Economics of Security

Draft discussion for block 2, group 13 IoT Honeypots

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

Security issue

Nowadays more and more devices are connected to the internet and thus connected to each other. We call all these devices combined the Internet of Things. Most of these devices are very vulnerable to attacks as they were never designed to be secure. Especially newly introduced IoT devices, like smart fridges, smart watches and children's toys, lack good security which make them vulnerable to be used in DDOS attacks for example[1]. Not only are the devices themselves insecure, they also impact the entire network they are connected to. When a device is infiltrated, data is exposed, and hackers can use the devices as entry point to infect other connected targets on the network.

For improving security, it is very useful to know what kind of attack methods are used. 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[2]. Generally, it consists of a computer, 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.

The 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

---

[1] *Techniques for detecting compromised IoT devices*
http://www.delaat.net/rp/2016-2017/p59/report.pdf (Last accessed 14-09-2017)
[2] *What is a honeypot?*
http://searchsecurity.techtarget.com/definition/honey-pot (Last accessed 18-09-2017)

‘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[3].
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 either steal data (via ftp) or scan/infiltrate the network of the victim.

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 would tell us which kind of attack was done on the system where the honeypot was in place. This information can then be used to put controls in place and to better protect IoT devices.

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 which 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. Below is a list of existing metrics for IoT-networks.

- Number of attacks per time unit
- Number of port probes
- Number of successful / unsuccessful 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 continuing operations

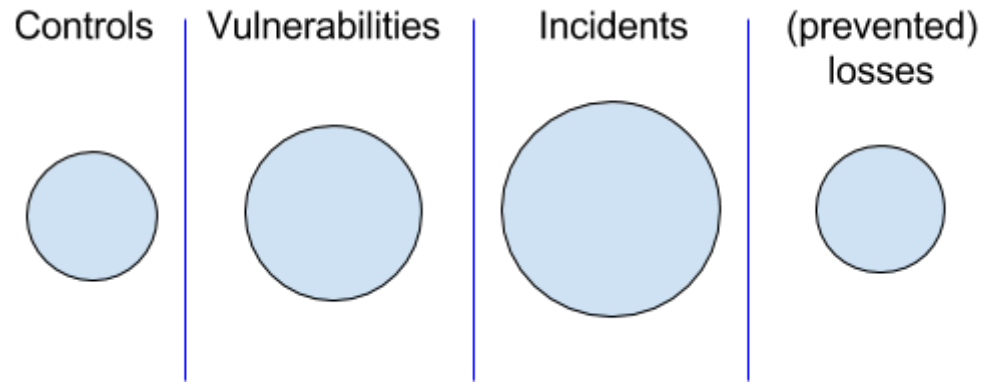
[3] https://krebsonsecurity.com/2016/10/europe-to-push-new-security-rules-amid-iot-mess/ (Last accessed 14-09-2017)

Metrics we can design from the dataset

In which we can see a few things we can measure: The number of connections made to the system, to which port, the source IPs, the message the attackers are sending.

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, uncategorized attacks, 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.

As with mostly any honeypot set-up, the focus mostly is 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 exercise

1. **What security issue does the data speak to?**
2. **What would be the ideal metrics for security decision makers?**
    a. Abstract variant of 4
3. **What are the metrics that exist in practice?**
    a. Is the default telnet password changed/changeable?
4. **A definition of the metrics you can design from the dataset**
    a. The number of telnet connections made to the system per time unit (minute/hour/day).
    b. Source IPs sending a lot of traffic (blacklist those)
5. **An evaluation of the the metrics you have defined. This should include graphical representations of the metrics (e.g., histograms, scatter plots, time series, bar charts).**

Reading material

- https://msmis.eller.arizona.edu/sites/msmis/files/documents/sfs_papers/ryan_chinn_sfs_masters_paper_0.pdf
- https://github.com/Phype/telnet-iot-honeypot
- https://security.cse.iitk.ac.in/sites/default/files/15111021.pdf
- https://securelist.com/honeypots-and-the-internet-of-things/78751/
- https://krebsonsecurity.com/2016/10/europe-to-push-new-security-rules-amid-iot-mess/
- https://www.synopsys.com/software-integrity/resources/datasheets/internet-of-things-security.html