Economics of Security

Draft discussion for block 2, group 13 IoT Honeypots

Ines Duits, Rob van Emous, Rien Heuver & Patrick van Looy

Introduction

For a couple of years now, we are witnessing a trend where more and more devices are connected to the internet. Many involved parties, both research and market competitors, have predicted that there will be at least tens of billions connected devices by 2020[1], and even objects as mundane as baby monitors or tires could all become part of this interconnected world. However, each device that gets connected introduces new privacy and security issues. Although an attacker could simply target an individual (company) by exploiting its IoT devices, for example by hacking into a smart door lock or alarm system to gain access to a building. a much more devastating strategy an attacker could employ is using many vulnerable devices together for launching DDoS attacks[2]. Moreover, an attacker can often use one infiltrated device within a network as entry point to infect other connected systems in the network.

For improving the security of any system, it is very useful to know what what type attackers to expect, what kind of attack methods are used and what the target(s) of those attackers would be. For this purpose, we can use Honeypots. A honeypot is a computer system that is setup to act as a decoy to lure cyber attackers, and to detect, deflect or study attempts to gain unauthorized access to information systems[3]. Generally, it consists of a computer, some running applications, and data that simulate the behavior of a real system that appears to be part of a network but is actually isolated and closely monitored. All communications with a honeypot are considered hostile, as there's no reason for legitimate users to access a honeypot. Viewing and logging this activity can provide an insight into the level and types of threat a network infrastructure faces while distracting attackers away from assets of real value. Using these incident based metrics, future attacks can be prevented by ensuring the right security controls or measures are put in place.

Security issue and problem owner

When defining the precise security issue, we have to think of the actors that are actually affected by this issue. Now, IoT devices are introduced to make our life a little easier as in, for instance, smart home applications. When thinking from an attacker's point of view, generally an attacker would not be interested in targeting a single end user of an IoT device since it is simply not that easy to make such an attack very profitable. However, as

---

[1] *Reality Check: 50B IoT devices connected by 2020 – beyond the hype and into reality* https://www.rcrwireless.com/20160628/opinion/reality-check-50b-iot-devices-connected-2020-beyond-hype-reality-tag10 (Last accessed 24-09-2017)

[2] *Techniques for detecting compromised IoT devices* http://www.delaat.net/rp/2016-2017/p59/report.pdf (Last accessed 14-09-2017)

[3] *What is a honeypot?* http://searchsecurity.techtarget.com/definition/honey-pot (Last accessed 18-09-2017)

addressed earlier, when an attacker is easily able to infiltrate and infect many IoT devices, he now has a complete digital army at its disposal for launching serious DDoS attacks. In late 2016 we have already experienced the severity of the security issues concerning IoT devices when they were used for launching massive DDoS attacks after being infected by the so called Mirai Botnet[4]. Therefore, the security issue we will be focussing on is the use of exploited IoT devices for launching sophisticated DDoS attacks.

Now that we have defined the security issue, we need to define the problem owner of this issue in order to determine relevant metrics. One might say that the owner of a compromised IoT device is the problem owner. However, since the owner itself is not likely to experience any problems at all, there is no incentive for the owner to do anything against it. The main victim of course is the target of the DDoS attacks originating from these infected IoT devices. Furthermore, there is a more indirect actor involved, namely the Internet Service Provider (ISP). The ISP will not only see its network flooded due to these attacks which can cause slow connections or even downtime for the ISP's customers, but will also see its customers being both the victim and originator of the attack. Another advantage of focussing on IPS is due to DHCP churn: dynamic allocation of IPv4 addresses by IPs to their customers. Without knowing the IP update routines of ISPs, it is difficult to keep track of botnet bots, but in this case we focus on the problem as if we were the ISPs and therefore have complete knowledge of the IP adress allocation.
We will therfore focus on the ISPs as problem owners for the remainder of the report.

Analysis of honeypot data

The provided data files contain connection (attempts) on a honeypot mimicking an IoT device. This information was collected in the summer of 2016. All lines of the honeypot data are like the following line:

```
2016-07-02 09:54:26$$193.251.75.165$$3344$$133.34.157.129$$23$$['root', 'xc3511', 'cat $SHELL']
```

Every line seems to be a connection attempt at 'timestamp' from a 'source IP' and 'source port' to a 'destination IP' and 'destination port' with a list of command arguments. As this is honeypot log data, the destination IPs probably belong to the honeypot machines connected to subnet 133.34.157.0/24.
After checking all lines of a few files, we saw that every connection is made to 'destination port' 23: the port used by Telnet. Furthermore, the first two commands seem to be the 'username' and 'password' combination used to log in. Therefore, we assume most attacks are focussed on establishing a root Telnet connection (see first command argument: 'root').
Most attacks assume the victim uses the root password 'xc3511'. This is a smart move, because this password is hardcoded in a lot of IP cameras and DVRs[5].
After this, a lot of attackers navigate to a random-looking IP address from which they download, run and then delete a number of shell scripts (bin1.sh, bin2.sh etc.). These scripts are probably used to establish access to be able to use the device in the attacker's botnet. They could also be used to either steal data (via ftp) or scan/infiltrate the network of the victim.

[4] Thomas, K., Invernizzi, L., & Bursztein, E. (2017). Understanding the Mirai Botnet.
[5] https://krebsonsecurity.com/2016/10/europe-to-push-new-security-rules-amid-iot-mess/ (Last accessed 14-09-2017)

Metrics

Metrics are effective tools to measure the performance of the detection and mitigation of attacks from the victim's point of view, but can also be used to measure the performance of an attack from the attacks point of view.

Ideal Metrics

The goal of the ISP is to keep the network clean from 'DDoS-requests'. However, an ISP currently cannot easily block a single device, since most homes use a NAT-router. This means the ISP can only block the entire home or nothing within the home at all. It is logically not desirable for the ISP nor its customers to block entire homes. A likely solution for an ISP would be to inform customers when one of their devices is part of a botnet, so the customer can take it offline and contact the manufacturer.

With the large adress space of IPv6, however, it is possible for ISPs to assign unique IPs to every single device.[6] When this protocol would finally be in use by the general public, alongside the notification of the customer as mentioned earlier, specific IoT devices could be blocked by the ISPs themselves. A drawback of IPv6 is that the 'firewall effect' of NAT would no longer exist and would make the infection of vulnerable (IoT) devices even more easy than before[7].

In order for an ISP to be able to put this measure into place, it needs to determine which homes are affected, or more specifically, which IP-addresses are used in botnets. Therefore, the ideal metric for an ISP would be the specific IP-addresses that are used in botnets.

Existing metrics

Since the IoT and its (in)security is a rather recent occurrence, not many research addresses this topic. This is especially the case when talking about metrics. However, there are a few attempts that try to define relevant metrics regarding the IoT. Herein, we see similarities with metrics for other security issues like DDoS attacks for example. Of course is not that of a surprise since IoT devices have become an interesting approach for attackers to initiate DDoS attacks. Different metrics on different levels exist. Onis a list of existing metrics for IoT-networks.

---

[6] *NETWORK ADDRESS TRANSLATION (NAT) PROS & CONS* https://www.ipv6.com/nat/network-address-translation-nat-pros-cons/ (Last accessed 25-09-2017)

[7] *With IPv6 do we need to use NAT any more?* https://security.stackexchange.com/questions/44065/with-ipv6-do-we-need-to-use-nat-any-more (Last accessed 25-09-2017)

- Number of attacks per time unit
- Number of port probes
- Number of successful / unsuccessful (Telnet) logons
- Number of vulnerable IoT-devices in the network
    - Number of vulnerable passwords (such as default passwords or simple, short words)
    - Number of open ports
- Value of IoT-devices in the network
    - Amount of valuable data on the device
    - Access rights of the device in the network
    - Importance of the device continuïng operations

Metrics we can design from the dataset

In the provided dataset, we can see a few things we can measure: The number of connections made to any system (IP address), to which port, the source IPs and the commands the attackers are executing on the victim machines.

To create a level of how secure the system is. We can categorize all the known attacks for which a defence is in place and did not get through the real system. If there are a lot of unknown and uncategorized attacks, thus not protected against, we could say the system is not that secure. If there are almost only known attacks, for which defences are in place, we would define the system as more secure.

Evaluation of metrics

As with most of honeypot set-ups, the focus lies on incidents and vulnerabilities since the main goal of a honeypot is to log (and analyse) those. Of course, all this data then can be used to define controls. These controls can then again be used to calculate (prevented) losses. The relative focus of these metrics (size of the circle) is shown in the picture below.