How to Ensure That Your Home Automation System Is Secure

By Taylor Ampatiellos

Abstract

The invention of the remote control was surely a momentous occasion. No longer would consumers have to get up and cross the room to change the channel – now they could do so without even leaving the couch! Technology that makes life at home easier has been progressing rapidly over the past few decades, and in today's modern society most homes will have multiple devices connected to the "Internet of Things". From light switches that can be controlled from miles away to security cameras that can be viewed on an iPad while a person's at work, the average home is quickly becoming an interconnected hub of small network-enabled devices. While these devices and systems may make life much easier for the consumer, with any network device comes the possibility of threats from outside parties. An outside party controlling your lights may only be seen as a nuisance, but what happens when someone can put your heating bills through the roof while you're away, or can unlock all of your doors with a simple button press on their phone? In this paper I intend to analyze multiple examples of insecure home automation systems with the intention of informing the average consumer on how they can best choose/implement one of these systems to ensure that their home is safe and data is secure.

Introduction: What exactly *is* the "Internet of Things"?

The internet of things, often referred to as the IoT, is the conglomeration of a wide variety of devices, all of which share one thing in common: network connectivity. While in the past this only referred to computers, with each passing year more and more items are being given access to the internet. Phones, televisions, and media players are obvious additions to the IoT, but more recently there have been many unique devices being given network connectivity. Webcams, light switches, and thermostats are all examples of the IoT branching out in innovative new ways. With the IoT growing so quickly, it is becoming increasingly difficult to keep these devices secure.

The IoT is "growing faster than the ability to defend it." [1]

The internet of things is expanding at an alarming rate, and there are both pros and cons to this situation. On one hand, the IoT is an incredible testament to the technological advancements of our civilization, with many IoT devices making our lives easier and safer. Unfortunately, it would seem that the producers of IoT devices care more about these advancements (and the money made from them) than they do about the security of these devices. "The losses involved are so small compared to the revenue that it's easier to take a chance and write off any losses should they occur. In other words, worrying about data breaches isn't worth it to them." [2] While it is true that cutting corners on security and just accepting the risks can save a company money, it has a devastating effect on the individuals whose systems are attacked and exploited due to lack of security.

Having an insecure IoT device in a home is one matter, but what happens when a device is part of a system intended to keep the home secure? The IoT has made its way into home automation systems -- devices that can remotely control light switches, door locks and motion detectors, and perform a wide range of security-oriented tasks. When designed poorly, these systems can be the most dangerous IoT devices to have in a home, providing a sense of security while in fact making it even easier for a tech-savvy attacker to cause havoc.

To the Community

Not all home automation systems are created equal. The true security of these systems can vary greatly, and it can be difficult for the average consumer to determine which ones are the safest to use. The goal of this document is to explain some of the prevalent shortcomings in the home automation systems of today, and to outline the key ideas that should be considered when purchasing or implementing one of these systems. This paper contains examples of insecure systems from not only this year, but from within the past few years as well. This should emphasize that issues with home automation security are in no way new – this has been a problem for many years.

Why should you care?

Having an insecure IoT home automation device in a home can have many different consequences, ranging in levels of severity. A simple attack could be someone exploiting a vulnerability in a light-controlling system and becoming a nuisance by flipping lights on and off at their discretion, whereas a more harmful attack could be someone gaining control of a heating system, turning on the heat full-blast while a family is away on vacation and increasing their heating bill (or turning *off* the heat and causing pipes to freeze). An extremely severe attack could be an attacker taking down or exploiting vulnerabilities in a front door's security system and ransacking the home.

Example #1: The October 2016 DDoS Attack

This past October, the servers of Spotify, Amazon, Twitter, GitHub, and several other large companies were temporarily brought down in what was one of the largest DDoS attacks in history. A DDoS attack involves many systems targeting a single system in an effort to overload it and cause a Denial of Service. The systems used to bring down the servers in the October attack were in fact

compromised IoT devices, primarily certain Chinese-manufactured webcams that had atrocious security protocols.

What went wrong?

Following the attack, Robert Graham, CEO of Errata Security, posted to his Twitter account a collection of pictures and comments detailing his experience testing the security of one of the cameras in question. [3] The results were not pretty. Within minutes, Graham found that the webcam had been infected with what is known as the Mirai worm, malware that turns computer systems running Linux into remote-controlled "bots." [4] While these bots are most often used for large-scale attacks, in localized attacks similar viruses can be used to send video from the camera to an attacker. Besides the obvious implications of having someone covertly watch you through your webcam, this can also be used to steal sensitive information (especially if the webcam has a built-in microphone…).

The Mirai worm is self-spreading. Once it infects an IoT device, it uses the infected device to attack other insecure IoT devices by performing a wide-ranging scan on IP addresses. These insecure devices are accessed by brute-forcing passwords – Mirai tries to guess the login credentials based on common or easily guessable usernames and passwords. In most cases, these credentials are part of a factory default (such as admin:admin or admin:password). [4] Devices for which the login credentials were changed were much less vulnerable to these attacks, proving that it is always important to change factory-set usernames and passwords to more unique credentials. While a device itself may have other security flaws, changing pre-set credentials is an effective way to prevent simple attacks such as the brute-forcing executed by the Mirai Worm.

Example #2: SmartThings

Earlier this year, a research document was published discussing the security flaws in SmartThings, a Samsung-owned "smart home programming framework that supports third party app development." [5] After a thorough analysis of this system, it was found that attackers could create their own door codes, steal existing codes, and even set off the fire alarms in the home.

What went wrong?

The SmartThings framework had two major flaws, both of which were correlated to app privileges. It was found that "over 55% of SmartApps in the store are overprivileged due to the capabilities being too coarse-grained. Moreover, once installed, a SmartApp is granted full access to a device even if it specifies needing only limited access to the device." [5] In other words, apps created by third parties were given much more access to the SmartThings system than they needed. While these third-party apps may not have been maliciously created with the intent of being used in system attacks, nonetheless their security protocols can be exploited. The security analysis of SmartThings found flaws that could be placed into five main categories:

1. SmartApps being overprivelaged; having access to more than they need to/should.
2. Sensitive data not protected against insecure or malicious SmartApps ("unauthorized SmartApps can eavesdrop on sensitive events"). [5]
3. Insecure interactions between SmartApps that could be eavesdropped upon.
4. Unsanitized external inputs (command injection).
5. Unrestricted external communication abilities for untrusted/insecure Smartapps ("Internet access and SMS access are open to any SmartApps without any means to control their use."). [5]

While in the previous example security issues could be lessened by direct actions of the user (changing preset passwords), in this case it would be extremely difficult for a user to fix these many

vulnerabilities. The exploits were completely the fault of the system's creator. Thankfully, the authors of this research document had the knowhow to bring these issues to light. This is a valid argument towards not purchasing security systems that are brand-new to the market – it may be helpful to wait until security reviews from trusted, outside sources have been published.

Example #3: HomeMatic

HomeMatic, a home automation system developed by the German company eQ-3, enables users to control their door locks, adjust their heater, and receive alerts from a motion detector. At the 30th Chaos Communication Congress held in Hamburg in December of 2014, hackers Sathya and Malli gave a live demonstration in which they gained unauthorized access to each of these systems in a process that took *less than an hour*. They discovered these exploits when, in an effort to improve the capabilities of HomeMatic, they began to write their own firmware for the device, soon realizing that it was less secure than they had initially thought. [6]

What went wrong?

The exploits found by Sathya and Malli could have been easily remedied by the user. The attacks utilized a known default key for HomeMatic's encryption system (called AES), and if the owner were to change this key the attacks could be prevented. Unfortunately, changing the key often caused issues with AES (a bug which was the fault of the company), meaning that users tended to avoid changing away from the default. [6] Regardless, the exploit stemmed from the software having a default key which could be left as-is, causing many systems to have the exact same encryption key. In order to increase the security of the system, the company should have either fixed the AES issues and then required all users to change the key in order to use the system, or at the very least should not have used the same default encryption key for all systems.

Example #4: Xfinity Home Security

Last year, security researchers at Rapid7 found vulnerabilities in Comcast's Xfinity Home Security system. These flaws in the system would "falsely report that a property's windows and doors are closed and secured even if they've been opened." and "could also fail to sense an intruder's motion." [7]

What went wrong?

The Xfinity Home Security system communicates and operates over the 2.4 GHz radio frequency band using a ZigBee-based protocol, ZigBee being a "wireless language that everyday devices use to connect to one another." [7, 8] The system has major flaws surrounding this method of communication. The first is that the signals between sensors and the main hub can be blocked using radio-jamming equipment. These sensors are the ones monitoring window and door security, as well as motion inside or outside the home. To make matters worse, the system "fails positive" when these signals are blocked, meaning that the system cannot detect that communication has halted -- the system essentially assumes that no news is good news. When the blocked signals finally reconnect (which can take anywhere from a few minutes to *three hours*), there is still no indication from either side that there was a break in communication. [7]

This system is faulty on so many levels. First, a security system should not be designed in such a way that something as simple as a radio jammer can take down the entire system. Even if the other flaws were fixed, this is still an insanely blatant error. That being said, the effect of this exploit could be greatly lessened by allowing the system to detect when there has been a block in communication. This is the heart of the issues surrounding the system. The system should be able to recognize when a sensor has suddenly stopped communicating with the main hub. Silence from a sensor should be taken as an alert, not ignored. Should this alert system fail, there should also be a "backup plan" in which the sensors can also detect this disconnection. This way, upon reconnection,

the sensor that had been blocked can send an alert to the hub that communication was blocked. This would make it much more difficult for an attacker to just send false data to the hub – they would also need to deal with sending data to the sensors being blocked. All in all this is just a horrifically-designed system. The only advice for a homeowner purchasing this system would be to not purchase this system in the first place (once again proving that waiting and researching a system before purchasing it can be extremely valuable).

Common Vulnerabilities

The examples discussed above are only a few examples of the many security issues plaguing IoT devices today, however many of the insecurities discovered in these systems stem from the same three overarching issues: Weak Authentication, Web Vulnerabilities, and Local Insecurity. [9]

Examples of weak authentication include devices which do not use mutual authentication or do not enforce strong passwords. Often times these systems even go so far as to limit the user's ability to set up a strong password by limiting the size and usable characters (such as systems which only use a four-number PIN code). If on top of this there are no methods for preventing brute-force password-cracking attacks (one such prevention being a lockout for a set amount of time after getting the password wrong multiple times), or no support for two-factor authentication (verifying your identity via email or SMS in tandem with your login credentials), then the system becomes even more vulnerable to attackers.

There are already a plethora of known web vulnerabilities including SQL injection, remote file inclusion, remote code execution, and unauthorized path traversal. Home automation systems using web interfaces can also suffer from these vulnerabilities. In a test done by Symantec, not only were many of these issues found, but some were very severe issues, one being a door lock which could be "opened remotely over the internet without even knowing the password." [9]

Finally, there are local vulnerabilities – issues which cannot be exploited remotely, but rather in a targeted, local attempt (such as bringing down the aforementioned Xfinity system using a radio jammer). A prevalent example of a local vulnerability is a home automation device which locally transmits passwords in clear text (or has no password altogether). If an attacker breaks into the home's wifi network, they can easily locate these passwords and gain full access to these systems. This is a great example of a chain only being as strong as its weakest link – if a homeowner is connecting systems to a local wifi network, they need to take the necessary measures to ensure that the network itself is secure from attackers.

How can a user protect themselves?

This paper is not meant to discourage the use of home automation systems. When implemented correctly these systems can not only be extremely valuable to the security of a home, but can also make running a home much easier in general. There are, however, many ways in which an uninformed user can make mistakes in either the setup of a home automation system or in the decision to purchase a certain system in the first place, often resulting in a home being even less secure than if it had no system at all. Here are some suggestions on how a user can reduce the risk of a potential attack on their home automation system [9]:

- **Do extensive research before choosing a system.** Don't purchase a system without first researching its potential risks. Search for risk analyses published by security professionals *not* affiliated with the brand in question.
- **Use strong and unique passwords.** This also includes changing default passwords, and choosing a system which allows for strong passwords to be implemented.
- **Secure local Wi-Fi networks.** Use strong encryption methods (such as WPA2).

- **Disable unnecessary features.** Better yet, only buy a system with the features needed. When doing this also ask whether a "smart" system is even needed, or if a normal system would suffice.
- **Turn off remote access when not in use.** Only use remote access features if they are actually needed/being used, such as when away on vacation.
- **Wired connections are more secure than wireless connections.** Use these connections whenever possible.
- **Do not purchase used devices unless they are from a VERY trusted source.** These devices can be tampered with, allowing the original owner access to the system after it has been sold.
- **Make sure that any disconnection in communication due to network failure or jamming won't result in an insecure state.** Any block in communication should result in an immediate alert to the user, even if the user is aware of the issue (such as during a power outage).

Conclusion

The advancement of home automation technology over the past few years has been incredible, but it is important to not get too distracted by all of the bells and whistles associated with these systems. No matter what fascinating features a system may have, if the system as a whole is insecure it should never be used – having a system with amazing functions means nothing if it can't actually keep one's valuables safe. A user should exercise caution when choosing a system – following the guidelines outlined above could save thousands of dollars down the road when a serious attack is successfully prevented.

Resources:

1) Greenemeier, Larry. "The Internet of Things Is Growing Faster Than the Ability to Defend It." *Scientific American*. N.p., 25 Oct. 2016. Web. 08 Dec. 2016.
2) Sherman, Erik. "The Main Reason Companies Don't Fix Cybersecurity." *CBSNews*. CBS Interactive, 12 Mar. 2015. Web. 09 Dec. 2016.
3) Graham, Rob. "1/x: So I Bought a Surveillance Camera Pic.twitter.com/HbmPzrZgFK." *Twitter*. Twitter, 18 Nov. 2016. Web. 09 Dec. 2016.
4) Zeifman, Igal, Dima Bekerman, and Ben Herzberg. "Breaking Down Mirai: An IoT DDoS Botnet Analysis." *Incapsula.com*. N.p., 26 Oct. 2016. Web. 09 Dec. 2016.
5) Fernandes, Earlence, Jaeyeon Jung, and Atul Prakash. "Security Analysis of Emerging Smart Home Applications." *2016 IEEE Symposium on Security and Privacy (SP)* (2016): 1-2. Web.
6) Renzenbrink, Tessel. "30C3: Hacks Demonstrate Insecurity of Home Automation Devices." *Elektor*. N.p., 10 Jan. 2014. Web. 08 Dec. 2016.
7) Zetter, Kim. "Comcast Xfinity Home Security System Leaves Home-Owners Unsecured." *Slate Magazine*. N.p., 06 Jan. 2016. Web. 10 Dec. 2016.
8) "What Is ZigBee?" *The ZigBee Alliance*. N.p., n.d. Web. 10 Dec. 2016.
9) Wueest, Candid. "Is IoT in the Smart Home Giving Away the Keys to Your Kingdom?" *Symantec*. N.p., 12 Mar. 2015. Web. 10 Dec. 2016.