WM0824TU Group9

Chris Berg, 4216776
Martin Koster, 4371011
Radinka Yorgova, 4952545
Wilko Meijer, 4224426

September 17, 2018

Code and data:
https://github.com/wkmeijer/WM0824TU_Group9

1 Security Issue

Mirai is malware targeting IoT devices with the goal of creating a botnet of IoT devices. IoT devices are infected through other infected IoT devices which are scanning the Internet for vulnerable IP addresses. When an infected IoT device found a vulnerable IP address it uses a table with default factory login passwords to get the Mirai malware on the target device.
In general the user of the IoT device is not the one who has to be defended in this case. Maybe the device will work a little bit slower but there is nothing more than that. The ones that have to be defended are the victims of the botnet attacks performed by the mirai bots. Because of the fact that all the bots have a different IP address, it is very difficult for servers to distinguish legitimate traffic from traffic of a botnet attack. So when all the bots are trying to access the server all at once, the server will be disrupted temporarily or indefinitely.
The original Mirai code was published openly. So now, after the creators stopped, there are still attackers who use this code or even evolve this code.

2 Methodology

To understand the topics of the assignment everybody watched the video lectures and read the papers. In this way it was a lot clearer for us to know what we can expect and use from the metrics. After that we wanted to first completely understand what the problem is with the subject of our group. With this information we could answer also the first question. For the other questions we could use information from the lectures. Everyone worked separately on the following tasks:

- Extracting data
- Ideal metric
- Existing metrics
- Metrics for dataset

After all this information is collected we can actually apply the metrics on our dataset and evaluate the results.

3 Metrics

Security metrics are critical tools designed to facilitate decision-making and improve performance and reliability through collection, analysis, and reporting of relevant performance-related data. The right metrics should help the decision maker to allocate security spending and justify the investments, to get actual security and gain certain benefits.

For a decision maker to justify any security investment there are two conditions: to quantify the costs of security and to quantify the benefit. The connection between cost and benefit is described by the security production function (1).

This function goes through a middle step security level. First it maps the cost of security into the security level and then in the second step, the security level into the benefit.

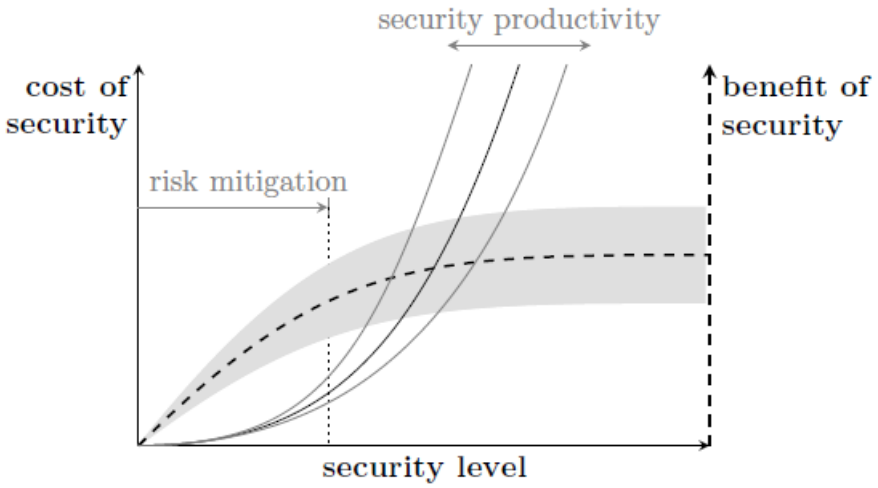

Figure 1: Security production function.

The graphic in Figure 1 (1) shows that from some point spending more and more will get you smaller and smaller improvement in security level and also, after a certain point, further increasing the security level leads only to marginal benefits.

But all that is in the perfect theoretical model.

3.1 Ideal metrics for security decision makers

Before we answer to the question what is the ideal security metric we need an overview of their classification.

There are described four types of metrics for measuring the security levels. Or more precisely said four types of metrics measuring indicators that reflect different aspects of the security level.

The four categories metrics are based on controls, on vulnerabilities, on incidents and on prevented losses.

The first category are metrics based on controls. Controls are the measures implemented to mitigate risk. They can be physical (door locks, building specifications) organizational (incident response team/employee), procedural (credential management) or technical (like firewalls). Controls exclude the threat environment. Vulnerabilities are weaknesses in the controls that can fail by a certain type of attack.

The next type metrics is vulnerabilities. The vulnerabilities can be known and unknown. For the known there are different approaches to check whether known vulnerabilities are present in the systems. Against the unknown vulnerabilities the typical techniques are penetration testing or red teaming. It is important to stress that the vulnerability metrics are driven by attack scenarios and they are static.

The next two metrics are driven by the incident itself. The last metric, prevented losses, try to map incidents on losses, i.e. it is driven also by the economic impact of the incident. They are the most advanced metrics.

Incidents and prevented losses are stochastic. They are driven by unknown attacker behavior and the actions of the defender. Moreover they are driven by events (for example a data breach) wheres controls are mainly driven by actions (installing a new firewall).

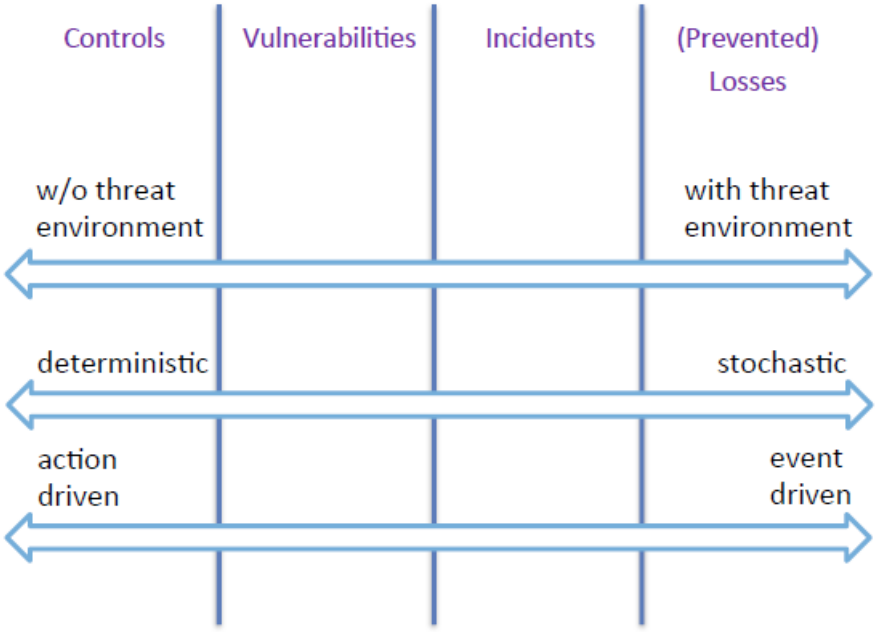

Figure 2: Types of metrics

To be back to the question what would the ideal metric be. A combination of different types of metrics would be the most powerful security metric. The ideal metric should also have reasonable proportion between *cost of security- security level- benefit of security* given in Figure 1.

3.2 Metrics that exist in practice

Earlier we discussed the concept of the security production function (Figure 1). There are existing metrics which measure those three units (cost of security, security level and benefit of security). Those metrics are shown in Figure 3. The metrics for the costs and benefits of security are shown order from concrete to abstract. The metrics more to abstract are harder to measure. The security level is in the range from deterministic to probabilistic. Again if the metrics go to the probabilistic side they are becoming harder to measure.

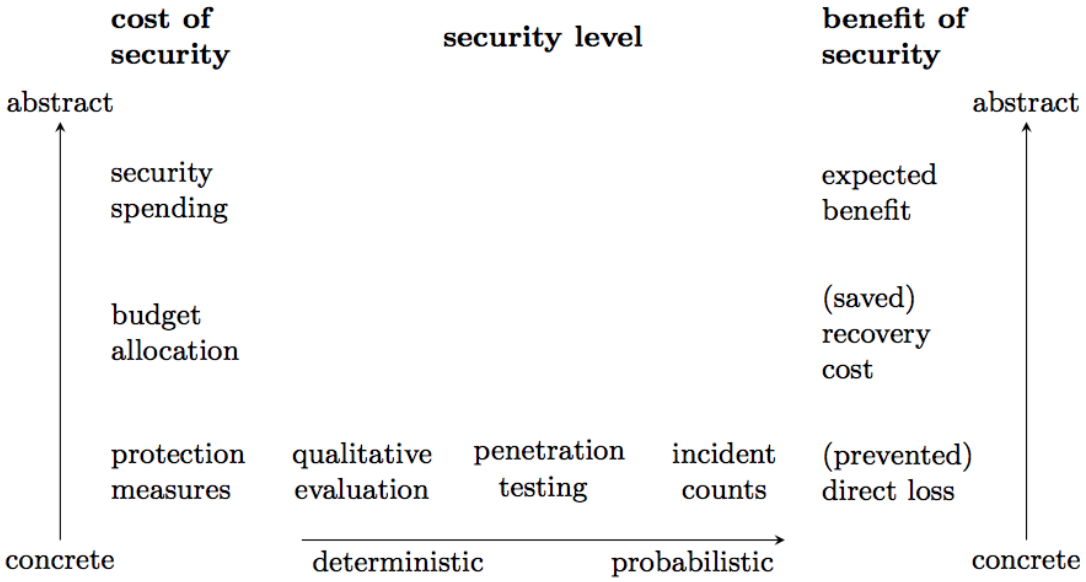

Figure 3: Measurements in the different categories

There are also some existing models for the four categories within the security level (see Figure 2):
- Cloud Security Alliance Control Matrix
- Security Service Level Agreement
- Software Security Maturity Model
- National Cyber security Assessment for The Netherlands

Some examples of metrics stated in the videolectures:
- Incident rate
- Rate over time per country in absolute numbers (this is dependent not only on counter measures but also on attackers behaviour)
- Rank order which country got infected the most in a time period.
- Plot amount of users against amount of infections.

3.3 Definition of metrics from dataset

Does the bot-net spread mostly inside or outside the country

- Spread by country: for each country, entries per week/month - stack chart
- Infection of neighboring countries:

Which autonomous systems are prone to attacks

- Frequently targeted autonomous systems: bar chart of top 10

Could there be a new (currently unknown) compromised autonomous system?

- Sudden increase in targeted AS: increase of frequency in percentage over month
  -

4 Evaluation of metrics from dataset

The entire dataset contains around 230 000 ip addresses that have shown behavior somewhere between February 2017 and September 2018 indicating an infection of the Mirai malware. In Figure 4 the 10 most frequent Autonomous Systems and their frequency are displayed. The figure shows that a very large portion of the infections occurs in a very small part of the AS's, about 100 000 infections in 10 AS's, where there are in total 7523 AS's in the dataset. This suggests that the malware spreads more easily within an AS or that specific AS's are targeted. Security decision makers should thus be more concerned about the malware if they are operating within an AS that already shows a substantial amount of infections.

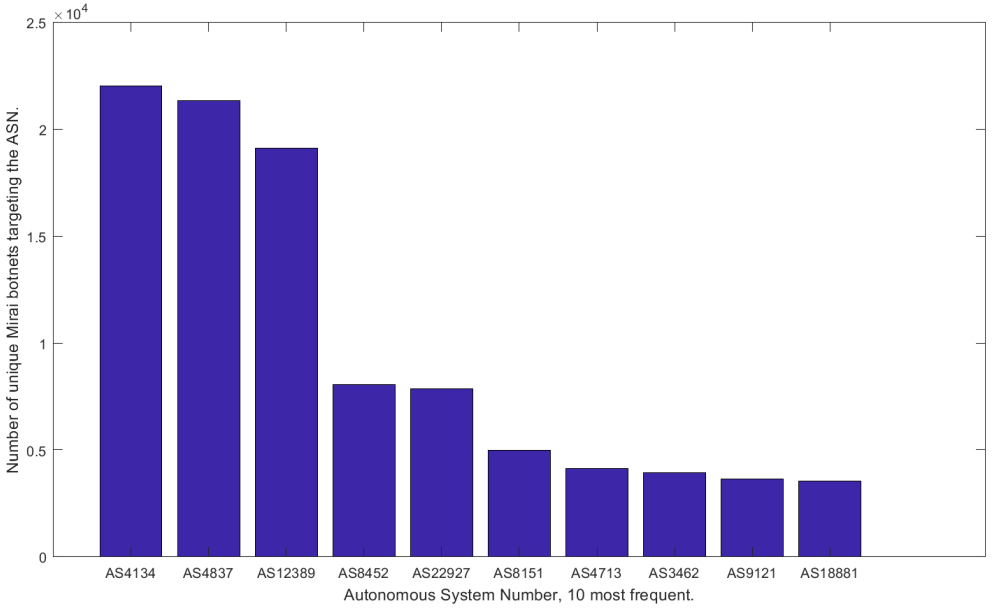

Figure 4: Frequently targeted autonomous systems, registered between 2017-02-18 and 2018-09-12.

References

[1] R. Böhme,Security Metrics and Security Investment Models, Advances in Information and computer Security, pp 10-24, 2010.