Possibilities for abuse and security of smart watch

Almer Lubomír

Univerzity of Defence, Faculty of Military Leadership,
Kounicova 65, 66210 Brno, Czech Republic
E-Mail: lubomir.almer@unob.cz

Abstract. This article was focused on Possibilities for abuse and security of smart watch. In first part I will describe what is the smart watch and how is that work. Then I will describe principally possibilities for abuse of smart watch and in last part of this paper is about how it is possible to secure our smart watch. For this paper I choose Sony Smart Watch SW2.

Keywords: smart watch, smart device, exploit, abuse, security

1 Introduction

We are living in an era of smart devices that we sync with our smart phones and make our lives very simple and easy, but these smart devices which inter-operate with our phones could leave our important and personal data wide open to hackers and cyber criminalist. In this paper I will describe what are the smart watches and their functions. Specifically I will describe smart watches Sony Smart Watch SW2 which I have to use on this project. Then I will describe two opportunities how to connect smart watches to smart device. Next chapter will be focused on possibilities for abuse of smart watches, there I will describe two possibilities how is it possible to abuse smart watches and I will show one specific case of these attack. Last part of this paper will be focused on how to secure ours devices between previous attacks.

2 Smart Watches

Smart watch is a computerized wristwatch with functionality that is enhanced beyond timekeeping. While early models can perform basic tasks, such as calculations, translations, and game-playing, modern smart watches are effectively wearable computers. Many smart watches run mobile apps, while a smaller number of models run a mobile operating system and function as portable media players, offering playback of FM radio, audio, and video files to the user via Bluetooth headset. Some smart watches models, also called “watch phones”, feature full mobile phone capacity, and can make or answer phone calls. Such devices may include features such as a camera, accelerometer, thermometer, altimeter, barometer, compass, chronograph, calculator, cell phone, touch screen, GPS navigation, map display,

graphical display, speaker, scheduler, SD cards that are recognized as a mass storage device by a computer, and rechargeable battery. It may communicate with a wireless headset, heads-up display, insulin pump, microphone, modem, or other devices. Some also have "sport watch" functionality with activity tracker features as seen in GPS watches made for training, diving, and outdoor sports. Functions may include training programs, lap times, speed display, GPS tracking unit, route tracking, dive computer, heart rate monitor compatibility, cadence sensor compatibility and compatibility with sport transitions. Like other computers, a smart watch may collect information from internal or external sensors. It may control, or retrieve data from, other instruments or computers. It may support wireless technologies like Bluetooth, Wi-Fi, and GPS. However, it is possible a "wristwatch computer" may just serve as a front end for a remote system, as in the case of watches utilizing cellular technology or Wi-Fi. For this paper I choose Sony Smart Watch SW2.

2.1 Sony Smart Watch SW2

Sony Smart Watch SW 2 is equipped with a single-core ARM Cortex M3, which is clocked at 200 MHz. The display has a resolution of 220 x 176 pixels, which is displayed with the size of 1.6 inches fineness of 176 PPI. In terms of connectivity the watch can be connected to smart phone devices in two ways. First one is by Bluetooth and the second by NFC. Bluetooth is version 3.0 and watches can be extended from the smart phone device up to 5 meters. NFC is a big advantage pairing mileage is just a touch. For connection is necessary to download application Smart Watch 2 SW2 from Google store.

This smart watch is possible to connect with any smart devices with operation system Android 4.0 (Ice Cream Sandwich) and newer. After first switching the smart watches had 4 applications: Alarm, battery, notification and options.

2.2 NFC

Near Field Communication is modular technology radio wireless communication between electronic devices over short distances (up to 4 centimeters) with magnification devices. This architecture defines a set of standards ISO. Current and projected use of this technology is primary in the exchange of key data in contactless financial transactions and simplified connection configuration of radio devices, such as Wi-Fi. With the use of this technology allows for mutual communication between two active devices or between active devices and passive devices as a card with contactless payment card.

2.3 Bluetooth

Bluetooth is a proprietary informatics open standard for wireless communication that connect two or more electronic devices, such as mobile phone, PDDA, personal

computer or wireless headphones. It was created in 1994 by Ericsson as a wireless replacement for wired serial interface RS-232.

2.4 Google play

Google play is an online distribution service. Currently, Google Play provides several types of digital content which can be accessed from a computer or mobile phone equipped with Android operating system or through Google TV. Google Play is primarily focused on the distribution of application just for smart phones and tablets with Android, this part is called the Google Play Store.

3 Possibilities for abuse of smart watch

Because smart watch is connected to our mobile phone devices, there is a big threat of misuse. Specifically by our interconnection of all ours smart devices together. We are trying to simplify our lives. Interconnection make ours live easier. All information which we have in our smart phone we have on our wrist available in few seconds. Terms of time it is big advantage, but we have to take care about security. Part time which we save we should devote security of this devices.

In case of alienation it is big advantage is disconnection of smart watch from smart phone. If a smart watch isn't connected they are not able to show any massages or something else. This reduce the risk of abuse our private information which we are trying to protect. From my opinion smart watches aren't tempting target for potential attackers. But attackers could take advantage of connection between smart watches and smart devices, for example wiretapping communications and so on.

Security researchers have proven that the data sent between the smart watch and Android smart phone aren't very safe and would be subject to brute force hackers to intercept and decode data users, including everything from texting on Google handouts cottages and facebook chat.

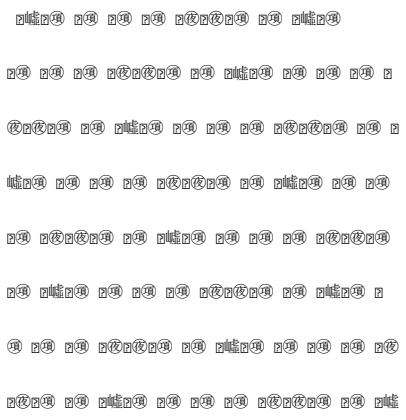
Bluetooth communication between the smart watches and Android device rely on six-digit PIN code in order to transfer. Six digits PIN means about one million possible keys that can be easily brute force attackers converted to plain text. In the case of the attacker away from the subject of his interest it is possible that the attack carried out. That is one possible type of attack on smart watches and Android device.

The second type of attack on smart watches is overloading services. In this paper I will deal with this attack. This has overloaded the non availability of equipment and its restart, or in the worst case restart and factory restart of our smart device. These attacks will use precut exploit. Specifically, I will target the application WhatsApp and the specific name of the exploit is a WhatsApp Crash Exploit. This exploit it's free to download on the internet. These exploits created before or flooding reports are also other applications than just WhatsApp, for example on Facebook Messenger.

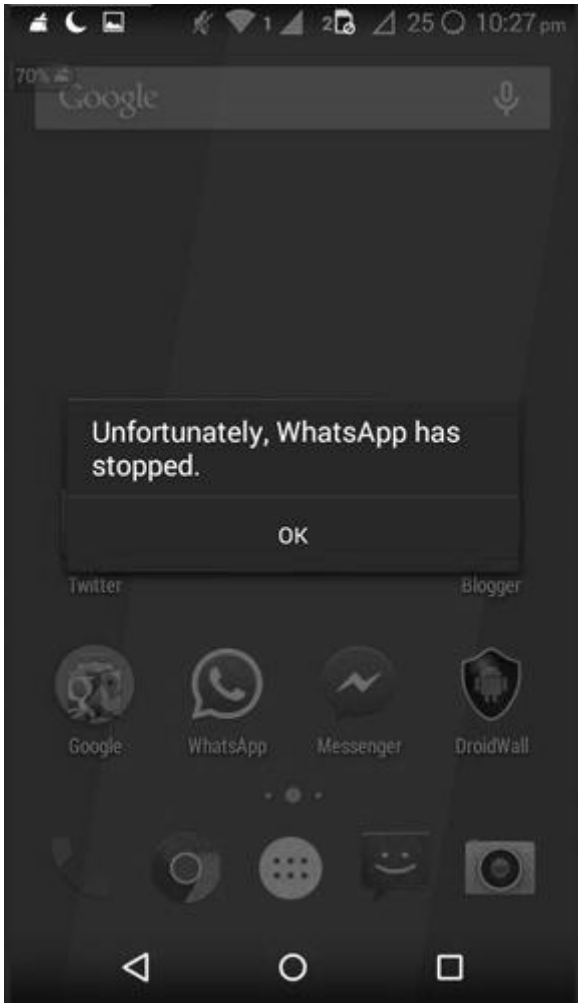
3.1 WhatsApp Crash Exploit

If we want to use this exploit to an unexpected application you simply copy and send a message to the body to which the application overloads. This message had 2 kilobits and contains 2000 words in message in special character set which can crash WhatsApp messenger application. Before this crash message there was another crash message which is too big (greater than 7 megabytes in size). WhatsApp could crash victim device and app immediately, but using this new exploits attacker only needs to send a very small size message to the victim. This vulnerability has not been tested on iOS, but it is sure that all version of WhatsApp including 2.11.431 and 2.11.432 are affected with this bug. Also the attack does not work on Windows 8.1. Any member of your WhatsApp group could intentionally send a specially crafted message to exit people from the group and delete the group. Also, for example, if I don't want someone to keep records of my chat with them, then I can also send the same message exploit to the person.

Below is a sample piece of malicious code which is able to cause this unavailability. This entire code has 66 lines, which are almost all the same.



3.2 How is it look like after



4 How to secure our smart watch

In first case to protect ourselves to be a victim of such attacks, use Near Field Communication to safety transmit a PIN code to compatible smart watches during pairing, but that would likely increase the cost and complexity of the devices. Another option is to use original equipment manufacturers (OEMs) by Google as an alternative to make data transfers between either devices more secure. Or other possibility we could supersede the entire Bluetooth encryption between both device and smart watches and use a secondary layer of encryption at the application level.

Security of second case should be more uncomfortable for us. My recommendation for this is to not install messenger applications like WhatsApp, Viber and Facebook Messenger or else from my point of view it is best step which we can do. If we do not want to do that we have to be careful which messages we are opening. If we cannot open a malicious message, this message cannot overload our application.

Beyond the above steps would not be wrong to follow the general safety measures. First step is to install application only from trusted sources. Further reading license conditions and if we don't accept this term don't use and download this application. Next step should be disclosure of access to third part to devices. For example with numerical password of touch screen, without this password we can't unlock device. It would also be good to have antivirus protection installed on smart devices. Next step is to be careful on which network we are connecting. For example, to public network will not connect. There is greater risk of becoming the aim of the potential attacker. Finally, perform regular updates of all applications and the operating system. Producers are always trying to achieve the highest possible level of safety of their products. As a final point of increasing security of smart devices I have made regular cleaning programs for this purpose.

References

1. The Hacker News: Cyber Security, Hacking, Internet Security, Technology News, http://www.thehackernews.com.
2. Pastebin.com - #1 paste tool s 2002, http://www.pastebin.com.
3. Sony Xperia TM – smartphony a tablet Android a příslušenství SmartWear – Sony Xperia (Česká Republika), http://www.sonymobile.com/cz/.
4. Engadget | Technologz News, Advice and Features, http://www.engadget.com.
5. Wikipedia, http://www.cs.wikipeadia.org/wiki/Hlavní_strana.