Checking the Time: Exploring the Security and Potential Vulnerabilities of the Apple Watch

Lane Gramling, Keshawn Triplett

December 2018

Introduction

As of 2018, data on smartwatch unit sales worldwide indicate that the smartwatch is being adopted at an exponential rate of growth over the last 5 years, and looks like a primary contender for being the next device to grow out of the repertoire of the enthusiast and into the ubiquitous ecosystem of portable devices, joining tablets, smartphones, and laptops in enjoying widespread adoption. The Apple Watch remains the top-selling watch in the smartwatch market with over 46 million devices estimated to have been sold so far. Thus, its exploration into a new and uncharted territory of device, combined with its unique cases for portability and its blistering adoption rate, raise the call for a look into how this new avenue may be opening up new lanes of attack for malicious actors.

Background

Apple Watch Communications.

The Apple Watch uses three major methods of communication with wi-fi and bluetooth as primary network communication methods accompanying an electromagnetic wave interface used for sensing vitals data. The watch carries out its internet communications through wifi while independent of a parent phone, and otherwise makes use of it in ways to be expected of a typical wifi-enabled device. Bluetooth is used for communications between the watch and its parent device, and in particular leverages the Bluetooth Low Energy (BLE) protocol for its need to conserve power due to real-estate limitations impeding battery size. This also compliments with the watch's typical usage pattern, because the proportion of time it spends passively connected to the phone with low communication traffic is higher than that of an average Bluetooth device. When the watch's paired iPhone is near and Bluetooth is available, the watch leans on Bluetooth for internet communications passed between itself and the iPhone as a method for saving power. If this Bluetooth connection with the phone is not available, the watch then leans on wi-fi to handle its communication. This exchange is carried out seamlessly by means of the software network interface implemented in its operating system, watchOS. Additionally, there are Apple Watch models which can connect to cellular networks to handle communications, but this use case is regarded as a minority due to its inferiority to both wifi and BLE communications in satisfying the unique needs of the watch, compounded by the tiny portion of time where the watch is out of range of both a suitable wifi network and its parent iPhone for routing its communications through their BLE pairing. Security measures used in bluetooth communication with the watch's paired device are further detailed later in part C. Lastly, the electromagnetic wave interface is a physical interface on the bottom of the device which uses light in both the visible and infrared spectrum for much of its data collection on the wearer's vitals, including the heart rate of the wearer. To observe the heart rate of the wearer, the watch makes use of a technique called photoplethysmography, which is a technique that has emerged somewhat recently as a convenient method for measuring blood volume and blood oxygen level changes in by sending light wave pulses to observe blood flow and color in the skin tissue. This technology has been implemented in the Apple Watch by simply using green and infrared LEDs placed on the underside of the watch to serve as the source of the wave pulses.

A. Potential Attack Vectors and Security Risk

Analysis: iPhone-Apple Watch Relationship.

Because the Apple Watch's watchOS is built on top of the iOS core, it enjoys much of the reputable security track record that iOS is known for. This benefit is perhaps the biggest contributor to why the Apple Watch has been attributed the status as the most secure major device in the smartwatch market. Nonetheless, there are still weak points which raise areas of concern. Thus, we will first explore some key areas on the hardware and OS level. It should be noted that these weak points pose exceptionally greater risk when users do not take advantage of the extra security measures offered out-of-the-box in watchOS, such as its passcode and activation locks as immediate deterrents to unauthorized physical access, or its location tracking and remote deactivation capabilities to lock down its data if the owner happens to lose it or have it stolen.

The first of these weak points is in the communication link between the watch and its paired iPhone. There is a large amount of personal data communicated between the phone and watch, including messages, contacts, notifications, and even sensitive information like card credentials for Apple Pay and real-time vitals data from the watch's health monitoring. Fortunately for the Apple Watch, its foundation on iOS means that all communications between itself and its companion iPhone are carried out using TLS to securely transmit the data, guarding against eavesdropping, forgery, and other man-in-the-middle attacks. Furthermore, all health data is encrypted upon local storage, and remaining so through transmission and storage on iCloud servers if the feature is enabled by the user. Each of these measures mean that a third party's ability to eavesdrop on the device's communication is not nearly as simple as capturing the network activity from the watch, which is surprisingly the case with many competing smart watches produced even in the current market. However, this does not yet rule out a potential attack by an adversary capable of spoofing the identity of one of the endpoints to hijack communications from either the phone or the watch. Because a phone acts as a parent device to the watch upon which the watch is dependent, in addition to the limitations of watchOS, we will focus on the phone as the primary endpoint for further inspection within the scope of our analysis on Apple Watch-iPhone communications.

Apple Watch-iPhone Communication Link.

First, we will explore relevant aspects of the relationship between the Apple Watch and its parent iPhone. For a watch to pair with a phone, the process requires multiple steps of extensive authentication and identity verification. The two devices use a dedicated out-of-band channel for communicating public keys followed by a Bluetooth Low Energy shared secret, leading the watch to then display an animated pattern containing a visually encoded secret used for the pairing - similar in function to a QR code - which is finally captured by the iPhone's camera, completing the pairing authentication sequence. Assuming everything passes, the phone and watch pair and the watch enables its iPhone-dependent features. It is at this point that the watch begins to communicate the user's personal data. The watch also uses wrist detection that allows it to lock whenever removed from the owner's wrist, and an activation lock to remotely lockdown the device in the event that the device is lost or stolen. Additionally, only one iPhone may be paired to a watch at a given time. In the case that an iPhone is unpaired from an Apple Watch, the phone instructs the watch to remove all data associated with the phone before disconnecting from the phone. Further details on the watch's authentication scheme are provided in part C.

B. Attacks on Apple Watches

Targeted Attacks on Individual Watches

So far, our exploration of the Apple Watch's authentication scheme and iPhone communications carves us out enough room to take a moment and clarify our threat model for an attack following a scenario where an individual watch is chosen as a specific target. Below, we have proposed a minimum threat model.

Threat Model - Targeted Attacks

i. The owner has not already locked down the device using the remote Activation Lock.

The remote activation lock completely obstructs access by any entity and acts as the nuclear option for protecting the device from intrusion.

ii. The owner has not protected the device with a passcode lock or wrist detection lock.

These features drastically reduce the duration which a watch remains available while idle or unattended. (Note that if the passcode is disabled, Apple Pay marks any card credentials on the Watch as invalid, and thus unable to be retrieved in any form from the watch.)

Threat Model - Discussion

In this specification, satisfying the first point makes room for further assumptions to be made that the owner is unaware the device is being targeted for attack or jeopardized in some manner that may elicit a defensive action in response. Particularly in the case of a smartwatch, direct physical access to the device is nearly impossible as the wearer is highly likely to be cognizant of its presence or vulnerability to physical tampering -- leaving the obviously doomed prospect of meddling around the wearer's wrist as the only hope for physical access. As such, we work with avoiding direct physical access as a heavy consideration when formulating our attacks.

In the second point, these features differ from the first security measure by offering improved security while the device is experiencing typical use, while the first remains the nuclear option. Wrist detection is a feature that when enabled by the user, allows the Apple Watch to detect when it has been removed from the wearer's wrist, where it is then capable of automatically locking itself with a passcode. When enabled, this shuts out what would otherwise be the ripest opportunity for gaining direct physical access in a vulnerable state. When disabled, it is still important to be aware that the unlocked state of the device is unlikely to last long as the device will lock when out of range of its paired iPhone through BLE or of course when the owner inevitably realizes it is missing, adding a time constraint as another consideration in attacks relying on any sort of physical access.

Given this, our attack scenarios on targeted devices will require either zero physical access, or merely *proximal* physical access, which we categorize as access either within the same wifi network, within range of the target watch's BLE communicator, or the device is exercising access to cellular networks in some capacity.

Scenario I. Eavesdropping Attack

One possibility for an attack on a targeted watch while having proximal physical access is an eavesdropping attack. While the potential of an eavesdropping attack is severely limited by both iOS and watchOS' system-level use of TLS for all network communications over wifi, the possibility remains for detecting behavior indicative of communication between an Apple Watch-iPhone pair via TCP fingerprinting. This can prove useful for eavesdropping as, from what we can find, there is no specific enforcement of DNS servers supporting encryption, nor enforcement of HTTP proxying or VPN usage in public or otherwise insecure networks. In the Apple Watch's case, DNS queries made during API calls or web browsing can still be eavesdropped upon under the proper conditions.

Scenario II. Augmented Cell-tower Location Triangulation.

In the case of geolocation by an entity with the necessary resources, it is worth considering the augmentation that the Apple Watch provides in cell-tower geolocation capabilities. One fact that is immediately apparent is that in the vast majority of situations where a user is wearing an Apple Watch, it is the second cellular device (to their phone) being carried by the user. Given knowledge of the watch's owner in the case of law enforcement, for example, this provides a second device to reduce error in the geolocation process; likewise, it further narrows the possibilities when trying to track a user down by the simple fact that it is less likely to leave the user's person (either intentionally or unintentionally) than the user's mobile phone.

Widespread Targeting with Malicious Software

Widespread Targeting: Motivation.

By relaxing our focus from the scope of a targeted attack on a specific watch, the playing field begins to widen. If there is no desire to target a specific user/device, this means that a scenario such as the deployment of a malicious or misleading application to the App Store for indiscriminate users to download becomes the most ideal option. The most obvious vector for deploying malicious code to a watch is through an app that is voluntarily downloaded by the user onto their iPhone from the App Store. By developing an inconspicuous application for the iPhone to be used in concert with the Apple Watch via Apple's watchKit framework, this angle presents an avenue which is much more likely to go unnoticed, and is even likely to maintain the trust of the user for indefinitely long periods of time.

Scenario I. Augmenting a Hypothetical Data-collection Malware to Reach the Apple Watch.

To name one example of how this is feasible, Wang, Lu, et. al. demonstrated in *Jekyll on iOS: When Benign Apps Become Evil* that despite the App Store's track record of extensive vetting of its hosted apps, exploitative techniques can be used to alter the control-flow of an app's execution, allowing a piece of code to transform from a seemingly harmless gadget into something which is capable of carrying out an evil task, like maliciously collecting private data from the compromised device and sending it to a remote server -- in such a manner that is undetectable by Apple's apparent forms of code and program analysis used in vetting candidate apps. By leveraging this existing vector for distributing malicious code to iOS devices, a malicious actor can build an app which seems to innocently provide the user with some utility afforded by the watch, meanwhile quietly collecting more data behind the scenes than its apparent functionality necessitates, and continuously aggregating this data all to a remote server. Additionally, because the code is within an app that has been voluntarily downloaded and executed by the user under a perceived trust, this information can be tied to an identity either provided by the user explicitly or gleaned from what information about the user the app is otherwise privy to.

Scenario II. Motion Data and Side-channels.

To show how overly liberal collection and remote storage of a user's iPhone and Apple Watch data can be exploited beyond its raw form, we provide an example case of how side-channels are opened up by the expanded range of data afforded to an iPhone that is augmented with an Apple Watch. In Wang, Lai, and Choudhury's paper MoLe: Motion Leaks through Smartwatch Sensors, the researchers demonstrated that the turbulence recorded by the Apple Watch's motion sensor from the wrist during typing can be used as a side-channel to determine the keystrokes being made by a wearer using a keyboard, and reconstruct them into words with reasonable accuracy. If properly implemented, this could prove useful by enabling the adversary to determine information that victim is typing, and thus various pieces of personal information like interests for serving tailored ads tied to the user's identity, and of course the potential to leak sensitive information such as usernames and passwords, if the accuracy was honed enough. Fortunately for the victim, the technique relies on error correction with predictions to reduce noise and improve accuracy in word parsing/guessing enough that a piece of sensitive information that exists in a less predictable form, i.e. a sequence of digits such as a credit card number, would be difficult if not impossible to record with sufficient accuracy due to the lack of ability to use context characters in predicting uncertain ones.

As far as data collection, other Apple Watch data can be used for unethical marketing practices such as personalizing advertisements around the apparent health of the individual as determined through the vitals data. Of course, there are certainly a number of other insidious ways this data could be used against the benefit of the user that we will leave for the imagination.

C. Apple Watch Security Measures

In the Apple Watch, the security features and technology built for iOS are utilized. These security features serve to to help protect data on the device, as well as communications with its paired iPhone and the Internet. This includes technologies such as Data Protection and Keychain access control. With this, the user's passcode is also entangled with the device UID to create encryption keys. When a watch is paired with the iphone, an out-of-band (OOB) process is used to exchange public keys, followed by the Bluetooth Low Energy (BLE) link shared secret. Apple Watch displays an animated pattern, which is captured by the camera on an iPhone. The pattern contains an encoded secret that is used for BLE 4.1 out-of-band pairing. Once the Bluetooth Low Energy session is established and encrypted using some of the highest security protocol available in Bluetooth Core Specification, Apple Watch and iPhone exchange keys using a process similar to what is done in Apple's iMessage to ensure to utmost protection. After the keys have been exchanged, the Bluetooth session key is discarded, and all communications between Apple Watch and iPhone are encrypted using IDS, with the encrypted Bluetooth, Wi-Fi, and Cellular links providing a secondary layer of encryption. The BLE Address is rotated at 15-minute intervals to reduce the risk of traffic being compromised.

The secure boot chain, code signing, and runtime process security all help to ensure that only trusted code and apps can run on a device. To support apps that need streaming data, communications over BLE use the maximum level security protocol for protection of user data. The IDS service provided by the paired iPhone is used for internet connectivity. In order to keep the files of the watch protected, the Apple Watch enforces hardware-encrypted storage, plus class-based protection of files and Keychain items. Access-controlled keybags for Keychain items are also used. Keys used for communications between the watch and iPhone are also secured using class-based protection.

Key Security Features

Passcode Lock.

The most accessible method of protection for the watch is with the passcode lock setting. If you use the watch for Apple Pay, the passcode is required to be enabled, otherwise card credentials will not be accepted upon any attempts to use Apple Pay.

Passcodes can be 4-10 digits, thus exhibiting

$$\sum_{i=4}^{10} (10^i) \;==\; 11111110000$$

possible combinations for passcodes.

Erase Data.

The Apple watch offers the option to automatically wipe out the data of your smartwatch after 10 failed passcode attempts. This makes it more difficult for others to gain access to the watch through trying to brute force the passcode.

Activation Lock.

With activation lock active, anyone who finds or steals an Apple Watch will have to provide the associated Apple ID and password before it can be erased and used with a new iPhone. It also kicks in when someone attempts to unpair your watch from an iPhone or by attempting to disable the location feature. Therefore, unless they are able to pull your Apple ID and password out of thin air, the watch will essentially be a tiny useless brick.

Find My iPhone.

The Apple Watch is included in Apple's Find my Iphone service, allowing the user to view a map that will show the last known approximate location of the device using the last known *trusted* wifi connection.

D. User Survey

The purpose of our survey was to find what security features are actually utilized by users to keep their devices secure. We posed the survey to University of Kansas students that own an Apple Watch. The surveyed questions are listed below.

i. *How often do you wear your Apple Watch?*
ii. What type of Apple watch do you have?
iii. How long have you owned your Apple Watch?
iv. How Secure do you think your Apple Watch device is?
v. Do you have Password Lock enabled on your device?
vi. Do you have Erase Data enabled on your device?
vii. Do you have Activation Lock enabled on your device?
viii. Do you have Find my Iphone enabled on your device?

After getting results from 16 students, we found the following portions of people regarding their use of the security features:

87.50% of those surveyed have Password Lock enabled.
31.25% of those surveyed have Erase Data enabled.
75.0% of those surveyed Activation Lock enabled.
81.25% of those surveyed have Find my Iphone enabled.

Survey Results

These results tell us that a majority of the iPhone users surveyed take advantage of the security features offered by the Apple Watch. What we did find concerning was the number of participants that did not have Erase Data enabled on their devices. Without Erase Data enabled, users fall susceptible for their private data to fall into the wrong hands if their watch is lost or stolen. Erase data allows for all data to be wiped from the device after 10 failed passcode attempts. It leaves the watch more susceptible to password brute forcing. Our Hypothesis for why users may express an aversion to the erase data option is that due to its permanence and extremity, it is perceived as a nuclear option that many users may prefer to take the risk of avoiding rather than risk losing their data due to an event triggered by something seeming as simple to carry out as 10 failed passcode attempts. Compounding with that, the act of wiping the data is out of the control of the owner and rather in control of who is attempting to intrude into the device, which may be disconcerting to owners, and maybe even perceived by some as the attacker winning anyway, just by destroying the data of the device owner. Perhaps this is a limitation of the base security settings that could be improved on Apple's end, simply by re-evaluating the functionality of this option and the criteria for it to trigger.

E. Future Work

For this project, we were able to learn much about how secure Apple watches are. We found that they have many security features put into place to keep users privacy and data safe. However, we also learned that through some imagination the Apple Watch can be turned against the owner as an augmentation of malicious actions, namely data collection or spying, carried out against the owner of the Apple Watch under attack. Our future work with this project would include finding new attack vectors and vulnerabilities with the watches, or trying to carry out more attacks on the watches. One goal of ours moving forward is to choose one of these attacks to give a shot at an implementation of.

F. References

iOS Security Whitepaper - Released by Apple
https://www.apple.com/la/business/site/docs/iOS_Security_Guide.pdf

Communications for Wearable Devices
https://arxiv.org/ftp/arxiv/papers/1705/1705.03060.pdf

Smart Watches as a Web Technology: Android Wear
https://pdfs.semanticscholar.org/19e1/c2ffeed755e14683e289aa242f40d687a456.pdf

Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5038811/

Jekyll on iOS: When Benign Apps Become Evil https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_wang_2.pdf

I Am a Smartwatch and I Can Track my User's Arm
https://simbalab.cs.purdue.edu/papers/armtrak_mobisys16.pdf

MoLe: Motion Leaks Through Smartwatch Sensors
https://synrg.csl.illinois.edu/papers/mole.pdf

A novel method for accurate estimation of HRV from smartwatch PPG signals (Abstract only)
https://ieeexplore.ieee.org/document/8036774

Global Smartwatch Unit Sales 2014-2018
https://www.statista.com/statistics/538237/global-smartwatch-unit-sales/

Apple Watch Security Features
https://www.igeeksblog.com/apple-watch-security-features/

Smartwatch Security Fails to Impress - Top Devices Vulnerable to Cyberattacks
https://www.zdnet.com/article/smartwatch-security-fails-to-impress-top-devices-vulnerable-to-cyberattack/

Apple Watch Series 3 - Security Testing With Failed Attacks
https://www.iot-tests.org/2018/08/apple-watch-series-3/

Communicating With Your Smartwatch, Part I & II (Good article summarizing BLE & communications)
https://medium.com/@chris.coverdale24/communicating-with-your-smart-watch-part-1-what-is-blue-tooth-low-energy-b763cd9b0e80
https://medium.com/@chris.coverdale24/communicating-with-your-smart-watch-part-2-structure-of-communication-5b251afc2375