SECURITY RESPONSE

Insecurity in the Internet of Things

Mario Ballano Barcena
Candid Wueest

Version 1.0 – March 12, 2015

> *All of the potential weaknesses that could afflict IoT systems, such as authentication and traffic encryption, are already well known to the security industry...*

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

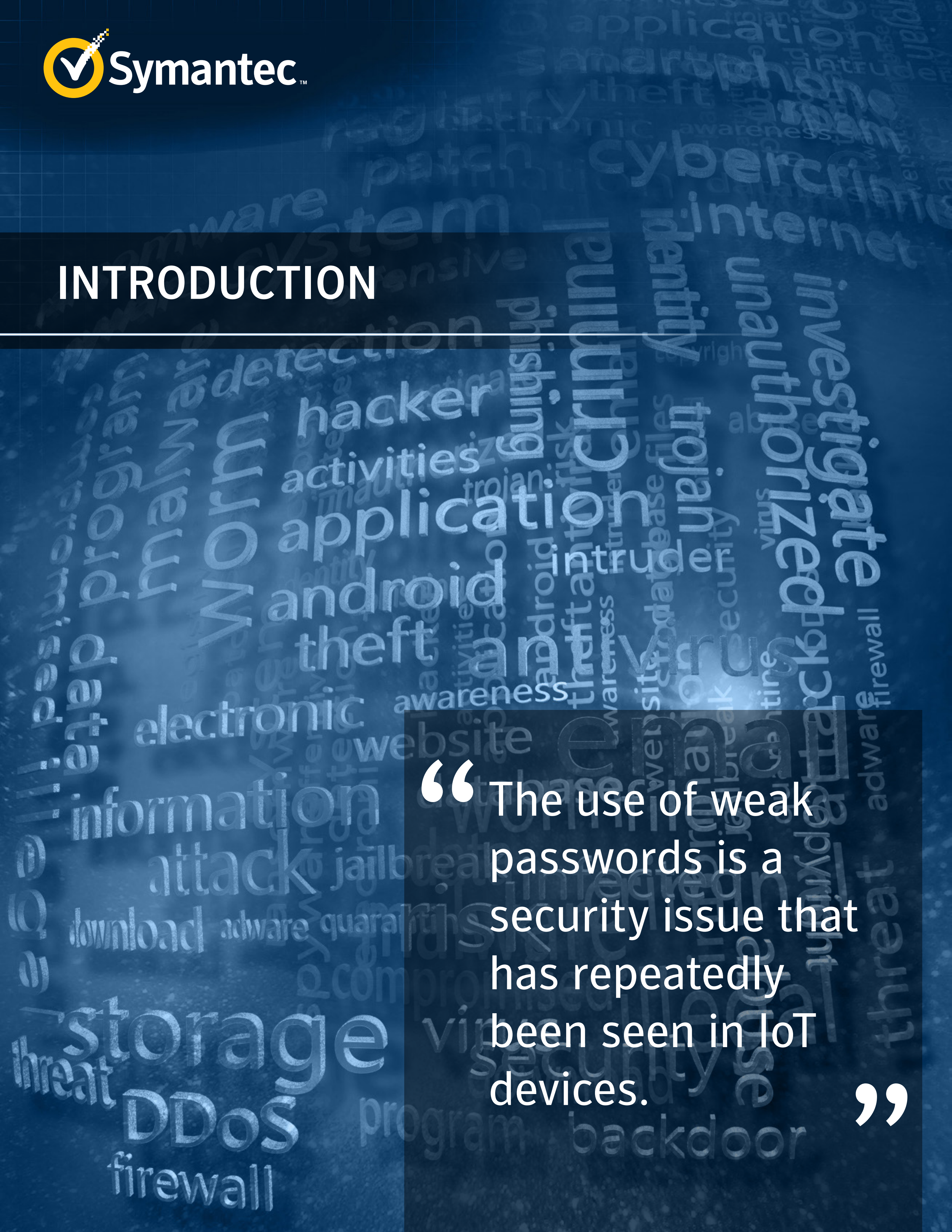
CONTENTS

OVERVIEW

The Internet of Things (IoT) market has begun to take off. Consumers can buy connected versions of nearly every household appliance available. However, despite its increasing acceptance by consumers, recent studies of IoT devices seem to agree that “security” is not a word that gets associated with this category of devices, leaving consumers potentially exposed.

To find out for ourselves how IoT devices fare when it comes to security, we analyzed 50 smart home devices that are available today. We found that none of the devices enforced strong passwords, used mutual authentication, or protected accounts against brute-force attacks. Almost two out of ten of the mobile apps used to control the tested IoT devices did not use Secure Sockets Layer (SSL) to encrypt communications to the cloud. The tested IoT technology also contained many common vulnerabilities.

All of the potential weaknesses that could afflict IoT systems, such as authentication and traffic encryption, are already well known to the security industry, but despite this, known mitigation techniques are often neglected on these devices. IoT vendors need to do a better job on security before their devices become ubiquitous in every home, leaving millions of people at risk of cyberattacks.



INTRODUCTION

> “The use of weak passwords is a security issue that has repeatedly been seen in IoT devices.”

Key findings

During our research, we found issues such as the following:.

- Around 19 percent of all tested mobile apps that are used to control IoT devices did not use Secure Socket Layer (SSL) connections to the cloud
- None of the analyzed devices provided mutual authentication between the client and the server
- Some devices offered no enforcement and often no possibility of strong passwords
- Some IoT cloud interfaces did not support two-factor authentication (2FA)
- Many IoT services did not have lock-out or delaying measures to protect users' accounts against brute-force attacks
- Some devices did not implement protections against account harvesting
- Many of the IoT cloud platforms included common web application vulnerabilities
- We found ten security issues in fifteen web portals used to control IoT devices without performing any deep tests. Six of them were serious issues, allowing unauthorized access to the backend systems.
- Most of the IoT services did not provide signed or encrypted firmware updates, if updates were provided at all

Introduction

Recent Gartner research predicts that there will be more than 2.9 billion connected IoT devices in consumer smart home environments in 2015[1]. These connected devices could provide a much larger surface for attackers to target home networks.

Currently, most proposed IoT attacks are proof-of-concepts and have yet to generate any profit for attackers. This does not mean that attackers won't target IoT devices in future, even if it is just to misuse the technology or have a persistent anchor in a home network.

The use of weak passwords is a security issue that has repeatedly been seen in IoT devices. These devices often do not have a keyboard, so configuration has to be done remotely. Unfortunately, not all vendors force the user to change the devices' default passwords and many have unnecessary restrictions which make the implementation of long, complex passwords impossible.

The Open Web Application Security Project's (OWASP) List of Top Ten Internet of Things Vulnerabilities sums up most of the concerns and attack vectors surrounding this category of devices:

- Insecure web interface
- Insufficient authentication/authorization
- Insecure network services
- Lack of transport encryption
- Privacy concerns
- Insecure cloud interface
- Insecure mobile interface
- Insufficient security configurability
- Insecure software/firmware
- Poor physical security

[1] Gartner Press Release, Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015, published November 11, 2014, http://www.gartner.com/newsroom/id/2905717

CONNECTED HOME DEVICES

> “With the Internet of Things (IoT) finding its way into the homes, there are lots of new devices that can connect to the same network.”

Connected home devices

There are many different smart home devices available on the market today, and the number is steadily increasing. For this paper, we looked at 50 different devices from the following categories:

- Smart thermostats
- Smart locks
- Smart light bulbs
- Smart smoke detectors
- Smart energy management devices
- Smart hubs

Our findings could also apply to other IoT devices and smart home products, such as:

- Security alarms
- Surveillance IP cameras
- Entertainment systems (smart TV, TV set-top boxes, etc.)
- Broadband routers
- Network attached storage (NAS) devices

Smart home devices may also use a back-end cloud service to monitor usage or allow users to remotely control these systems. Users can access this data or control their device through a mobile application or web portal.

Home network topology

Today's home networks are typically made up of a broadband router offering internet access to devices through Wi-Fi and Ethernet connections. Most of the devices that connect to these home networks include laptops, desktop computers, and mobile devices, such as phones and tablets. Everything is connected in the local network and can communicate freely with one another. Connections to the internet are directed through the central router, which may contain basic firewall filtering functionality.

With the Internet of Things (IoT) finding its way into the homes, there are lots of new devices that can connect to the same network. These devices can be classified in two basic categories. One category, which includes TV set-top boxes, uses already-existing networking technologies such as Wi-Fi and Ethernet connections. The other category, which includes sensors, may use different wireless technologies that better suit some of the devices' needs, such as lower energy consumption or ad-hoc network coverage. There is currently no single standard protocol in IoT.

As a result, we have seen IoT devices that support some of the following communication methods:

- Z-Wave
- Zigbee
- Powerline
- Bluetooth 4.0
- Other radio frequency (RF) protocols

Z-Wave, Zigbee and Powerline are the most common protocols used by home automation manufacturers at the moment. There are some hybrid solutions that use both Powerline and custom RF protocols. Among the smart hub devices that we tested, 66 percent offered Z-Wave and 48 percent offered ZigBee connectivity.

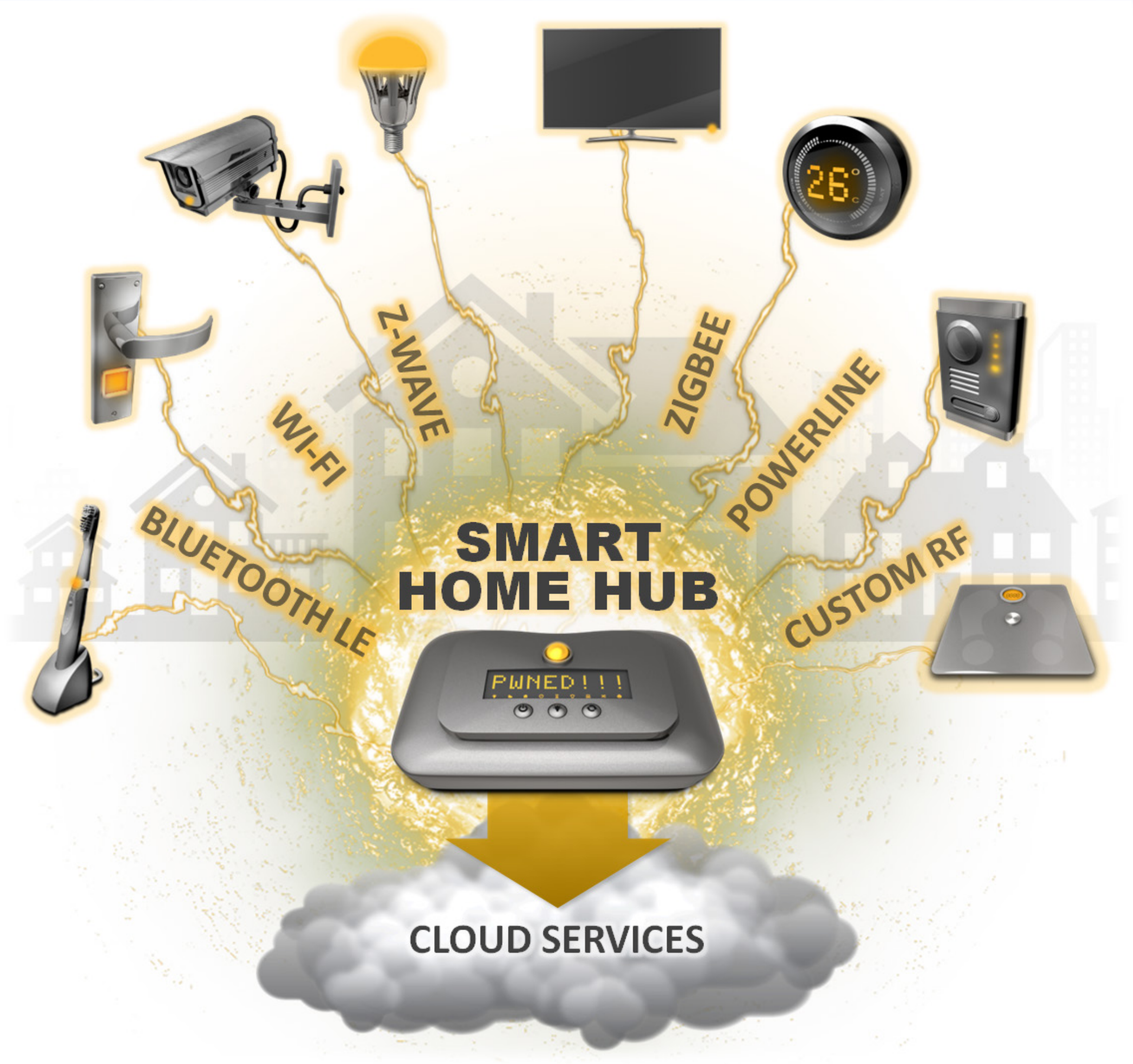


Figure 1. The smart home ecosystem

Devices that use a single wireless connectivity protocol often rely on a central hub device to handle the coordination of the communication. This could, for example, be a smart light bulb that can be switched on or off through a web portal running on a local hub. The user can access the web portal through their web browser and control light bulbs connected to the hub. Due to IoT's need to use simple integrations and the broad use of the IEEE 802.11 wireless standards, many new devices have switched to regular Wi-Fi for communication where possible.

Some classes of devices try to provide every possible option for connection. Out of all of the devices we looked at, 58 percent supported Wi-Fi connectivity.

Table. Features offered in analyzed IoT devices

Home device features	Number of analyzed devices that support feature	Percentage of analyzed devices that support feature
Supports Wi-Fi connections	29	58%
Supports Ethernet wired connections	18	36%
Offers a mobile phone application	42	84%
Uses a cloud service	34	68%

EXAMPLE ATTACKS

> “For our test, we used the precondition that the attacker has successfully cracked the Wi-Fi password and has access to the local network.”

Example attacks

In order to show how simple it is to conduct an attack against connected home devices, we will describe two of the attack scenarios that we performed during our tests. We used the LightwaveRF and Belkin WeMo smart hubs in these examples, though similar attacks are possible against other devices.

For our test, we used the precondition that the attacker has successfully cracked the Wi-Fi password and has access to the local network. We believe that this is a reasonable assumption to make, given that many people use weak passwords to protect their wireless network at home.

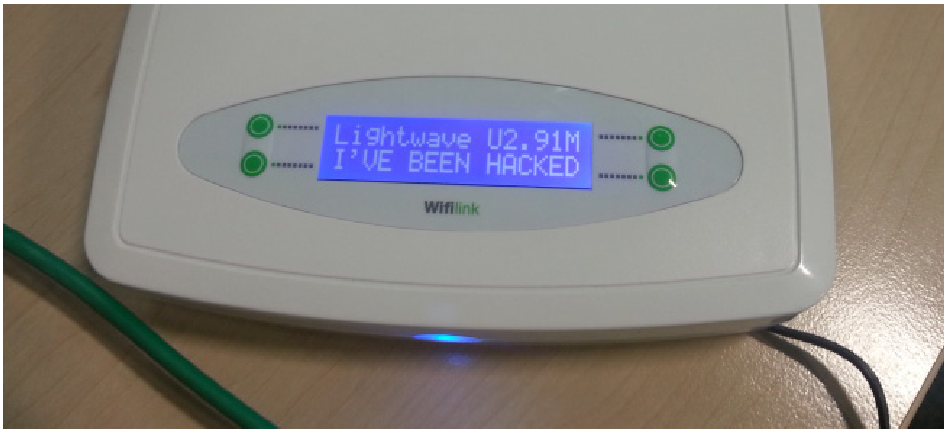


Figure 2. Smart hub device running modified firmware

By using a network sniffer such as Wireshark to analyze the network traffic, we noticed that the LightwaveRF smart hub generates certain network traffic each time it restarts and every 15 minutes to check for firmware updates. The device sends this traffic to a remote Trivial File Transfer Protocol (TFTP) server on the Internet. Since this connection is neither encrypted nor authenticated, it can easily be targeted by an attacker with access to the network, allowing them to conduct a man-in-the-middle (MITM) attack.

In our tests, we chose to use Address Resolution Protocol (ARP) poisoning to redirect the smart hub's request to our own TFTP server. Since the firmware update is an unsigned blob in a raw format, it is easy to unpack and modify it. Once the modified firmware update is served to the device and installed, the attacker gets full control over the smart hub device and could start attacking other connected devices from there.

In addition to this, attackers can sniff the RF link for command packets and replay them. With a smart hub that just turns devices on and off, it only receives a small number of different command packets. As a result, the attackers don't need to worry about breaking any pairing if they are close enough to the device to inject spoofed packets. This can allow them to take control of the targeted device.

Another attack example focuses on the Belkin WeMo connected switch. In this case, we analyzed the network traffic that was sent from the device's controller application. The device did not require the user to provide authentication in order to connect to it. If the attacker is on the same network as the device, they can send any commands they want to the connected switch.

Researchers have created publicly available modules for the penetration framework Metasploit that could give attackers a way to inject code in the Belkin WeMo connected switch. This could allow them to run commands as the root user on the switch. Along with this, the switch's firmware is encrypted with GNU Privacy Guard (GPG), but the private key has been extracted and shared on the internet. Attackers could target both of these issues and completely reprogram the switch. Researchers discovered further vulnerabilities in the switch last year, which have since been fixed by the vendor.

Attack surface

Attackers can intercept or change the behavior of smart home devices in many ways. Some methods require physical access to the device, making an attack more difficult to conduct. Other attacks can be carried out over the internet from a remote location. The following sections list the different attack scenarios based on the access level that the attacker may have.

Physical access

An attacker can gain the highest level of access to the smart home device if they get physical access to it. Although this might seem like an improbable attack vector, it is still a plausible threat. Your friends could gain physical access to your IoT device to play a prank while visiting you. An ex-boyfriend or girlfriend could attempt to reconfigure some of the devices while they still have access to the home. For some devices, such as security camera, an attacker could simply cut the cables to turn them off.

Another plausible physical access attack scenario takes advantage of the market for second-hand IoT devices. Some users might buy a used device off the internet in order to save some money, but could end up with a device that has been compromised to spy on people.

Smart home devices could also be compromised through supply chain hacks. In this scenario, attackers compromise a supplier company's network and Trojanize their software updates, allowing the threat to spread to any device that avails of the poisoned update. This is not a new scenario; we have seen attack groups conduct supply-chain attacks to spread their malware to traditional computers many times before, such as during some of the Hidden Lynx attackers' campaigns. Unfortunately, there is currently no easy way to verify that an IoT device has not been tampered with.

Having physical access to the device allows the attacker to alter configuration settings. These could include issuing a new device pairing request, resetting the device to factory settings and configuring a new password, or installing custom SSL certificates and redirecting traffic to a server controlled by the attacker.

Physical access may also allow a skilled attacker to read the device's internal memory and its firmware. They could do this by accessing programmatic interfaces left on the circuit board, such as JTAG and RS232 serial connectors. Some microcontrollers may have disabled these interfaces, but could still allow direct reads from the attached memory chips if the attacker solders on new connection pins.

Reading the internal memory and reversing the firmware allows an attacker to better understand how a device works, allowing them to find vulnerabilities, cryptographic key materials, back doors, or design flaws that could be used to perform further attacks. If the attacker gains a full understanding of the firmware, they could use this knowledge to create their own malicious version of the firmware and upload it to the device. This could give the attacker full control over the device. This act of reflashing the device may be conducted through the JTAG or RS232 connection.

Most new devices offer ways for users to update the firmware throughout the lifecycle of the device. These updates could arrive through a USB connection, an SD card, or over the network. The majority of tested devices did not use encrypted nor digitally signed their firmware updates, making it easy for an attacker to generate a valid, malicious firmware update that could be installed.

Local attacks over Wi-Fi/Ethernet

An attacker with access to the local home network, either wirelessly or through an Ethernet connection, is able to perform various attacks against smart home devices. There are generally two common modes of for smart home devices: cloud polling and direct connection. Depending on the function, the device may use either of these methods to receive commands.

Cloud polling

In the case of cloud polling, the smart home device is in constant communication with the cloud. The device checks the cloud server to see if there are any commands to be executed and then uploads its current status. The device may use this method if it wants to keep polling the cloud server to check if there is a new firmware version available that needs to be downloaded and installed.

Attackers may need to perform an MITM attack to target such an implementation. For this to succeed, the attackers can try and redirect network traffic with network-level attacks, such as ARP poisoning or by modifying the domain name system (DNS) settings. A self-signed certificate or tools such as SSLstrip can help attackers intercept HTTPS connections.

Unfortunately, some of the tested devices do not verify if the certificate is trusted and belongs to the vendor at all—they approve of the connection as long as it's done over HTTPS. To make matters worse, none of the tested devices perform a mutual SSL authentication, where both sides authenticate with one another instead of just the server authenticating with the client. Most devices completely ignore certificate revocation lists, allowing an attacker to use keys that were obtained through a data breach without any problem.

Direct connection

Some devices use direct connections to communicate with a hub or application in the same network. For example, a mobile app may be able to scan the local network for new devices and locate them by probing every IP address for a specific port. Another method is to use the Simple Service Discovery Protocol/Universal Plug and Play (SSDP/UPNP) protocol to discover the devices. This means that any attacker could do the same to easily find these devices.

A common mistake that we've seen in these devices is the use of unencrypted network communications. Almost two out of ten (19 percent) of the tested devices communicate to their back-end cloud service or application without encryption, such as SSL. For communications in the local network, the number of unencrypted connections is even higher. The lack of encryption raises a major privacy concern. Devices may pass personal data, login credentials, or tokens in clear text, letting an attacker intercept them.

The most common method for users to interact with an IoT device is through a web browser or a smartphone app. More powerful devices run a small web server and allow the user to use a web-based GUI to send commands. Other devices offer their own application programming interface (API) that the user can interact with. If the user wants to remotely control the devices when they're not at home, then they need to be able to open an inbound port at the router. This may be done through a UPNP request or may be manually implemented by the user.

Many of these interfaces have been found to be vulnerable to common and known types of vulnerabilities, including the following:

- Use of unauthenticated requests to perform actions (for example, reconfiguration, data retrieval, management functions, etc.)
- Ability to perform unrequested firmware upgrades
- Command injections
- Buffer/heap overflows
- OWASP's List of the Top Ten Web Vulnerabilities:
    - Infection flaws
    - Broken authentication
    - Cross-site scripting (XSS)
    - Insecure direct object references
    - Security misconfiguration
    - Sensitive data exposure
    - Missing function-level access control
    - Cross-site request forgery (CSRF)
    - Use of components with known vulnerabilities
    - Invalidated redirects and forwards

Cloud infrastructure attacks

A smart home device may include a back-end cloud service, depending on the category of the device. In our tests, 68 percent of the devices offered a cloud service. Such a service could be used for statistical purposes, such as logging the home's electricity usage or CO2 levels over a number of months. Other cloud systems allow the remote management of IoT devices, such as light bulbs or heating. Some vendors even force the user to connect to their cloud back-end system and do not provide users with the option of locally managing their devices. The companies either provide access to the cloud service through a smartphone application or a web portal, where users can log in.

Unfortunately nearly all of the tested IoT cloud services allow the user to choose weak passwords, such as "1234". Even worse, many services prevent the user from using strong passwords with a sufficient level of complexity, due to unreasonable restrictions. One service, for example, restricted the user to a PIN code with a maximum length of four numbers. This makes it easy for any attacker that knows the user's email address to brute-force their PIN code and take over their account.

Most of the analyzed services don't lock users out of their accounts after a number of failed login attempts, further allowing attackers to brute-force accounts. None of the analyzed back-end cloud services provided the option of two-factor authentication (2FA).

Some of the cloud interfaces have an unsecure password recovery method or reveal too much information during the recovery process, such as displaying the validity of an account. This could lead to account-harvesting attacks, which may allow the attackers to take control of the IoT devices and gather the users' personal data.

All of the tested cloud management consoles used SSL encryption for communications. The servers were patched against the OpenSSL Man in the Middle Security Bypass Vulnerability (CVE-2014-0224), more commonly known as the Heartbleed bug. Unfortunately, some of the services were still vulnerable to the SSL Man In The Middle Information Disclosure Vulnerability (CVE-2014-3566), also known as the Poodle bug, and allowed the use of weaker cipher methods.

Some cloud services have logical errors, which could allow an attacker to obtain sensitive customer information or access devices without authentication. These services also contained common management console vulnerabilities, including those listed in OWASP's List of the Top Ten Web Vulnerabilities. While observing network traffic for 15 applications, we found and reported ten vulnerabilities related to cross-site scripting (XSS), path traversal, unrestricted file uploading (remote code execution), and SQL injection. One of the tested cloud console was for smart locks, so this vulnerability could have allowed anyone to remotely open the locks.

For example, we found that one cloud management console was susceptible to a blind SQL injection attack. This allows an attacker to read the console's database, which contained the login credentials for other users. Once the attackers obtains the credentials, they could use them as part of a simple script that sends requests to turn off connected devices or delete entire accounts altogether. We informed the vendor and the issue has now been patched. The most concerning part is that these web management platforms are accessible to everyone over the internet. Attackers could gain unauthorized access to these services without needing local access to the home network. Our research in this area has only scratched the surface, the relevant cloud service vendors would need to conduct full web application tests in order to find all of the potential issues in their devices and services.

Malware

Malicious software installed on any device connected to the home network could have the ability to interact with smart home devices and let the attacker perform the attacks as previously described. Most likely, a compromised smartphone or computer could be used to attack other devices. One of the biggest concerns is that an infected IoT device would remain compromised for a very long time, as there is currently no integrated security software that could detect it and no user interface that could inform the user of any issues.

Fortunately, as of now, we have not seen widespread malware attacks against IoT devices. The news report about spam-sending fridges turned out to be untrue, but technically, it is possible. Proof-of-concept malware has been developed for IoT devices, such as smart TVs. Furthermore, we have seen malware attacking routers, NAS, and similar devices for a while now.

It is just a matter of time until attackers find a way to profit from attacking IoT devices. This may lead to connected toasters that mine cryptocurrencies or smart TVs that are held ransom by malware. Unfortunately, the current state of IoT security does not make it difficult for attackers to compromise these devices once they see the benefit of doing so.

Mitigation

Unfortunately, it is difficult for a user to secure their IoT devices themselves, as most devices do not provide a secure mode of operation. Nonetheless, users should adhere to the following advice to ensure that they reduce the risk of these attacks:

- Use strong passwords for device accounts and Wi-Fi networks
- Change default passwords
- Use a stronger encryption method when setting up Wi-Fi networks such as WPA2
- Disable or protect remote access to IoT devices when not needed
- Use wired connections instead of wireless where possible
- Be careful when buying used IoT devices, as they could have been tampered with
- Research the vendor’s device security measures
- Modify the privacy and security settings of the device to your needs
- Disable features that are not being used
- Install updates when they become available
- Use devices on separate home network when possible
- Ensure that an outage, for example due to jamming or a network failure, does not result in a unsecure state of the installation
- Verify if the smart features are really required or if a normal device would be sufficient

Manufacturers of smart home devices should ensure that they implement basic security standards at the very least:

- Use SSL/TLS-encrypted connections for communication
- Mutually check the SSL certificate and the certificate revocation list
- Allow and encourage the use of strong passwords
- Require the user to change default passwords
- Do not use hard-coded passwords
- Provide a simple and secure update process with a chain of trust
- Provide a standalone option that works without internet and cloud connections
- Prevent brute-force attacks at the login stage through account lockout measures
- Secure any web interface and API from bugs listed in the OWASP List of Top Ten Web vulnerabilities
- Implement a smart fail-safe mechanism when connection or power is lost or jammed
- Where possible, lock the devices down to prevent attacks from succeeding
- Remove unused tools and use whitelisting to only allow trusted applications to run
- Use secure boot chain to verify all software that is executed on the device
- Where applicable, security analytics features should be provided in the device management strategy

CONCLUSION

“Any code that is run on a smart device, be it the firmware or application, should be verified through a chain of trust.”

Conclusion

Our analysis of 50 smart home devices painted a disturbing picture. Despite an almost constant stream of media reports of cyberattacks and hacking incidents, there are still many devices that do not use encrypted communications or proper authentication. It is crucial that smart home devices, or any IoT devices for that matter, use mutual authentication and encryption. IoT devices often have less memory and slower CPUs, so they may be unable to use the same encryption methods as a traditional computer does, but that is no excuse for the lack of strong encryption. There are efficient cryptographic methods designed for small scale devices, such as Elliptic Curve Cryptography (ECC), which can be used.

Concepts such as roots of trust and secure boot are important to ensure the integrity of the device. Any code that is run on a smart device, be it the firmware or application, should be verified through a chain of trust. Protecting the code and securing the device creates a trusted baseline.Vendors should provide a simple and automated way for users to update their device in order to ensure that common security issues can be fixed quickly and efficiently. IoT devices should only accept signed firmware as standard. Where applicable, security analytics features should be provided in the overall device management strategy.

Cloud control interfaces present another weak point of many IoT. Users should not be forced to use cloud setups if all they want to do is to do basic tasks such as turning on the lights in their homes. Vendors need to allow strong, complex passwords to be used. Restricting authentication to simple four-digit PIN codes does not sufficiently protect the device, especially if this issue is combined with the lack of any brute-force protection mechanism. Even when strong passwords are use, we found that common web application vulnerabilities, such as SQL injection or remote file inclusion, are often present in these cloud control portals as well. Vendors need to ensure that their services are not vulnerable to the OWASP’s top ten web application vulnerabilities.

For IoT devices such as smoke alarms, it is also crucial that the vendor has considered what happens when there is a power outage or the network gets jammed. Will the user be notified or will the malfunctioning safety device go unnoticed?

In the near future, a lot of people could have a variety of devices connected to their home networks. This will lead to smarter smart hubs that allow commands based on logical conditions, such as “if this, then that”. This adds to the complexity of the problem, as now a problem in one device can trigger the shutdown of another. There are already applications available which allow you to do exactly this. In order to perform the actions, the application needs to be authorized to access the smart devices. This makes the smart hub an ideal central point of attack, as changing such rules could have a catastrophic effect on all devices connected to the network.

With all of these issues affecting the devices on different levels, it is currently not easy to deploy multiple smart devices in a secure fashion at home. Fortunately, there are ways to improve the overall security, as we highlighted above. Symantec hopes that the security of smart devices will increase in the near future, allowing anyone to conveniently use this technology to automate tasks at home.

APPENDIX

Appendix

In this section, we assess the security of some of the common IoT technologies. For the purpose of this assessment, we assume that the attacker is within range of the device's wireless transmission and can interact with it. These attacks can be achieved from outside of the building, for example in a parking lot, with an antenna. Some of the attacks require the attacker to be on the same local wireless network. All of the following technologies mentioned are potentially prone to radio jamming, allowing an attacker to disrupt connectivity to the device.

IoT wireless protocols are potentially vulnerable to the following attacks:

- Sniffing network traffic
- Injection
- Tampering/forging
- Jamming
- Exhaustion of battery
- Collision and Unfairness (link layer)
- Greed, homing, misdirection, black holes (network layer)
- Flooding, desynchronization (transport layer)

Wi-Fi networks (802.11)

Getting access to the home's Wi-Fi network allows an attacker to perform attacks against any connected device. The Wi-Fi standard Wired Equivalent Privacy (WEP) is considered to be insecure and should not be used. Even though Wi-Fi Protected Access II (WPA2) encryption is widely adapted, attackers can still brute-force weak passwords with a dictionary attack and get access to the network. Some broadband providers do not allow the user to change the Wi-Fi password, potentially helping attackers to brute-force accounts. Some vendors use Wi-Fi Protected Setup (WPS), which has long been found to be vulnerable to WPS PIN brute-forcing.

Some manufacturers implemented client isolation security mode for Wi-Fi access points, but internet providers don't usually enable this option in home routers to allow devices to interoperate within a home network. As a result, devices connected to the network can typically access each other, not just the gateway, which is a good and desired layout.

Z-Wave protocol

The Z-Wave protocol itself is considered to be secure. However, researchers have previously found implementation flaws affecting specific manufacturers that allowed them to take full control of devices in Z-Wave networks.

"This vulnerability was not due to a flaw in the Z-Wave protocol specification, but because of an implementation error in disabling the use of temporary key after initial network key exchange during inclusion of a node to the network," stated the research paper's authors Behrang Fouladi and Sahand Ghanoun.

Similar implementation pitfalls may affect other smart home device manufacturers.

ZigBee

Similarly to Z-Wave, the ZigBee protocol is considered secure from its ZigBee PRO version onwards. There have been some security concerns regarding support for plain text over-the-air (OTA) key exchange in certain profiles, which is meant to be used by manufacturers when provisioning units for the first time. Researchers have found that certain manufacturers have misused this feature.

Another security concern lies in the protocol's shared network key. By stealing one of the nodes of a ZigBee network, an attacker could dump the node's internal memory and retrieve this network key, giving them access to the network. Such a scenario may be particularly dangerous in certain configurations used for home networks that have sensors deployed outside of the house, such as an external lamp.

Powerline

The two main home automation protocols that make use of Powerline are:

- X10 (also supported over RF)
- Insteon (A hybrid of RF and Powerline)

One of the main concerns around these Powerline protocols is that signals can easily bleed over to the the next connected networks, allowing people near the network, such as neighbors, to spy on these communications. In order to counter this, these protocols and other Powerline-based systems typically support encryption.

Bluetooth Low Energy

Bluetooth Low Energy, also known as Bluetooth Smart, is often used for smart home devices that do not require an internet connection, such as door locks or light bulbs. Users can typically control these devices using a mobile phone and a dedicated app.

The Bluetooth Smart standard is quite flexible and leaves space open for faulty implementations that could allow attackers to remotely control these devices. For example, recently, the Bluetooth LE implementation of a wearable fitness bracelet had been completely reverse-engineered, allowing exposing the device to attack.

Other RF protocols

Some vendors have implemented their own radio protocol for their devices. This may result in protocols that are vulnerable to similar attacks, as with the previously described standards. For example, LightwaveRF is considered to be vulnerable to replay attacks.

Authors

Mario Ballano Barcena
Sr Threat Analysis Engineer

Candid Wueest
Principal Software Engineer

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings -- anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenues of $6.7 billion.

To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/social/.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY . The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.