WEARABLE TECHNOLOGY DEVICES SECURITY AND PRIVACY VULNERABILITY ANALYSIS

Ke Wan Ching and Manmeet Mahinderjit Singh

School of Computer Sciences,University Sains MalaysiaPenang, Malaysia

ABSTRACT

Wearable Technology also called wearable gadget, is acategory of technology devices with low processing capabilities that can be worn by a user with the aim to provide information and ease of access to the master devices its pairing with. Such examples are Google Glass and Smart watch. The impact of wearable technology becomes significant when people start their invention in wearable computing, where their mobile devices become one of the computation sources. However, wearable technology is not mature yet in term of device security and privacy acceptance of the public. There exists some security weakness that prompts such wearable devices vulnerable to attack. One of the critical attack on wearable technology is authentication issue. The low processing due to less computing power of wearable device causethe developer's inability to equip some complicated security mechanisms and algorithm on the device.In this study, an overview of security and privacy vulnerabilities on wearable devices is presented.

KEYWORDS

Wearable Technology; Wearable Devices; GoogleGlass; Smartwatch

1.INTRODUCTION

Wearable Technology (WT), or called as wearable is a computing technology device that can be worn on the human body, either a computer that are incorporated as an accessory or as part of material used in clothing [1]. These devices come in many different forms such as watches, glasses, wristbands or even jewelry items [2]. Wearable devices are defined by six main characteristics which are un monopolizing, unrestrictive, observable, controllable, attentive and communicative [3]. The development of the applications that can work with WT cover a broad field from those focused on healthcare and fitness, to industrial applications, and even entertainment and arts [2].

WT offers new opportunities to monitor human activity continuously with the miniature wearable sensors embedded. It improves efficiency, productivity, service and engagement across industries [4]. However, there are few challenges faced on WT which are power consumption, communication capacity, design constraints, and security issue [5]–[8]. Due to limited bandwidth and processing power, wearables provide less security compared to other computing devices [5]. In the consequences, the possibilities for the security vulnerabilities exploited increases to an array of possible attacks which will put users' safety and privacy appear at risk. Wearable computing brings new challenges and opportunities for user authentication.

DOI: 10.5121/ijnsa.2016.8302

One main challenge in adopting a good approach to a secure authentication in wearable is due to the nature of its operations in which wearable devices are not standalone devices as they will require to pair with other gadget such as Smartphone to perform most functions. This complexity of communication creates security vulnerabilities such as man-in-the-middle attack. Imagine a user who uses his smartwatch to control his smart home. The need for a communication between the smartwatch and the application which is stored within the smartphone is prone to information leakage leading to other security attacks through the art of manipulation of data. The other challenge is the lack a keyboard, and often times even a touchscreen causes difficulty in providing authentication mechanism.

The work present an aim to present a brief review on security and privacy attacks that occur in wearable technology to understand its security andprivacy loophole that exists in wearable technology and present a security analysis on various wearable technology devices. A security analysis is done by evaluating three main wearable devices such as Google Glass, Fitbit and Smartwatch.The outline of the paper is as the following. Section II provides some related work. Section III demonstrates a comprehensive security and privacy. Section IV presents the discussion and conclusion.

2. RELATED WORK

Wearable Technology is the latest technology in the electronic devices field. It has been designed in many different forms that can be worn on the human body from head to toe such as glasses, shirt, wristband, watches and other forms [2]. It not only can perform the basic task like what smartphones do, but the embedded, wearable sensors also recognize and provide wearer’s actionable information in a real time context. Wearable device has the following characteristics such as [3], [9]:

- hands-free (unrestrictive), so that users can do other thing when using the wearables.
- always on (controllable), it is a responsive system as it is always in the ON status, so users can grab control of it at any time.
- environment-aware (attentive), wearables are environmentally aware, multimodal and multisensory.
- attention-getting (observable), it can keep users continuous attention when users want it to such as receiving alerts, messages or reminders.
- connected (communicative), the wearables are connected to a wireless network so that information exchange can be happened in the real-time situation.
- un monopolizing, which mean it does not cut users off from the outside world.

2.1 WEARABLE TECHNOLOGY SENSORS EXAMPLES

Wearable sensors are often combined with the other sensors to detect human activities of daily living (ADL) such as walking, running, sitting and eating. There are many possible applications for activity recognition with wearable sensors, for instance in the areas of healthcare, elderly care, personal fitness, entertainment, or performing arts. Different sensors are deployed on wearable devices depending on what kind of activity monitoring information to be collected.

Accelerometer is used to measure linear acceleration [10]. It is measured in three axis to measure position in three dimensions. The accelerometer embedded inside wearable can determine whether the device is horizontal or vertical, and whether it’s moving or not. The basic function of an accelerometer in wearable is to count steps on people’s activities such as walking.Gyroscope determines the orientation by using Earth's gravity based on principle of rotation [10]. Both accelerometer and gyroscope are IMU (Inertial Measurement Unit) sensors that are commonly used in wearables. Both of them can determine orientation, but the gyroscope provides greater precision and it gives measurements for angular velocity. More importantly, they are implemented in vary applications despite their similar purpose [24].

GPS (Global Positioning System) is a location sensor that is widely used for navigation. Most wearables now include an integrated GPS tracking system to locate a person's location. It detects the location using either GPS, triangulation of cell towers or Wi-Fi networks with a database of known location [25].A microphone is defined as acoustic sensor that converts sound into an electrical signal [26]. Most wearables are embedded with this sensor for voice activity detection. Next an analysis on various wearable devices such as Google Glass, Fitbit devices and Samsung Smartwatch in term of their security aspect is given.

2.2 SECURITY ANALYSIS ON REAL EXAMPLES OF WERABLE DEVICES

2.2.1 GOOGLE GLASS

Google Glass or simply called as Glass can say as the first wearable device that kick start the growth of WT. Glass is an eyewear device that has built-in computer in the frame of a pair of glasses. It provides numerous innovative features that make people life more fun. However, many concerns have been raised from various sources regarding to some issues that could be threatened wearer's security and privacy.

There are few research findings that point out some vulnerability in term of security and privacy aspect on Google Glass. For example, Glass does not have a secure enough PIN system or authentication in place currently [11-12]. Besides authentication issues, [13] found that the privacy of user' appears at risk as well by the eye tracking technology supported in Glass. In addition, Seyedmostafa and Zarina [11] revealed that pictures and videos can be recorded without user's consent which violate people privacy policy. More importantly, there are several real cases regarding security vulnerability associated with Glass were reported at the time of Google release. For example, engineers at the security firm Lookout Mobile [14] revealed a serious security vulnerability on how Glass interpret QR (Quick Response) codes while it snaps a photo back in May 2013. They found that Glass would scan a malicious QR code that forced it to be connected to a hostile wifi access point and someone could remotely gain root access to a Glass device and take control of it without the wearer's knowledge. Fortunately, the bug has been reported to Google and a patch was released to fix the problem in a timely manner.

However, a few months later, Symantec reported that Glass is still vulnerable to Wi-Fi Hijacking [15] despite QR photobombing. This happened because someone can set up a Wi-Fi access point using the same Wi-Fi name as the one that people previously use to connect before using a device called Wi-Fi Pineapple. It can impersonate any network that a device searches for by borrowing the network SSID (Service Set Identifier). For example, when Glass checks to see if that prior network is available the attacker's Wi-Fi Pineapple will simply answer the request and pretend to be that specific network. It causes Glass to be at risk with the same sort of attacks that can arise when connecting to a hostile network such as sniffing traffic or redirection to malicious sites.

Lastly, wearable technology raises the issues of privacy as described in [10], ninety percent of the survey target feel uncomfortable if someone recording a video of them using Google Glass. The feature and functionality of any wearable device allow user to capture images or record video using their wearable device without the notice of their target. Some entertainment place like cinema and casino have even banned the usage of such devices in their business area due to the privacy problem. In this case, we may conclude that the level of acceptance of people with certain wearable devices is low due to the fact that such device affects people's perception of their privacy.

2.2.2 Fitbit Devices

Fitbit [16] is known for its products which is a smart fitness band that can be worn on the wrist. It provides human activity measurement such as number of steps walked; sleep quality and other personal health metrics like heart-rate and body temperature.However, one of the major security vulnerabilities found in Fitbit is lack of authentication. [17]-[19] presented that Fitbit is lack of authentication on tracker side and potential attacker can easily get the data from without the knowledge of users. For instance, Mahmudur et.al [18] built a tool, FitBite to launch several attacks on Fitbit devices such as data injection attack, DoS and battery drain hacks to prove the statement. The result showed that the vulnerable Fitbit device could allow malicious hackers to hijack Fitbit users' account, access or even manipulate their personal health data to earn monetary rewards.In addition, Fitbit Flex is vulnerable due to leaky BTLE (Bluetooth Low Energy) technology. This is because it did not change the privacy address [20] or MAC address remains the same [21] and it can be easily tracked based on the Fitbit's Bluetooth advertisement. In consequences, it could lead to privacy breach as third parties can track activities for specific users. Insurance companies may also take this advantage to create a "gray market" for getting users' health information data. Besides that, Fitbit devices could potentially threaten users' privacy risk. For example, it allows malicious people to track users location or places visited to make phishing attack such as send fake email that offer deals with the link that actually linked to spyware or a virus [19].

2.2.3 Samsung Smartwatch

Samsung Smartwatch is another wearable device that offers significant innovative functionalities that makes the enhancement of people's daily life. In fact, the biggest selling point is the notification features in Android Wear Smartwatch. It has enabled to synchronize data to the phone and all the important alert and notifications will get pushed directly on the wrist. However, according to an HP recent study [22] (See Figure 1) on top 10 popular Smartwatches in the market, found that 100 percent of the tested Smartwatches contain significant vulnerabilities, including poor authentication, lack of encryption and privacy issues. For instance, there are 70% of watch firmware was transmitted without encryption. 3 in 10 watches were vulnerable to account harvesting, which is an attack that gain access to the device and data by looking for weak passwords and lack out account lockout. Only 50% of tested devices offered

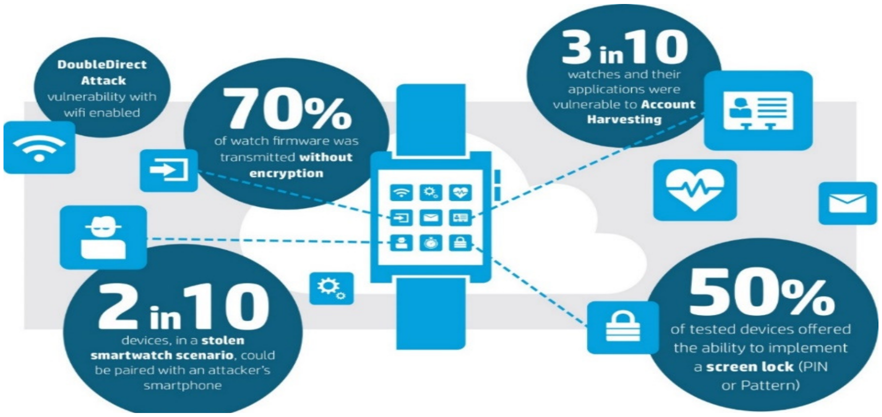
DoubleDirect Attack vulnerability with wifi enabled
70% of watch firmware was transmitted without encryption
3 in 10 watches and their applications were vulnerable to Account Harvesting
2 in 10 devices, in a stolen smartwatch scenario, could be paired with an attacker's smartphone
50% of tested devices offered the ability to implement a screen lock (PIN or Pattern)

Figure 1: Security Vulnerability Factson 10 Different Tested Smartwatches [22]

the ability to implementa screen lock either PIN or pattern. Therefore, it can be deciphered easily using brute force attack and gain control access to the device. For instance, researchers from Romania-based Bitdefender [23] had created proof of concept hack to access a Samsung Gear Live Smartwatch, paired with a Google Nexus 4. The result showed that the six-digit PIN code and Bluetooth communication between the two paired devices could be deciphered easily using the brute force attack by using any open source sniffing tool. And thus the users' security and privacy are in risks without a strong authentication scheme in place. Besides that, user does not need to unlock the Smartwatch and thus data can be accessed from a computer without authenticated [24]. For instance, [25] revealed that information data such as messages, emails and contacts can be pulled out easily from Samsung Gear 2 as Samsung did not do encryption properly as it needed for the Smartwatch devices. After the security analysis has been done for the selected wearable devices, the security vulnerabilities and security attacks on the devices are summarized and listed in Table 1.

Table 1: Summary of Security Vulnerabilities and Security Attacks Found in Various Wearable Devices

Wearable Devices	**Security Vulnerabilities**	**Attacks**
Google Glass	Unsecure PIN system or authentication in place [11]-[12]	The gesture-based authentication scheme easily to be recorded by people nearby
	Privacy: pictures and videos can be recorded without user's consent [11] and unauthorized eye movement tracking [13]	Eavesdropping and spyware
	It relies on QR codes for Wi-Fi setup [14]	QR photobombing malware
	Unsecure network and hostile environment [15]	Wi-Fi-hijacking, man-in-the-middle attacks such as session hijacking or sniffing
Fitbit Devices[16]	Lack of authentication [17]-[23]	Data injection attack [22], Denial of Service (DoS) and battery drain hacks
	Leaky BTLE (Bluetooth Low Energy) technology [20-21]	It can be easily tracked
	Privacy: Users location or places visited can be tracked [19]	Phishing
Samsung Smartwatch	Authentication mechanism not secure enough [22]-[23]	Brute force attack [22]

From Table 1, it showed that there is a common security vulnerability exists between the selected wearable devices that have been chosen to be analysed which is lack of authentication. From the table, we can observe that without proper security authentication implemented, wearable devices can be exploited to some several attacks such as eavesdropping, DoS, and brute force attacks. For instance, Samsung Smartwatch analysis showed that it can be deciphered using brute force attack and easily gain control access to the device. Next, a wearable device such as Google Glass is selected for further security analysis.

3. WEARABLETECHNOLOGY (WT) CHALLENGES: SECURITY AND PRIVACY ISSUES

There are a few key challenges faces in WT which are power consumption, communication capacity, design constraints, and security and privacy issues. Furthermore, the major challenge in WT which is the security issues is highlighted as it is the focus of this research study. It can be further categorized into three major parts which are security vulnerabilities, attacks and security solutions. The security vulnerabilities in WT can be exploited by an array of possible security and privacy attacks. The security attacks can be further divided according to two main types: passive attack and active attack. Passive attacks try to get the user's password and sensitive information without breaking and affect the system while active attacks contrast with passive attacks, in which try to break and alter the system. When the security vulnerability is exploited, there will be a loss. The loss can be loss in term of Confidentiality, Integrity, Availability or Authenticity. On the other hands, privacy attacks are categorized by user identity and data integrity attacks and time and location based attacks.

The security solutions can mainly be discussed using two different terms which are authentication and encryption. Authentication can be further divided into two main types which are single-factor authentication and multi-factor authentication. There are several common challenges identified in the wearable technology that will need to be addressed by further researchers in order to improve it which include:

- Power consumption [7]-[8]. One of the major challenges is the high power consumption of wearable devices. The battery power of wearable devices can only last for one to two days since most devices use wireless networks, GPS, and other technologies that consume a lot of power. Hence, short battery life and high power consumption of wearable devices will cause people reducing the usage and adoption.
- Communication capacity. The communication range is limited, which mean that the covered area range of wireless transmissions is usually limited because of both technological and energy-savings considerations [7]-[8].
- Design constraints. Some wearables are designed in bulky size and it does not really make users feel comfortable to it such as "Holter-type" system [6].
- Security issues [5]-[8], [27]. Security, privacy is still an unresolved issue in WT. The wearable devices contain a lot of user's data which putting users' security and privacy on the risk. Moreover, it also may consist of sensitive information data such as address, credit card number, and health-related data. Therefore, security issues will be the key challenges for WT to be adopted widely in the market.

3.1 WEARABLETECHNOLOGY (WT) SECURITY VULNERABILITIES

Security and privacy issues could be the major reasons of it. It can lead to the serious breach and loss if the security vulnerability is not handled properly. The loss could be either static assets such as files, documents or dynamic asset like credit card number. At the end, it will cause data and financial loss or even safety issues. Furthermore, user's trustworthiness towards wearable will decrease and discourage people to get their own wearable. For instance, among the top consumer concerns about the IoT, which is defined as devices that connect with each other or to the Internet—28% of respondent's concern about "or someone hacking into the device and doing something malicious" and 26% concern about "not knowing how the information collected by the devices will be used" [28]. This implies that security issues are the major concerns that potentially reduce user acceptance and trustworthiness towards devices. Therefore, it is important to investigate on the security vulnerability on the devices for user protection. Basically, wearable devices can be exploited from different attack surfaces shown in the Figure 2.

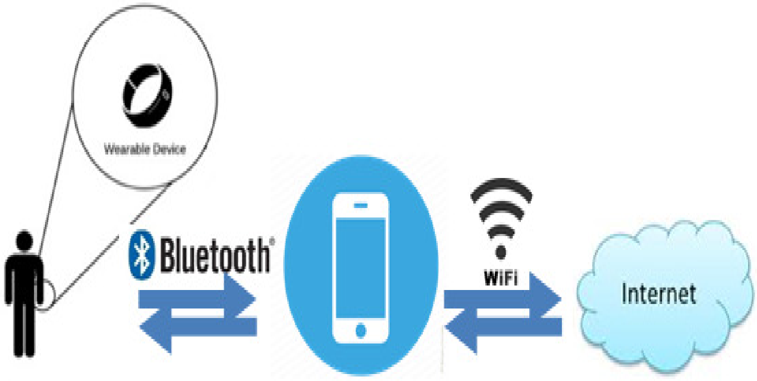

Figure 2: Generic Data Acquisition Architecture in Wearable Technology

The most common security vulnerabilities that can be found in wearable devices from the attack surfaces shown in Figure 2. The factors such as i) Unsure transmission of data Bluetooth for local device storage; ii) Software communication to the Cloud via a cellular or Wi-Fi network; iii) Insecure data storage on Cloud; (iv) Lack of authentication and authorization and (v) Lack of physical security controls that contributes to the security attacks are discussed below.

(i) Unsecure transmission of data via Bluetooth for local device storage

Wearable devices rely on Bluetooth (see Figure 2) to do transmission of data collected from embedded wearable sensors to integration devices such as smartphone as currently it cannot communicate directly to the Internet. As a result attacker can exploit the bug in the device to extract data stored locally, such as health-related records by using wearable as an access point. For example, an attacker can simply make use of sniffers [29] to steal unauthorized data by detecting the broadcast signals while a wearable device communicated over Bluetooth. As a consequence, there will be a loss on either in term of monetary, the safety or even life of the people.

(ii) Software communication to the Cloud via a cellular or Wi-Fi network

This is more vulnerable compared with the transmission of data via Bluetooth for local device storage discussed previously. This is because more personal sensitive data can be stolen as data transmitted from the local storage in the smartphone to the Cloud application (see Figure 2.3) is typically combined with personally identifiable data such as name, email, telephone number, and location to ensure that the data is being sent to a proper account. The attacks that can take place by exploiting this security vulnerability include man-in-the-middle and redirection attacks, which could cause data to be sent to the wrong server. Hence, the potential loss of private data is high and privacy and safety issues might arise as well if the wearer is identified.

(iii) Insecure data storage on Cloud

Cloud refers to a public or semi-public space on transmission lines that exists between the endpoints of a transmission [30]. Cloud storage provides better file accessibility, which the file stored in the Cloud can be accessed at any time from any place as long as you have the internet access. This could be the most vulnerable area in the wearable world due to the amount of Personally Identifiable Information (PII) that is available [29]. The data synchronized to Cloud could be posed by a number of risks, including distributed denial of service (DDoS) attacks, SQL injection, or back door attacks. The attacks on the Cloud are typically carried out by highly skilled cyber criminals. For instance, a cybercriminal gang was reported to steal up to $1 Billion by impersonating bank employees through the use of malware [31].

(iv)Lack of authentication and authorization

Most of the wearable devices are often do not come with a built-in security mechanism such as user authentication or PIN system protection features and they usually store data locally without encryption [32]. Besides that, wearable devices require higher communications [33] security regarding encryption, data integrity, confidentiality and other security services since it relies on the uncontrolled wireless network either Bluetooth or Wi-Fi connection to transfer data. However, it is difficult to apply with higher security measurements due to its' small size and limited bandwidth and finally, result in easier to be attacked. For instance, HP study [34] revealed that 30 percent of the tested smartwatches were vulnerable to account harvesting, which is an attack that gain access to the device and data by looking for weak password policy, lack out account lockout and user enumeration.

(v) Lack of physical security controls

The other security vulnerability for wearable devices is the potential for the loss of the device itself. The small and tiny size of wearable device such as fitness band is most likely to be misplaced or lost. The lost or stolen devices will pose a risk on the exposure of the personal data information complies with its confidentiality, integrity and availability if it has fallen into the wrong hands. Furthermore, most of the wearable devices are often do not come with a built-in security mechanism such as user authentication or PIN system protection features and they usually store data locally without encryption [32]. For instance, Apple Watch and Google's Android Wear platform do not have any security measures in place protecting their pricey wearables from loss or theft [35].

Next an analysis on various privacy challenges and attacks on wearable devices aspect is given.

3.2 WT PRIVACY CHALLENGES& ATTACKS

Apadmi [36] conducted a survey that asked their respondents about "Do you feel wearable technology poses a threat to your privacy?" The results show that 42 percent said yes and another 40 percent were doing not knows and remaining 18 percent replied no. This implies that people worry about wearable technology that exposes the potential privacy risks of devices that can record and capture personal private data. The privacy issue is one of the major challenges yet to be solved in wearable computing. Not only because wearable can sense, capture and store sensitive information about the users, and his surrounding but it also able to do it continuously and discreetly [37]. The privacy attacks that poses in WT can be categorized into user-based privacy and data-based privacy time-based privacy and location-based privacy.

i)User Identity and Data Privacy

Embedded sensors such as cameras and microphones, capture data about the individual and also the surroundings, often without their consent. These data often personal,confidential and sensitive, which invade users' privacy and poses privacy challenges such as surveillance. For example, Glass can be easily hacked as it has no strong authentication implementation [38]. The attacker can take full control the Glass and monitor everything the owner doing with the camera and microphone. Besides that, security researcher from Stanford University and Israel's defense research group Rafael found that gyroscope, a sensor that used to measure angular velocity can even eavesdrop on the conversation as well [39] despite of using microphones. They found that the MEMS (microelectromechanical systems) gyroscope is sensitive enough to recognize the sound and can pick up some sound waves and turn them into crude microphones. Therefore, it proved that the conversation could easily eavesdrop without user consent since iOS and Android do not require special permissions from users to access gyroscope.

ii)Time and location-based privacy

GPS embedded inside wearable able to track a person's location at a specific time. It brings greater benefits for people to do navigation, but it also poses greater risks as well. It raises serious issues on the user's privacy, if the location of the people can be tracked. For instance, Symantec [40] revealed that wearable can also do location tracking, although there is no GPS sensor built-in. This happened because the data exchange process between phone and fitness band could potentially broadcast the location information. They performed an experiment to illustrate that by using a portable scanner, a unique hardware address that each fitness tracker emits when syncing to the user's phone via Bluetooth could be picked up. In addition, some collected data that are shared consist some information that an individual did not intend to share. For example, IMU sensor data such as accelerometers and gyroscopes shared with caregivers may reveal some sensitive medical conditions, such as seizures, that one may wish to keep private [41].

3.3 DISCUSSION : WHY AUTHENTICATION PROBLEMS EXIST IN WEARABLE DEVICES?

Based on the research findings done in the previous section, all of the wearable devices that have been analysed are lack of authentication. Why this happened? It is supposed that wearable devices should be protected with secure authentication mechanism as it contains a huge amount of sensitive information. The reason could be wearable devices are typically lacking a keyboard or even a touch screen. Therefore, it is a challenge to implement password or PIN-based authentication. On the other hand, due to its' small device size so their processing power and bandwidth are further limited and this makes it difficult to apply with higher security measurements. In addition, Symantec threat researcher Candid Wueest [42] recently revealed that the danger of wearable devices at this point is that developers are not prioritizing security and privacy. Hence, wearable device resulted to be less security compared with other devices without a strong authentication scheme in place.

However, as wearables making more and more use of user personal data - from fitness stats to health records, security should be put into a high priority. Unlike mobile devices, wearable devices are potentially always-on and always gathering data. In this way, it not only bring the uniqueness on the WT with the added dimension, but at the same time it is also open to more threats to user sensitive information and activities at any time anywhere without user's consent. Security measures are not only important for protecting personal data, but are critical as smartwatch are introduced to the workplace and connected to corporate networks as well. Therefore, it is very important to be paid extra attention to maintaining confidentiality, integrity and availability (CIA triad) for wearable displays.

Could you imagine how serious security breaches could happen if the wearable device that has poor user authentication are being attacked? Take for an example, a smartwatch can be used to make online transactions. However, the smartwatch is lack of user authentication with unencrypted data. If in the case that the smartwatch was stolen or lost, someone with bad intention could likely access all of your personal data or even modify transaction content or insert additional transactions with the credit card information. In the consequences, it not only causes loss of security, but it violates the confidentiality and integrity policy and results in loss of money as well.As a result, the users' security and privacy are in risks without a strong authentication scheme in place. It is important to be paid more attention on wearable authentication in order to protect users' data from malicious, unauthorized access since a massive quantity of private data to be collected from the wearables. Security measures are not only important for protecting personal data, but are critical as smartwatch are introduced to the workplace and connected to corporate networks as well. Therefore, authentication issue must be tackled definitely to ensure the security of wearable is preserved thoroughly.

4. CONCLUSION

As the IoT market advances, WT is growing in popularity for their convenience and capabilities. WT offers better functionalities by providing real time data communication, but also poses a greater security and privacy risks. This two major challenges would be the obstacles for WT to be adopted widely in the market. People are concerned about the security of the wearable as the data collected might consist sensitive information about themselves and their surroundings such as identity, health-related information, credit card number, and the location.

Although this advance technology does benefit people but there are still some security loophole and privacy issues that required extra attention and effort of designer in designing wearable technology model. In this paper, some background study on security and privacy revolving wearable technology is presented. A security vulnerability analysis for real-example is also presented. Overall, one major attack that occurs is authentication issue. Thus, in the future, more study in authentication will be done and a more better authentication mechanism will be presented.

REFERENCES

[1] Tehrani, Kiana, and Andrew M. (26 Mar, 2014). Wearable Technology and Wearable Devices: Everything You Need to Know. (cited 18 Sep, 2015). [Online] Available: http://www.wearabledevices.com/what-is-a-wearable-device/

[2] Transparency Market Research. (05 Jun, 2014). Wearable Technology Market Research Report 2018. (cited 21 Sep, 2015). [Online]Available: http://www.transparencymarketresearch.com/article/wearable-technology-market.htm

[3] Viral M. (01 Apr, 2012). Wearable Computer. (cited 18 Sep, 2015). [Online] Available: http://www.slideshare.net/fbviralmehta/wearable-computer-12242345

[4] PricewaterhouseCoopers B.V. 2014. Consumer intelligence series - The wearable future. (cited 19 Sep, 2015). [Online] Available: https://www.pwc.se/sv/media/assets/consumer-intelligence-series-the-wearable-future.pdf

[5] Al-Muhtadi, J., D. Mickunas, and R. Campbell. Wearable security services. in Distributed Computing Systems Workshop, 2001 International Conference on. 2001.

[6] McAdams, E., et al. Wearable sensor systems: The challenges. in Engineering in Medicine and Biology Society, EMBC, 2011 Annual International Conference of the IEEE. 2011.

[7] Pietro, R.D. and L.V. Mancini, Security and privacy issues of handheld and wearable wireless devices. Commun. ACM, 2003. 46(9): p. 74-79.

[8] Uddin, M., et al., Wearable Sensing Framework for Human Activity Monitoring, in Proceedings of the 2015 workshop on Wearable Systems and Applications. 2015, ACM: Florence, Italy. p. 21-26.

[9] Authentify. (2016). Out-of-Band Authentication. (Cited 28 Feb, 2016). http://authentify.com/solutions/authentication-concepts/band-authentication/

[10] Ghoreishizadeh, S.S., et al. A lightweight cryptographic system for implantable biosensors. in Biomedical Circuits and Systems Conference (BioCAS), 2014 IEEE. 2014. IEEE.

[11] Safavi, S. and Z. Shukur, Improving google glass security and privacy by changing the physical and software structure. Life Science Journal, 2014. 11(5): p. 109-117.

[12] Geran S. (18 Apr, 2014). Is Google Glass a Security Risk? (cited 19 Oct, 2015).[Online] Available: https://blog.bit9.com/2014/04/18/is-google-glass-a-security-risk/

[13] Daniel D. 2013. Privacy Implications of Google Glass. (cited 21 Oct, 2015).[Online] Available: http://resources.infosecinstitute.com/privacy-implications-of-google-glass/

[14] Marc R. (17 Jul, 2013). Hacking the Internet of Things for Good. (cited 19 Oct,2015).[Online] Available: https://blog.lookout.com/blog/2013/07/17/hacking-the-internet-of-things-for-good/

[15] Candid W. (18 Jul, 2013). Google Glass Still Vulnerable to WiFi Hijacking Despite QR Photobombing Patch. (cited 21 Oct, 2015).[Online] Available: http://www.symantec.com/connect/blogs/google-glass-still-vulnerable-wifi-hijacking-despite-qr-photobombing-patch

[16] [fitbit. (cited 21 Oct, 2015).[Online] Available: https://www.fitbit.com/my

[17] Michael S. (11 Jun, 2015). Internet of Things Security Evaluation of nine Fitness Trackers. (cited 21 Oct, 2015).[Online] Available: https://www.av-test.org/fileadmin/pdf/avtest_2015-06_fitness_tracker_english.pdf

[18] Rahman, M., B. Carbunar, and M. Banik, Fit and vulnerable: Attacks and defenses for a health monitoring device. arXiv preprint arXiv:1304.5672, 2013.

[19]J acob B. (03 Aug, 2015). Surveillance Society: Wearable fitness devices often carry security risks. (cited 21 Oct, 2015).[Online] Available: http://www.post-gazette.com/news/surveillance-society/2015/08/03/Surveillance-Society-Wearable-fitness-devices-often-carry-security-risks/stories/201508030023

[20] Cyr, B., et al., Security Analysis of Wearable Fitness Devices (Fitbit). Massachusets Institute of Technology, 2014.

[21] Carly P. (24 May, 2015). iPhone users' privacy at risk due to leaky Bluetooth technology. (cited 24 Oct, 2015).[Online] Available: http://www.v3.co.uk/v3-uk/news/2409939/iphone-users-privacy-at-risk-due-to-leaky-bluetooth-technology

[22] Kristi R. (22 Jul, 2015). HP Study Reveals Smartwatches Vulnerable to Attack. (cited 4 Oct, 2015).[Online] Available: http://www8.hp.com/us/en/hp-news/press-release.html?id=2037386#.Vi18G7crLIU

[23] Liviu A. (12 Sep, 2014). Bitdefender Research Exposes Security Risks of Android Wearable Devices. (cited 24 Oct, 2015).[Online] Available: http://www.darkreading.com/partner-perspectives/bitdefender/bitdefender-research-exposes-security-risks-of-android-wearable-devices-/a/d-id/1318005

[24] Ryan G. (01 Oct, 2013). Accelerometer vs. Gyroscope: What's the Difference? (cited 23 Oct, 2015).[Online] Available: http://www.livescience.com/40103-accelerometer-vs-gyroscope.html

[25] Indian Institute of Technology Kanpur Commonwealth of Learning Vancouver. 2013. SENSORS ON ANDROID PHONES. (cited 23 Oct, 2015).[Online] Available: http://m4d.colfinder.org/sites/default/files/Slides/M4D_Week2_sensors.pdf

[26] Engineer’s Handbook. 2006. Mechanical Components - Sound Sensors. (cited 2 Oct,2015).[Online]Available:http://www.engineershandbook.com/Components/soundsensors.html

[27] Technavio. (21 Jul 2014). Exploring Five Challenges in the Wearable Technology Market. (cited 31 Oct, 2015). [Online] Available: http://www.technavio.com/blog/exploring-five-challenges-in-the-wearable-technology-market

[28] Julie F. (12 Nov, 2014). ISACA Survey: Most Consumers in Australia Aware of Major Data Breaches, But Fewer Than Half Have Changed Key Shopping Behaviors. (cited 4 Oct, 2015).[Online] Available: http://www.isaca.org/About-ISACA/Press-room/News-Releases/2014/Pages/ISACA-Survey-Most-Consumers-in-Australia-Aware-of-Major-Data-Breaches-But-Fewer-Than-Half-Have-Changed-Shopping-Behaviors.aspx

[29] Nroseth. (27 Mar, 2015). Data Security in a Wearables World. (cited 4 Oct, 2015).[Online] Available: http://www.swatsolutions.com/data-security-in-a-wearables-world/

[30] Vangie B. cloud. (cited 4 Oct, 2015).[Online] Available: http://www.webopedia.com/TERM/C/cloud.html

[31] David E. Sanger and Nicole P. (14 Feb 2015). Bank Hackers Steal Millions via Malware. (cited 17 Oct, 2015).[Online] Available: http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r

[32] Michael C. Wearables security: Do enterprises need a separate WYOD policy? (cited 17 Oct, 2015).[Online] Available: http://searchsecurity.techtarget.com/answer/Wearables-security-Do-enterprises-need-a-separate-WYOD-policy

[33] Mellisa T. (May 30, 2013). 4 Security Challenges for Fitbit, Google Glass + Other Wearable Devices. (cited 4 Oct, 2015).[Online] Available: http://siliconangle.com/blog/2013/05/30/4-security-challenges-for-fitbit-google-glass-other-wearable-devices/

[34] Kristi R. (22 Jul, 2015). HP Study Reveals Smartwatches Vulnerable to Attack. (cited 4 Oct, 2015).[Online] Available: http://www8.hp.com/us/en/hp-news/press-release.html?id=2037386#.Vi18G7crLIU

[35] Eric Z. (14 May, 2015). Apple Watch, Android Wear Lack Theft Protection. (cited 17 Oct, 2015). [Online] Available: http://www.informationweek.com/it-life/apple-watch-android-wear-lack-theft-protection/a/d-id/1320430

[36]Apadmi. Apadmi’s Wearable Tech Study:Do Potential Customers Think Wearable Tech Poses a Privacy Risk? (cited 20 Oct, 2015).[Online] Available: http://www.apadmi.com/wearable-technology-trends/wearable-tech privacy/#WTP-2

[37] Motti, V. and K. Caine, Users’ Privacy Concerns About Wearables, in Financial Cryptography and Data Security, M. Brenner, et al., Editors. 2015, Springer Berlin Heidelberg. p. 231-244.

[38] Charles A. (01 May, 2013). Google Glass security failings may threaten owner's privacy. (cited 20 Oct, 2015).[Online] Available: http://www.theguardian.com/technology/2013/may/01/google-glass-security-privacy-risk

[39] Michalevsky, Y., D. Boneh, and G. Nakibly. Gyrophone: Recognizing speech from gyroscope signals. in Proc. 23rd USENIX Security Symposium (SEC’14), USENIX Association. 2014.

[40] Lisa E. (09 Oct, 2014). A New Wave Of Gadgets Can Collect Your Personal Information Like Never Before. (cited 22 Oct, 2015).[Online] Available: http://www.businessinsider.my/privacy-fitness-trackers-smartwatches-2014-10/#GDuZGvtShqZO79S5.97

[41] Raij, A., et al., Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2011, ACM: Vancouver, BC, Canada. p. 11-20.

[42] Mano.T. (2014). Wearables and Quantified Self Demand Security-First Design. (cited 18 Feb, 2016).[Online] Available: http://www.wired.com/insights/2014/10/wearables-security-first-design/