Smart watch- *A Vulnerable Fashionable Dangerous*

Mohammad Abdul Haque Anu

Although the market for smartwatches is still in its infancy, there has been a steady increase in the popularity of this sophisticated technological gadget. Smartwatches produced by technological giants, such as Apple and Google, are not only fashionable accessories, but also multifunctional devices that can send messages, use mobile apps, and serve as fitness and health sensors.

What especially distinguishes a smartwatch from regular smartphones is the capability of receiving important alerts on a wrist device while driving, biking, or working out. However, due to the novelty of wearable technology, the security features of smartwatches may not be fully developed.

In this article, we will examine the major smartwatch vulnerabilities (Section 2). Further, we will provide 10 recommendations on how to protect your privacy while using a smartwatch (Section 3). Finally, a conclusion is drawn (Section 4).

Smart watch Vulnerabilities

The smartwatch market was unpleasantly surprised by a research conducted by HP Fortify Software Security Center in mid-2015. The research report indicated that all 10 tested smartwatches produced by the major companies were vulnerable to information security attacks. The study distinguished a number of major security issues that are mostly related to collection and transmission of sensitive personal data. The list of identified smartwatch vulnerabilities is briefly discussed below.

Weak authentication : In order to guarantee security, smartwatch applications are usually protected by a password. However, the research identified that most smartwatch credentials are protected by weak passwords and the password recovery mechanisms are insecure. The research also found out that the tested smartwatches do not block an account after a number of failed attempts to submit identification data. The above characteristics make smartwatches susceptible to an account access attack carried out by guessing login details.

Dangerous network. Normally, smartwatches are connected to a smartphone or other device via Bluetooth. This connection allows receiving notifications from a smartphone and transmitting data back to the device. Although some smartwatches also allow a Wi-Fi connection, specialists warn that such a connection can be unsafe not only for the smartwatch itself, but also for other devices in the Wi-Fi network. Criminals may hack the devices in the Wi-Fi network by using existing DNS vulnerabilities in the smartwatches. Moreover, some smartwatches are also vulnerable to a double-direct attack that is aimed at hijacking and controlling the victim's website traffic.

Insufficient encryption. Smartwatches may transmit and keep data of a sensitive nature in a cloud storage. Therefore, the proper configuration of transport encryption is of utmost importance for protecting the data that is sent and saved in a cloud. Although many smartwatches use SSL/TLS encryption, some devices have vulnerabilities related to transport encryption, e.g., using weak ciphers or being susceptible to a Poodle attack.

Privacy issues : In order to perform operations, smartwatches collect personal data, such as heart rate, gender, address, and workout data. Security professionals stress the importance of protecting this sensitive information and preventing it from being exposed publicly or used by third parties. The lack of security features of some smartwatches may facilitate crimes related to data theft. For example, only half of the smartwatches tested by HP Fortify Software Security Center had a screen protected by a PIN code or a pattern screen lock. Moreover, some of the smartwatches could be easily paired with another unfamiliar smartphone.

Issues of cloud and mobile interfaces : Some of the tested smartwatches utilize cloud-based interfaces that raise security concerns related to account enumeration. Moreover, security professionals warn that the mobile interfaces used by smartwatches are also insecure. As a result, user account credentials can be obtained through feedback received after requesting a password reset.

Concerns about software and firmware security : The majority of the tested smartwatches raise concerns about the security of their firmware. Although the manufacturers took measures for preventing installation of contaminated files, the research revealed that the transmission of firmware updates was not encrypted. This endangers the privacy of the users of smartwatches.

Ten tips for protecting your smart watch

Taking into account a number of smartwatch security vulnerabilities indicated above, it is important for both enterprises and consumers to take measures to decrease the privacy risks of smartwatches. On the one hand, smartwatch manufactures can make their customers' privacy a priority by: (1) building secure smartwatch software; (2) using applications that request strong passwords; (3) implementing a transport layer security; and (4) providing specifically designed mobile applications;

On the other hand, the users of smartwatches can prevent potential data leaks by implementing simple security measures that usually do not require a lot of time or sophisticates technological skills. Ten of such security measures for smartwatch consumers are further discussed below.

Researching before buying : Before

▶

purchasing any sophisticated device that collects sensitive personal data, it is of utmost importance to research security measures implemented by a vendor. For example, before splurging on a targeted smartwatch, it is useful to know (1) whether the smartwatch software offers a strong two-factor authentication, (2) what are the anti-virus features of the smartwatch, and (3) what types of data will be collected by the smartwatch.

Proper security configuration : In order to use the device in a safest manner, it is crucial to configure its security settings. Since most of the smartwatches allow managing their functionalities, the configuration should be conducted before starting to use the device. In order to protect their smartwatch to the maximum possible extent, smartwatch users should: (1) enable passcode, screen lock, and fingerprint functionalities, (2) activate two-factor authentication and encryption; and (3) turn off sensitive access control functions.

Installing security apps : Encryption is considered to be one of the most efficient tools for data security. If a smartwatch does not use encryption, then it is worth considering installing security apps that encrypt sensitive data. Installation of such apps may significantly reduce the possibility of information leaks. Since a smartwatch is connected with its parent device, usually a smartphone, the gadget can also take advantage of security measures installed in the phone. Thus, it is important to protect both devices.

Deleting data : The information that is outdated or unnecessary for the functioning of a smartwatch should be deleted from a device or any cloud storage. This step would reduce the chance of hacking attacks as well as other types of unauthorized use of data.

Rejecting unknown pairing devices : Since a smartwatch is capable to pair with several other devices, a user should reject any unknown or suspicious devices (e.g., smartphones) that request pairing with the smartwatch. This simple security measure can help to avoid hacking attacks, information theft, and malicious contamination.

Inspecting downloads : In order to avoid device infection with malicious code received through email attachments, it is important to take security measures regarding downloaded files. Such prevention includes: (1) not opening files from unknown senders; (2) deleting messages with suspicious titles; (3) scanning email attachments with anti-virus programs; and (4) not clicking on suspicious links. Moreover, it is important to be aware that malicious code and viruses can also be installed in applications downloadable in various app market places. Thus, it is useful to inspect their security before installing them on a smartphone or a smartwatch.

Updating with newest operational system. To avoid becoming a target for hackers, it is useful to upgrade the operational systems and software of both smartwatches and parent devices. This step may help to fix the security bugs that can be identified in earlier versions.

Disabling unnecessary sensors : Wearable devices have a number of sensors that can track the motion of their users, such as walking, running, or keystrokes while typing on a keyboard. Associate Professor Romit Roy Choudhury from University of Illinois claims that this "sensor data from wearable devices will clearly be a double-edged sword. While the device's contact to the human body will offer invaluable insights into human health and context, it will also make way for deeper violation into human privacy." For example, an app that is designed to disguise as a pedometer can gather user's confidential data, including email information, search queries, and other activity patterns.

Avoid performing important operations on a smartwatch. Avoid making online payments, money transfers, or submitting credit card information to reduce the chance of being hacked. Since most hacking attacks aim at obtaining sensitive financial data, the transaction information that is recorded in a device or stored in a cloud may be an attractive target for hackers.

Maintaining physical security : Last but not least, securing a smartwatch from being lost is also a good prevention method against information leaks. In addition to protecting the device from water, hazards, and animals, it is important to prevent the potential theft of the gadget. Although some manufacturers implement various theft prevention systems, such as activation lock when a smartphone is removed from a wrist, a user should be conscious about excessively demonstrating the smartwatch in public places or leaving the device unattended. Such negligence can lead not only to losing a gadget, but also to endangering user's sensitive information.

Conclusion

Although a smartwatch is a relatively new technological device, it is becoming a fashionable accessory. According to statista.com, the shipment of smartwatches has significantly increased in 2015 and currently reaches almost 25 million units worldwide. Thus, the expansion of a smartwatch market also influences an increasing attention to the security of these trendy devices.

The research conducted by HP in mid-2015 introduced the smartwatch user community to potential security vulnerabilities of this wearable gadget, including weak authentication, insufficient encryption, and insecure cloud and mobile interfaces. It is also worth mentioning that another study revealed that the Apple Watch and smartwatches running Google's Android Wear have certain security vulnerabilities. Trend Micro, the company conducting the study, concluded that: "Physical device protection across all smartwatches was found to be poor, with no authentication via passwords or other means being enabled by default. This would enable free access if the wearable was stolen. All devices apart from the Apple Watch failed to contain a timeout function, meaning that passwords had to be activated by manually clicking a button."

The results of the studies by HP and Trend Micro warned smartwatch producers and consumers about the privacy risks of the smartwatches. This article has proposed and discussed ten important tips that can significantly decrease such privacy risks ◙