Report

Internet of Things Security Study: Smartwatches

Today's technology newcomer is the smartwatch, with a seemingly endless supply of buzz around its capabilities and promise. But from a security perspective, watches with network and communication functionality represent yet another attack surface area—potentially providing ways for someone to gain access to personal data or knowledge they should not have.

Gartner, Inc. forecasts that 4.9 billion connected things will be in use in 2015, up 30 percent from 2014, and will reach 25 billion by 2020

Gartner, Press Release, "Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015" November 2014,http://www.gartner.com/newsroom/id/2905717

Overview

For this study we evaluated 10 of the top smartwatches on today's market from an attacker's perspective. This includes looking at smartwatch management capabilities, mobile and cloud interfaces, network posture, and other elements that might also be exposed to attack.

The results of our research were disappointing, but not surprising. We continue to see deficiencies in the areas of authentication and authorization along with insecure connections to cloud and mobile interfaces. Privacy concerns are magnified as more and more personal information is collected (including health information). Issues with the configuration and implementation of SSL/TLS that could weaken data security were also present.

Methodology

Fortify on Demand used standard testing techniques that combine manual testing and verification along with automated scanning technology. Devices and their components were assessed based on the OWASP Internet of Things Top 10 and the specific vulnerabilities associated with each Top 10 category.

All data and percentages for this study were drawn from the 10 smartwatches tested. The numbers provided should prove a good indicator of the current security posture of smartwatches in general.

Research Findings

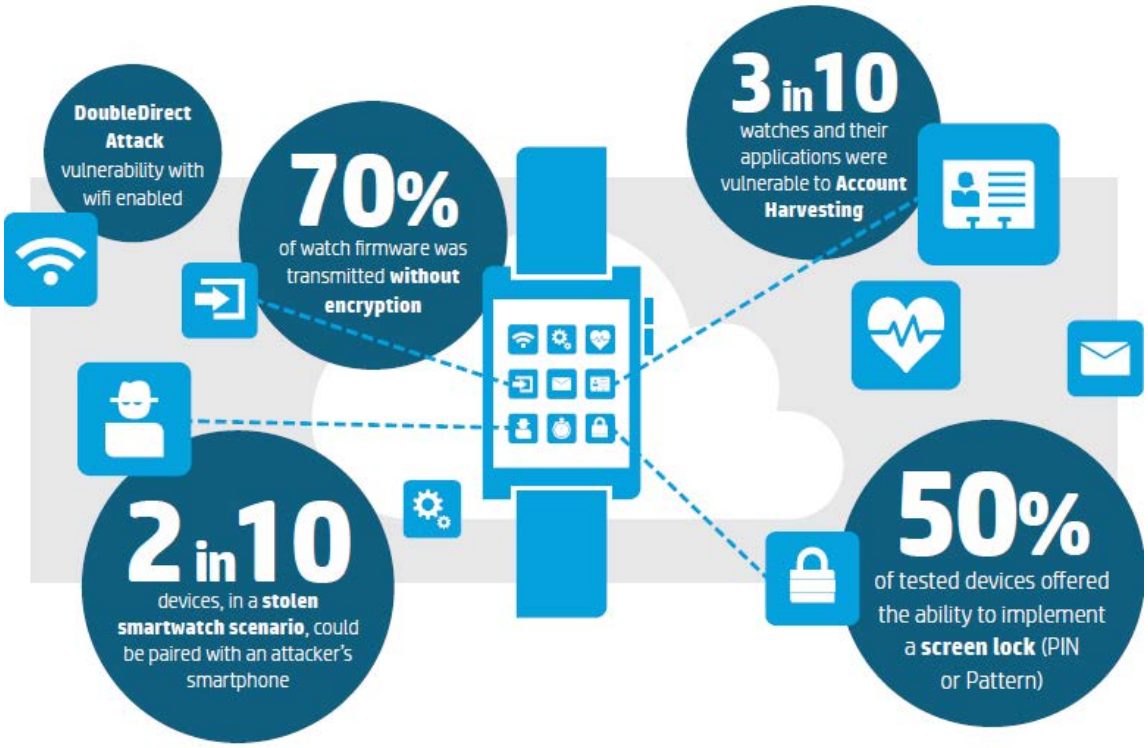
HP reviewed 10 popular smartwatches along with their paired Android or iOS mobile device and application.

Use cases for smartwatches include activity and health monitoring, messaging, email, checking schedules and the weather, among others. Whatever the functionality, they all depend on a mobile device to pass along that information to the watch. In this scenario, we are not only concerned with the security of the smartwatch, but also the security of the gateway mobile device.

Our research revealed some usual suspects, such as privacy issues, account harvesting, and firmware updates happening in the clear. What really surprised us was finding a running DNS service on one of the watches, which allowed it to be used as part of a DNS amplification attack.

Key Takeaways:

- Data collected initially on the watch and passed through to an application is often sent to multiple backend destinations (often including third parties)
- Watches that include cloud interfaces often employed weak password schemes, making them more susceptible to attack
- Watch communications are trivially intercepted in 90% of cases
- Seventy percent of watch firmware was transmitted without encryption
- Fifty percent of tested devices offered the ability to implement a screen lock (PIN or Pattern), which could hinder access if lost or stolen
- Smartwatches that included a mobile application with authentication allowed unrestricted account enumeration
- The combination of account enumeration, weak passwords, and lack of account lockout means **30% of** watches and their applications were vulnerable to Account Harvesting, allowing attackers to guess login credentials and gain access to user account



Insufficient Authentication/Authorization

An attacker can use vulnerabilities such as weak passwords, insecure password recovery mechanisms, poorly protected credentials, etc. to gain access to an application. Three smartwatches included both a cloud-based web interface and mobile interface which failed to require passwords of sufficient complexity and length. Two of the three smartwatches required only an eight character numeric password while the other only required an eight character alphanumeric password. All three systems also lacked the ability to lock out accounts after 3-5 failed attempts. These issues can all lead to Account Harvesting, allowing an attacker to guess login credentials and gain access to the system. None of the three offered two-factor authentication.

OWASP Internet of Things Top 10 – I2 Insufficient Authentication/Authorization

Insecure Network Services

Although 100% of the watches connected via Bluetooth to their parent device, only four offered the ability to utilize a WiFi connection for receiving notifications while away from the mobile device.

One product that incorporated WiFi had a functioning DNS server running on the smartwatch that allowed DNS Amplification attacks to be performed against other targets on the network. In addition to a DNS vulnerability, the same product was also vulnerable to the DoubleDirect attack, which is a man-in-the-middle attack utilizing the ICMP Redirect attack to view a victim's network traffic.

Only one other smartwatch was vulnerable to the DoubleDirect attack, but has since been patched to prevent this type of attack.

OWASP Internet of Things Top 10 – I3 Insecure Network Services

Lack of Transport Encryption

Transport encryption is crucial given that personal information is being transmitted to multiple locations in the cloud. While all products implemented transport encryption using SSL/TLS, we discovered that 40% of the cloud connections continue to be vulnerable to the POODLE attack, allow the use of weak cyphers, or still used SSL v2. Properly configured transport encryption is especially important since most of these products are transmitting data of a personal nature.

OWASP Internet of Things Top 10 – I4 Lack of Transport Encryption

Privacy Concerns

All smartwatches tested collected some form of personal information such as name, address, date of birth, weight, gender, heart rate (70%) and other health information. Exposure of this personal information is of concern, given the account enumeration issues and use of weak passwords on some products.

Additionally, we believe that coordinating a man-in-the-middle attack against a smartphone that is used in conjunction with a smartwatch would be an effortless operation, exposing personal information even when transport encryption is in use.

Only 50% of tested smartwatches offered the ability to enforce a screen lock, either by PIN or by Pattern, to help protect user data in the event the watch was lost or stolen. Two of the watches that had no PIN or Pattern screen lock protection

could be paired with an attacker's smartphone (without un-pairing from the owner's device) allowing all existing watch data to be synced to an attacker's smartwatch account.

OWASP Internet of Things Top 10 – I5 Privacy Concerns

Insecure Cloud Interface

Thirty percent utilized cloud-based web interfaces and all of those interfaces exhibited account enumeration concerns. Valid user accounts can be identified through feedback received from reset password mechanisms.

OWASP Internet of Things Top 10 – I6 Insecure Cloud Interface

Insecure Mobile Interface

Forty percent exhibited account enumeration concerns with their mobile application interface. Valid user accounts can be identified through feedback received from reset password mechanisms or from initial application setup and account creation.

OWASP Internet of Things Top 10 – I7 Insecure Mobile Interface

Insecure Software/Firmware

Seventy percent were found to have concerns with protection of firmware updates including transmitting firmware updates without encryption and without encrypting the update files. Many updates were signed, however, to help prevent the installation of contaminated firmware.

OWASP Internet of Things Top 10 – I9 Insecure Software/Firmware

Recommendations

HP has the following recommendations for those looking to use or produce smartwatch devices in a more secure manner:

Consumer

- Do not enable sensitive access control functions (e.g., car or home access) unless strong authentication is offered (two-factor etc).
- Enable passcode functionality to prevent unauthorized access to your data, opening of doors, or payments on your behalf.
- Enable security functionality (e.g., passcodes, screen locks, two-factor and encryption).
- For any interface such as mobile or cloud applications associated with your watch, ensure that strong passwords are used.
- Do not approve any unknown pairing requests (to the watch itself).

Enterprise Technical Teams

- Ensure TLS implementations are configured and implemented properly.
- Protect user accounts and sensitive data by requiring strong passwords.
- Implement controls to prevent man-in-the-middle attacks.
- Build mobile applications (specific to each ecosystem) into the device – in addition to any vendor-provided or recommended apps.

Conclusion

Despite their current limited footprint, smartwatches will likely replace smartphones as a convenient way to control communication and manage daily tasks. As watches become a common part of our daily workflow, we will likely use them for increasingly sensitive tasks like gaining access to our front door at home, entering and turning on our cars, and paying for purchases both in person and online. As this activity accelerates, the watch platform will become vastly more attractive to those who would abuse that access, and scrutiny will increase.

Our research shows that these wearables present a risk that goes beyond the device. The number of places that data are being sent during the standard use of a given application increases the number of access points. Whether using a health application, financial, or even gaming application, HP was able to intercept and detect the sensitive data being routed to multiple locations on the Internet.

This is often legitimate traffic destined for the authorized backend server, but in many cases the number of destinations is substantial, and it is worth questioning whether that many destinations are fully transparent to all parties involved, including the vendor who created the application and the consumer who will use it.

Learn more at
hp.com/go/fortifyresearch/iot