Security and Privacy Analysis of Wearable Health Device

A B M Kamrul Islam Riad, Hossain Shahriar, Chi Zhang

Department of Information Technology

Kennesaw State University

aislamri@students.kennesaw.edu{hshahria,czhang4}@kennesaw.edu

***Abstract*—Wearable technology allows for consumers to record their healthcare data for either personal or clinical use via portable devices. As advancements in this technology continue to rise, use of these devices has become more widespread. In this paper, we examine the significant security and privacy features of three health tracker devices: Fitbit, Jawbone and Google Glass. We also analyze the devices' strength and how the devices communicate via its Bluetooth pairing process with mobile devices. We explore possible malicious attacks through Bluetooth networking. The outcomes of this analysis illustrate how these devices allow third parties to access sensitive information, such as the device exact location, which causes the potential privacy breach for users. We analyze and compare how unauthorized party may access the user data and the challenges to secure user data on three wearable devices (Fitbit, Jawbone, and Google Glass) security vulnerability and attack type.**

Keywords: Fitbit, Jawbone, Google Glass, Security, Privacy, Mobile health, Wearable Technology.

I. INTRODUCTION

Wearable health devices are most commonly used for health fitness and user health status recording purposes. These devices have grown significantly in recent years and these wearable devices are normally in fashion wearable forms such as watches, glasses, wristbands or jewelry items [1]. In 2018, nearly 3.7 billion new Bluetooth enabled devices were shipped worldwide to consumers [2]. Wearable devices are connected to the cloud server through the internet that enables device owners to interact with their user records and exchange personal information such as heart rate, geolocation and daily eating habit. These wearable devices are connected to internet, such as Wi-Fi networks, more than ever before which have become part of the Internet of Things (loT). In theory, connecting devices through loT allows users to control or automate digital tasks so that various unexpected user data such as habit, daily activities, and location tracking records are delivered to third party observers [14]. Wearable devices provide less security compared to computing devices because of limited bandwidth and processing power [3]. Therefore, wearable devices bring new challenges in terms of user's security and privacy that increase to an array of possible attacks due to the limitation of its space and memory capacity. Fitness devices require pairing with smartphones to establish the connection with cloud server for data exchanging. The complexity of this communication among various paths generates security vulnerabilities such as personal information leaking and privacy hacking by hackers. Financial loss is possible as some fitness wearable devices allow their user to access their bank account for quick payment to selected financial institute or agency [21].

Researchers raise concerns about the security of wearable devices. HP labs found that most of the wearable devices are vulnerable to user data security breach because of poor security firmware system in devices [24]. In many cases researchers point out that firmware update vulnerability is the main cause in wearable devices because these devices allow attackers to inject malicious codes [25]. At the Hack.lu 2015 security conference in Luxembourg [26], a researcher reported that PC can be affected through malicious code injection when Fitbit devices plugging to PC through Bluetooth pairing within 10 seconds.

The weakness of firmware, the gateway of apps and the service of server are the main concern about security and privacy leakage of wearable fitness devices. The wearable devices build the connection through smartphone apps as a gateway to connect web service, the open interface for interoperability. Hackers target the weak point of these interfaces which has become a security threat for these wearable devices [27]. Therefore, the vulnerability such as SQL injection and Cross-Site Scripting (CSS) attacks takes place through the connection gateway [28].

In this paper, we discuss the strength and features of wearable devices and present detailed analyses and research reviews on user data security and privacy attacks that occur due to poor security firmware in wearable devices. The goal of the analyses is to understand security and privacy on wearable devices and user data transferring. We analyze the security and privacy issues of three main wearable devices including Fitbit, Jawbone and Google Glass, based on various related prior works and research.

The paper is organized as follows: Section II discusses related works. Section III describes the security and privacy of three wearable devices Fitbit, Jawbone and Google Glass. Section IV compares the weakness and provides

suggestions to secure the devices. Finally, Section V concludes the paper and future work.

II. Related Works

Wearable devices can help users monitor their health and fitness by tracking data from movements to heart rate and even blood pressure. Meanwhile, continued research actively focused on privacy and security of these devices. Research have been published with the focus on the user data security and privacy leakage for wearable devices. In 2014, Britt Cyr, published the user data security and privacy properties analysis of Fitbit devices focusing on the security weaknesses between Fitbit Bluetooth devices and a smartphone application during traffic synchronizing [4]. They found that Fitbit collected data without providing device owner's consent and that MAC address of Fitbit devices never changed which enabled correlated attacked [11]. Researcher reported that MITM attacks intercepted the BTLE credential during device pairing over TLS [4]. A follow-up study in 2018 by Matthew [5] analyzed three devices; Fitbit, Pebble and Jawbone and found out that all three devices exposed their connection forming packet when pairing that would enable server vulnerable attack because these packets allow an attacker to follow the connection after it is initiated [5].

In 2016 Ke Wan Ching, performed security analysis of wearable devices especially Google Glass that is eye wear device and they found the lack of authentication due to unsecure PIN system [17]. In addition, Seyedmostafa and Zarian[18] revealed that Google Glass can take pictures and record videos without the user's consent that breaches the user's privacy. One of the security and privacy concerns has been regulated from various research forums, the application of mhealth apps that makes an interaction between wearable devices and mobile phones to visualize the data record of users. In the Data Protection in the EU [19], the European Commission emphasizes data protection that tracking and monitoring patient's health information such as activities, location visited, and dieting habits would be severely vulnerable in future by using wearable devices and their applications. Similarly, a report [20] discusses user's data security and confidentiality that would be challenged to ensure compliance with HIPPA regulation due to wearable health devices vulnerability and their data compromising by third parties. Wu (Min Wu, 2019) identified that even a trustworthy network within the organization in terms of the enforced process of data encryption and authentication mechanism is vulnerable because third parties may gain elevated privileges due to secret access key and certification process from users' ends. They suggested that security key agreement and distribution among the node in the network could be the strong possible authentication process in accordance with HIPAA guidelines for privacy and data security [20].

A blog of vulnerability of fitness tracker [21] pointed out that most wearable fitness trackers need to be initiated as build in security mechanism while connecting other devices or applications for data collection. The wearable devices' data are stored in a local server without an encryption key. The lack of security mechanism causes the devices extremely vulnerable to cybercriminal attacks [21]. In this scenario, cybercriminal can inject random step computation values into memory and the wearable devices would generate this count value to the server as a valid encoded frame.

A group of researchers [22] (University of Toronto) investigate Bluetooth privacy, data integrity and transmission security of some fitness trackers. They discover that all of the wearable trackers have numerous user data security and privacy issues. They release the key findings of security and privacy leakage in many of the fitness trackers except Apple Watch. The Jawbone UP application consistently sends out the user's precise geolocation while Bellabeat, Garmin, and Withings application failed to use transit-level security that causes data visible in transmission level [23].

III. Analyzing Wearable Health Device

A. Analysis of Fitbit

The Fitbit tracker [6] tracks various user' activities including number of steps walked; sleep pattern and quality as well as other personal health measurements such as body temperature, pulse rate, food habit, and body weight. Fitbit introduced a series of technology on workout tracking such as PurePulse, SmartTrack and Sleep Tracking- a technology that automatically recognizes users' exercises and record the data through the smartphone app.

Strengths of Fitbit Devices: SmartTracking activities – Fitbit used a simple accelerometer that is called a smart algorithm. SmartTrack uses a 3-axis accelerometer to identify the intensity and patterns of the user movement and determines the type of activities. To collect thousands of possible activities accurately, a series of algorithms are applied to that data that shaping down all activities as a singular exercising in database server [6]. To measure heartbeat, a photoplethysmography, a low-cost and simple optical technique that can be used to detect blood volume changes, is used for PurePulse. Photoplethysmography is a light base technology used to measure blood circulation and the volume of the blood in the wrist changes. With Photoplethysmography, Fitbit uses optical heart rate monitor to detect the pulse by shinning a green light through the skin to see blood flow.

Data Security of Fitbit Devices: Data security is one of major security vulnerabilities found in many mobile health devices. Fitbit continuously adds software patches to improve the user data security and privacy for its devices [7]. For authentic security purposes the device protects data through regular firmware update. However, lack of authentication is one of the most vulnerabilities in Fitbit devices that generally occurs on trackers side [7] so the potential cybercriminal can easily collect the user personal data without their consent.

The University of Edinburgh conducted research on how personal information could be stolen from Fitbit divides such as the Fitbit One and Fitbit Flex wristband [8]. It was found that intercepting messages transmitted between cloud server and fitness tracker is possible. This allowed researchers to access users 'personal information that would cause sharing unauthorized personal data to the third parties [8].

Fitbit System Overview: The Fitbit devices are designed to rest in data buffer locally on the device and devices are worn by the user all day. Data synchronization is performed through smartphone applications for Android, iOS and desktop. Fitbit devices send the user's activity to the Fitbit cloud server over Wi-Fi or internet connection during data synchronizing. During data synchronization, the Fitbit application forwards the user's activity data to Fitbit warehouse. User data activities are fetched from Fitbit devices during each synchronization.

In Figure 1, synchronization is formed over Bluetooth between Fitbit devices and smartphone or personal computer. The BTLE [9] (Bluetooth Low Energy) is used for data synchronization between smartphones application or personal computers so over internet/Wi-Fi Fitbit Cloud service transpires in an encrypted session.

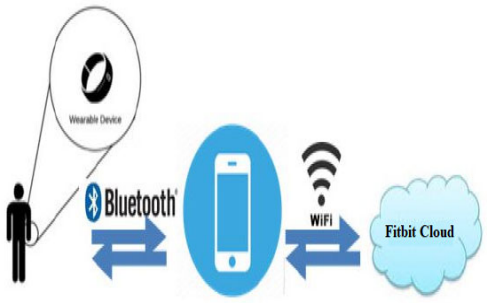

Figure 1: The Fitbit system components that shows the attack surface into five medias.

Analyzing Bluetooth Communication: Mobile health devices have built-in Bluetooth that permits devices such as smartphones, computers, and peripherals to transfer data or voice wirelessly over short distance [10]. Bluetooth is measured a reasonably protected wireless connection that is encoded, stopping casual snooping or eavesdropping from other devices in short distance. However, there is always security risk involved such as malicious attacks through Bluetooth networking by hackers. For instance, "bluesnarfing" is the unauthorized access of information from a wireless device through a Bluetooth connection, while "bluebugging" allows attacks to take over all functions of mobile phone [10]

A research group from Boston University recently has discovered a vulnerability in several Bluetooth devices including the Fitbit watch that could allow third parties to gain sensitive information from the devices such as exact locations [11]. The researchers identified that the information leak stems from the way different Bluetooth devices communicate with one another to establish a connection. In pairs of Bluetooth for transmitting information between two devices; one device must first establish central role in the connection and other device play peripheral role [11]. For example, in a pair of Bluetooth Fitbit SmartTrack to iPhone, iPhone would play the role of central device and Fitbit SmartTrack would be the peripheral device that indicates available connection where the signals contain the IP address of a mobile device and a payload containing data about the connection [11].

Fitbit Device Tracking: Since devices originate randomized addresses that automatically configure periodically, it attempts to improve privacy instead of maintaining one permanent address [15]. But it was discovered by researchers that the device to be tracked even as its random address originates. Random data is a unique identifier of the device that is supposed to be changed periodically but in that case this identifier doesn't change in sync with the address. In this case, the research team found that Fitbit devices lack address changes or randomization at all which is considered an extremely susceptible to tracking even without the use of a sniffer algorithm. [11]. The research further addressed that restarting the Fitbit device or draining its battery did not change the access address. It indicates that the data could be tracked in Fitbit devices if the Fitbit's access address never changes [11].

B. Analysis of Jawbone

Jawbone is a powerful health activity monitor, food and sleep tracker device that is wearable on the wrist like Fitbit wearable device. Jawbone uses an internal accelerometer and algorithm to track users' day to day activities and suggests helpful tips and lifestyle through the accompanying Up app [12]. Jawbone UP24 fitness tracker had a big upgrade from its original design, with new features and resolving some serious first generation issues [16].

Strength of Jawbone: The Jawbone UP tracker has a feature such as a hardware button to save battery from drainage while not aiming connection. One of the good security features of Jawbone is the Bluetooth activation switch that requires user paring pin code to initiate communication with smartphone applications. While establishing Bluetooth connection, the device starts publicizing and penetrating for other peers after pressing the button. In this situation, when paired devices are not reachable to connect demand devices, the device responds to connection requests from other Bluetooth devices.

Data Security of Jawbone Tracker: As the Bluetooth LE connection described, devices should change the Bluetooth device MAC address randomly in order to improve the privacy instead of maintaining one permanent address [38]. But unfortunately, the Jawbone tracker device is found absent in this security feature since it uses the same MAC address permanently. This causes the potential users data security and privacy issues, when the users can be traced easily for their precise location and user data could be manipulated by the attacker. While using GattTool command is one of the ways to write and read the potential features of the device, shell script is another way to pretend a Denial of Service(DoS) attack for originating connection requests and reading the characteristics of the devices. In this scenario, if the Jawbone UP tracker is connected to the paired device, it does not accept the further connection request.

Jawbone Up Tracker Overview: In [13] Parson's research team found that during the routing use of the device application, Jawbone UP trackers passively share the user precise current location. It was unclear to the researchers what the reason was for this passive location

tracking and that the collection of information was not linked with some given fitness activities. In general, when users open mobile application Jawbone tracker transmit longitude and latitude to its servers; these transmissions are connected with the predefined user events, such as syncing with the device and opening the application. These testing described that this geological data has a precision of up to fourteen decimal points and it effectively releases the fitness device location within a few millimeters. It was found that users did not know the location transmission occurring when the Jawbone UP users restore his or her timeline. The figure below shows the Jawbone UP tracker sends a user's exact location when the user connects with smartphone application.

Figure 2 shows that Jawbone routinely transmits precise geolocation information when users open the apps or syncing their wearable to their iPhone [13]. The research team found that Jawbone UP fitness data transmission between mobile application and health devices servers were generally secured using HTTPS. However, both Android and iOS applications have vulnerability because both applications create false generated fitness data for their individual account. Although HTTPS is a secure communication network between user and server, HTTPS does not cover the security and privacy protection from end users.

Figure 2: Jawbone Up phone application share user precise location while connecting.

C. Analysis of Google Glass

Google Glass is the earliest wearable device that boosts the growth of wearable technology. Google Glass is the frame of a pair of glasses which is built in a computer eyewear device. It affords various structures that users feel very comfortable to use it but google glass is only usable for enterprise version that means the google glass is not available for individual's usage. However, many concerns about users' data security and privacy issues have been raised from various researchers group that Google Glass is not free from vulnerability and it could be threatened for client data security and privacy.

Strength of Google Glass: Google Glass basically performs through user voice command [29]. Users can send messages without using their hands and it has video and camera capabilities that make a difference from other wearable fitness devices such as Fitbit and Jawbone. These glasses expose numerous distinct useful applications for health organization and hospital staffs [30]. Video conferences between doctors and medical associates is one of the most unique features in Google Glasses [30]. Google Glass facilitates a great amount of health cases throughout the conference about patient treatment between medical professionals and other co-facilitated health organizations.

Data Security of Google Glass: The connection system of Google Glass is content-based image retrieval (CBIR) that allows health staff to search accurate information for a patient's medical history while consulting with physicians and patients [31]. Apart from these facilities Google Glass has a major concern about patient data security and privacy [31]. Researchers find out Google Glass does not have a concrete authentication process to protect the user's data security and privacy due to lack of secure enough PIN system [32]. Google Glass privacy threat is significantly different from other fitness tracker that relatively uses mobile phone and apps to collect user data. Google Glass supports eye movement tracking that may cause authentication issues [32]. In addition, Sayed Mostafa and Zarina [33] revealed that Google Glass is able to capture user pictures and has a video recording capability which would be an violation of users' privacy without consent. Most significantly, there are numerous factual cases reported concerning data security and privacy associated with this Google Glass when it was first released.

A research team [34] exposed a stern security threat on how Google Glass interprets QR (Quick Response) codes while it snaps a photo back and they found that Google Glass could scan a malicious QR code that forces the device to connect to a hostile Wi-Fi access point so man-in-middle (MITM) can perform session hijacking or sniffing or remotely gain root access to a Glass devices and take control without the wearer's knowledge – Google Glass interprets QR(Quick Response) codes while snapping a photo back. Moreover, the QR code is not only the way to initiate the security breach, the sniffing or session hijacking can be performed by man-in-the middle (MITM) attacks and such an attack can be implemented without recognizing any QR code by Google Glass devices [34].

Google Glass Bluetooth Communication: The Google Glass Bluetooth pairing is comparatively the same as other fitness devices. It is essential to pair Glass to phone or tablet via MyGlass app from the Google play store that has full use of Bluetooth capabilities [36]. There is a concern that Google Glass battery gets drained more quickly while connected through Bluetooth rather Wi-Fi connection [37].

IV. COMPARISON AND SOLUTION

We analyze the strength of the selected devices, connection capabilities, and data storage structure. We also analyze the security and privacy concerns for the three selected devices. It is found that there are a number of vulnerabilities and chances that user data are compromised or gained by middle-of-the-man although there are a lot of

improvements that have taken place by the device manufacturers. The security vulnerabilities and potential security attacks on the wearable devices are summarized in Table 1.

Table 1 shows that the selected wearable devices are not free from common security vulnerability as well as the devices have been chosen for analyses having a lack of authentication. Without implementing proper security authentication, the devices can be accessed by unauthorized activities such as eavesdropping, DoS and Brute force attacks. Table 1 also shows that Jawbone Devices can reveal exact location that users recently visited. Thus, DoS attack can be deciphered and third parties can easily get access to the device. Similarly, Google Glasses are major privacy issues since glasses are capable of taking pictures and recording without people's knowledge. Therefore, eavesdropping and spyware attack can take place.

Table 1: Comparison of Security Vulnerability and Attacks for Fitbit, Jawbone and Google Glass

Wearable Devices	Security Vulnerability	Attacks
Fitbit Device	Week authentication Drainage BTLE (Bluetooth Low Energy Technology) Privacy: Tracked visited location	Data injection, DoS and Battery Drain hacks Easily Tracked
Jawbone	Lacking of Privacy Features Exact location tracked	Denial of Service
Google Glass	Unsecure PIN Privacy: Unauthorized picture and video recording capable Unauthorized Eye movement Unsecure Network and hostile environment For Wi-Fi setup require QR code	Wi-Fi hijacking Eavesdropping and spyware Easy recording system by people nearby due to gesture base authentication scheme QR photobombing malware

Data Securing within Mobile Health Devices: Data security is a major concern of mHealth devices. Fitness tracker are widely adopted and are easy to use. There are many concerns about lacking data security in fitness devices and it often escalates to the extremely vulnerable risks for users [35]. The following is a summary of the reasons for lacking data security and privacy in mHealth devices:

1) Lack of testing: Fitness devices are constantly updating their features due to market competition so there would be possible rushes to release products or the new features to the marketplace. As a result, there may be lack of proper testing and strong security coding overlook [35].

2) Size of the device: Most of the fitness devices are very tiny and there is very limited space to create security features by adding extra hardware which manufacturers would worry about the device weight and user experience.

3) Cost Down: Due to fierce competition in this market, the fitness devices generally cannot priced too high, which would be a possible cause for not having sufficient memory space and lack-of-quality coding leading to the failure of the strengthening of devices security.

Fitness Tracker's Secure Communication Model: Built-in-security mechanism is one of the most important features for the user authentication process because it generates the secure PIN system. Secure PIN system protects unauthorized access in a device or system because it tends to store data without encryption. Cyber-attack often takes place due to poor security management that causes the devices extremely vulnerable. The hacker could control every single aspect of the device through initial injection that calls firmware attack which allows attackers' access to local data storage. After a successful firmware attack, the devices are open for modification, encrypted key or Bluetooth functionality. As a result, attackers could send or inject random value into memory as a step count to the server as a valid encrypted frames [35].

Suggestions to add Security to Fitness Trackers: The following initiative and practice help cover the minimal security and privacy of fitness trackers:

1) Regular firmware needs to be updated or developed for all fitness devices. Gadget LE privacy and changes of MAC address should be required at randomly periodical times, such every ten minutes.

2)While a wearable device pairing with mobile phone, the wearable firmware should include fixed and private Identity Resolving Key (IRK).

3) In general, wearable firmware MAC addresses are permanent that cause theft of localhost address. But if the wearable firmware randomly generates new MAC addresses every 10 minutes on IRK, hackers would not be able to identify the host address number [13].

V. CONCLUSION

In this survey paper, we analyzed three smart health devices, Fitbit, Jawbone and Google Glass and summarized the security vulnerability found in prior research. User data on these devices could be compromised through Bluetooth connection to mobile applications that push and pull data from cloud server. Communication between server and app is found secure but MAC address could cause a significant data leak from devices. While all three devices provide a reasonable level of privacy and data security overall, the prior research calls for a concrete and secure data rest on server for those health devices as this would provide more user data security and privacy.

REFERENCES

[1] Transparency Market Research. (2020, January 28). Retrieved from Wearable Technology Market Research:https://www.transparencymarketresearch.com/article/wearable-technology-market.htm

[2] http://www.bu.edu/articles/2019/fitbit-bluetooth-vulnerability/

[3] Al-Muhtadi, J., D. Mickunas, and R. Campbell. Wearable security services. in Distributed Computing Systems Workshop, 2001 International Conference on. 2001.
[4] Britt Cyr, W. H. (2014). Semantic Scholar. Retrieved from Security Analysis of Wearable FitnessDevices(Fitbit):https://www.semanticscholar.org/paper/Security-Analysis-of-Wearable-Fitness-Devices-(-)-Cyr-Horn/f4abebef4e39791f358618294cd8d040d7024399
[5] Matthew L. Hale, K. L. (2018, September 09). Developing a platform to evaluate and assess the security of wearable devices. Retrieved from ScienceDirect:https://www.sciencedirect.com/science/article/pii/S2352864817302985
[6] https://www.fitbit/whyfitbit
[7] Martin, J. A. (2017, Mar 28). CIO. Retrieved from Security Risks of Wearables: https://www.cio.com/article/3185946/10-things-you-need-to-know-about-the-security-risks-of-wearables.html
[8] https://www.infosecurity-magazine.com/news/fitbit-vulnerabilities-expose/
[9] "How do fitbit trackers sync with android devices?" [Online]. Available: https://help.fitbit.com/customer/portal/articles/987748-how-do-fitbit-trackers-sync-with-android-de
[10]pinola, M. (2019, November 15). Bluetooth Basics.Retrieved from Lifewire: fhttps://www.lifewire.com/what-is-bluetooth-2377412
[11] Wells, S. (2019, July 17). How Fitbit, Other BluetoothDevices Make Us Vulnerable to Tracking. Retrieved from http://www.bu.edu/: http://www.bu.edu/articles/2019/fitbit-bluetooth-vulnerability/
[12] Jawbone. (n.d.). Retrieved from https://wearablezone.com/:https://wearablezone.com/companies/jawbone/
[13] Hilts, A.; Parsons, C.; Knockel, J. Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security; Technical Report; Open Effect: Toronto, ON, Canada, 2016
[14] https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
[15] Ansley, C. (2019). 2019 Fall Technical Forum. MAC Randomization in Mobile Devices, 12.
[16] Smith,C. (2019). WAREABLE. Retrieved from Fitness Tracker Wearable Technology Feature:https://www.wareable.com/fitness-trackers/remembering-the-jawbone-up24-7320
[17] Ke Wan Ching, M. M. (2016). Wearable Technology Devices Security and Privacy Vulnerability Analysis. International Journal of Network Security & Its Application (IJNSA), 12.
[18] 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.
[19] (2015). Retrieved from Data Protection, Directorate General for Communication. [online].: https://data.europa.eu/euodp/el/data/dataset/S2075_83_1_431_ENG
[20] Min Wu, P. a. (2019, November 25).Wearable Technology Applications in Healthcare: A Literature Review. Retrieved from HIMSS:https://www.himss.org/resources/wearable-technology-applications-healthcare-literature-review#_ENREF_1
[21] Makarevich, A. (2018, Septermber 24). Vulnerability of Fitness Trackers: Risk. Retrieved from R-Style Lab: https://r-stylelab.com/company/blog/iot/vulnerability-of-fitness-trackers-risks-they-are-facing-and-tips-to-minimize-them
[22] Andrew Hilts et.al. Every Step You Fake. https://openeffect.ca/reports/Every_Step_You_Fake.pdf.Accessed: 02.07.2020
[23] Hilts, A. (2016, April 5). Every Step You Fake: Final Report Released. Retrieved from Open Effect: https://openeffect.ca/every-step-you-fake-final-report-released/
[24] HP. (n.d.). Internet of Things: Security Study: Smartwatches. Retrieved from https://www.ftc.gov/system/files/documents/public_comments/2015/10/00050-98093.pdf
[25] Ching Wan(2016) International Journal of Network Security & Its Applications (IJNSA) Vol.8, No.3, May 2016http://aircconline.com/ijnsa/V8N3/8316ijnsa02.pdf
[26] Storm, D. (2015, OCT 26). ComputerWorld. Retrieved from Fitbit can be wirlessly hacked to infect PC's:https://www.computerworld.com/article/2997561/researcher-says-fitbit-can-be-wirelessly-hacked-to-infect-pcs-fitbit-says-not-true.html
[27] David Emm, A. N. (2015, December 3). Kaspersky Security Bulletin 2015. Top security stories. Retrieved from Kaspersky:https://securelist.com/kaspersky-security-bulletin-2015-top-security-stories/72886/
[28] Konstantinou C. and Maniatakos M., Impact of Firmware Modification Attacks on Power Systems Filed Devices, IEEE International Conference on Smart Grid Communications (2015)
[29] Sherly.(2014,Septermber3)Advantage &Disadvantage of Google Glasses. Retrieved fromHostOnNetBlog:https://blog.hostonnet.com/advantages-disadvantages-of-google-glasses
[30] A. Widmer, R. Schaer, D. Markonis and H. Müller, "Facilitating medical information search using Google Glass connected to a content-based medical image retrieval system," 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Chicago, IL, 2014, pp. 4507-4510.
[31] Schaer, Roger & Müller, Henning & Widmer, Antoine. (2016). Using Smart Glasses in Medical Emergency Situations, a Qualitative Pilot Study. 1-5. 10.1109/WH.2016.7764556.
[32] https://resources.infosecinstitute.com/privacy-implications-of-google-glass/
[33] 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.
[34]Marc R. (17 Jul, 2013). Hacking the Internet of Things for Good. (cited 15 Feb ,2020).[Online]Available:https://www.symantec.com/connect/blogs/google-glass-still-vulnerable-wifi-hijacking-despite-qr-photobombing-patch
[35]https://rstylelab.com/company/blog/iot/vulnerability-of-fitness-trackers-risks-they-are-facing-and-tips-to-minimize-them
[36]https://support.google.com/glass/answer/3064189?hl=en&ref topic=3056776
[37] Swider, M. (2017, February 21). Google Glass review. Retrieved from TechRader: https://www.techradar.com/reviews/gadgets/google-glass-1152283/review/7
[38] Woolley, M. (2015, April 2). Bluetooth TechnologyProtecting Your Privacy. Retrieved from Bluetooth: https://www.bluetooth.com/blog/bluetooth-technology-protecting-your-privacy/