Security threats of Smart Device technologies (IoT)

By Justin Schomburg

ITCN 4040

Abstract

Internet of thing security has become more and more prevalent and important in today's day in age. IoT devices are getting smart and growing in number. This means that these devices will become prime target for hackers looking to use them massive botnet attacks like the Mirai botnet attack on Dyn and there will be increase number of hackers looking for back backdoor into your network and into your IoT devices. Challenges from over replicated unsecure devices to engineers lacks security responsibility can challenge the security integrity of these devices. The challenges can be mitigated with security techniques from both users and developers to secure you IoT devices.

Internet of thing is a vast sea if smart devices connected to the internet and meant to help make tasks easier like turning on an oven with your phone before you get home or asking a Google home a simple question. Do you stop to think about if these devices are secure and what can happen if they are hacked? IoT security requires looking over several aspect, what are IoT devices, why is IoT security important, what are challenges to IoT security, examples of IoT security problems and how developers and users can prevent IoT security issues.

Let's start off with the basics, internet of thing devices is any physical thing that can be assigned and us an ip address that allows it to connect to the internet. There is such a large variety of these devices because they can be anything like a toothbrush, oven and even something like a pacemaker. It is estimated that in the past year that the amount of IoT devices in the world has grown 31 percent from last year to reach about 8.4 billion devices and is expected to reach upwards of 20 billion devices by 2020 (Tung, 2017).

When it comes to IoT security there are few common factors that relate to the security of your smart device. First is application security, which relates to how secure the application that is used to access the IoT devices. Next factor is password security relating to the default passwords and password strength in the applications and devices. Human error and hacker's intent are big factors in the security when it comes to how people plan attacks to gain access to networks using human errors that users don't know they are doing. Last of all are the lack of competence of engineers to add more security equipment or barrier coding in the devices to secure the devices more.

Internet of things security now a day is becoming more important than ever and this is do to several different reasons. First up is the factor that there are some many smart devices around the world and is growing exponentially day by day. This means that there are increasing amounts of targets for hackers can go after and also means more weapons for these hackers to use if they want to use them in a botnet. This has already been a factor in a major attack that will be talked about later in the article.

Business data and crucial information are very import things to protect for a business but an IoT devices can be used in accessing restricted information. If an IoT device has been infected with a virus then added to a corporate network or a IoT devices like a coffee pot is on the network and is infected by a device accessing it, the whoever controls that virus can use that coffee pot to access the network in the shadows. This is a way that hackers can get around network device scans and steal data from companies without them even knowing.

Personal safety is a huge importance that people think of when it comes to people's minds in today's age with all the smart tech in their homes from smart homes that listen to voice cue to security cameras around the house and even smart locks. People want use smart technology to make tasks easier and more convenient but don't want to worry about them causing personnel harm. If a hacker where to be able to access important devices like a pacemaker keeping a person alive, the steering of your car like what happened with Jeeps or even the security camera's or locks in your house. These breaches can lead to people being hurt or even dying, which should make the security of these smart devices a very important factor.

Internet of things security can factor a good majority of is problem to several different challenges of IoT security that have been identified by the people at Icon labs. The first challenge they identify was the fact that there are many IoT devices that have critical

functionality, in which their devices can be imbedded in crucial infrastructure or do very important tasks that can cause major problems if hacked (Icon Labs, The internet of secure things ...). These important devices will need stronger security and may cost more. Next challenge identified was the mass replication of devices, which is reverting to the fact that IoT many devices are being mass produced which means if an engineer makes a big mistake in the secure in the software or types security equipment need in the device then a large amount of devices, if not caught early can have the same flaws and be vulnerable to hacking (Icon Labs, The internet of secure things ...). This ties into the next challenge which is the security assumption of engineers that their device will not be a target of an attack. They apply not enough effort into the security of the device which leaves the device vulnerable to hacking (Icon Labs, The internet of secure things ...). There are challenges that come with trying to fixing security problems because some devices are not easily patched with frequent updates. This is due to some IoT systems are not created where they will push out updates automatically and force user to update it manually if they know about the update, also the device could not have enough storage to download and install the updated security patch (Icon Labs, The internet of secure things ...). Icon labs also identifies the challenge of more business based IoT devices being used outside of enterprise security perimeters, on networks that lack the security needed to help protect these devices. There are sure to be more challenges that go into IoT security then what Icon Labs has identified.

Botnets have become a big problem in the age of technology, hackers using phone, and computers to launch DDoS attacks on servers across the world. Now these hackers have been able to add IoT household devices to their minion horde of bots. On famous example of an attack that too advantage of IoT devices was called the Mirai botnet ("The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History", 2018). This botnet of things attacks took

advantage of millions of Linux based devices like web cam and other home appliances to use for DDoS attack on the Dyn Domain name servers in 2016. This caused some major website like Facebook and Twitter to be unaccusable for a good amount of the United States for several hours. The method the attackers used to gain access to these devices was relatively simple. Hackers uses a scanner process runs continuously on each device using telnet on TCP port 23 or 2323 to try and login to IP addresses at random (Corero). When the scan finds the devices, it uses a bank of over 60 different known default passwords that were commonly used as default passwords on IoT devices. Once they have gained access the malware is installed and waits for the command from the hacker. There has been a version of this malware that was able to infect windows devices but that version has not been seen in an attack date. With the ever-growing amounts of these IoT devices, the next botnet of things attack could be exponentially bigger then this Mirai attack.

When it comes to most IoT devices they have an application that is used to control them and secure the devices behind a security wall of Authentication using their email and password. Check Point researchers did a study on the LG SmartThinQ applications which is used to control smart LG home appliances. What the researchers found was that there was a security vulnerability in the application that allowed them to hijack internet devices like ovens, fridges and dryers manufactured by LG (Khandelwal, 2017). With this vulnerability is could allow hackers to log in remotely in remotely to the LG cloud application and take over the victims account. To perform the task of hijacking these devices, a rooted device is needed for intercepting the users traffic but there is anti-root and SSL-pinning function installed in the LG app that blocks the use of the rooted devices. The check point researchers where able to bypass the security function by decompile the source of the app, remove the functions that enable SSL

pinning and anti-root from the app's code, recompile the app and install it on their rooted device (Khandelwal, 2017). This allows the hacker to intercept the users traffic and change the user username and password. This will give the attacker complete control of the LG account and all the devices on it. This information was revealed to LG and was eventually patched.

What can be done provide a secure internet of thing environment? The people at Icon Labs have come up with a list a many thing that can be done to create a secure internet of things. First feature they listed was a secure boot which entails developing cryptographically signed code that is created only and install only by the manufacture and must be authenticated. Second feature the ability to securely updated code for patches using manufacturer code. After that they recommend encrypting all communication using SSH, SSL or etc... and storage on the devices and require all communication to the devices be authenticated by using a strong password (Icon Labs, The internet of secure things ...). The last couple features Icon Labs thinks should be included protecting against cyber-attacks by using embedded firewalls to provide a critical layer of protection, provide intrusion detection on the IoT devices to detect attacks and last is tampering detection to alert when something has been changed on the devices (Icon Labs, The internet of secure things ...). All these recommendation from Icon Labs for IoT device make can help keep data safe and people happy with very limited breaches to their IoT device security.

There are two sides of the spectrum when it comes to securing an IoT device. There is the developers in the last section, now we have to talk about the users strategies to strengthen their IoT device security. First thing is to create a strong password for the login to devices and never leave the default login password. Next is to make sure you update your IoT devices to keep up to date with security patches. Next parameters relate more to enterprise IoT networks device. First is to disable UPnP on routers unless needed. Second is to monitor ip ports 23/TCP and 2323/TCP

for unauthorized access attempts on your IoT devices using telnet (Bertino & Islam, 2017). This is exactly the way the Mirai botnet was creates. Last process to help users secure their IoT device is by monitoring for anomalous traffic on port 48101, this is the port that infected devices often use to spread their malware (Bertino & Islam, 2017).

Security will always be a big priority for computer and phone developer but as we have seen with the growing amount of IoT devices, the priority to secure these devices will become more important but yet more challenging. These devices will be targeted by hackers for botnets and to steal user's information. There are steps developers and users can take to make sure they have secure Internet of things devices but these steps will be ever changing year by year with development of IoT technologies.

References

Bertino, E., & Islam, N. (2017). Botnets and Internet of Things Security. Computer,50(2), 76-79. doi:10.1109/mc.2017.62

Blue, V. (2016, November 29). That time your smart toaster broke the internet. Retrieved April 05, 2018, from https://www.engadget.com/2016/10/28/that-time-your-smart-toaster-broke-the-internet/

Icon Labs. (n.d.). The Internet of Secure Things – What is Really Needed to Secure the Internet of Things? Retrieved April 16, 2018, from http://www.iconlabs.com/prod/internet-secure-things-–-what-really-needed-secure-internet-things

Kang, W.M., Moon, S.Y. & Park, J.H. Hum. Cent. Comput. Inf. Sci. (2017) 7: 6. https://doi.org/10.1186/s13673-017-0087-4

Khandelwal, S. (2017, October 27). Hackers Could Turn LG Smart Appliances Into Remote-Controlled Spy Robot. Retrieved April 05, 2018, from https://thehackernews.com/2017/10/smart-iot-device-hacking.html

Corero. (n.d.). Mirai Botnet DDoS Attack Type. Retrieved April 16, 2018, from https://www.corero.com/resources/ddos-attack-types/mirai-botnet-ddos-attack.html

The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History. (2018, February 15). Retrieved April 05, 2018, from https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/