Security Studies on Wearable Fitness Trackers

Kelvin Ly and Yier Jin

***Abstract*—Wearable technology has gained a significant amount of traction over the years, and has revolutionized the way we access customer information as well as track our fitness and well being. However, modern smart bands often lack proper protection, leaving user privacy at risk. In this paper, we will analyze four popular smart bands and demonstrate that improper protection schemes can be easily bypassed and that the devices can be compromised to leak user information.**

I. Introduction

According to the latest results from the NPD Group's recent Connected Intelligent Consumers and Wearables Report, one in ten U.S. adults now own a fitness tracker. It is also predicted that the market for wearable technology will increase by 40 percent over the next five years as consumers switch from mobile devices to smaller wearable technologies that provide the same functionality. The rise of wearable technology both at home and in the workplace has even attracted the attention of wireless carriers and smart phone companies who are interested in implementing this technology to complement their mobile devices and data streaming services.

The increased usage of wearable devices comes burdened with additional security and privacy concerns because compromise of said devices can cause safety issues and leak personal information. In most smart devices, security and privacy issues seem to be an afterthought and are not usually considered during the design and manufacturing phases [1]–[4]. With all of these vulnerabilities, attackers are easily able to bypass software-level protection methods and upload customized, and possibly malicious firmware onto these devices. Through malicious firmware, attackers are easily able to collect user information and remotely control these devices.

In this paper, we will introduce our work on analyzing the hardware and firmware security of various smart wristbands. We will demonstrate major security vulnerabilities in four popular smart bands. These exploits were found by first looking for potential flaws along each device's chain of trust, starting with the bootloader. Security protection methods to prevent the installation of malicious firmware including dedicated AES cores, CRC checksumming, and RSA checking were present on some of the devices, but we were able to circumvent these security measures and attain essentially full control of each of these devices through control of their firmware.

II. Device One: Nike+ FuelBand

The Nike Band uses an STM32L series microcontroller, which does not provide any security for the firmware, either in requiring a signature to verify the firmware, or providing some barrier to directly reading and writing the firmware memory. Consequently, all that was needed to reprogram the Nike Band was to change the logic level of one of the MCU's pins to allow it to boot in DFU mode. Customized firmware image can then be installed in the smart band to cause malicious consequences.

Kelvin Ly and Yier Jin are with the Department of Electrical and Computer Engineering, University of Central Florida, Orlando, FL 32816 USA email: kelvinly@eecs.ucf.edu, yier.jin@eecs.ucf.edu

III. Device Two: Huawei TalkBand

The Huawei TalkBand is slightly more secure than the Nike Band, in that its bootloader checked the firmware's signature before allowing it to boot. However, the bootloader itself was still writable over an exposed SPI interface, and the bootloader was patched so that it no longer checks the firmware's signature. After this change any firmware could be loaded onto the device to compromise the smart band.

IV. Device Three: Xiaomi Mi Band

In the Xiaomi Mi Band uses the Dialog DA14580, a very small Bluetooth-based System-on-a-Chip. However, the firmware flash was stored in an external SPI flash, making it possible to program using SPI. The bootloader did not check a signature, and consequently this band only required reverse engineering and locating the SPI lines to reprogram.

V. Device Four: Codoon Band

The Codoon Band uses a STM32L series microcontroller like the Nike Band. It was similarly easy to replace the firmware, leveraging the unprotected and exposed UART DFU mode to reprogram using UART.

VI. Conclusion

In this paper, we showed real-world demos on how modern wearable devices are vulnerable to hardware and firmware attacks. Through our work, we have also shown that improper protection on firmware integrity can be easily bypassed. In our future work, we will focus on trusted and secure wearable device design through hardware-firmware co-protection.

References

[1] O. Arias, J. Wurm, Khoa Hoang, and Y. Jin, "Privacy and security in internet of things and wearable devices," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 99–109, 2015.

[2] Grant Hernandez, Orlando Arias, Daniel Buentello, and Yier Jin, "Smart Nest Thermostat: A smart spy in your home," in *Black Hat USA*, 2014.

[3] Orlando Arias, Grant Hernandez, and Yier Jin, "Privacy and security in internet of things: A case study on google nest thermostat," in *Design Automation Conference*, 2015, (Poster).

[4] Jacob Wurm, Orlando Arias, Khoa Hoang, Ahmad-Reza Sadeghi, and Yier Jin, "Security analysis on consumer and industrial iot devices," in *21st Asia and South Pacific Design Automation Conference (ASP-DAC 2016)*, 2016, pp. 519–524.