Report

Internet of Things Research Study

Overview

Suddenly, everything from refrigerators to sprinkler systems are wired and interconnected, and while these devices have made life easier, they've also created new attack vectors for hackers. These devices are now collectively called the Internet of Things (IoT). IoT devices are poised to become more pervasive in our lives than mobile phones and will have access to the most sensitive personal data such as social security numbers and banking information. As the number of connected IoT devices constantly increases, security concerns are also exponentially multiplied. A couple of security concerns on a single device such as a mobile phone can quickly turn to 50 or 60 concerns when considering multiple IoT devices in an interconnected home or business. In light of the importance of what IoT devices have access to, it's important to understand their security risk.

The Internet of Things is here
Few revolutionary technologies have created new value pools, displaced incumbents, changed lives, liquefied industries, and made a trillion dollar economic impact. That is, until the Internet of Things (IoT) sprang to life. Today, the next big thing is embedding sensors, actuators and traditional low-power Systems on Chips (SoCs) into physical objects to link them to the digital world.

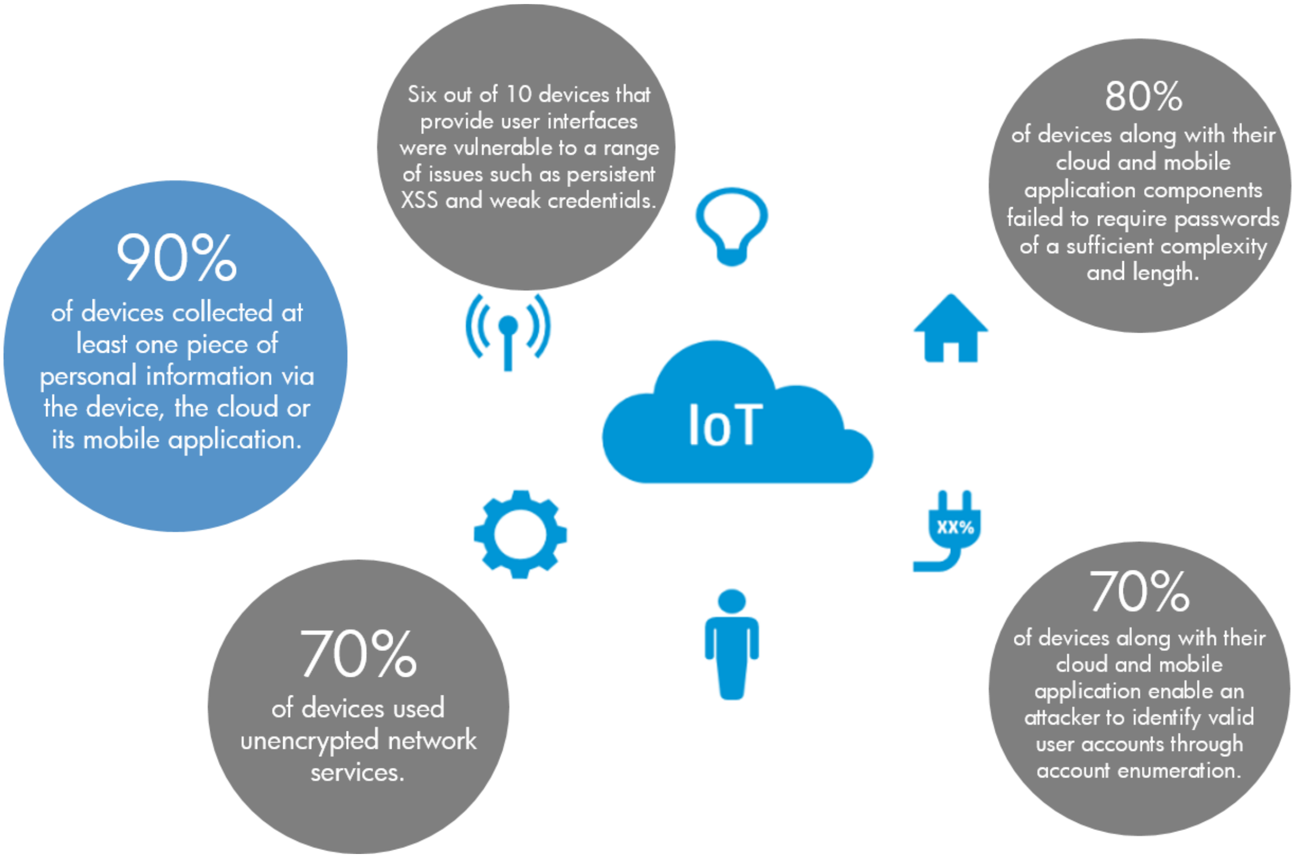
Report Findings

HP Security Research reviewed 10 of the most popular devices in some of the most common IoT niches revealing an alarmingly high average number of vulnerabilities per device. Vulnerabilities ranged from Heartbleed to Denial of Service to weak passwords to cross-site scripting.

Background on Devices

- Analyzed IoT devices from manufacturers of TVs, webcams, home thermostats, remote power outlets, sprinkler controllers, hubs for controlling multiple devices, door locks, home alarms, scales and garage door openers.
- A majority of devices included some form of cloud service
- All devices included mobile applications which can be used to access or control the devices remotely

Research Findings



Six out of 10 devices that provide user interfaces were vulnerable to a range of issues such as persistent XSS and weak credentials.

80% of devices along with their cloud and mobile application components failed to require passwords of a sufficient complexity and length.

90% of devices collected at least one piece of personal information via the device, the cloud or its mobile application.

70% of devices used unencrypted network services.

70% of devices along with their cloud and mobile application enable an attacker to identify valid user accounts through account enumeration.

Privacy Concerns

With many devices collecting some form of personal information such as name, address, data of birth, health information and even credit card numbers, those concerns are multiplied when you add in cloud services and mobile applications that work alongside the device. And with many devices transmitting this information unencrypted on your home network, users are one network misconfiguration away from exposing this data to the world via wireless networks. Cloud services, which we discovered most of these devices use, are also a privacy concern as many companies race to take advantage of the cloud and services it can provide from the internet. Do these devices really need to collect this personal information to function properly?

OWASP Internet of Things Top 10 – I5 Privacy Concerns

80% of devices raised privacy concerns

Insufficient Authentication/Authorization

An attacker can use vulnerabilities such as weak passwords, insecure password recovery mechanisms, poorly protected credentials, etc. to gain access to a device. A majority of devices along with their cloud and mobile components failed to require passwords of sufficient complexity and length with most allowing passwords such as “1234” or “123456”. In fact, many of the accounts we configured with weak

80% failed to require passwords of sufficient complexity and length passwords were also used on cloud websites as well as the product's mobile application. A strong password policy is Security 101 and most solutions failed.

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

Lack of Transport Encryption

Transport encryption is crucial given that many of these devices are collecting and transmitting data that can be considered sensitive in nature. We found that a majority of the devices failed to encrypt network services transmitting data via the internet and the local network. The importance of transport encryption rises significantly when you consider that data is being passed between the device and the cloud and a mobile application.

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

70% did not encrypt communications to the internet and local network

Insecure Web Interface

Six of the 10 devices we tested displayed concerns with their web interface. These concerns were issues such as persistent cross-site scripting, poor session management and weak default credentials. We identified a majority of devices along with their cloud and mobile counterparts that enable an attacker to determine valid user accounts using mechanisms such as the password reset features. These issues are of particular concern for devices that offer access to devices and data via a cloud website.

OWASP Internet of Things Top 10 – I1 Insecure Web Interface

60% raised security concerns with their user interfaces

Insecure Software/Firmware

Given that software is what makes these devices function, it was rather alarming that 60% of devices displayed issues including no encryption during downloading of the update along with the update files themselves not being protected in some manner. In fact some downloads were intercepted, extracted and mounted as a file system in Linux where the software could be viewed or modified.

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

60% did not use encryption when downloading software updates

Conclusion

A world of interconnected "smart" devices is here, albeit in the early stages. By 2020, Gartner predicts, the Internet of Things will be made up of 26 billion "units"[1]. Fortunately, there's still time to secure devices before consumers are at risk. Below are some actions that manufacturers of these devices can take now to secure these devices:

[1] Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020

Conduct a security review of your device and all associated components
This includes some fairly straightforward and simple testing such as automated scanning of your web interface, manual review of your network traffic, reviewing the need of physical ports such as USB, reviewing authentication and authorization and reviewing the interactions of the devices with their cloud and mobile application counterparts. To help in the review process an OWASP Internet of Things Top 10 site has been created to assist vendors with securing their products. After all it's better to find vulnerabilities on your own terms rather than having someone else find them for you.

Implement security standards that all devices must meet before production
There are many basic security controls which, once put in place, can raise the security posture of a device significantly. Many of the vulnerabilities identified as part of this research are considered "low hanging fruit" and are relatively easy to remediate without affecting the experience of your users.

Ensure security is a consideration throughout the product lifecycle
Implement security and review processes early on so that security is automatically baked in to your product. Updates to your product's software are extremely important and ensuring there is a robust system in place to support this is key. And when it comes to your products end of life, do your best to leave that product as secure as possible to both protect your brand and to be a good internet of things citizen.

Methodology

Fortify on Demand used standard testing techniques, which combined manual testing along with the use of automated tools. Devices and their components were assessed based on the OWASP Internet of Things Top 10 list and the specific vulnerabilities associated with each top 10 category.
All data and percentages for this study were drawn from the 10 IoT devices tested during this study. While there are certainly large numbers of IoT devices already on the market, and that number continues to grow on a daily basis, we believe the similarity in results of this subset provides a good indicator of where the market currently stands as it relates to security and the Internet of Things.

Learn more at
hp.com/go/fortifyondemand