Report

How safe are home security systems?

An HP study on IoT security

Table of contents

The Internet of Things (IoT) will undoubtedly continue to make headlines in 2015, with the issue of security becoming more prevalent. Following up on the 2014 Internet of Things Research Study from HP that reviewed the security of the top 10 most common IoT devices, we now explore the security of some of the newest, connected home security systems. The simplicity and convenience of home security systems is unquestionable, especially with their remote monitoring capabilities. But do these smart security devices actually make our homes safer or put them more at risk by providing easier electronic access via an (insecure) IoT device?

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[1]

Overview

Connected home security systems offer a myriad of features including door and window sensors, motion detectors, video cameras, and recording mechanisms—all connected via the cloud to a mobile device or the Web.

In our ongoing research, we continued to see significant deficiencies in the areas of authentication and authorization along with insecure cloud and mobile interfaces. It is of particular concern to see these deficiencies in systems where the primary function is security.

While we discovered a significant increase in the use of transport encryption such as Secure Sockets Layer/Transport Layer Security (SSL/TLS), we also identified issues with the configuration and implementation that could weaken the data security normally provided by such encryption mechanisms.

Report findings

HP reviewed and performed security testing on ten off-the-shelf home security systems revealing an alarmingly high number of authentication and authorization issues, along with concerns regarding mobile and cloud-based Web interfaces.

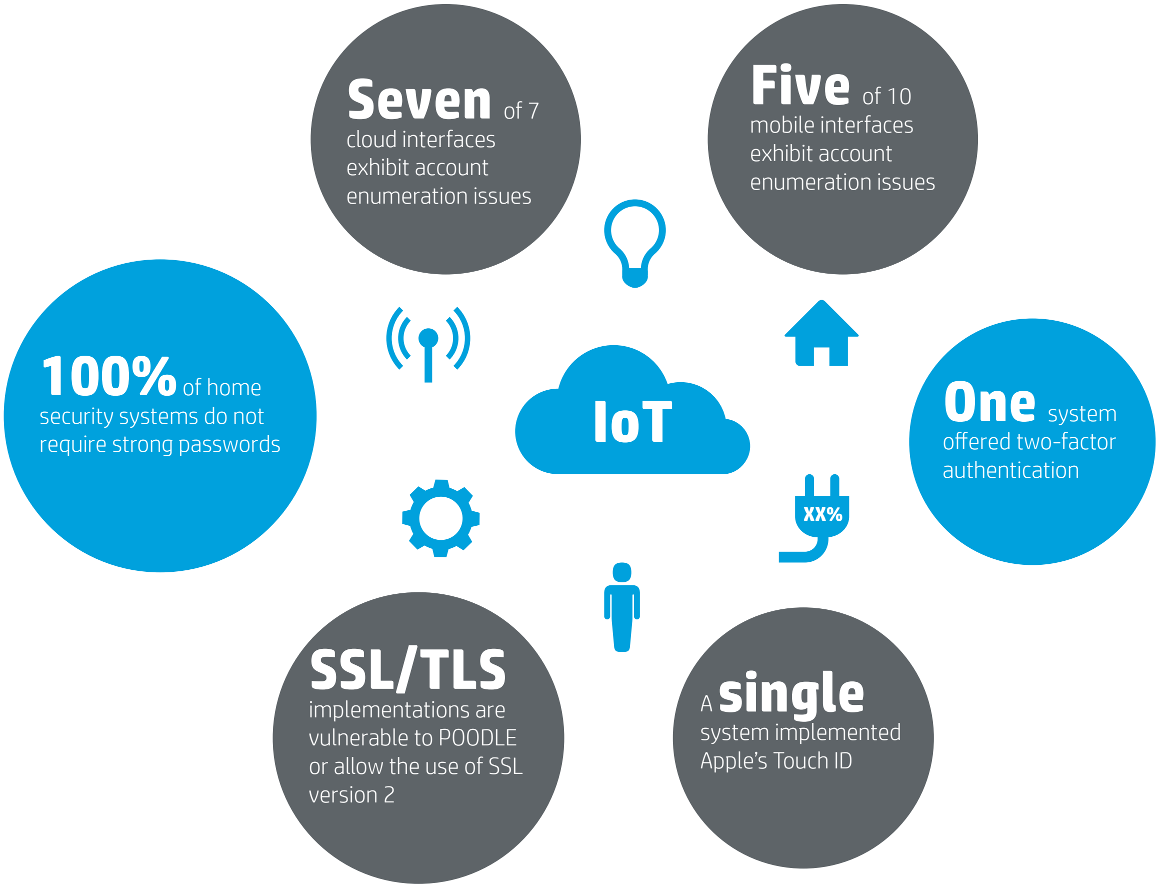
The intent of these systems is to provide security and remote monitoring to a homeowner, but given the vulnerabilities we discovered, the owner of the home security system may not be the only one monitoring the home.

Methodology

HP Fortify on Demand conducted the research using standard techniques to test the IoT systems, which combined manual security testing along with the use of automated tools. Devices and their components were assessed based on the OWASP Internet of Things Top 10 Project and the specific vulnerabilities associated with each top 10 category.

The resulting data and percentages in this report were drawn from the 10 IoT systems tested. While there are many more IoT devices currently on the market, we believe the similarity in results of the 10 devices provides a good indicator of where the market currently stands as it relates to security and the IoT.

[1] Gartner says 4.9 billion connected "things" will be in use in 2015, Gartner, November 2014. gartner.com/newsroom/id/2905717



Seven of 7 cloud interfaces exhibit account enumeration issues

Five of 10 mobile interfaces exhibit account enumeration issues

100% of home security systems do not require strong passwords

One system offered two-factor authentication

SSL/TLS implementations are vulnerable to POODLE or allow the use of SSL version 2

A **single** system implemented Apple's Touch ID

Insufficient authentication and authorization

An attacker can use vulnerabilities such as weak passwords, insecure password recovery mechanisms, poorly protected credentials, and other loopholes to gain access to a system. All systems that included their cloud-based Web interfaces and mobile interfaces failed to require passwords of sufficient complexity and length with most only requiring a six character alphanumeric password. Most systems also lacked the ability to lock out accounts after a certain number of failed attempts. These issues can all lead to account harvesting, which allows an attacker to guess login credentials and gain access to the system. A single system offered two-factor authentication and only one implemented Apple's Touch ID for authentication to the mobile application interface.

Moreover, many of these systems included the ability to add users to the system. Even if the new users are known (e.g., neighbors or family members), the additional accounts using weak passwords, which allow access to facilities such as video cameras, only raises the risk.

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

100 percent allowed the use of weak passwords

100 percent lacked an account lockout mechanism that would prevent automation attacks

100 percent were vulnerable to account harvesting, allowing attackers to guess login credentials and gain access

Four of seven systems that had cameras, gave the owner the ability to grant video access to additional users, further exacerbating account harvesting issues

Two of the systems allowed video to be streamed locally without authentication

A single system offered two-factor authentication

Lack of transport encryption

50 percent exhibited improperly configured or poorly implemented SSL/TLS

Transport encryption is critical for all communications that travel across the Internet in order to protect sensitive data such as credentials, personal information, device security settings, private video, and more. The importance of properly configured transport encryption is especially important since security is a primary function of these home security systems. While all systems implemented transport encryption using SSL/TLS, we discovered that many of the cloud connections are vulnerable to the POODLE attack and even allowed the use of SSL v2.

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

Insecure cloud interface

70 percent allowed unrestricted account enumeration through their cloud-based Web interface

Mobile application testing revealed that seven of the 10 systems made use of cloud-based Web interfaces and it was discovered that all cloud-based Web interfaces exhibited account enumeration concerns. Valid user accounts can be identified through feedback received from reset password mechanisms, credential input, and sign-up pages.

OWASP Internet of Things Top 10–I6 Insecure Cloud Interface

Insecure mobile interface

50 percent allowed unrestricted account enumeration through their mobile application interface

Five of the 10 systems tested exhibited account enumeration concerns with their mobile application interface. Valid user accounts can be identified through feedback received from reset password mechanisms and credential input.

OWASP Internet of Things Top 10—I7 Insecure Mobile Interface

Insecure software and firmware

60 percent indicated no obvious update capabilities and none offered any kind of automatic update functionality

Several systems had concerns with protection of firmware updates including transmitting updates without encryption and without encrypting the update files. In one instance, firmware was retrieved via FTP allowing the capture of credentials that would give an attacker write access to the update server. We did not find obvious update capabilities in six out of 10 systems and none offered any kind of "automated" update functionality which the user could trigger by means of an update button.

Three of 10 systems allowed the user to decide whether to accept or decline the latest firmware update when an update became available. None of the systems we tested indicated both the latest firmware date and version.

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

Privacy concerns

70 percent made video streaming available through their cloud-based Web interface or mobile application interface

All systems collected some form of personal information such as name, address, date of birth, phone number, and even credit card numbers. Exposure of this personal information is of concern given the account enumeration issues and use of weak passwords across all systems.

It is also worth noting that the use of video is a key feature of many systems with viewing available via mobile applications and cloud-based Web interfaces. These systems carry a concern with data privacy, as well as the privacy of video images from inside the home due to the use of video cameras.

OWASP Internet of Things Top 10—I5 Privacy Concerns

Conclusion

The Internet of Things continues to impress with both its promise and its offerings as we enter 2015. Products, services, and ecosystems around IoT will increasingly offer a wide range of benefits that can entice both consumers and businesses.

This research does not aim to dampen that enthusiasm but to inform users that these capabilities come with risks, and that it's in everyone's best interest to understand those risks before activating these systems.

Recommendations

HP has the following recommendations for those looking to implement IoT devices in a more secure manner:

Consumer

- Include security in the feature considerations when evaluating potential IoT product purchases
- Avoid using system defaults for usernames and passwords whenever possible, and choose good passwords when the option is available

Enterprise

- Implement segmentation between IoT devices and the rest of the network using a firewall or other filtering technology
- Configure supplemental security features (that may not be enabled by default); examples might include password strength policies, account lockouts, event logging, and two-factor authentication

Learn more at
hp.com/go/fortifyondemand

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-7342ENW, March 2015