved from <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical-analysis-of-the-dolls-bouvet.pdf>

- Fox-Brewster, T. (2015, September). It's depressingly easy to spy on vulnerable baby monitors using just a browser. *Forbes*. Retrieved from <https://forbes.com>
- Fox, A. K., & Hoy, M. G. (2019). Smart devices, smart decisions? Implications of parents' sharenting for children's online privacy: An investigation of mothers. *Journal of Public Policy & Marketing*, 38(4), 414–432. <https://doi.org/10.1177/0743915619858290>
- Fuertes, W., Quimbiulco, K., Galárraga, F., & Garcia-Dorado, J. (2015). On the development of advanced parental control tools. *Proceedings of 1st International Conference on Software Security and Assurance (ICSSA)*, 1. <https://doi.org/10.1109/ICSSA.2015.011>
- Gartner. (2013). Forecast: The Internet of Things, worldwide, 2013. Retrieved February 4, 2018, from <https://www.gartner.com>
- Gaur, A. S., & Gaur, S. S. (2009). *Statistical methods for practice and research: A guide to data analysis using SPSS*. Los Angeles, CA: Response.
- Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., Baldini, G. (2017). Security and privacy issues for an IoT based smart home. *40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1292. <https://doi.org/10.23919/MIPRO.2017.7973622>
- Green, J. (2004, November). *The Internet of Things reference model*. Paper presented at the Internet of Things World Forum, Chicago, Illinois. Retrieved from http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf
- Groves, R. M. (2009). *Survey methodology*. Retrieved from <https://ebookcentral.proquest.com>
- Gusmeroli, S., Piccione, S., & Rotondi, D. (2013). A capability-based security approach to manage access control in the Internet of Things. *Mathematical and Computer Modelling*, 58, 1189–1205. <https://doi.org/10.1016/j.mcm.2013.02.006>
- Harwell, M., & Gatti, G. (2001). Rescaling ordinal data to interval data in educational research. *Review of Educational Research*, 71(1), 105. <https://doi.org/10.3102/00346543071001105>
- Hasbro. (2019a). *Furby Connect*. Retrieved October 13, 2019, from <https://furby.hasbro.com/en-us>
- Hasbro. (2019b). *furReal StarLily, My Magical Unicorn interactive plush pet toy, light-up horn, ages 4 and Up*. Retrieved October 30, 2019, from <https://shop.hasbro.com>

- Hewlett Packard Enterprise. (2014). *HP study reveals 70 percent of Internet of Things devices vulnerable to attack*. Retrieved February 4, 2018, from <http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WnY8wKLxxe9>
- Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, 37(1), 275–298. Retrieved from <http://www.misq.org/>
- Howard, M. C. (2018). Scale pretesting. *Practical Assessment, Research & Evaluation*, 23(5). Retrieved from <http://pareonline.net>
- Institute for Security and Open Methodologies. (2009). Open source security testing methodology manual. Retrieved from: <http://www.isecom.org/mirror/OSSTMM.3.pdf>
- Internet of Things. (2019). In *English Oxford Living Dictionary*. Retrieved from https://en.oxforddictionaries.com/definition/internet_of_things
- Javelin Strategy and Research. (2018). *2018 Child Identity Fraud Study*. Retrieved from <https://www.javelinstrategy.com/coverage-area/2018-child-identity-fraud-study>
- Jodka, S. (2017). *The Internet of Toys: Legal and privacy issues with connected toys*. Retrieved September 11, 2018, from <http://www.dickinson-wright.com/news-alerts/legal-and-privacy-issues-with-connected-toys>
- Jones, M. L., & Meurer, K. (2016). Can (and should) Hello Barbie keep a secret? *IEEE International Symposium on Ethics in Engineering, Science and Technology (ETHICS), Ethics in Engineering, Science and Technology*, 1. <https://doi.org/10.1109/ETHICS.2016.7560047>
- Juniper Research. (2018). *Smart toys: Hardware, technology & leading vendors 2018–2023*. Retrieved November 5, 2018, from <https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-to-grow-by-almost-200>
- Kambourakis, G., Kolias, C., & Stavrou, A. (2017). The Mirai botnet and the IoT zombie armies. *IEEE Military Communications Conference (MILCOM)*, 267. <https://doi.org/10.1109/MILCOM.2017.8170867>
- Kelley, P., Bresee, J., Cranor, L., & Reeder, R. (2009). A nutrition label for privacy. *Paper presented at the Symposium of Usable Privacy and Security (SOUPS'09)*. <https://doi.org/10.1145/1572532.1572538>

- Kickstarter. (2018). CogniToys: Internet-connected smart toys that learn and grow. Retrieved November 10, 2019, from <https://www.kickstarter.com/projects/cognitoys/cognitoys-internet-connected-smart-toys-that-learn>
- Kismet. (2019). *Kismet*. Retrieved from <https://www.kismetwireless.net>
- Kliarsky, A. (2017). *Detecting attacks against the 'Internet of Things'*. Retrieved from: <https://www.sans.org/reading-room/whitepapers/internet/detecting-attacks-039-internet-things-039-37712>
- Knapp, T. R. (1990). Treating ordinal scales as interval scales: An attempt to resolve the controversy. *Nursing Research*, 39(2), 121–123. Retrieved from <http://www.ovid.com>
- Kshetri, N., & Voas, J. (2018). Cyberthreats under the bed. *Computer*, 51, 92. <https://doi.org/10.1109/MC.2018.2381121>
- Kumar, K., Mouli, C., & Kumar, U. (2017). A survey on the Internet of Things-based service orientated architecture. *International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECOT)*, 435. <https://doi.org/10.1109/ICEECOT.2017.8284544>
- Kurio. (n.d.). *KurioWatch*. Retrieved November 1, 2019, from <https://kurioworld.com/uk/products/kurio-watch-2/>
- Laplante, P., Voas, J., & Laplante, N. (2016). Standards for the Internet of Things: A case study in disaster response. *Computer*, 5, 87. <https://doi.org/10.1109/MC.2016.137>
- Leonardi, L. (2018). Multihop real-time communication over BLE industrial wireless mesh networks. *IEEE Access*, 4, 1. <https://doi.org/10.1109/ACCESS.2018.2834479>
- Lin, J., Yu, W., Nan, Z., Xinyu, Y., Hanlin, Z., & Wei, Z., (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications, *IEEE Internet of Things Journal*, 4(5). 1125–1142. <https://doi.org/10.1109/JIOT.2017.26832>
- Lindqvist, U., & Neumann, P. G. (2017). The future of the Internet of Things. *Communications of the ACM*, 60(2), 26–30. <https://doi.org/10.1145/3029589>
- Liu, C., Yang, C., Zhang, X., & Chen, J. (2015). External integrity verification for outsourced big data in cloud and IoT: A big picture. *Future Generation Computer Systems*, 49, 58–67. <https://doi.org/10.1016/j.future.2014.08.007>
- Liu, C. (2015). Feature: Securing networks in the Internet of Things era. *Computer Fraud & Security*, 13–16. [https://doi.org/10.1016/S1361-3723\(15\)30028-2](https://doi.org/10.1016/S1361-3723(15)30028-2)

- Mahmoud, M., Hossen, Z., Barakat, H., Mannan, M., & Youssef, A. (2017). Towards a comprehensive analytical framework for smart toy privacy practices. *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, 64–75.
<https://doi.org/10.1145/3167996.3168002>
- Mahmoud, M. (2018). *An experimental evaluation of smart toys security and privacy practices* (Master's thesis, Concordia University, Quebec, Canada). Retrieved from <https://spectrum.library.concordia.ca/983590/>
- Many young people with SEN have not been taught about staying safe online. (2014). *British Journal of School Nursing*, 9(2), 60. Retrieved from <https://www.magonlinelibrary.com>
- McAfee. (2016). *McAfee Labs 2017 threats predictions*. Retrieved from <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-threats-predictions-2017.pdf>
- McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., & Roesner, F. (2017). Toys that listen: A study of parents, children, and internet-connected toys. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 5197–5207.
<https://doi.org/10.1145/3025453.3025735>
- Michele, B., & Karpow, A. (2014). Demo: Using malicious media files to compromise the security and privacy of smart TVs. *IEEE 11th Consumer Communications and Networking Conference (CCNC)*. <https://doi.org/10.1109/CCNC.2014.6994414>
- Miedema, T. E. (2018). Engaging consumers in cybersecurity. *Journal of Internet Law*, 21(8), 3–15.
- Mills, K. (2017, February 14). Hackers can unlock your homes front door with an innocent looking doll and you won't even know they've done it. *The Mirror*. Retrieved from <https://www.mirror.co.uk/news/uk-news/hackers-can-unlock-your-homes-9816119>
- Misra, S., Maheswaran, M., & Hashmi, S. (2017). *Security challenges and approaches in internet of things*. <https://doi.org/10.1007/978-3-319-44230-3>
- Moini, C. (2017). Protecting privacy in the era of smart toys: Does Hello Barbie have a duty to report. *Catholic University Journal of Law & Technology*, 25(2). Retrieved from <https://scholarship.law.edu/jlt/vol25/iss2/4>

- Mordor Intelligence. (2020). Smart toys market – Growth, trends, and forecast (2020–2025). Retrieved January 5, 2020, from <https://www.mordorintelligence.com/industry-reports/smart-toys-market>
- Mozilla. (2018). *CogniToys Dino*. Retrieved June 5, 2019, from <https://foundation.mozilla.org/en/privacynotincluded/products/cognitoys-dino/>
- Munro, K. (2016). Hacking kettles & extracting plain text WPA PSKs. Yes really! Retrieved September 12, 2018, from <https://www.pentestpartners.com/security-blog/hacking-kettles-extracting-plain-text-wpa-psks-yes-really/>
- Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34, 47–66. <https://doi.org/10.1016/j.cose.2012.11.004>
- National Cyber Security Center. (2019). Most hacked passwords revealed as UK cyber survey exposes gaps in online security. Retrieved October 10, 2019, from <https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security>
- New Zealand IoT Alliance. (2017). *The Internet of Things: Accelerating a connected New Zealand*. Retrieved from <https://iotalliance.org.nz/wp-content/uploads/sites/4/2018/09/Accelerating-a-Connected-New-Zealand-eBOOK.pdf>
- Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, 32, 17–31. <https://doi.org/10.1016/j.adhoc.2015.01.006>
- Nikken, P., & Schols, M. (2015). How and Why Parents Guide the Media Use of Young Children. *Journal of Child & Family Studies*, 24(11), 3423–3435. <https://doi.org/10.1007/s10826-015-0144-4>
- NIST. (2014). *Assessing security and privacy controls in federal information systems and organizations*. Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>
- NIST. (2016). *NIST Special Publication 800-183 Networks of ‘Things’*. Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf>
- NIST. (2017a). *Special Publication (NIST SP) - 800-63-3 Digital Identity Guidelines*. Retrieved from <https://www.nist.gov/publications/digital-identity-guidelines>

- NIST. (2017b). *Special Publication 800-121 Guide to Bluetooth Security*. Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf>
- Offensive Security, 2019. *What is Kali Linux ?* Retrieved October 30, 2019, from <https://docs.kali.org/introduction/what-is-kali-linux>
- Office of the Privacy Commissioner (n.d). Privacy law reform. Retrieved December 1, 2019 from <https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-law-reform/>
- Office of the Privacy Commissioner. (2013). Retrieved March 21, 2019, from <https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-act-and-codes-introduction>
- Öğütçü, G., Testik, Ö., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83–93. <https://doi.org/10.1016/j.cose.2015.10.002>
- OWASP. (2014a). Internet of Things top ten IoT vulnerabilities. Retrieved from https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf
- OWASP. (2014b). *Testing Guide 4.0 Release*. Retrieved from <https://www.owasp.org/images/1/19/OTGv4.pdf>
- OWASP. (2018). *Internet of Things (IoT) Top 10 2018*. Retrieved June 10, 2019, from https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10
- Park, Y. (2011). Digital literacy and privacy behavior online. *Communication Research*, 40(2), 215–236. <https://doi.org/10.1177/0093650211418338>
- Parsons, K., Calic, D., Butavicius, M., McCormac, A., Pattinson, M., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, 66, 40–51. <https://doi.org/10.1016/j.cose.2017.01.004>
- Pallavi, S., & Smruti R., S. (2017). Internet of Things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*. <https://doi.org/10.1155/2017/9324035>
- Pickering, P. (2017). Adventures in toyland: Barbie meets the IoT. *Electronic Component News*, 61(1), 24–25. Retrieved from <https://www.ecnmag.com>

- Poston, H. (2019). What is black box, grey box, and white box penetration testing? Retrieved August 5, 2019, from <https://www.infosecinstitute.com>
- Prandini, M., Ramilli, M. (2010). Towards a practical and effective security testing methodology. <https://doi.org/10.1109/ISCC.2010.5546813>
- Radovan, M., Golub, B., & Daimler, A. (2017). Trends in IoT security. *40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1302. <https://doi.org/10.23919/MIPRO.2017.7973624>
- Rafferty, L., Hung, P., Fantinato, M., Marques Peres, S., Iqbal, F., Kuo, S., & Huang, S. (2017). Towards a Privacy Rule Conceptual Model for Smart Toys. In J.K.T Tang & P. C. K Hung (Eds.), *Computing in smart toys* (pp. 85–102). https://doi.org/10.1007/978-3-319-62072-5_6
- Rafferty, L., Farkhund, I., & Hung, P. K. (2017). Security threat analysis of smart home network with vulnerable dynamic agents. In J. K. T. Tang & P. C. K Hung (Eds.), *Computing in smart toys* (pp. 127–147). https://doi.org/10.1007/978-3-319-62072-5_8
- Rafferty, L., Fantantino, M., & Hung, P. K. (2015). Privacy requirements in toy computing. In P. C. K. Hung (Ed), *Mobile services for toy computing* (pp. 141–173). <https://doi.org/10.1007/978-3-319-21323-1>
- Ray, P.P. (2016). A survey on Internet of Things architectures. *Journal of King Saud University – Computer and Information Sciences*, 2016. <https://doi.org/10.1016/j.jksuci.2016.10.003>
- Raza, S., Seitz, L., Sitenkov, D., & Selander, G. (2016). S3K: Scalable Security with Symmetric Keys—DTLS key establishment for the Internet of Things. *IEEE Transactions on Automation Science and Engineering, Automation Science and Engineering*, 3, 1270. <https://doi.org/10.1109/TASE.2015.2511301>
- Reeder, R. W., Ion, I., & Consolvo, S. (2017.). 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy*, 15(5), 55–64. <https://doi.org/10.1109/MSP.2017.3681050>
- Rivas, M.L. (2017). *Securing the home IoT network*. Retrieved from: <https://www.sans.org/reading-room/whitepapers/internet/securing-home-iot-network-37717>

- Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57, 2266–2279.
<https://doi.org/10.1016/j.comnet.2012.12.018>
- Salami, S., Baek, J., Salah, K., & Damiani, E., (2016). Lightweight encryption for smart home. *11th International Conference on Availability, Reliability and Security (ARES)*, 382.
<https://doi.org/10.1109/ARES.2016.40>
- Salkind, N. J. (2010). *Encyclopedia of research design*.
<https://doi.org/10.4135/9781412961288>
- Sato, H., Kanai, A., Tanimoto, S., Kobayashi, T. (2016). Establishing trust in the emerging era of IoT. *IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 398.
<https://doi.org/10.1109/SOSE.2016.50>
- Scarfone, K., Cody, A., Souppaya, M., & Orebaugh, A. (2008). *Technical Guide to Information Security Testing and Assessment (NIST Special Publication 800-115)*. National Institute of Standards and Technology. Retrieved from
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>
- Scheuren, F. (2005). What is a survey? Retrieved January 10, 2019, from
<https://web.uta.edu/faculty/eakin/busa3321/whatisasurvey.pdf>
- Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical & Computer Engineering*, 1, 25. <https://doi.org/10.1155/2017/9324035>
- Sha, K., Alatrash, N., & Wang, Z. (2017). A secure and efficient framework to read isolated smart grid devices. (2017). *IEEE Transactions on Smart Grid*, 6, 2519.
<https://doi.org/10.1109/TSG.2016.2526045>
- Sha, K., Wei, W., Andrew Yang, T., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. *Future Generation Computer Systems*, 83, 326–337.
<https://doi.org/10.1016/j.future.2018.01.059>
- Shahid, N., & Aneja, S., (2017). Internet of Things: Vision, application areas and research challenges. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, 583. <https://doi.org/10.1109/I-SMAC.2017.8058246>

- Sharma, G., Bala, S., & Verma, A. K. (2012). Security Frameworks for Wireless Sensor Networks-Review. *Procedia Technology*, 6, 978.
<https://doi.org/10.1016/j.protcy.2012.10.119>
- Sicari, S., Rizzardi, A., Grieco, L., & Coen-Porisini, A. (2015). Survey paper: Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164.
<https://doi.org/10.1016/j.comnet.2014.11.008>
- Silvestro, M., & Black, J. (2016). “Who am I talking to?”--The regulation of voice data collected by connected consumer products. *Business Law Today*, 1–4. Retrieved from
<https://businesslawtoday.org/>
- Sphero. (n.d.). *R2-D2*. Retrieved October 10, 2019, from
<https://support.sphero.com/category/0jf8702ah-r-2-d-2>
- Spin Master. (2019). *FPV Race Car*. Retrieved December 10, 2019, from
<http://www.airhogs.com/en-us/detail/p21275>
- StatCounter, (2019a). Desktop Windows version market share New Zealand. Retrieved October 30, 2019, from <https://gs.statcounter.com/os-version-market-share/windows/desktop/new-zealand>
- StatCounter. (2019b). Mobile & tablet Android version market share New Zealand. Retrieved October 30, 2019, from <https://gs.statcounter.com/os-version-market-share/android/mobile-tablet/new-zealand>
- Statista. (2018). Active internet users as percentage of the total population in New Zealand from 2015 to 2018. Retrieved October 10, 2018, from
<https://www.statista.com/statistics/680688/new-zealand-internet-penetration>
- StatsNZ. (2013). *2013 Census*. Retrieved October 4, 2018, from <http://nzdotstat.stats.govt.nz>
- Stout, W., & Urias, V. (2016). Challenges to securing the Internet of Things. *IEEE International Carnahan Conference on Security Technology (ICCST)*, 1.
<https://doi.org/10.1109/CCST.2016.7815675>
- Sun, M., & Tay, W. P. (2017). Inference and data privacy in IoT networks. *IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 1. <https://doi.org/10.1109/SPAWC.2017.8227701>

- Sundararajan, K. (2017). *Privacy and security issues in brain computer interfaces* (Master's thesis, Auckland University of Technology, Auckland, New Zealand). Retrieved from <http://hdl.handle.net/10292/11449>
- SurveyMonkey. (2018). *Privacy policy*. Retrieved October 10, 2018, from <https://www.surveymonkey.com/mp/legal/privacy-policy/>
- Tang, J., & Hung, P. K. (Eds.). (2017). *Computing in smart toys*. <https://doi.org/10.1007/978-3-319-62072-5>
- Tankard, C. (2015). Feature: The security issues of the Internet of Things. *Computer Fraud & Security*, 2015(9), 11–14. [https://doi.org/10.1016/S1361-3723\(15\)30084-1](https://doi.org/10.1016/S1361-3723(15)30084-1)
- Taylor, E., & Michael, K. (2016). Smart toys that are the stuff of nightmares. *IEEE Technology and Society Magazine*, 35(1), 8–10. <https://doi.org/10.1109/MTS.2016.2527078>
- Thomas R. M. (2003). Present-status perspectives quantitative. In R. M. Thomas (Ed.), *Blending qualitative & quantitative research methods in theses and dissertations* (pp. 41–56). <https://doi.org/10.4135/9781412983525>
- Tomczyk, L. (2019). Skills in the area of digital safety as a key component of digital literacy among teachers. *Education and Information Technologies*, 25, 471–486. <https://doi.org/10.1007/s10639-019-09980-6>
- Torre, I., Adorni, G., Kocova, F., & Sanchez, O. (2016). Preventing disclosure of personal data in IoT networks. *12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, 389–396. <https://doi.org/10.1109/SITIS.2016.68>
- Townsend, K., Akiba, C., & Davidson, R. (2014). *Getting started with Bluetooth Low Energy*. Sebastopol, CA: O'Reilly.
- Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the “Online Privacy Literacy Scale” (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333–365). Dordrecht, The Netherlands: Springer.
- Tung, L. (2017, November 15). UK consumer group calls for vulnerable smart toys to be taken off shelves. *CSO Online*. Retrieved from <https://www.cso.com.au>

- Udoh, E., & Alkharashi, A. (2016). Privacy risk awareness and the behavior of smartwatch users: A case study of Indiana University students. *2016 Future Technologies Conference*, 926–931. <https://doi-org/10.1109/FTC.2016.7821714>
- Vtech (2015). Terms and Conditions. Retrieved December 20, 2019, from http://contentcdn.vtechda.com/data/console/GB/1668/SystemUpgrade/FirmwareUpdateTnC_GBeng_V2_20160120-170000.txt
- Wi-Fi Alliance (n.d.). WPA2. Retrieved January 20, 2019, from <https://www.wi-fi.org/discover-wi-fi/specifications>
- Wireshark. (n.d.). *About Wireshark*. Retrieved September 10, 2019, from <https://www.wireshark.org/>
- Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*, 42, 120–134. <https://doi.org/10.1016/j.jnca.2014.01.014>
- Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, 129(2), 444–458. <https://doi.org/10.1016/j.comnet.2017.09.003>
- Zachary, R. (2019). Industry cloud adoption by industry vertical, 2019. Retrieved December 30, 2019, from <https://www.idc.com>
- Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). Review: A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, 84, 25–37. <https://doi.org/10.1016/j.jnca.2017.02.009>

Appendix A: Survey Participant Invitation and Information Notices

Participant Information Sheet

An Invitation

Hello, my name is Nicole Girvan, a Master of Information Security and Digital Forensics student at Auckland University of Technology. I would like to invite you to participate in my research study that focuses on Smart Toy Security and Privacy Awareness by completing a short survey.

What is the purpose of this research?

The purpose of this research is to gain information from New Zealand Parents/Guardians about current levels of concern and awareness around Smart Toy Privacy and Security. The findings may be used as part of a thesis document and for academic publication and presentations.

Why am I being invited to participate in this research and what will happen in this research?

You have been invited to participate as you are a New Zealand Parent or Guardian with a child (or children) under the age of 18 and you have seen my information poster in writing or online. If you agree to participate you will be asked to answer a short set of questions about Security, Privacy and Smart Toys.

How do I agree to participate in this research?

Your participation in this research is voluntary (it is your choice) and whether or not you choose to participate will neither advantage nor disadvantage you. You are able to withdraw from the study at any time and you do not have to answer any question you don't wish to. You agree to participate by visiting the survey link and completing the questionnaire. Completion of the questionnaire will be taken as your consent to participate.

What are the discomforts and risks?

There are no discomforts or risks foreseen. You are able to withdraw from the study at any time and you do not have to answer any questions. All answers given to the questions are valid.

How will my privacy be protected?

Your survey responses will be completely anonymous. That means I cannot know who you are. You will not be asked for any personal or identifying information at any time.

What are the costs of participating in this research?

The survey is expected to take about 15 minutes of your time.

What opportunity do I have to consider this invitation?

The survey will be open until 30 June 2019 and you can join at any stage until it closes.

Will I receive feedback on the results of this research?

If you wish to know what I have discovered, a summary of the results can be found on the following link in July 2019 when the survey is closed:

<https://www.facebook.com/Smart-Toy-Privacy-and-Security-Awareness-Survey-551495515313242/>

What do I do if I have concerns about this research?

Any concerns regarding the nature of this project should be notified in the first instance to the Project Supervisor,

Dr. Alastair Nisbet: alastair.nisbet@aut.ac.nz +64 9 921-9999 ext. 5879

Concerns regarding the conduct of the research should be notified to the Executive Secretary of AUTC, Kate O'Connor, ethics@aut.ac.nz, 921 9999 ext. 6038.

Whom do I contact for further information about this research?***Researcher Contact Details:***

Nicole Girvan: ppq0819@autuni.ac.nz

Project Supervisor Contact Details:

Dr. Alastair Nisbet: alastair.nisbet@aut.ac.nz +64 9 921-9999 ext. 5879

Approved by the Auckland University of Technology Ethics Committee on 04 February, 2019, AUTC Reference number 19/27.

Do your Children play with Smart Toys?



I am wanting to find out about Smart Toy
Security and Privacy Awareness amongst
New Zealand Parents/Guardians...

Would you be willing to help me?

Hi, my name is Nicole and I am conducting a short survey to
find out how aware New Zealand Parents/Guardians are
around the Privacy and Security risks related to Smart Toy use.

If you are interested in helping me, I would like you to
complete a short survey that will take a maximum of 15
minutes of your time.

Please visit:

<https://www.surveymonkey.com/r/SmartToy> for more
information and to participate.

Appendix B: Survey Questionnaire



Smart Toy Privacy and Security Risk Awareness

Hello, my name is Nicole Girvan, a Master of Information Security and Digital Forensics student at Auckland University of Technology. I would like to invite you to participate in my research study that focuses on Smart Toy* Security and Privacy Awareness by completing a short survey.

What is the purpose of this research?

The purpose of this research is to gain information from New Zealand Parents/Guardians about current levels of concern and awareness around Smart Toy Privacy and Security. The findings may be used as part of a thesis document and for academic publication and presentations.

Why am I being invited to participate in this research and what will happen in this research?

You have been invited to participate as you are a New Zealand Parent or Guardian with a child (or children) under the age of 18. If you agree to participate you will be asked to answer a short set of questions about Security, Privacy and Smart Toys. You are able to withdraw from the study at any time and you do not have to answer any question you don't wish to. You agree to participate by completing the questionnaire. Completion of the questionnaire will be taken as your consent to participate.

What are the discomforts and risks?

There are no discomforts or risks foreseen. You are able to withdraw from the study at any time and you do not have to answer any questions. All answers given to the questions are valid.

How will my privacy be protected?

Your survey responses will be completely anonymous. That means I cannot know who you are. You will not be asked for any personal or identifying information at any time.

What are the costs of participating in this research?

The survey is expected to take about 15 minutes of your time.

What opportunity do I have to consider this invitation?

The survey will be open until 30 June 2019 and you can join at any stage until it closes.

Will I receive feedback on the results of this research?

If you wish to know what I have discovered, a summary of the results can be found on the following link in July 2019 when the survey has closed:

<https://www.facebook.com/Smart-Toy-Privacy-and-Security-Awareness-Survey-551495515313242/>

What do I do if I have concerns about this research?

Any concerns regarding the nature of this project should be notified in the first instance to the Project Supervisor,

Dr. Alastair Nisbet: alastair.nisbet@aut.ac.nz +64 9 921-9999 ext. 5879

Concerns regarding the conduct of the research should be notified to the Executive Secretary of AUTECH, Kate O'Connor, ethics@aut.ac.nz, 921 9999 ext. 6038.

Whom do I contact for further information about this research?

Researcher Contact Details:

Nicole Girvan: ppq0819@autuni.ac.nz

Project Supervisor Contact Details:

Dr. Alastair Nisbet: alastair.nisbet@aut.ac.nz +64 9 921-9999 ext. 5879

This research has been approved by the Auckland University of Technology Ethics Committee.

Thank you for completing this survey. Your feedback is important.

** A Smart Toy is a toy that can connect to the Internet and/or other devices and may have sensors such as cameras, microphones etc. An example is "Furby Connect" by Hasbro.*



Smart Toy Privacy and Security Risk Awareness

Qualifying Questions

* 1. Do you reside in New Zealand?

- ☐ Yes
☐ No

* 2. Are you the Parent or Guardian of a Child (under the age of 18 years)?

- ☐ Yes
☐ No



Smart Toy Privacy and Security Risk Awareness

Demographic Information

1. Are you?

- ☐ Male
☐ Female
☐ Gender Diverse

2. What is the highest level of education you have completed?



Smart Toy Privacy and Security Risk Awareness

Concern around Smart Toy use

1. I am concerned about the Security risks of using Smart Toys (*such as a stranger taking control of my device*).

- ☐ Strongly agree ☐ Disagree
☐ Agree ☐ Strongly disagree
☐ Neither agree nor disagree

2. I am concerned about the Privacy risks of using Smart Toys (*such as my personal information being stolen or misused*).

- ☐ Strongly agree ☐ Disagree
☐ Agree ☐ Strongly disagree
☐ Neither agree nor disagree

AUT

Smart Toy Privacy and Security Risk Awareness

Knowledge of the technical capabilities of smart toys

These questions relate to possible common features found in smart toy products.

1. A Smart Toy can remain connected to the Internet even when not switched on.

- ☐ True
☐ False
☐ Don't Know

2. A Smart Toy can use sensors to determine who is playing with it.

- ☐ True
☐ False
☐ Don't Know

3. A Smart Toy can be equipped with a microphone and/or camera to capture audio, photo, and video.

- ☐ True
☐ False
☐ Don't Know

4. Smart Toys can use Bluetooth and Wi-Fi technologies to transmit data to other smart devices such as other toys, mobile phones, and smart televisions.

- ☐ True
☐ False
☐ Don't Know

5. A Smart Toy is simply a traditional toy that helps my Child become smarter.

- ☐ True
☐ False
☐ Don't Know

6. A Smart Toy can engage in real-time location tracking of my Child.

- ☐ True
☐ False
☐ Don't Know

AUT

Smart Toy Privacy and Security Risk Awareness

Knowledge of potential smart toy security and privacy risks and vulnerabilities

These questions relate to potential smart toy security and privacy risks and vulnerabilities.

1. A Smart Toy can passively gather information about its surroundings (such as location, and temperature etc.).

- ☐ True
☐ False
☐ Don't Know

2. Data captured by Smart Toys may be intercepted and read by a stranger located nearby.

- ☐ True
☐ False
☐ Don't Know

3. All Smart Toys can receive security updates.

- ☐ True
☐ False
☐ Don't Know

4. Smart toys that present content to a child such as songs or images may be intercepted and the content maliciously replaced with pornographic or other inappropriate material.

- ☐ True
☐ False
☐ Don't Know

5. Some Smart Toy mobile applications can track your location even if you haven't launched them.

- ☐ True
☐ False
☐ Don't Know

6. A stranger may take control of a Smart Toy using their smartphone.

- ☐ True
☐ False
☐ Don't Know

AUT

Smart Toy Privacy and Security Risk Awareness

Knowledge of the data procedures of Smart Toy Companies and Affiliates.

These questions focus on smart toy company data use procedures such as data retention strategies, and their data use declaration practices such as privacy statements.

1. A Smart Toy Company may store any personal data they collect about me for an indefinite duration.

- ☐ True
☐ False
☐ Don't Know

2. A Smart Toy Company may sell my personal data to third party organisations.

- ☐ True
☐ False
☐ Don't Know

3. Smart Toy Companies always have strong security so the data they collect cannot be stolen.

- ☐ True
☐ False
☐ Don't Know

4. A Smart Toy Company's Privacy Statement always informs me where my personal data is stored.

- ☐ True
☐ False
☐ Don't Know

5. Smart Toy Companies always store personal data that they collect, such as user names and passwords, completely anonymously.

- ☐ True
☐ False
☐ Don't Know

6. A Smart Toy Company may send my Child's Personal Data abroad.

- ☐ True
☐ False
☐ Don't Know

AUT

Smart Toy Privacy and Security Risk Awareness

Knowledge of the data protection and legal aspects of Smart Toy use in New Zealand.

This section focuses on applicable data legislation as it applies to New Zealand consumers.

1. The New Zealand Privacy Act 1993 prevents any International Toy Companies from misusing my personal information.

- ☐ True
☐ False
☐ Don't Know

2. Parent or Guardian consent is required by law before a Child under the age of 13 may use a Smart Toy.

- ☐ True
☐ False
☐ Don't Know

3. All Smart Toy companies operating in New Zealand are legally obligated to inform you if the data they collect about you has been hacked or exposed.

- ☐ True
☐ False
☐ Don't Know

4. If a New Zealand Smart Toy company requests your personal information they must inform you how it will be used.

- ☐ True
☐ False
☐ Don't Know

5. Parental Consent is legally required before a Smart Toy can record your child's voice.

- ☐ True
☐ False
☐ Don't Know

6. All Smart Toys purchased online by New Zealand parents must comply with the New Zealand Privacy Act 1993.

- ☐ True
☐ False
☐ Don't Know

AUT

Smart Toy Privacy and Security Risk Awareness

Knowledge of personal security and privacy protection strategies

This section focuses on common protection strategies that a user can employ to enhance security and privacy.

1. When creating a password for my Smart Toy, I should include easy to remember details such as the name of my street.

- ☐ True
☐ False
☐ Don't Know

2. I should limit the information that I provide to a Smart Toy company.

- ☐ True
☐ False
☐ Don't Know

3. Remote viewing should always be enabled in Smart Toys that have Cameras.

- ☐ True
☐ False
☐ Don't Know

4. I should disable a Smart Toys Bluetooth in the device settings when it is not in use to enhance security.

- ☐ True
- ☐ False
- ☐ Don't Know

5. Disabling default location tracking in a Smart Toy will stop real-time location information being saved.

- ☐ True
- ☐ False
- ☐ Don't Know

6. I should only use my Smart Toy when connected to a secure, trusted Wi-Fi network.

- ☐ True
- ☐ False
- ☐ Don't Know

Appendix C: Pre-Test Technical Consultation and Pilot/Target Audience Feedback

Consolidated Results and outcomes from Consultation 2 (Target Audience Consultation)

A group of 10 of the target audience (New Zealand Parents/Guardians) were given a Preview and Feedback link to the Survey and asked to complete it online and make comments wherever they felt unclear or uncertain about a question due to language or for any other reason.

General feedback was also invited on any aspect of the process.

Survey Section	Feedback Received	Action Taken
Qualifying Questions	1. Isn't age of consent 16 and over?	1. Age of an "adult" varies depending on what are you talk about. I have determined a Child will be defined as under the age of 18 years for the purpose of this study.
Demographic Information	No feedback received	
Level of concern	1. It may be difficult to understand what the difference is between a security risk and a privacy risk. 2. What do you mean by security risk? 3. Just asking me makes my level of concern rise I think	1. Examples will be included to assist in defining these terms 2. As per 1. 3. No action taken
Knowledge of the Technical Capabilities of Smart Toys	1. These all seem relevant 2. No comments 3. Just seems standard today, haven't really thought about this 4. Is this going to include drones and stuff like that?	1. No action taken 2. No action taken 3. No action taken 4. No action taken other than response to question. Whilst drones can sometimes be marketed as toys, they are also potentially an adult device. Final toy selection and criteria for testing has yet to occur but it is unlikely drones will be included.
Knowledge of potential smart toy security and privacy risks and vulnerabilities	No feedback received	

Knowledge of the data procedures of Smart Toy Companies and Affiliates.	No feedback received	
Knowledge of the data protection and legal aspects of Smart Toy use in New Zealand.	<ol style="list-style-type: none"> 1. They should protect us 2. I wouldn't know the laws themselves, only what I think they should be lol 	<ol style="list-style-type: none"> 1. No action taken 2. No action taken
Knowledge of personal protection strategies	<ol style="list-style-type: none"> 1. Question seems a bit easy (Q1) 2. I don't know the answer to all of these and feel like I should 3. What is a trusted network? 	<ol style="list-style-type: none"> 1. No action taken. Some questions will be easy to some participants and yet difficult for others. 2. No action taken 3. No action taken – if the participant does not understand then this will indicate a lower level of awareness and therefore question is retained.
General Feedback	<ol style="list-style-type: none"> 1. Felt it went a little slow but maybe that was my computer 2. This is good. Very relevant. 3. Should you say what a Smart Toy is first? 	<ol style="list-style-type: none"> 1. No action taken as yet 2. No action taken 3. Decided not to define a smart toy as I want to measure concern and awareness without initially educating any participants.

Consolidated Results and outcomes from Consultation 1 (Technical Expert Consultation).

Dimension 1: Knowledge of the Technical Capabilities of Smart Toys

This dimension aims to test knowledge around the common features of smart toy products available to consumers.

1. A Smart Toy can remain connected to the Internet even when not switched on.

This Question is _____ of Dimension 1

- ☐ Clearly Representative (10 responses)
- ☐ Somewhat Representative (0 Responses)
- ☐ Not Representative (0 Responses)

Outcome:

Question to be included in survey and remain unchanged.

2. A Smart Toy can use sensors to determine who is playing with it.

This Question is _____ of Dimension 1

- ☐ Clearly Representative (10 responses)
- ☐ Somewhat Representative (0 Responses)
- ☐ Not Representative (0 Responses)

Outcome:

Question to be included in survey and remain unchanged.

3. A Smart Toy cannot record a Child's conversation without the user's knowledge.

This Question is _____ of Dimension 1

- ☐ Clearly Representative (1 response)
- ☐ Somewhat Representative (8 responses)
- ☐ Not Representative (1 Responses)

Outcome:

Question to be removed from the survey due to low score.

Appendix D: Smart Toy Descriptions

A description of each smart toy included in the scope of this research is provided below.

Kurio Watch 2.0

The Kurio Watch is a smartwatch targeted to children aged six and above. It comes with a built-in camera, motion sensor, speaker, and microphone, and is designed to be used with a companion Android messenger application that allows the user to send video, pictures, and text messages to a paired phone or another watch. The watch comes preloaded with games and an emergency section that holds data such as emergency contact details, medical details, doctor information, and blood type of the user (Kurio, n.d.). No previous research on this watch was found.

Furby Connect

Furby Connect is a soft toy animal created by Hasbro recommended for children ages six years and above. The toy is designed to connect and interact with other Furbys and with the “Furby Connect World App” using Bluetooth Smart via a variety of Android or iOS devices. The app requires an internet connection (3G, 4G, LTE, or Wi-Fi) for the initial download, updates, new content and in-app purchases. The toy connects to the internet via BLE to a companion phone device (Hasbro, 2019a).

Furby Connect has two microcontrollers. One is from General Plus and used for movement and speech. The other is from Nordic Semiconductor and used for all BLE (also called Bluetooth Smart) communication, AI, LED eyes, body sensors, and the smart beak (Condon, 2019). Furby toys have been successfully hacked by security researchers who have subsequently documented their methods. Successful hacking techniques take advantage of developer settings that enable unauthenticated commands to be sent to the toy. This feature is not considered a specific vulnerability as the Smart Toy is designed to receive these commands (Condon, 2019).

R2-D2 Droid

The R2-D2 Droid by Sphero is an app-enabled droid. Designed for use with the Star Wars companion application available for Android and iOS, it contains integrated speakers and LED, motion detection, and GPS capability (Sphero, n.d.). Designed for children eight years of age and above, the R2-D2 Droid transmits using BLE 4.0 at a frequency of 2402–2480MHz. The droid is designed to patrol the surrounding areas, react to Star Wars films by providing commentary over the movies, and interact with Sphero’s other Star Wars toys (Sphero, n.d.). No previous security research was found on this smart toy.

Air Hogs FPV High Speed Race Car

Designed for children eight years and older, the Air Hogs FPV (First Person View) High Speed Race Car is a remote controlled car that streams video straight from the car’s dashboard camera to the user’s headset. Operating at a frequency range of 2.4GHz, it uses Wi-Fi to connect to a

companion application available for Android. Racing videos and photographs can be recorded, uploaded, and shared via the companion application (Spin Master, 2019). No previous security research was found on this smart toy.

Toy Mail Talkie Unicorn

Toy Mail Talkie Unicorn is targeted at children aged three years and above. It is designed to send voice messages between the toy and approved contacts by way of a companion application, or between two toys. It connects over 2.4Ghz home Wi-Fi. The free companion application is available on Android, Kindle and iOS, and an optional cloud service may also be purchased to receive further functionality such as games. The Talkie Unicorn contains a microphone, speaker, accelerometer, and built-in Wi-Fi chip (ToyMail, 2019). No security research was found that included this toy.

CogniToys Dino

CogniToys Dino is a smart toy dinosaur aimed at children five to nine years old. The Dino is cloud-connected through Wi-Fi and uses IBM Watson AI to hold a conversation, tell jokes, and answer questions. The Dino must be set up by connecting to the companion application available for Android or iOS. CogniToys Dino contains a speaker, a microphone which is activated through a button on the toys stomach, and speech recognition technology (Kickstarter, 2018).

Once connected, the Dino no longer requires a smartphone; however, the toy remains directly connected to a cloud server via a Wi-Fi network while in operation. The Dino can connect to networks which support 802.11b/g/n, operating at 2.4GHz. It is not compatible with 802.11a/ac, enterprise Wi-Fi, or networks operating at 5.0GHz. Mozilla completed a review of the CogniToys Dino as part of an online series of articles discussing privacy within the smart home. It reviewed encryption practices of the toy and concluded that it did not know if encryption was used, and outlined its various features such as the use of a microphone that may impact user privacy (Mozilla, 2018).

Toy-Fi Teddy

Toy-Fi Teddy, designed for children three years and above, is a Bluetooth enabled teddy bear that allows a user to record messages on a companion application and send them to the bear. The teddy will receive messages sent and play them via the onboard speakers. Return messages can then be recorded directly onto the toy. A British consumer watchdog group has previously expressed concern that the Toy-Fi Teddy may enable a stranger to communicate with a child uninvited due to the Bluetooth protocol that the toy uses (Tung, 2017).

Star Lily Unicorn

The furReal StarLily, My Magical Unicorn Interactive Plush Pet Toy responds to voice and touch using inbuilt body sensors for sound and motion detection. The unicorn is designed for ages four and above, and a companion application is available on Android and iOS to enable interactive play (Hasbro, 2019b). No previous research on Star Lily Unicorn was found.