TEST Engineering & Management

March - April 2020
ISSN: 0193-4120 Page No. 4342 - 4348

A Study of Security System in Wearable Devices

Joo-Young Lee[1], Sam-Jin Jeong[*2]
[1]Student, Dept. of Information Protection, Baekseok University, Cheonan, 310-65, Korea,
[*2]Professor, Div. of ICT, Baekseok University, Cheonan, 310-65, Korea
sarahub@naver.com[1], sjjeong@bu.ac.kr[*2]

Article Info
Volume 83
Page Number: 4342 - 4348
Publication Issue:
March - April 2020

Article History
***Article Received**: 24 July 2019*
***Revised**: 12 September 2019*
***Accepted**: 15 February 2020*
***Publication**: 26 March 2020*

Abstract

Wearable device means a device that can be worn on a computer-capable body. To design security solution of future wearable computing environment, it is needed to study about security system in wearable devices. It is important to preliminary study for using security service in wearable computing environment. We study about specification and security mechanism of wearable devices. We study related works in security threats of wearable device development. We also analysis about trend of future wearable computing environment, and investigate contents such as security requirements and security measures in wearable devices.

Security problems for wearable devices are deepening as problems with personal information leaks, privacy and life threats arise. Advancing closely with modern life, MITM (Man-in-the-middle) and APT (Advanced Persistent Threats) are under attack, and the damage is increasing. This study analyzed weaknesses of wearable devices and explored ways to improve them. We provide a reference guide for development of security mechanism in wearable computing environment. We also suggest the basis knowledge for analysis of enhanced wearable computing communication system. Through this research, the research for the safe use of various kinds of wearable devices is continuously needed by referring to the wearable device security requirements.

Keywords: *Wearable Device Security, Security Attacks, Security Threats, WBAN, Security Measures.*

1. Introduction

The wearable device refers to a device worn on a body capable of computing in a form that can be attached to or worn on the body. The term wearable used to be a type of accessory that was worn directly such as clothing, glasses, watches, shoes, etc. (1st-generation device), but recently, it has evolved from fabric-integrated (2nd-generation devices) to body-attached recognition type (3rd-generation devices) [1]. Figure 1 shows a picture of a watch-type of wearable devices. Many people wear watch-type wearable devices by default and need security services for such devices [2]. Table 1 shows several types of wearable devices.

Figure 1. Watch type wearable device.

Wearable functions include a watch that records the number of steps and sleep information, a t-shirt that measures heart rate, breathing, and movement, and glasses that check and interpret the information of surrounding objects. The device can be used freely while moving, and the size and weight are reduced. By moving to 3rd generation devices, it will evolve to maximize flexibility. At this time, battery and wireless power technologies, integrated and de-attached electronic circuits are essential. As technology advances, devices are used in a variety of industries, including healthcare, fitness, infotainment, and the military industry.

Figure 2 shows forecast wearables unit shipments worldwide from 2014 to 2022. According to the Consumer Electronics report, global wearable device shipments are expected to increase from 140.5 million units in 2019 to 199.8 million units in 2022. The figures from 2020 to 2022 were calculated by Statista according to the figures for 2019 and 2022 and the compound annual growth rate of 7.9% [3]. Related businesses are expected to increase along with others together after 2020.

Table 1. Types of wearable devices

division	*Representative product*
Accessory type	*Smart glasses, smart watch*
All-in-one clothing	*SmartWare, all-in-one computer*
Body attachment type	*Skin patch type sensor*
Bio transplantation type	*Implantable sensors and devices*

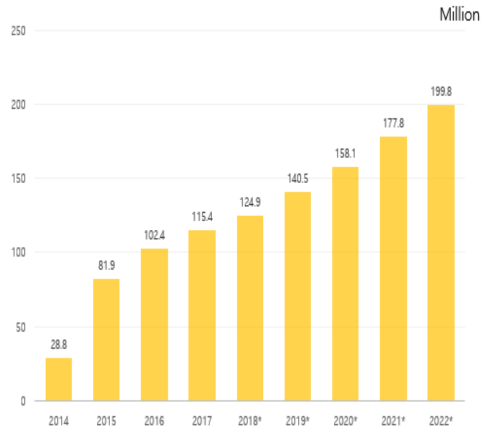


Figure 2. Forecast Wearables Unit Shipments Worldwide from 2014 to 2022 (in millions)

2. Related Works in Security Threats

Wearable devices operate at low power, low heat, and low capacity, which presents significant security vulnerabilities in the OS. Table 2 shows the security treats and attack types by layer. Wearable devices can be vulnerable to each attack.

Bluetooth uses UHF propagation to define short-range data communication [4]. It is used in many devices and sends and receives text and voice digitally at low speed. Bluetooth is now mounted by default on many models. Using Bluetooth, it sends a portion of the user's MAC address to the channel. If an attacker sniffs communication, most of the MAC address can be extracted from the packet. Bluetooth Low Energy uses an unencrypted channel to send a randomly changing random address to signal the device's connection. However, in this method, the attacker detects a part of the address change method and keeps track of the device by identifying the communication pattern using the difference between the address and the information update period. This attack is called Blueborne.

Using WBAN (Wireless Body Area Network), information such as biometric signals are collected through sensors and devices, and transmitted in real time using devices or other base stations. At this time, the PIN information is sent in plain language through remote control, and the PIN is tapped by intercepting the data packets.

Each device type has a different communication packet first 4 bits and a different PIN value.

Table 2. Security Threats and Attack Types

Layer	*Attack*
Physical	*Jamming, Tempering*
Data Link	*Conflict, negation, exhaustion*
Network	*Spoofing, Select Forwarding, Civil*
Transport	*Flooding, asynchronous*

In addition, there are integrity attacks (selective transmission of two consecutive packets), privacy attacks (eavesdropping on wireless links), and availability attacks (jamming communication channels by abnormal operation) without PIN information.

In a WBAN environment, confidentiality is important to prevent information disclosure.

Table 3 shows the integrity attack, privacy attack, and availability attack.

Table 3. Privacy attack, integrity attack, availability attack

Attack	*Explanation*
Privacy attack	*Eavesdropping attacks on wireless links. It is related to information disclosure. An attack that can be made between open doors.*
Integrity attack	*Without information about the PIN device using selective transmission of two consecutive packets, an attacker could send inaccurate information.*
Availability Attack	*Jamming the communication channel between devices causing incorrect behavior. Without validating the communication protocol, an attacker can know the PIN device and make a false report.*

MITM (Man-in-the-middle) attacks using sniffing can capture packets using the 802.11 protocol, and when using Wi-Fi, the traffic exchanged between devices is in plaintext. It can steal or modify information entered on the device. The MITM attack is also used in the Blueborne attack mentioned above.

Watch-type wearable device provides the functionality of a PPT controller. The PPT controller connects to other PC devices using Bluetooth, and using a MITM attack on a vulnerable device allows an attacker to remotely move files from the PC to the mouse pointer or steal information.

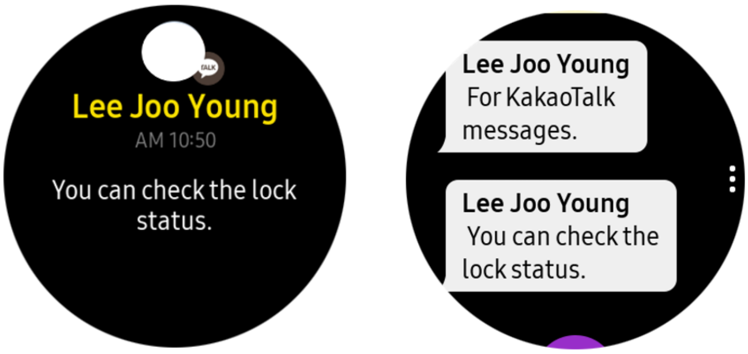
Sensors embedded in wearable devices also pose a number of threats. Among the apps mounted on the wearable device, malicious apps and malicious sites access and operate sensors mounted in the device without the user's permission when using the wearable device. Personal information is stolen by comparing users' usage history with sensor movement. It also uses a method of attacking by analyzing sensor usage over long distances. As such, the sensor contains a lot of user information and makes it possible to predict it.

GPS tracking information can be used to detect a user's location and attack like short range Blueborne. Ransom ware is also susceptible to infection within wearable devices. If an infected smartphone is used, ransom ware is pushed into the wearable device and infected.

APT (Advanced Persistent Threats) attack is also known as Artificial Persistent Threats [5-6]. APT attacks use dedicated applications to disguise malicious apps and install them on the device without the user's knowledge. After installation, users' usage patterns are analyzed, and vulnerabilities of wearable devices and smart devices are identified to prepare for attacks silently. Users should not be aware of the attack and should be careful because it can affect all connected devices starting from the wearable device. There is no notification on the operating system, so APT attack is used as a spy tool.

If any software responds to the user's voice, the device collects voice information at all times. Infected devices can eavesdrop or record personal conversations. Infected devices can also eavesdrop on personal conversations. Wearable devices are a security model in which both the proxy and the device share a secret key to save power. Because secret keys use symmetric key authentication and password, they are more power efficient than public keys, making them suitable for the use of small micro controllers. All communication of authentication is through the proxy, and after the proxy and the user authenticate each other, the user makes the request as a proxy.

The required verification is then done by the proxy. The proxy checks and validates the access control list and, if successful, forwards the request to the device. If not, responds with an error message. As wearable devices have high accessibility, security threats are difficult to recognize because they are convenient. App notifications of the watch-type wearable device for ease of use is linked with the smartphone using LTE, it is possible to receive notifications and messages even when the smartphone is far away. Regardless of the lock and notification status of your smartphone, you can easily check received messages, previous conversations, and unread messages. The message works in real time with the smartphone. Figure 3 shows the appearance of the wearable device when a message is received from the KakaoTalk APP.

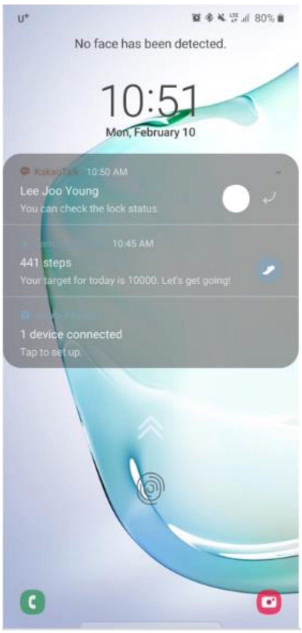


Lee Joo Young
AM 10:50
You can check the lock status.

Lee Joo Young
For KakaoTalk messages.

Lee Joo Young
You can check the lock status.

Figure 3. Message on wearable device.



No face has been detected.

10:51
Mon, February 10

KakaoTalk 10:50 AM
Lee Joo Young
You can check the lock status.

10:45 AM
441 steps
Your target for today is 10000. Let's get going!

1 device connected
Tap to set up.

Figure 4. Messages in my smartphone.

Figure 4 shows that the smartphone device is locked so details cannot be viewed on the smartphone. By using radio waves, device malfunctions, and sniffing of the information of personal location are difficult for the user to find. Most devices are linked to smartphones, enabling users to steal information from smartphones. If a single device experiences a security problem, the problem occurs throughout the network. In particular, medical devices are directly linked to life, and security threats are expanding [7-8].

Diseases such as strokes require emergency medical activities within the Golden Time after an advance warning occurs. The real-time monitoring system using such a wearable device may lose a life when an emergency situation occurs when a hacker cannot correct information transmitted to the wearable device and deliver accurate information. In addition, if the patient's medical records are leaked to the outside, use may be avoided with fear of use [9].

3. Security requirements and Security Measures

For wearable devices, requirements such as authentication, location services, and access control are essential. The three main conditions of security are confidentiality and integrity availability. Basically, all three elements of security must be satisfied, and Sensitive information should be maintained in integrity and confidentiality. Various information such as biometric information and location information of the user are collected and stored in the user's device. Care should be taken to maintain confidentiality so that information is not disclosed. For this, an access control list is needed.

When data is generated illegally by WBAN, access control, forced deletion of authorized node permissions, and data deletion/recovery are required. Non-authenticated data injection from the WBAN should be prohibited [10]. If wearable devices are lighter, they are more likely to be lost or damaged, and sensitive information is likely to be leaked. In particular, sensitive information in files or certificates should be protected through file passwords when communicating directly between devices, such as LTE. In addition, when users are aware of device loss, both locating the device and locking the data should be possible. If sensitive information is leaked, privacy issues can become bigger.

User authentication is also important. User authentication methods vary from device to device. In some cases, such as passwords, devices such as watches use passwords and patterns, or may not have user authentication at all. Devices that can be accessed without user authentication can be accessed by unauthorized users. Because attackers are easily accessible and have weak security, a simple user authentication method is required. Recently, the biometric recognition method has been in the spotlight.

However, it is necessary to be careful because the method of generating an error in the method of authenticating a user by using a material such as skin or using a color printer is also used.

Wearable devices are only allowed in limited environments and limited users, so user certificates are usually required. In the case of a biocompatible device such as medical device, and if a device such as an AED incorrectly recognizes biometric information, a user's life may be dangerous. Due to the characteristics of the wearable device, a lightweight certificate is required. If the key is generated using the characteristics of the biological signal, it can be used more reliably than a device operating in a given time or state. By using the wearable device's own functions and using multiple biometric functions such as heart rate and electrocardiogram, a secure key can be extracted [11-13].

A feature of a predetermined biosignal is extracted from a biosignal using a predetermined algorithm, and the feature is processed as binary string data. It conceals any key and securely transmits the processed data using the hidden key and a single message. The concealed key verifies the received data. For secure communication, all smart devices must generate a session key using a hash function by applying a public/private key pair and a DH key exchange protocol. The session key should be used as a one-way hash function. For access control, users include access control lists inside their certificates. It needs to be managed using the access control session key so that no one but the user can access it. When forcing access, the access control list can be extracted and forcibly restricted.

The session key must also be encrypted and transmitted for secure transmission, and all unauthorized access must be blocked. The security of the firmware itself is also important. If there is a problem inside a running application, a hole in security is used when using the user interface.

4. Conclusion

As more of the information comes and goes as the wearable device market evolves, security issues become more important. As the IoT develops, there is a need for a solution for protecting information on all connected devices in addition to simple personal information. It is the first device and the user running the self-managed device, having an interest in security. Device users should not make as unauthenticated network connections as possible, implement device management such as changing system passwords periodically, and pay attention to security. Developers should identify maintenance and security requirements to prepare necessary security measures. Because of the limited environment, it is necessary to use big data technology to identify attack intent and block attacks in order to analyze, predict and respond to various attacks that may occur. The security problem of wearable devices will increase. If the hacking of wearable devices damages users, it will be difficult to develop the technology of wearable devices if consumption is reduced. As the issue of privacy invasion becomes important, relevant legislation must be added not only to individuals but also to the state. If reliable security is maintained through the efforts of individuals and organizations to protect their information, wearable devices will consume more. We need to work hard to advance IT by enhancing the competitiveness of wearable devices.

5. Acknowledgment

This research is supported by 2020 Baekseok University Research fund.

References

[1] Ashok RL, Agrawal DP. Next-generation wearable networks. Computer. 2003 Nov; 36(11): 31-39.

[2] Muhtadi JA, Mickunas D, Campbell R. Wearable security services. Proceedings 21st International Conference on Distributed Computing Systems Workshops, Mesa, AZ, USA. 2001; 266-271.

[3] Consumer Electronics. Forecast wearables unit shipments worldwide from 2014 to 2022. [Internet]. 2018 [Release date 2018 Sept]. Available from: https://www.statista.com/statistics/437871/wearables-worldwide-shipments/ (website)

[4] Arias O, Wurm J, Hoang K, Jin Y. Privacy and Security in Internet of Things and Wearable Devices. IEEE Transactions on Multi-Scale Computing Systems. 2015 April-June; 1(2): 99-109.

[5] Shenwen L, Yingbo L, Xiongjie D. Study and research of APT detection technology based on big data processing architecture. 2015 IEEE 5th International Conference on Electronics Information and Emergency Communication, Beijing. 2015; 313-316

[6] Li M, Huang W, Wang Y, Fan W, Li J. The study of APT attack stage model. 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), Okayama. 2016; 1-5.

[7] Bouhenguel R, Mahgoub I, Ilyas M. Bluetooth Security in Wearable Computing Applications. 2008 International Symposium on High Capacity Optical Networks and Enabling Technologies, Penang. 2008; 182-186.

[8] Hung K, Zhang YT, Tai B. Wearable medical devices for tele-home healthcare. The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, San Francisco, CA. 2004; 5384-5387.

[9] Fu K. Medical device security: The first 165 years. 2016 International Great Lakes Symposium on VLSI (GLSVLSI), Boston, MA. 2016; 5-5

[10] Joshi J, et al. Secure and Wearable Computing in WBANs. 2016 International Conference on Information and Communication Technology (ICICTM), Kuala Lumpur. 2016; 65-70.

[11] Meena U, Jha MK. An efficiency model for authentication approaches in WBAN. 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi. 2015; 476-481.

[12] Yu H, Kim Y. True Random Number Generator Using Bio-related Signals in Wearable Devices. 2018 International SoC Design Conference (ISOCC), Daegu, Korea (South). 2018; 231-232.

[13] Thierer AD. The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. Rich. J. Law Technol. 2015; 21: 6-15.