Common Security Issues in IoT Devices

Dawei Sun
sdw14@mails.tsinghua.edu.cn

ABSTRACT

Internet of things(IoT) has been very popular in the past few years. As they play an important role in our life and take over some of our privacy, once they are weak, bad hackers will go into our lives via them. In this paper, we illustrate some common issues in IoT devices and analyse the reasons. We also give a simple experiment to show how to find vulnerable devices. Finaly, we give a brief conclusion and some advices to facilitate a better future of IoT.

KEYWORDS

IoT, Security, Vulnerability

1 INTRODUCTION

Internet of things(IoT) has been very popular in the past few years. More and more devices are connected to the Internet and changing our lifestyles. We use web cameras to monitor our houses, use smartphones to turn on lights and air-condition in our house when we are on the way home. IoT devices make our life easier. However, convenient connection always means more vulnerabilities. As they play an important role in our life and take over some of our privacy, once they are weak, bad hackers will go into our lives via them.

There are some reasons cause IoT security issues. Firstly, access threshold to this area is really low because only some simple techniques are required to manufacture IoT devices. So, many companies crowded into this area and earned a lot of money. Unfortunately, some of these companies have no idea how security matters. Secondly, many people have no idea how security matters too. They will set very weak passwords for their devices or even leave them open access. Thirdly, most of IoT devices are designed and built on the base of some open-source systems. Once these base systems are reported vulnerable, these devices will suffer the same vulnerabilities. Even worse, most manufacturers have no abilities to distribute security updates to their devices.

In the next section, I will talk about the backgrounds of IoT security issues. I will talk about some common IoT security issues in section 3 and show some experiment results in section 4. Finally, I will give a conclusion.

2 BACKGROUND

Welcome to the era of the IoT, where digitally connected devices are encroaching on every aspect of our lives, including our homes, offices, cars and even our bodies.[2] IoT researchers from ABI Research predict that the number of wireless connected devices will exceed 40 billion by 2020[1], more than double from the level in 2014. More devices mean more possibilities for cyber criminals.

In the past few years, with the rapid progress of IoT, we have heard some new type of cyber attacks. Hackers can control a car via a network without permission of the owner. Hackers can also access a pacemaker generating 830v voltage to kill its owner. ATM was also on the list. Barnaby Jack attacked an ATM in 2010, which threw money to him later. Once the hackers take over many devices, they can create a botnet with these IoT devices. With a botnet, it's easy to make a Distributed Denial of Service(DDOS) attack. France-based hosting provider OVH got DDoS attacks that reached over one terabit per second (1 Tbps) in 2016. These DDOS attacks exceeded the previous record of DDoS scale. Behind the big attacks, there were over 152,000 hacked IoT devices[8].

John Matherly launched a website called Shodan[7] in 2009. Shodan is a meta-data search engine that lets the user find specific types of computers (webcams, routers, servers, etc.).[11] Shodan can be used to find dangerous systems on the Internet, like traffic lights.[3] We can find lots of web cameras via Shodan, and most of them are open access.

3 COMMON ISSUES

3.1 Insufficient Authentication/Authorization

Insufficient authentication/authorization was very common in the computer area. In the era of IoT, some people only see the benefit brought by smart devices, but not the potential issues. They use the default passwords or very weak passwords for their devices, which record their daily lives, monitor their babies, and can be a tunnel to their lives.

For example, webcamXP is a popular webcam and network camera software for Windows. By default, webcamXP will launch an HTTP server on the port 8080 and permit anonymous access. If someone uses the default settings and connects his camera to the Internet, it will share a live stream with people all over the world. We can find a lot of webcamXP instances via Shodan with a simple keyword "webcameraxp". In my test, I find 1422 cameras, and the distribution is shown in Figure1.

3.2 Vulnerabilities in Base Systems

Most of IoT devices are designed and built on the base of open-source systems. Once these base systems are reported vulnerable, these devices will suffer the same vulnerabilities. Even worse, most manufacturers have no abilities to distribute security updates to their devices.

For example, hackers released an exploit of Windows' Server Message Block (SMB) protocol called EternalBlue in March 2017. Later, Microsoft issued a "critical" security patch on 14 March 2017 to remove the underlying vulnerability on supported versions of Windows. However, WannaCry ransomware attack began on Friday, 12 May 2017, and infected more than 230,000 computers in over 150 countries[9]. Many IoT devices like ATM, were attacked because these IoT manufacturers have not applied the security patch.

Many IoT devices are based on Linux (or something very similar, like OpenWRT). Once a bug in Linux kernel is reported, these devices are in danger. Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel memory management subsystem. Almost all of the kernel versions were affected. Some

Figure 1: With keyword "webcameraxp", I find 1422 webcamras. I attempted to connect the top 10 of them, and 8 cameras can be access without a password.

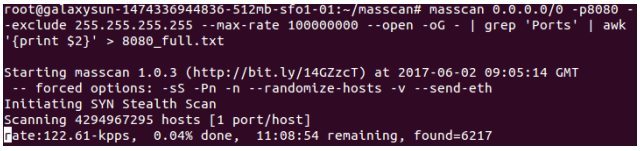

Figure 2: Scan the whole Internet with Masscan! It took about 14 hours and generated a 200M file.

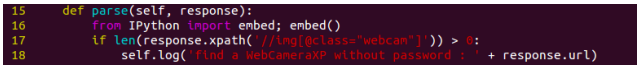

Figure 3: One of the most unique and simple feature is that these html sources have "img" tags with class attribute "webcam". We can recognize these pages easily.

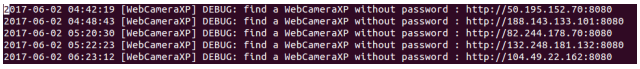

Figure 4: After a 3 hours searching, I find 5 open-access webcameras.

of IoT devices are still not fixed even if Linux have released some patches. Hackers can use this bug to get root privilege once they have access to an IoT device.

3.3 Back Doors by Manufacturers

Many IoT devices manufacturer will open some back doors at the developing stage, but some of them forgot to close the doors when they sell their product.

For example, Chinese ARM SoC-maker Allwinner wrote their own kernel based on Linux 3.4. Researchers found that there is a back door in their open source code. After writing "rootmydevice" to "/proc/sunxi_debug/sunxi_debug", the current process will got root privilege. Allwinner's SoC took a big market share in cheap Android gadgets and smart devices area.

Analyze the firmware shipped with smart devices, and we can find some default passwords and user names. Some of these devices will start telnet or ssh services by default, so everyone can login these systems with the default passwords.

4 EXPERIMENTS

4.1 Scan Open-access webcameraXP server

To show that how easy it is to find vulnerable devices, I write some code[1] from scratch to find all of the open-access webcameraXP instances listening on port 8080.

4.1.1 Find all of the 8080 HTTP servers. To find potential HTTP server listening on port 8080 all over the world, I have to scan the whole Internet. Thanks to the great scanner MASSCAN[10], I can scan the whole Internet within a reasonable time on a cheap server with a single command. Finally, I found 14040527 hosts with port 8080 opened. It took about 14 hours to finish this task.

4.1.2 Launch the Spider. With the IP addresses list in hand, I have to build a network spider to find webcameraXP server from these 14040527 hosts. I chose scrapy[5] as the spider framework. Scrapy is an open source and collaborative framework which can do large scale data collecting. After a quick analysis of the webcameraXP web page source, I found some features can be used to recognize webcameraXP servers. One of the most unique and simple features is that these HTML sources have "img" tags with class attribute "webcam". So, my spider is shown in Figure3

Unfortunately, I have only one machine to running my spider, and the average speed is about 450 hosts/min. It will take 20 days to test over all the 14040527 hosts. After a 3 hours searching, I find 5 open-access webcameras. Some of these live streams is shown in Figure5.

4.2 GSM and GPRS Attacks

Some old devices use GSM (Global System for Mobile communication) or GPRS (General Packet Radio Service) to communicate. These technologies are not encrypted and can suffer a man-in-the-middle attack. Some GSM devices will choose the base station with the strongest signal, so if we can build a fake base station we will be the man in the middle. OpenBTS[4] is a great open source software-defined base station project. It's easy to build a fake base station with OpenBTS and a software-defined radio device like USRP (Universal Software Radio Peripheral)[6].

I built a fake base station and do some test with a GSM/GPRS MODEM in Figure6. The whole system is shown in Figure7.

After I start the base station, some clients found this "strong" base station and connected to it, as shown in Figure8. Not only the

[1]The code can be find in https://github.com/sundw2014/naive_IoT_scanner

Figure 5: There are some live streams.

test modem connected to my fake base station, some others in the building connected too. However, I did not see any communication between the clients and the servers.

5 CONCLUSIONS

Many IoT devices are in danger. As users, we should pay attention to the security issues of IoT devices, use more complex passwords and hide devices behind firewall or VPN if possible. Vendors should increase the priority of security at developing stage and take action as soon as possible after a bug was raised.

REFERENCES

[1] ABIResearch2014. 2014. The Internet of Things Will Drive Wireless Connected Devices to 40.9 Billion in 2020.
[2] Ben Dickson. 2015. Why IoT Security Is So Critical.
[3] DAVID GOLDMAN. 2013. The Internet's most dangerous sites.
[4] https://openbts.org/. 2013. OpenBTS.
[5] https://scrapy.org/. 2013. Scrapy.
[6] https://www.ettus.com/. 2013. Universal Software Radio Peripheral.
[7] Robert O'Harrow Jr. 2012. Cyber search engine Shodan exposes industrial control systems to new risks.
[8] Swati Khandelwal. 2016. World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices.
[9] BBC News. 2017. Cyber-attack: Europol says it was unprecedented in scale.
[10] David Robert and Graham. 2013. MASSCAN: Mass IP port scanner.
[11] Wikipedia. 2017. Shodan.

Figure 6: A very old module used in some IoT devices.

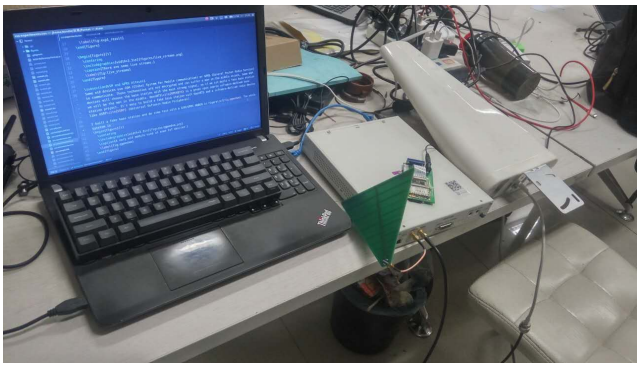

Figure 7: The fake station system, including a laptop running OpenBTS, a USRP, a victim modem, and some antennas

```
OpenBTS> tmsis
IMSI            TMSI IMEI            AUTH CREATED ACCESSED TMSI_ASSIGNED
502181104701640 -    353267060514710 2    12s     12s      0
460110709134574 -    862427039757090 2    284s    284s     0
460001933101546 -    351246004709870 2    5m      5m       0
```

Figure 8: Not only the test modem connected to my fake base station, some others in the building connected too.