2017

Assessment of security vulnerabilities in wearable devices

Brian Cusack
Auckland University of Technology

Bryce Antony
Auckland University of Technology

Gerard Ward
Auckland University of Technology

Shaunak Mody
Auckland University of Technology

DOI: 10.4225/75/5a84e6c295b44
Cusack, B., Antony, B., Ward, G., & Mody, S. (2017). Assessment of security vulnerabilities in wearable devices . In Valli, C. (Ed.). (2017). The Proceedings of 15th Australian Information Security Management Conference, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia. (pp. 42-48).

ASSESSMENT OF SECURITY VULNERABILITIES IN WEARABLE DEVICES

Brian Cusack, Bryce Antony, Gerard Ward, Shaunak Mody
Cyber Forensic Research Centre, Auckland University of Technology, Auckland, New Zealand
brian.cusack@aut.ac.nz; bryceantony2@gmail.com; fx6207@autuni.ac.nz; shaunakmody14892@gmail.com

Abstract

Wearable devices have proliferated in usage and human experience, and they provide convenience for personal information requirements. These devices are both sensory and immersive for the diverse global network that is generally termed the Internet of things (IoT). The immediacy of the two-way communication created in the IoT has made vulnerable human behaviour and raised debate around information ownership and privacy expectations. The legitimacy of ownership of information and its reuse are prevalent problems. In this research, we tested four wearable devices that share 44% of the current market, for security vulnerabilities. We found serious weaknesses that could result in the unplanned disclosure of information and recommend further research into users expectations for safety.

Keywords: Wearable Devices, Vulnerabilities, Privacy, Hacking, Disclosure

INTRODUCTION

Wearable devices have been around for decades in the form of small electronic devices that compensate for human failure in for example, sight and hearing. Wearable hearing aids have been available in different forms for an extended period; however, the technology today is very different in flexibility and functionality from what was available 15 or 20 years ago. Today wearable devices are integrated into a body area network (BAN) for two-way communication and placed into a context that is generally termed the "Internet of Things" (IoT) (PwC, 2016). The purpose of these devices is not only to compensate for human physical and psychological failure, but more commonly to extend the reach of the human through interconnectivity with information sources (NIST, 2010). Consequently, today a human using a wireless Bluetooth earpiece may not be compensating for physical challenges but rather extending their sensory capability by connecting with personal or remote information sources. Developments that are more recent have included devices that monitor personal biological data, geolocation, and emotions. Some of these are used for health purposes, information exchange, and others for navigating around unfamiliar environments. The value of this technological opportunity is a global human experience of interconnectivity that has collapsed the barriers between internal and external environments and provided full personal immersion. In this fashion, a human may experience a fully augmented reality for the betterment of themselves and the systems in which they participate. The simplest functional architecture provides a connection between a wearable broadcast mechanism and a receiving station (Zhou, et al., 2014). Because most people have a smart phone on them most of the time, then the smart phone has become the receiving station for a multiplicity of different devices that the human may carry within their BAN. There are many examples of connectivity that both transmits information and receives information in the two-way relationship between the base station and the broadcast mechanism or sensors. The eyeglass that streams information to the user and directly to the eye has significant publicity. In addition, wearable watches and biometric monitoring equipment such as the Fitbit, provide personal information for decision-making (Burlacu, 2016; Stack, 2015).

The personal nature of the information managed by the BAN has raised the issue of information ownership (Schelleus, et al., 2014). Personal expectations to control the information from a wearable device, such as a Fitbit, may be a foregone conclusion of the user, and yet the patient owners of the device, the owners of the software, and the owners of the cloud services, and others involved in the brokerage and intermediation of services may all assert ownership of the data. The borderless interconnectivity of human and networks also presents inter-jurisdictional challenges regarding ownership of informational properties, and identification of who has the rights of disclosure and transaction. The fundamental principles of security design require the confidentiality, integrity, and accessibility to information. In situations where the user of a wearable device expects the exclusive ownership of the information that they produce using the device (Zhou, et al., 2014), then the confidentiality and the integrity of the information has to be preserved. Our research is concerned the vulnerability of wearable devices to attacks that can disclose the information the device produces. This research is an attempt to satisfy customer expectations for the confidentiality of their information, and the management of unwarranted disclosures. We tested four wearable devices that had 44% of the market share at the end of 2016 (IDC, 2016), for the presence of security

mechanisms that would preserve the confidentiality of information the device produced from the user actions. Each of these devices was presented on a watch strap to be attached to the wrist of the human. Each device had sensors that trapped a range of biometric data from the end user and also had interconnectivity to broadcast that information for processing, archiving, and providing feedback to the user. The majority of the information processing was done by cloud services in the form of historical logs that tracked and kept account of the user biometric data. All of the devices relied upon Bluetooth low energy as the wireless communication protocol for synchronisation back to the user smart phone (Great Scott, 2015). If the user did not wish to use their smart phone in for example, a gymnasium or a motor vehicle, then they could tether the device to the exercise machine, the motor vehicle network, or to any other local wireless network via the Bluetooth low energy connection for the same effect. The Bluetooth wireless and the tethering protocol is vulnerable to attacks that could violate the confidentiality of information, the integrity of information, and the accessibility to information when hijacked and subjected to service disruption (Cyr, et al., 2014).

BACKGROUND LITERATURE AND METHOD

A consistent theme in literature is the security vulnerability during the pairing of the wearable device with the base station. At the point of pairing the exchange of information is vulnerable. When pairing for the very first time Bluetooth employs one of three Secure Simple Pairing (SSP) strategies:

- Just works – pairs automatically as it requires with no user interaction. Convenient for IoT accessibility but the least secure.
- Numeric comparison - When pairing for the first time both the wearable and smartphone display an identical four to six-digit numerical key. If they match, the smartphone prompts the user to accept the connection.
- Passkey entry - both devices have a user interface for entering a four to six-digit code. One, or both devices must enter a passkey to successfully pair. The authors credit this approach as being the most secure (Lotfy & Hale, 2016; Pieterse & Olivier, 2014)

A review of three wearables by Lotfy and Hale (2016) found that the security of pairing strategies had significant gaps and potential vulnerabilities including:

- Man-in-the-middle attacks, eavesdropping, and packet injection. These kinds of attacks allow attackers to actively spy on wearable devices (user-correlation) and misuse the data.

The Pairing processes are defined as:

- Generic Access Profile (GAP) – the wearable defines a specific advertising protocol. This is important in our research design as this happens subsequent to initial pairing during recurring connection instances.
- Generic Attribute Profile (GATT) – service framework on top of the underlying transport protocol, called ATT (Attribute Protocol), which sets the mutually agreed data transfer standard.
- Both GAP and GATT operate in the 2.4 GHz bandwidth, transmitting at a speed of 1Mbit/sec.

While Bluetooth Low Energy (BLE) operates on the same frequencies as other Bluetooth technologies, it operates differently on the link and physical layer. BLE uses 40 total channels; three are used for advertising by unconnected wearables. The remaining 37 channels are used during GATT for data transmission after pairing. The sequential pairing process is shown in Figure 1 (Lotfy and Hale, 2016, p.3).

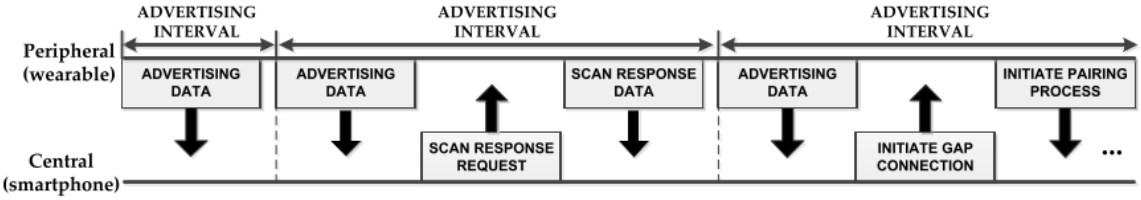

Figure1: GAP BluetoothLE advertising process showing advertising data, scan request, scan response and gap initiation packets

Personally identifiable information (PII) is information that is assignable to a particular human system factor and in some jurisdictions has legal protection (Boyle & Panko, 2014). Broadcasting a fixed MAC address, tied to an

individual's identity would fail the PII test by creating a unique user signature. When wearables create such a risk without user notification, then breaches the privacy has to be considered jurisdiction by jurisdiction. For example, the European Parliament's, Protection of Personal Data Directive, enacted on 5 May 2016 and requiring member states to have introduced into their national law by 6 May 2018, extends the definition of personal data to include that which can "*be identified, directly or indirectly*" (European Parliament, 2016, p. 3). A fixed MAC address, which risks unseen surveillance, breaches this requirement. The literature analysis identified that there are many attack classes (see Figure 2) in and around the use of Bluetooth connectivity. To focus our research and to make it feasible in the laboratory we selected the two attack classes and the five specific attacks highlighted in blue (Hassen, et al., 2017). In respect to Surveillance class, the risk created by a digital signature can be sub-categorised as:

i. **Blue-Printing** – MAC address spoofing for a man-in-the middle attack.

ii. **Blue-Stumbling** - Forced re-pairing attack.

iii. **Blue-Tracking** – a brute force attack designed to determine the data encryption key if one is used.

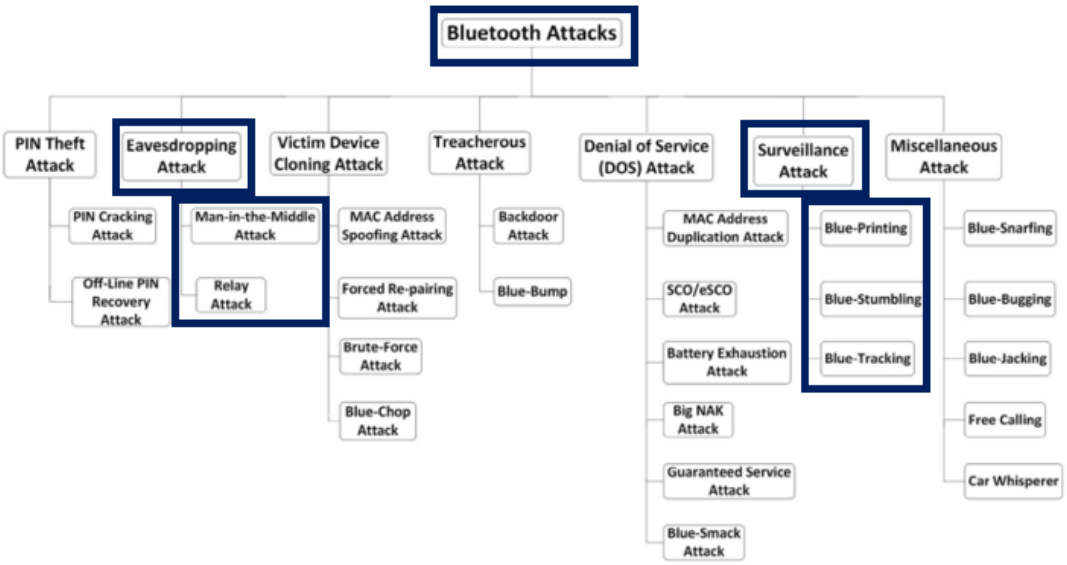

Figure 2 – Classification of Bluetooth Attacks (Hassan et al., 2017, p. 5)

In this research we tested four wearable devices that were selected from the top sales performers in the market and together they held a 44% share of the market at the end of 2016 (Cry, et al., 2014; Guo, 2015). The analysis was conducted in the research laboratory during the first two months of 2017. Figure 3 shows the release dates and devices selected (software versions were those at the time and do not account for any more recent updates).

Reference	Model	Release Date
1	Fitbit Charge	November-14
2	Firbit Surge	January-15
3	Xiaomi Huami	August-16
4	Samsung Gear3	November-16

Fitbit Charge HR	Firbit Surge	Samsung Gear3	Xiaomi Huami, or Amazfit
			
BLE version 4.0	BLE v. 4.0	BLE v. 4.2	BLE v. 4.0

Figure 3. The wearable devices tested

The research was structured to address concerns around device information visibility, pairing visibility, surveillance potential, and information disclosure. The major focus was on potential eavesdropping and surveillance attacks. All of the wearable devices relied upon Bluetooth low energy (BLE) as the wireless communication protocol for data synchronisation between the device and the user smart phone (or other paired network) (Grassi, 2014). The only variation was the Samsung Gear3 that was using version BLE 4.2 rather than

BLE 4.0. The testing with different smart phones was to confirm the consistence of the protocol on different devices. BLE is feasible for use across the Apple iOS, Android, Apple Mac OS, Linux and Microsoft Windows operating systems. In the testing we used a Samsung S6 edge, HTC 1M7, and an Apple iPhone 5S, but did not detect any variations in the BLE protocol execution that related to research concerns. For sniffing tools we selected Ubertooth, the HCI snoop log and the Adafruit sniffer (Lofty, et al., 2016).

The method used two Android phones, and the Adafruit for capture of the BLE packets, and TCP dump in to pcapng and pcap files respectively. The files acquired were then uploaded into Wireshark, an open source packet analyser with a graphical user interface and filtering capability. Using Wireshark the data was examined to determine whether it was transmitted in plain text, or in an encrypted format. Other analysis proceeded to locate any digital signatures, device identification, mappings for the wearer's movements and habits, internet access to device logs and databases, and geolocation correlation data. All the wearables include a back-end cloud service in which an individual's data is stored to ensure portability across devices, and we looked for any credentials providing access rights. The research design is shown in Figure 4, and the blue box indicates the target zone for the sniffing of pairing activity.

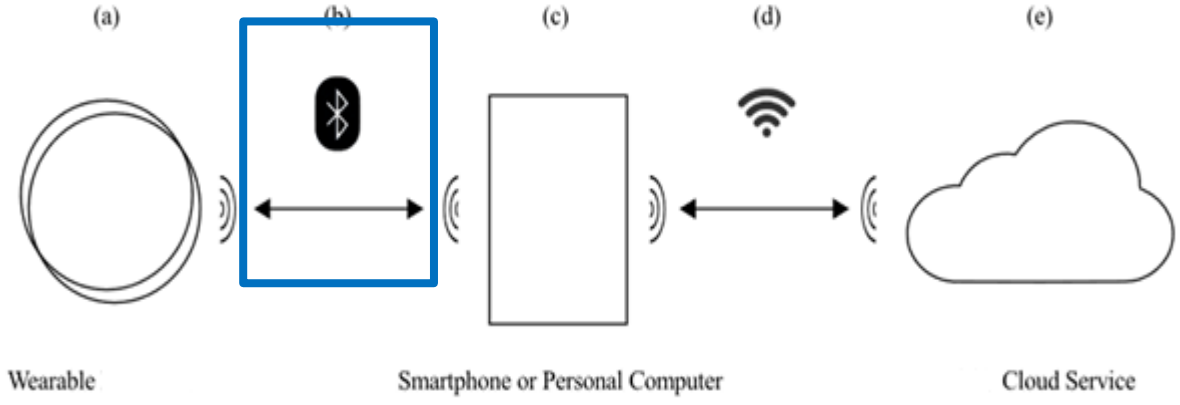

Figure 4. Research Design

FINDINGS

The HCI snoop log is an application that sits on smart phones. It was used in each instance to successfully capture the BLE log file which was then uploaded to Wireshark for analysis. Both encrypted and unencrypted information was found. The unencrypted packets were advertising packets that included the connection request and response. The remainder of the packets were encrypted suggesting that once the exchange protocols and keys have been agreed, all messages were encrypted. We found that the majority of the wearable devices packets were encrypted and the extent of the security mechanisms varied on a device-by-device basis, despite all of them relying upon the BLE protocol. The Adafruit sniffer could successfully follow a device once the connection had been established. The Ubertooth had a similar performance. Using the Adafruit for interception we found that when the wearable device and the base station paired the identity was disclosed in plain text. It may be good for efficiency purposes to have the brand and the watch identity publicly displayed in the wireless network, but for an attacker this is a bonus and makes an easy target. Each wearable device had a different performance and a different susceptibility to attack. Surprisingly the Amazon fit broadcasted the long-term encryption key in plain text during the initial setup as shown in Figure 5.

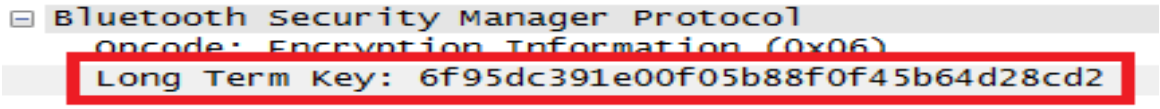

Figure 5. A Plain Text Encryption Key captured

Notably the other wearable devices had encrypted this information. However, the MAC address of the Charge and Surge did not change once connected, an identical result to the Amazon fit. The literature we had read stated that Fitbit had addressed the MAC vulnerability, but our findings suggested otherwise. A fixed MAC address for a session creates the risk of an attack vector based on user correlation or blue tracking. However, the research did

show that some of the previously reported vulnerabilities had been addressed by the end of 2016. For example, the Gear S3 was found to have advanced security mechanisms that were in keeping with the newer BLE version 4.2, and was the most secure. However, our research showed that the HCI snoop log functionality found in most smartphones captured the identity of the message senders, as well as the message in plain text. With this function enabled the smart phones owner's conversations using email, SMS and messaging applications such as Facebook are preserved until a log is deleted. In Figure 6 this vulnerability is illustrated from our experiments.

```
04-22 21:26:05.706  WearableManager.Make extender protocol for
04-22 21:26:05.707  WearableManager.Action Found = Reply to Mom
04-22 21:26:05.707  WearableManager.Action:: Put action for id : 1857
04-22 21:26:05.708  WearableManager.Empty page list
04-22 21:26:05.709  WearableManager.No Pages
04-22 21:26:05.711  ForwardManager.forwardNotification(com.whatsapp), Source = 5
04-22 21:26:05.713  NotificationServiceAPI.getAppNotificationLevel(packageName : com.whatsapp, sourceType : 2)
04-22 21:26:05.717  Config.com.whatsapp id: 2130840151 get resource: android.content.res.Resources@b6eeba1
04-22 21:26:05.778  ForwardManager.info list size = 1
04-22 21:26:05.781  DBMemory.checkDuplicationNotification(1, com.whatsapp, 1492843322000)
04-22 21:26:05.793  DBMemory.[color] createNotificationUnit : 0(0)
04-22 21:26:05.794  ForwardManager.Lock ReleasedDuplicate MEssage Discarded
04-22 21:26:05.794  ForwardManager.Lock released
04-22 21:26:05.823  WearableJsonBuilder.action id : 1857 getIcon :2130840151
04-22 21:26:05.856  [WearableManager][JSON_BUILDER] WExtender JSON : is privacy
04-22 21:26:05.857  Main.WearExtender action found
04-22 21:26:05.859  [Main]jsonObj :  is privacy
04-22 21:26:05.860  Main.Group:: pushSchedulerForParseAndForward() noti : com.whatsapp
04-22 21:26:05.861  ForwardScheduler.pushScheduler : Type: 6
04-22 21:26:05.862  Main.handleMessage()
04-22 21:26:05.863  ForwardScheduler.Got message in scheduler Handler: 6
04-22 21:26:05.864  Main.MSG_NOTIFICATION_43_FORWARD
04-22 21:26:05.865  Config.isSamsungDevice()
04-22 21:26:05.871  ForwardManager.forwardNotification(com.whatsapp), Source = 5
04-22 21:26:05.872  NotificationServiceAPI.getAppNotificationLevel(packageName : com.whatsapp, sourceType : 2)
04-22 21:26:05.877  ForwardManager.info list size = 1
```

Figure 6. Snoop log plaintext disclosures

Overall, the lab testing of these devices shows that manufacturers have made big steps to improve the security around wearable devices. The security improvements in BLE version 4.2 have shut down some of the previous attack vectors and undoubtedly, further improvements are evolving during 2017. In the wearable devices tested, the security vulnerabilities detected indicate the threat classes potentially faced by a user. It is also notable that the different wearable devices have different vulnerabilities but the most predominant issue to date is the disclosure of the MAC, which allows for user correlation and blue printing attacks. The Amazfit performed the poorest out of the four tested. It failed in each of the four threat classes, whereas the Gear S3 with the updated BLE version performed the best in our tests. The implication of these findings is for corporates, such as health insurers, who provide benefits to the customer when they are using wearable devices that have health control feedback loops (MLC, 2017). In the case of a wearable device that is vulnerable to manipulation, the sponsoring corporate may not have confidence that the information they are receiving, and the information on which they will make decisions regarding providing benefits to their customer, can be trusted. In the bigger picture, wearable devices may fail compliance criteria such as the requirements of the European Personal Data Directive. In these situations, the purchaser requires notification in the specifications of the device regarding the security precautions for information protection. There also needs to be independent testing so that the shrink-wrap claims may have some external validation. Figure 7. shows the results from the laboratory testing.

Threat Class	Charge	Surge	Gear S3	Amazfit
Public Name	x	x	x	User Correlation Blue-Printing
MAC	Blue-Printing User Correlation	Blue-Printing User Correlation	x	Blue-Printing User Correlation
Key	x	x	x	Blue-Tracking
Notification	x	x	Breach of PII	Blue-Printing

Figure 7. Summary of Vulnerability

CONCLUSION

Wearable devices are convenient technologies that extend human natural senses and capabilities. Our research shows that further consideration of information protection is required to avoid disclosure failures. The improvement of information security by adopting countermeasures for pairing vulnerabilities will allow the producer of the information choices regarding the control of its ownership. Further research topics arising from this research for future projects are:

The HCI Snoop log paired with the base station – Is the number of log files, and degree of information captured controlled by the base station, the device, or both?

The Decrypt packets of the Amazfit – Future research should confirm that having the long term key is sufficient to decrypt the information exchanged with the smartphone. Also, consumer testing should be broadened to include data synchronisation from the smartphone to the web application.

PII failings – Determine whether the security vulnerabilities breach consumer privacy laws in key markets.

A broader range of attacks – Extend the man-in-middle attacks to intercept and manipulate communications. This has far-reaching implications, not just limited to wearables but also to other IoT setups.

Framework – A compliance framework which brings visibility to data protections in wearables, addresses standards, and reduces industry wide variations.

Further research is required to establish baselines for wearable device user expectations. At present the technology is made functional and accessible to users but we argue that development is required to meet the full scope of socio-technical expectations. Current users want the advantages of the technology, they are using it in increasing numbers, but they also want assurances unwanted surprises of a personal nature will not be forthcoming. Such unwanted attention is unsolicited advertising, personal profiling, geolocation matching, and so on. Our research shows that the confidentiality and potential integrity of data produced by wearable devices tested were easily compromised. More than a regular patch-by-patch updating of software is required to assure users their information safety has been adequately addressed.

REFERENCES

Boyle, R. J., & Panko, R. R. (2014). *Corporate computer security*. Essex, England: Prentice Hall Press.

Burlacu, A. (2016). *Fitbit Tracker Likely Saved This Man's Life, Leading Doctors To Shock His Heart Back To Normal*. Retrieved 20 March 2017, from http://www.techtimes.com/articles/149164/20160411/fitbittrackerlikelysavedthismans lifeleadingdoctorstoshockhisheartbacktonormal.htm

Cyr, B., Horn, W., Miao, D., & Specter, M. (2014). Security Analysis of Wearable Fitness Devices (Fitbit). *Tech.rep.Massachusetts Institute of Technology, 2014, pp. 1-14.*

European Parliament. (2016). *Directive (EU) 2016/680*. Retrieved 22 May 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

Grassi, M. (2014). *How to capture Bluetooth packets on Android 4.4*. Retrieved 6 March 2017, from https://www.nowsecure.com/blog/2014/02/07/bluetooth-packet-capture-on- android-4-4/

Great Scott Gadgets. (2015). *Bluetooth Low Energy mode for Ubertooth*. Retrieved15 March 2017, from https://github.com/greatscottgadgets/ubertooth/blob/master/host/README.btle.md

Guo, F. (2015). Securing Wearable Devices. Retrieved 22 May 2017, from http://www.leiphone.com/news/201511/cMxCXDonsugGN892.html

Hassan, S. S., Bibon, S. D., Hossain, M. S., & Atiquzzaman, M. (2017). Security threats in bluetooth technology. *Computers & Security, ,*. doi: 10.1016/j.cose.2017.03.008.

IDC. (2016). *Fitness Trackers in the Lead as Wearables Market Grows 3.1% in the Third Quarter, According to IDC.* Retrieved from http://www.idc.com/getdoc.jsp?containerId=prUS41996116

Layton, J., & Franklin, C. (2016). *How Bluetooth Works*. Retrieved1 June 2017, from http://electronics.howstuffworks.com/bluetooth2.htm

Lotfy, K., & Hale, M. L. (2016). Assessing Pairing and Data Exchange Mechanism Security in the Wearable Internet of Things Symposium conducted at the meeting of the 2016 IEEE International Conference on Mobile Services (MS) doi:10.1109/MobServ.2016.15

MLC. (n.d.). *MLC Life Insurance On Track*. Retrieved 20 March 2017, from https://www.mlc.com.au/personal/importantupdates/ontrack

NIST. (2010). *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*. Retrieved SP 800-37 Rev. 1, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

Pieterse, H., & Olivier, M. S. (2014). Bluetooth Command and Control channel. *Computers & Security, 45*, 75-83. doi:http://dx.doi.org/10.1016/j.cose.2014.05.007

PwC. (2015). The Internet of Things: The next growth engine for the semiconductor industry. Retrieved from https://www.pwc.de/de/technologie-medien-und- telekommunikation/assets/pwc-studie-prognostiziert-boom-in-der- halbleiterbranche.pdf

Schellevis, M., Jacobs, B., Meijer, C., & de Ruiter, J. (2016). Getting access to your own Fitbit data.

SIG. (n.d.). *Security, Bluetooth Low Energy*. Retrieved 2 June 2017, from https://www.bluetooth.com/~/media/files/specification/bluetooth-low-energy- security.ashx?la=en

Stack Overflow Community. (2015). *Analyzing Bluetooth Low Energy Traffic*. Retrieved from http://stackoverflow.com/questions/32640581/analyzing-bluetooth-low-energy-traffic

Stallings, W. (2014). *Cryptography and Network Security: Principles and Practice, 6th Edition*: Pearson.

Zhou, W., & Piramuthu, S. (2014, 18-21 June 2014). Security/privacy of wearable fitness tracking IoT devices Symposium conducted at the meeting of the 2014 9th Iberian Conference on Information Systems and Technologies (CISTI) STI.2014.6877073