Staying Secure while Getting Fit

Nawras Alkassab, Phani Soumya Inguva, Krishna Sindhuja Kalusani, Ajay Kumar Koduri, Siddharth Pathak, Aaron Pecora, Manasa Suthram

Abstract: Wearable smart devices are the new product on the block when it comes to the latest technology with the possibility of being as ubiquitous as the smartphone. One of the primary purposes for purchase of wearable smart devices is the tracking of a wearer's fitness. These devices include multiple sensors to measure fitness, but these sensors also can be exploited. The data they measure and send over Bluetooth is very susceptible for the ingenious malicious attacker. We explore the devices available, the Bluetooth medium they all commonly use and possible exploitation, justifying why securing these communications is vital to the wearer.

I. Introduction

The Wearable devices market is estimated at 2 billion dollars and some analysts predict it will grow to be a 5.9 billion dollar market by 2019 [1]. With 20% of the general population owning at least one wearable and 10% using it daily, this demand will likely continue, as 52% of technology consumers are aware of wearables and 33% are likely to buy one [2].

To meet these wants of the user, components such as accelerometers, gyroscopes, digital compasses, heart monitors, altimeter, light sensors and more have been made smaller and smaller to fit within such devices to uninhibitedly be with the user at all times.

These extra components have been so effectively engineered that their precision can be measured to the millimeter and therein this lays a great vulnerability. The ability to precisely track fine movements of a user opens up the opportunity for the malicious attacker to track things such as ATM PIN entry, or to even track keystrokes on a keyboard [4]. Though a fitness band is on only one wrist of the user, it has been studied that one could fairly confidently infer a user's input from both hands with Machine Learning techniques [5]. Other studies have tracked the entire arm without utilizing Machine Learning techniques [6].

By meeting the customers' "wants", the companies have surpassed the implementation of the customers' "needs" i.e. Security. Though smart devices such as phone and tablets have been in the market longer and therefore matured in companies' security hardening efforts, the advent of wearable smart devices has left open many vulnerabilities. Unfortunately, but predictably since the security has been overlooked the precision by these components are ripe for the malicious attacker.

Transmitting what the user actually wants and only needs, is an area for consideration. It could possible to have a third-party software on a device that acts as a "firewall" of sorts, only transmitting data the user wants, if developers do not provide selectable options to the user.

Our aim is to understand to what extent wearable devices are vulnerable to malicious attacks and to what extent these wearables reveal personal information about their users by either sharing users' personal information to a cloud server or by asking the user for more permissions. According to [2], there are five categories of information that wearables share with cloud servers on the internet. These categories are: basic personal information, fitness information, location information, social information, and device identifiers.

We will discuss the background Wearable devices, Fitness trackers, the security of Bluetooth, Bluetooth's vulnerabilities and the exploitation of data from wearable devices.

II. Wearable Devices

Humans have always had an insatiable zest to invent new tools to make any task easier and more convenient. In the current world with new discoveries in technology every day, one direction of interest is implementing that technology into things we are already familiar with using. That next big thing is wearable devices: smart watches, smart glasses, wristbands for health monitoring, etc. The market for this kind of technology growth is showing signs of change of motive from external interaction with the web to the possible internal substitution of a certain function of our brain. **NEED REFERENCE**

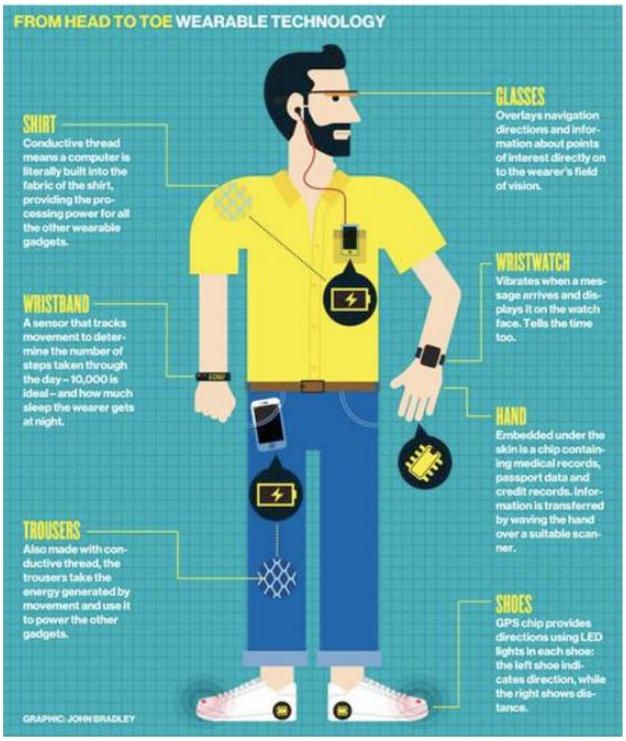

Figure 1 Various Smart wearable devices [7]

Coming to the fact of invention, the major devices that are ruling the wearable devices' innovation world are the smart watches, fitness trackers and head mounted displays.

The watches are no longer more mere stylistic time pieces; they have become mini notification centers banded on your wrist which has more than half of the capabilities that the user's smart phone has. And all major companies such as Apple, Samsung, and LG have invested into developing this market working harmoniously with the user's phone for further interaction with the wearable device.

Fitness trackers have become an integral part of some persons and in fact an overall motivation for a better and healthier world. The concept is that these devices provide information that will in turn keep us fit, reminding of health concerns, following up with the cycles, and help us maintain fitness routines. Not only have major technology companies invest into this area as well, but also those from various industries as well like Garmin, Fitbit, Jawbone, Misfit, etc.

The method of creating the performance and the props featured within a smart wearable device was inspired by Giulio Jacucci's thesis *Interaction as Performance* [10]. This interaction design provides methods to analyze interactions by focusing on the expressive movements that reveal our moods. The relationship between the smart wearable devices and the user has the analogy of a parent and child. Similarly, the performance is compared with human routine in a full day.

The wearable devices open up opportunities for the new design and development applications to be incorporated on these platforms. To help accomplish this, Google has expanded its Android platform to Android Wear for developing applications that can work various wearable devices.

A. Fitness Trackers Background

Wearable smart devices specifically designed for tracking and monitoring physical measurements for fitness are known as fitness trackers. Fitness trackers are usually worn on the wrist in the form of a bracelet to assist people in understanding their fitness levels either it be for weight management issues, sleeping patterns, heart health or numerous other things by aggregating measured input data and outputting into some desired format. A simple example is that a number of the activity trackers measure the step count and heart rate or the wearer, but the more useful activity trackers can differentiate between activities and step counting. Fitbit Alta and Misfit Ray are examples of fitness trackers that automatically recognize when the user starts and ends an activity. These devices send notifications when the user jiggles or jostles their body more than normal [11].

There exist some other trackers in the market that let the user manually record an activity by pressing a button, which could be helpful when the user is particular over the start and stop times of activity tracking, the way many runners do. The Garmin Vivoactive - another brand of fitness tracker uses this method, as does pretty much every other device that's a hybrid runner's watch and fitness tracker. Activity trackers such as Sleepace RestOn or Misfit Beddit are used to track pattern of sleep [11].

Figure 2 Common Interface with Fitness Band [12]

The fitness trackers use sensors to record data. The data collected by the device is transferred to a mobile application, either through wireless Bluetooth syncing or plugging the device into a phone, where goals, progress and activity can be tracked [13]. The transmission of syncing data from the device to the smartphone is the main focus of our paper.

B. Studies with Fitness Trackers

A study that incorporates an empowerment theoretical framework was conducted to evaluate the quality of life and physiological outcomes for a duration of 12 weeks. The nurse practitioner student facilitated remote management strategy utilizing a fitness tracker to log diet and exercise in 75 overweight adult participants. The participants demonstrated an improvement in quality of life and physiological factors at a .05 level of significance [14].

In another study performed to examine the ability of the Basis Band Fitness Tracker to measure heart rate and movement compared to research grade activity monitors, it was suggested that the basis band did not accurately quantify heart rate or physical activity as seen in Table 1 below [15]. Nonetheless, users are still purchasing devices as it still gives some type of measurement of their fitness.

Variables	Chest strap Heart Rate	Basis Band Heart Rate	P - value	Total Sample ICC (n= 17)	Average ICC (n= 17)
Sedentary Behavior	84 ± 11 (1,027)	81 ± 11	<0.05	0.85 (1,027)	.63 ± .35 (.00-.96)
Light Physical Activity	91 ± 13 (751)	84 ± 15	<0.05	0.63 (751)	.36 ± .30 (.00-.83)

MVPA	123 ± 31 (90)	105 ± 22	<0.05	0.63 (90)	.26 ± .30 (.00-.80)
Overall	89 ± 16 (1,868)	83 ± 14	<0.05	0.78 (1,868)	.59 ± .25 (.00-.90)

Table 1 Chest vs Band measurements [15]

And as seen in research [16] a sample was conducted of 210 individuals (143 women, 67 men) to determine the following observations:

Participant characteristics and descriptive measures (N = 210).

	n	n %		n	n %
Age			Country of residence		
<15	1	0.5%	US	156	74.2%
15–25	21	10.0%	UK	15	7.1%
26–35	64	30.5%	Canada	7	3.3%
36–45	58	27.6%	Netherlands	5	2.4%
46–55	30	14.3%	Australia	4	1.9%
56–65	18	8.6%	Sweden	4	1.9%
66–75	10	4.8%	Other	19	9.0%
>75	8	3.8%			
Brand of Wristband			How long have you been using your wristband?		
Fitbit	81	38.6%	0–5 months	93	44.3%
Jawbone	48	22.8%	6–12 months	42	20.0%
Misfit	26	12.4%	1–2 years	39	18.6%
Nike	21	10.0%	2 years	36	17.1%
Garmin	20	9.5%			
Other	14	6.7%			
Gender					
Male	67	31.9%			
Female	143	68.1%			

Table 2. Age groups in use of Fitness Bands[16]

This shows that over half of those who have fitness devices are higher in the 26-45. However, there is still a large portion, nearly a third over 45 hence showing the appeal of such devices to various generations.

III. Security of Fitness Trackers

As the fitness tracker is a device worn by the user as often as a garment, the convenience of them is the wireless synchronization of the data they collect to another device such as the user's smart phone or computer. To accomplish this, the developers of the device employ Bluetooth.

A. Bluetooth Security

Bluetooth technology is the most popular wireless connectivity solution which has been integrated into many types of business and consumer devices. Bluetooth enabled devices are increasing rapidly and are becoming a target for attackers, thus stealthy security issues still remain around this Bluetooth technology. It is important to develop and communicate company policies for Bluetooth enabled devices so that the important information of users is not compromised. Organizations should mitigate risks to their Bluetooth implementations by applying countermeasures to address specific threats and vulnerabilities. Few Bluetooth vulnerabilities include denial of service attacks, fuzzing attacks, encryption attacks, eavesdrop etc.

Bluetooth standard specifies three main security modes [17]:

- No security: device operates on indiscriminate mode allowing any Bluetooth device to connect.
- Service level security: security is initiated after the channel is established. (supports authentication, authorization, encryption)
- Link level security: security is initiated before the channel has been established. (supports authentication and encryption)

Bluetooth, along with other wireless networks, can form ad hoc networks, which have different security attributes and vulnerabilities than a fixed network. The entire topology is dynamic and complex which makes security issues complicated.

B. Risk mitigation strategy and countermeasures:

The countermeasures recommended below do not guarantee a secure Bluetooth environment and cannot prevent all insecure penetrations [18]. In addition, security comes at a cost—expenses related to security equipment, convenience, maintenance, and operation.

- Perform comprehensive security assessments at regular intervals to fully understand the organization's Bluetooth security posture.
- Ensure that wireless devices and networks involving Bluetooth technology are fully understood from an architecture perspective and documented accordingly.
- Provide users with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft.
- A complete inventory list of Bluetooth-enabled wireless devices can be referenced when conducting an audit that searches for unauthorized use of wireless technologies.
- Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the organization.
- Ensure that link keys are not based on unit keys.
- Many Bluetooth stacks are designed to support multiple profiles and associated services. The Bluetooth stack on a device should be locked down to ensure only required and approved profiles and services are available for use.
- Enable encryption for all broadcast transmissions.

The general nature and mobility of Bluetooth-enabled devices increases the difficulty of implementing traditional security measures across the network. Policy documents should include a list of approved uses for Bluetooth and the type of information that may be transferred over Bluetooth networks. The security policy should also specify a proper password usage scheme for the users.

Bluetooth is a great addition to the business productivity toolbox. However, it must be understood by the technical team and its deployment should be closely managed. Although it has been accepted as IEEE 802.15 standard, there have been known exploitations of it as we discuss in the next section.

IV. Bluetooth vulnerabilities

A Bluetooth device uses radio waves instead of wires or cables to connect to a phone or product. There are several devices which are embedded with this technology which enables this communication and they are increasing over time. With the increase in such devices the security issues associated with them also increases multifold. The use of less hardware for this setup has made it a popular means of communication.

An ideal scenario is one where a connection is established between 2 devices and no other device should be able to obtain the information that is shared between them. Furthermore, no one should be able to determine the identity of the communicating devices. These are the primary security requirements of devices connected via Bluetooth. Malicious attackers may try to gain access to the secret information that is transmitted between devices or may try getting the geographical location of the devices by launching certain types of attacks.

It's the responsibility of the security experts to construct devices with robust security and also the responsibility of the users to be aware of the different kinds of attacks and

what measures can be taken from their side to prevent from being attacked.

In [19] the researchers explore three different types of vulnerabilities that can be exploited in Bluetooth. Below are the details of Bluetooth specifications that are relevant to the attacks.

A. Bluetooth Specifications

Device modes: A device can be in one out of the two modes: discoverable and non-discoverable. When in discoverable mode, the device will respond to inquiries. Also, the device can be in connectable or non-connectable mode. When in connectable mode, it will respond to messages it receives from already discovered devices.

Addressing: "Bluetooth device address" is used to uniquely identify every device. Device access code (DAC) is used to address the device. Also a certain type of channel is used for point-to-point and point-to-multipoint communication. Every channel has a certain channel access code (CAC). CAC & DAC are always transmitted in clear.

Establishment of Initialization Key: A series of communication steps are carried out which involves choosing of a random number to compute the initialization key by the communicating parties and several acknowledgement steps.

Cipher Use: The encryption key is generated from the link keys that have been set up. The encryption key is used to seed the stream cipher and the output of the stream cipher is used to encrypt plaintexts.

Considering these specifications, the first attack is a type which an adversary under some conditions will be able to determine the key exchanged by the two devices.

B. Methods of Attack

Offline PIN crunching: In this method two different types of attacks occur, eaves-dropping and stealing by participation. In eavesdropping, the attacker launches a brute force attack and guesses PINs. He then compares this PIN with the PIN that is transmitted in plain text. If they match with a high probability, then it's confirmed that the guessed PIN is correct. Here, the adversary can silently listen to communication parties without their knowledge.

Another method is stealing by participation:- The attacker guesses the PIN first and uses the challenge- response protocol in which it checks with the victim device to see if the guessed PIN is correct or not. If its 'incorrect' then the attacker moves on to guess another PIN and then tries again. The moment there is a 'correct' response from the challenge-response protocol; it means that the guessed PIN is correct.

Location attacks: When a device wants to respond to connect with another device, it sends the information about its identity on a band. The attacker can determine the location of victim devices by maintaining geographically distributed devices which continuously inquire all devices entering within their reach and using the information transmitted on the band. The attacker can also introduce a device to scan for devices and connect to it. To use this, the attacker must have installed corrupt software on the victim device that automatically reveals the identity when requested.

Cipher attacks: In this, the attacker uses "reverse engineering" to guess the cipher transmitted between the devices. In the process, he computes the contents of the 39-bit register by using the outputs of the other LFSRs and the summation register. He then checks whether his guess is correct by

comparing a string of actual output to the generated output.

These show different methods in which Bluetooth devices are attacked. Other research [20] expand on the types and classification of such attacks.

The paper explores the Bluetooth Vulnerabilities in Smartphones as follows.

Bluesnarf: Using this, an attacker can connect to a Bluetooth enabled device without going through the normal process of authentication. This allows him to get access to stored data such as phone book information, calendar details, clock setting and other information. BlueSnarf++ is a variation of BlueSnarf which attacker to view and manipulate the files in the file system, on SD cards and memory sticks. Again these are possible because of certain implementation flaws.

BlueBug: AT command set is used to configure and control communication devices like modems. An attack on this will allow the attacker to gain access on the application level. When he has such a control, he can divert call, manipulate phonebook and carry out other kinds of disruptive actions. These are possible because of poor implementation of Bluetooth stack. If unpublished service is created in RFCOMM channel, the attacker can exploit this without pairing.

BlueSmack: In this attack, the attacker tries to overwhelm the vulnerable device by sending large ping packets without requiring an open L2CAP channel. This can cause buffer overflow or may lead to denial of service attacks.

Bluejacking: The attacker can modify the content of phonebook of the victim's device using OBEX protocol object push feature. When exploited, the attacker sends undesirable messages to the victim's phone which are disguised as someone else. This may cause annoyance to the victim. Although launching them may be difficult, once launched, the attacker can access sensitive data owned by the user.

Backdoor: Some implementation flaws can leave the previous pairing information on a device unremoved. An attacker after attacking the device may be able to retrieve the information about this other device and even connect to it, or steal its information. The attacker can secretly pair the devices. The attacker can also access WAP and GPRS services of the victim devices.

Blueprinting: All Bluetooth devices have a unique attribute which uniquely identifies the device. If an attacker comes to know of this then he can use this to masquerade as that device. Every Bluetooth device has a service record handle field which uniquely identifies each service. This is hard coded with certain firmware. This firmware may be improperly implemented. So, the attacker can access the device ID by breaking this ID. So, a firmware which is robust has to be used instead of a weak one.

Since, all these attacks are prevalent on Bluetooth devices, it is mandatory to implement proper security regulations in such devices.

V. Exploiting Wearable Devices

During our research, we asked ourselves how aware the users of wearable devices are when it comes to their privacy and the security of their wearable devices. Fortunately, we came by [2] where the authors had surveyed 1,782 Internet users in order to identify what are they concerns about wearables and what worries them the most. The authors had identified concern factors where the user get upset if at some point when one or more of these factors are

shared. To measure whether a content that's being shared with other is annoying to the end user, the researchers had identified a Very Upset Ratio (VUR) where, as shown in following table, different VUR with different data types.

Rank	Data	VUR	σ	Distribution
1	video of you unclothed	95.97%	0.31	
2	bank account information	95.91%	0.35	
3	social security number	94.84%	0.26	
4	video entering in a PIN at an ATM	92.67%	0.47	
5	photo of you unclothed	92.59%	0.46	
6	photo of you that is very embarrassing	91.39%	0.55	
7	username and password for websites	89.55%	0.62	
8	credit card information	88.98%	0.56	
9	video of you that is very embarrassing	88.41%	0.53	
10	photo of you at home	87.50%	0.60	
	⋮			
64	eye patterns (for eye tracking)	40.51%	1.27	
65	exercise patterns	38.66%	1.26	
66	when you are happy or having fun	34.75%	1.27	
67	television shows watched	30.20%	1.40	
68	when you are busy or interruptible	29.50%	1.26	
69	music on device	28.06%	1.43	
70	your heart rate	27.50%	1.40	
71	age	24.29%	1.43	
72	language spoken	15.86%	1.49	
73	gender	15.00%	1.45	

During the survey, the researchers had asked the users "What do you think are the most likely risks associated with wearable devices?" The users' answers to this open-ended question are shown below in the following table:

Concern	Responses	Frequency
Privacy	452	25.32%
Being Unaware	275	15.40%
Health Risk	191	10.70%
Safety	185	10.42%
Social Impact	157	8.80%
Financial Cost	151	8.46%
Security	144	8.07%
Accidental Sharing	69	3.87%
Miscellaneous	57	3.19%
None	51	2.86%
Social Stigma	39	2.18%
False Information	33	1.85%
Don't know	31	1.74%
Aesthetics	19	1.06%
Don't care	11	0.62%

In this section, we research whether smartwatches are vulnerable to attacks.

Imagine a user typing on a laptop keyboard while wearing a smartwatch. We ask whether motion sensors from the watch can leak information about what the user is typing. If an attacker had installed a malware in the user's smartwatch, the attacker can remotely know what the user is typing through the motions of the smartwatch. The authors of MoLe (Motion Leaks through Smartwatch Sensors) [5] had found that when motion signal processing is combined with patterns in English language, the leakage is substantial. Reported results show that when a user types a 'W', it is possible to shortlist a median of 24 words, such that 'W' is in this shortlist. When the word is longer than 6 characters, the median shortlist dropped to 10. The authors of MoLe had proved that sensor data from smart watches can leak information what the user is typing on a keyboard while wearing his/her smartwatch. The privacy of the end user's life can be penetrated easily if the attacker had managed to install malware in the smartwatch and keep tracking of its motions. Unfortunately, smart watch companies still produce them without caring about the end user privacy.

References:

[1] Andrew Hilts, Christopher Parsons, and Jeffrey Knockel, Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security. Open Effect Report (2016). Available at: https://openeffect.ca/reports/Every_Step_You_Fake.pdf.

[2] Lee, Linda, et al. "Risk Perceptions for Wearable Devices." arXiv preprint arXiv:1504.05694 (2015).

[3] Chen Wang, Xiaonan Guo, Yan Wang, Yingying Chen, and Bo Liu. 2016. Friend or Foe?: Your Wearable Devices Reveal Your Personal PIN. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (ASIA CCS '16). ACM, New York, NY, USA, 189-200. DOI: http://dx.doi.org/10.1145/2897845.2897847

[5] H. Wang, T. T.-T. Lai and R. Roy Choudhury. Mole: Motion leaks through smartwatch sensors. In Proceedings

of the 21st Annual International Conference on Mobile Computing and Networking, pages 155–166. ACM, 2015.
[6] Sheng Shen, He Wang, and Romit Roy Choudhury. I am a Smartwatch and I can track my user's arm. In Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services, ACM MobiSys '16.
[7] Levorse, Sean, From Human to Cyborg (2016) Available at: https://people.rit.edu/sml2565/iimproject/wearables/index.html
[8] Mary Ellen Berglund, Julia Duvall, Lucy E Dunne, 2016. A Survey of the Historical Scope and Current Trends of Wearable Technology Applications. ISWC '16, SEPTEMBER 12–16, 2016, HEIDELBERG, GERMANY.
[9] Sarah Homewood. Maintaining Relationships with Our Devices. CHI 2016, San Jose, CA, USA
[10] Jacucci, G. Interaction as Performance. Cases of Configuring Physical Interfaces in Mixed Media. Oulu University Press (2004), Oulu, Finland.
[11] DUFFY, J 2016, 'Make the Most of Your Fitness Tracker', *PC Magazine*, p. 126, MasterFILE Premier, EBSCO*host*, viewed 4 November 2016.
[12] https://www.powerfulpatients.org/2015/10/06/ can-digital-wearables-help-in-clinical-trials/
[13] Lunney, A, Cunningham, N, & Eastin, M 2016, 'Full length article: Wearable fitness technology: A structural investigation into acceptance and perceived fitness outcomes', Computers In Human Behavior, 65, pp. 114-120, ScienceDirect, EBSCOhost, viewed 5 November 2016.
[14] Stukenberg, E, & Friess, M 2015, 'A Quantitative Pilot Study on the Use of a Fitness Tracker in the Preventative Management of Employees at Risk of Chronic Disease in a Health Care Facility', Online Journal Of Nursing Informatics, 19, 3, pp. 1-7, CINAHL Plus with Full Text, EBSCOhost, viewed 4 November 2016.
[15] DESILETS, PIER-ALEXANDRE MAHAR, MATTHEW T. International Journal of Exercise Science; 2016, Vol. 9 Issue 3, p258-269, 12p, 6 Charts, 2 Graphs,2016
[16]Nelson, E, Verhagen, T, & Noordzij, M 2016, 'Full length article: Health empowerment through activity trackers: An empirical smart wristband study', Computers In Human Behavior, 62, pp. 364-374, ScienceDirect, EBSCOhost, viewed 5 November 2016.
[17] Olzak, T. (2016). Secure your Bluetooth wireless networks and protect your data - TechRepublic. TechRepublic. Retrieved 5 November 2016, from http://www.techrepublic.com/article/secure-your-bluetooth-wireless-networks-and-protect-your-data/.
[18] Padgette, J., Scarfone, K., & Chen, L. (2012). Guide to Bluetooth Security. Retrieved 6 November 2012, from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-121r1.pdf.
[19] Jakobsson, M., Wetzel, S.: Security Weaknesses in Bluetooth. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, p. 176. Springer, Heidelberg (2001)
[20] Lih Wern Wong; Potential Bluetooth Vulnerabilities in Smartphones, AISM, 2005, The School of Computer and Information Science & Edith Cowan University, Perth, Australia.