ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

A Detailed Study on Security Threat Analysis in Wearable Devices

[1] Srimanth DS, [2] Sudhanva Krishna V, [3] Vishwajith M V, [4] Venkatesan S
[1] Pre final Year Department of Computer Science & Engineering
[2] Assistant Professor, Department of Computer science & Engineering
[3] Professor Department of Computer Science & Engineering

***Abstract*— Wearable devices can be anything from small wrist-mounted systems to bulky backpack computers. Wearable device is a combination of devices typically a belt or backpack PC, head-mounted display, wireless hardware and some input devices. The fundamental principle of wearable device is to collect data ubiquitously and continuously, about the individual user and also their surroundings. This can pose many privacy challenges and are hindered by poor security. They are not mature yet in term of device security and privacy acceptance of the public. Low processing power of wearable device leads to developer's inability to implement certain complicated security mechanisms and algorithms on the device. This paper analyzes various security issues and attacks on the user's data.**

Keywords: **Wearable device, Bluetooth Low Energy(BLE),Near Field Communication(NFC), Handheld Wearable Wireless(HWW).**

I. INTRODUCTION

Wearable is a computing device that can be worn on the human body, either a computer that are incorporated as an accessory or as part of the material used in clothing. We see a lot of wearable devices around us and it has evolved beyond our wildest dreams. There are many forms of wearable devices such as smart glasses, smart watches, health trackers, smart jewelry, etc. The wearable devices are mainly defined by six characteristics – Monopolizing, Unrestrictive, Observable, Controllable, Attentive and Communicative.

The developments of application that can work with wearable devices are majorly used at home, and office, control and automation, logistics and transportation, environmental monitoring, healthcare, security and surveillance, etc. 2014[5] was addressed by the experts as the "year of wearable", reflecting the revolution of new wearable products such as smart. It is estimated that wearable devices might increase from 109 million in 2014 to 578 million by 2019.

The principle of wearable device being a ubiquitous device which collects the data can pose serious problem over security and privacy of the user. But due to the limited bandwidth and processing power wearable devices provide less security compared to other computing devices. Wearable continuously collects, transmit and stores data and handle information that are often considered as personal, private, sensitive or confidential. This information can be publically available and can be posted elsewhere. Though the data collection and sharing brings many benefits for end users, it also brings novel security threats and privacy challenges for stakeholders involved in the creation of wearable devices and its applications.

II. SECURITY ATTACKSON WEARABLE DEVICES

This section deals with attacks a wearable device is prone to, there can be two types of attacks [1]-

- ***Passive attacks*** - An attack which may occur while routing the data packets in the system, where the attacker may change the destination of packets or make routing inconsistent. Itis a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose of this attack is to gain information about the target (Observation of information) and data is not been changed during the attack.
- ***Active attacks*** – In the case of an Active attack, the attacker attempts to break the system by directly changing the information intended to the destination

After the attack, the possible damage done to the data is given below -

- **Data modification** - The attacker can delete or replace part or all of eavesdropped information and send the modified information back to original receiver to achieve some illegal purpose. Health data are vital. Modifying them may result in system failure and cause disaster for a person.
- **Impersonation attack** - If an attacker eavesdrops a wireless sensor node's identity information, it can be uses to cheat the other nodes.
- **Eavesdropping** - For the open features of wireless channel used by sensor networks, any opponent can

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

intercept radio communications between the wireless nodes freely and easily. Data stole may be used for malicious acts.

- **Replaying** - the attacker can eavesdrop a piece of valid information and resend it to original receiver after a while to achieve same purpose in different case.

The following figure shows eavesdropping and man-in-the-middle attack

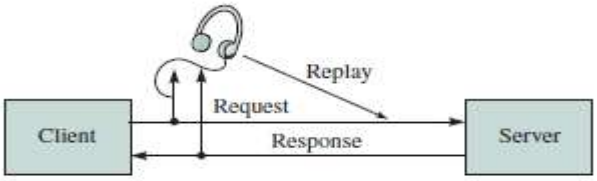

Figure 1 – Eavesdropping

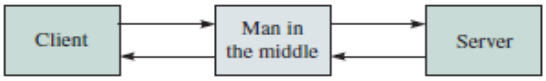

Figure 2 – Man-in-the-Middle

III. ATTACK SCENARIO:

SCENARIO 1:

In this scenario [2],wearable devices are connected into a server through a wearable gateway (using BLE, NFC), collaborating on a variety of wearable services. Smartphone are generally used as the wearable gateway whichcollects data from the wearable devices and continuously send the collected data into the server via WLAN as shown in the Figure 1.

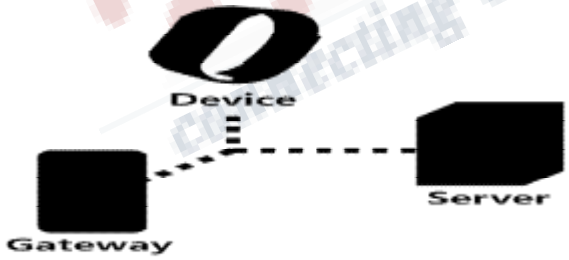

Figure 3–Three aspects for assembling weakness in a wearable service

Based on the methodology described in the previous section, there existsvulnerability in each component used in the model. These vulnerabilities are formulated in the following table 1.

Aspect	Vulnerabilities
Wearable device	Insecure firmware, insufficient security capability and poor physical security.
Wearable gateway(smartphone)	Insecure apps, unsafe mobile interface and insufficient authentication.
Server	SQL injection, cross-site scripting, session fixation and information leakage.

Table 1. Aspect-Vulnerability

These vulnerabilitiescan cause three major attacks such as- Illegal device pairing attack, the fake wearable gateway attack and the insecure code attack.

In the first attack, an unauthorized gateway can connect to a wearable device while in the second attack; a fake gateway intercepts data between a device and a server. Finally, in the third attack, malicious code is injected into the server through a gateway.

In this paper [2], the author has surveyed on the user's health data and HP research work, and formulates the work as shown in the table 2.

Attack Scenario	Effect
Illegal device pairing attack	1) Unauthorized gateway can access wearable devices 2) Health data in a device is leaked into a gateway
Fake wearable gateway attack	1) An attacker can change the original user's password 2) Data managed in a server can be sniffed
Insecure code based attack	1) An attacker can obtain sensitive data from apps 2) An attack query can be sent into a server

Table 2. Attack Scenario with their security attacks

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

SCENARIO 2: In this work [13] the authors discuss security issues on HWW (Handheld Wireless Wearable) devices. This work proposestwo network models -

- **Flat Web Presence model**: Web Presence model deals with anywhere, anytime paradigm of the wearable devices. Here, a wearable device must have sort of intelligent, context aware agent so that the overall traffic load will be decreased and thus resulting in savings of both communications and battery consumption.
- **Hierarchical Web Presence Model**: This model defines the local interoperability among HWW devices. Multihop communications are allowed on demand by relaying on some sort of backbone and thus it simplifies the design of network infrastructure

According to the two models discussed above, the authors [13] have identified three basic security requirements. Those are:

- **Confidentiality** - Information must be disclosed only to intended user.
- **Integrity** – Unauthorized modification of information is prevented.
- **Availability** – It refers to the ability of a user to access information or resources in a specified location and in the correct format.

System Security – In the scenario of devices which communicates over a long distance has to communicate with multihops. This can pose a serious problem on every particular node it is used for communication. Further if the length of the communication path is increased, the probability of the attack will be increased (such as the man-in-the-middle attack). Finally, the authors have considered the application flaws, where the software running on an HWW device can be hacked as in the wired paradigm. Hacking can be performed exploiting a flaw in the application's design phase or in the implementation phase. The applications for the HWW environment are designed with very tight hardware constraints such as less memory, low battery consumption, simple security algorithms.
Thus, the applications which are implemented in the wearables are inherently weaker than those developed for the wired paradigm

SCENARIO 3: Security Attacks on different wearable devices

In this work [14] the author discusses the security issues on three different wearable devices –

SMART GLASSES–
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 [15-16]. Besides authentication issues, [17] found that the privacy of user' appears at risk as well by the eye tracking technology supported in Glass. In addition, Seyedmostafa and Zarina [15] revealed that pictures and videos can be recorded without user's consent which violate people privacy policy

FITBIT DEVICES –
Fitbitis known for its products which is a smart fitness band that can be worn on the wrist.
Itprovides 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. [18] - [20]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 [19] built a tool, FitBit to launch several attacks on Fitbit devices such as data injection attack, DoS and battery drain hacks to prove the statement.

SAMSUNG SMARTWATCH –

Samsung Smart watch 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 Smart watch. 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 on top 10 popular Smart watches in the market, found that 100 percent of the tested Smart watches contain significant vulnerabilities, including poor authentication, lack of encryption and privacy issues. For instance, there are 70% of watch firmware was transmitted without encryption.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

IV.CONCLUSION

In this work, the characteristics of wearable devices are discussed. Also the various security threats related to the wearable devices are analyzed in three different levels – Illegal device pairing attack, the fake wearable gateway attack and the insecure code attack in scenario 1, attacks on HWW devices in scenario 2, and attacks on various wearable devices like smart glasses, fitbit devices, and Samsung smart watch in scenario 3.
Further research effort in this direction is required in order to improve the system security.

REFERENCES

1. Security and Privacy Issues in Wireless Sensor Networks for Healthcare ApplicationsMoshaddique Al AmeenJingwei Liu Kyungsup Kwak

2. Security threat on wearable services: Empirical study using a commercial smartband
Myeonggeon Lee, Kyungmook Lee, Jaewoo Shim, Seong-je Cho, Jongmoo Choi, Department of computer Science and Engineering, Dankook University, Yongin, Gyeonggi 16890, Korea

3. 1. Borisov, N. et al. Intercepting mobile communications: The insecurity of 802.11. In *Proceedings of ACM/IEEE MOBICOM 2001*; 180–189.
4. Carman, D.W. et al. Constraints and approaches for distributed sensornetwork security. NAI Labs Technical Report. (Sept. 2000);www.nai.com/research/nailabs/cryptographic/a-communications-security.asp
3. Chan, H. et al. Random key predistribution schemes for sensor networks.In*Proceedings of the IEEE Symposium on Security and Privacy*
(May 2003, Oakland, CA).
4. Coulouris, G. et al. *Distributed Systems: Concepts and Design.* AddisonWesley, Reading, PA., 2001.
5. Di Pietro, R. et al. Providing secrecy in key management protocols forlarge wireless sensor networks. *J. Adhoc Networks.* To appear.
6. Fox, A. and Gribble, S. Security on the move: Indirect authenticationusing Kerberos. In *Proceedings of ACM/IEEE MOBICOM 1996;*
155–164.
7. Guan, Y. et al. Preventing traffic analysis for real-time communicationnetworks. In *Proceedings of IEEE Milcom*(Nov. 1999), 744–750.
8. Harter, A. et al. The anatomy of a context-aware application. In *Proceedingsof ACM/IEEE MOBICOM 1999;* 59–68.
9. Hermann, R. et al. DEAPspace—Transient ad hoc networking of pervasivedevices. *Computer Networks 35* (2001), 411–428.
10. Kindberg, T. et al. People, places, things: Web presence for the realworld. *MONET 7*, 5 (Oct. 2002), Kluwer A.P., 365–376.
11. Myers, B.A. Using handhelds and PCs together. *Commun. ACM 44*, 11(Nov. 2001), 34–41.
12. Sandhu, R. et al. Configuring role-based access control to enforcemandatory and discretionary access control policies. *ACM Trans. Info.And System Security 3*, 2 (May 2000) 85–106.
13. Security and privacy issues of handheld and wearable wireless devices byRobertto Di Pietro,and Luigi V.Mancini
14. Wearable Technology devices security and privacy vulnerability analysis Ke Wan Ching and ManmeetMahinderjit Singh School of Computer Sciences,UniversitySainsMalaysiaPenang, Malaysia
15 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.
16. 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/
17. Daniel D. 2013. Privacy Implications of Google Glass. (cited 21 Oct, 2015).[Online] Available:http://resources.infosecinstitute.com/privacy-implications-of-google-glass/
18. 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_201506_fitness_tracker_english.pdf
19. Rahman, M., B. Carbunar, and M. Banik, Fit and vulnerable: Attacks and defenses for a health monitoring device. arXiv preprint arXiv:1304.5672, 2013.
20. 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/surveillancesociety/2015/08/03/Surveillance-Society-Wearable-fitness-devices-often-carry-securityrisks/stories/201508030023