Assignment 1 - Security Metrics

WM0824TU Economics of Cybersecurity (2019)

Brennen Bouwmeester[4446461], Hsin Cheng[4771230], Kevin Su[4438108], and Jochem Vlug[4165993]

Delft University of Technology, Delft 2628BX, NLD

Abstract. In this paper, a summary of insights has been written to further elaborate on data that has been gathered on Distributed Denial of Service (DDoS) attacks. This paper gives a short introduction to the topic, then elaborates on the importance of DDoS attacks on the economics of cybersecurity. Furthermore, data is explained using current metrics found in literature as well as ideal metrics are discussed. Afterwards, an existing database of DDoS attacks from SOURCE is used as an example of showing potential purposes of applying data for policy making in the Economics of cybersecurity field.

Keywords: DDoS · Metrics · Economics of Cybersecurity · policy making

1 Introduction

Distributed Denial of Service (DDoS) attacks form a major threat to the reliability and services in the information and communication sector. Disruptions in critical infrastructure suffer from major consequences as society relies more on the services provided in the information and communication domain. Unreliability of services can branch out to high costs, reputation loss, and loss of customers for the company (*Lose a Fortune: One DDoS Attack Can Cost a Company Over $1.6M | Kaspersky*, n.d.). Cases have already occurred where portions of the world did not have access to the internet (Newman, 2016). In essence, multiple machines work together to make services unavailable in a DDoS attack. As multiple machines increase the strength of an attack it also makes it difficult to determine the source of the attack (*Understanding Denial-of-Service Attacks | CISA*, n.d.).

Concept: - add introduction to the used dataset

2 Methodology

In order to get a better view on the existing threat of DDoS attacks, this report will discuss the phenomenon in the following steps: Firstly, the exact security issue that is threatened by DDoS will be discussed. Secondly an ideal way to measure the threat and its effects will be explained. Then, this ideal, non-existing metric will be compared with the existing metrics in literature, after which also the possible metrics in the received data set will be elaborated on. The report ends with a conclusion that combines the findings.

3 Security Issue

(1. What security issue does the data speak to?) Before looking at any metrics that can evaluate the size of DDoS attacks, it is important to focus on the value that is actually threatened. In security, three parts should be clear. THe first is to know Who or what should be protected. In this case this can be any organization. The second part is what value should be protected, which is availability of services in the case of DDoS attacks. If a DDoS is executed successfully, the service of the corresponding organization will be unavailable for some time, which is not desirable, as has been explained in the introduction.

4 Ideal Metrics

(2. What would be the ideal metrics for security decision makers?) To security decision makers, it would be ideal to have a complete overview of all parts of the existence of DDoS attacks before any attack takes place. This includes the periods before, during and after the attack. Before the attack takes place, decision makers would be fully informed if all existing reasons for a DDoS attack are known. If a company or governmental organization would have access to this information, they could pinpoint potential attackers and try to remove the corresponding reason. From this reason a probability should be known that shows the chance of a certain organization being attacked by a DDoS attack. If it is known that an attack is probable in the coming hours, the organization could put preventive protection in place such as a dynamic IP address. Lastly, it can be useful for decision makers to know how vulnerable the organizations system are and where these vulnerabilities come from.

In the case that a DDoS attack does take place, it is important that the victim and security deicsion makers are completely up to date on the size of the attack and the location of the botnet/attack cluster of the attack, in order to mitigate as soon as possible.

After a potential attack is finished or dealt with, it is important for decision makers to know about the damages that the attack caused. This should be both the size of the costs, as well as the type of costs, which could be any of the damages named in the introduction.

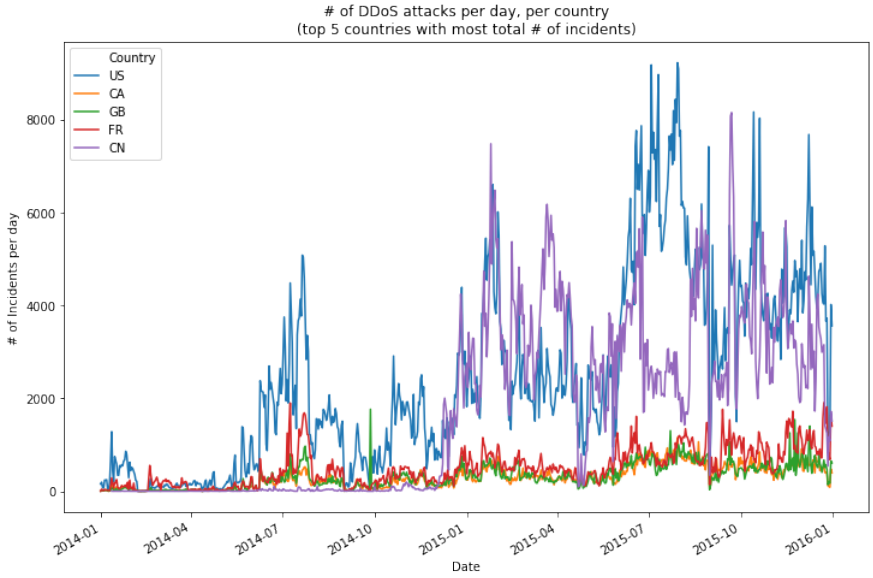
Concept: - Specify metrics further

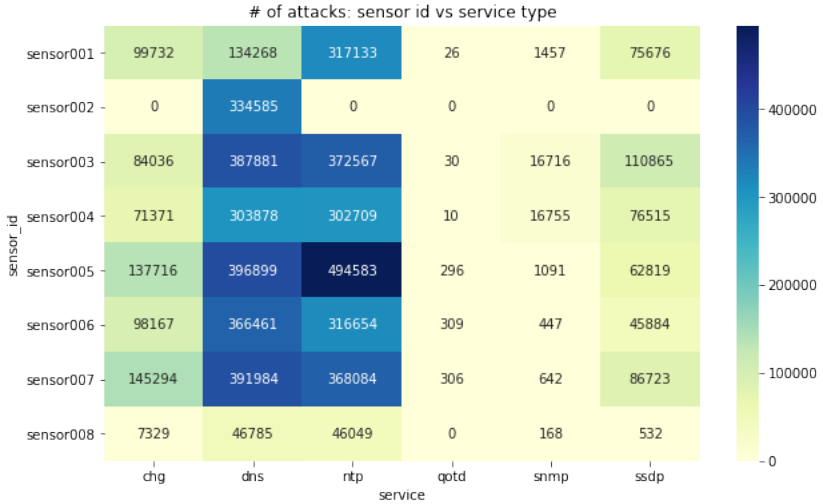
5 Existing Metrics

(3. What are the metrics that exist in practice?)
Types of metrics:
- Controls
- Vulnerabilities
- Incidents
- (Prevented) losses

6 Present Metrics

(4. A definition of the metrics you can design from the dataset)
- Number of attacks per day per country - of attacks per sensor id and service type





7 Evaluation of Metrics

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).

8 Conclusion

Exciting

References

Lose a Fortune: One DDoS Attack Can Cost a Company Over $1.6m | Kaspersky. (n.d.). Retrieved 2019-09-16, from https://www.kaspersky.com/about/press-releases/2016$_l ose-a-fortune-one-ddos-attack-can-cost-a-company-over-1.6m$

Newman, L. H. (2016, October). What We Know About Friday's Massive East Coast Internet Outage. *Wired*. Retrieved 2019-09-16, from https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

Understanding Denial-of-Service Attacks | CISA. (n.d.). Retrieved 2019-09-16, from https://www.us-cert.gov/ncas/tips/ST04-015