Assignment 1: Security Metrics
WM0824TU Economics of Cybersecurity (2019)

Brennen Bouwmeester, Hsin Cheng, Kevin Su, and Jochem Vlug

Group 5 (DDoS), Delft University of Technology

Abstract. In this paper, a summary of insights has been discussed to further elaborate on data that has been gathered on DDoS attacks. This paper gives a short introduction to the topic, then elaborates on the importance of DDoS attacks in the economics of cybersecurity. Furthermore, current metrics found in literature as well as ideal metrics are discussed, that can put the data into perspective. Afterwards, the "AmpPot" DDoS attack database is used as an example of showing potential purposes of applying data for policy making in the field of economics of cybersecurity.

Keywords: Distributed Denial-of-Service (DDoS) · Security Metrics

1 Introduction

Distributed denial-of-service (DDoS) attacks form a major threat to the reliability and services in the information and communication sector. These malicious attempts, through overloading the capacity of the target service or its surrounding infrastructure with a flood of Internet traffic, aim to disrupt normal traffic of a targeted server, service or network. Disruptions in critical infrastructure lead to more serious 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 (Kaspersky.com, 2015).

To protect stakeholders from DDoS attacks and prevent losses, enterprises have been spending on security investments. The key question in management of information security is if this money is being spent well (Böhme, 2010). To answer this, security metrics, which are the essentials of security investment models, are designed to describe the cost of security investment, security level and the benefits (Böhme, 2010). However, the selection or design of security metrics is challenging due to the nature of cybersecurity, e.g., security level is a "latent construct" which cannot be observed or measured directly.

In this assignment, we look into the theories and practices of security metrics with a case analysis on DDoS attacks using the AmpPot dataset (Krämer et al., 2015). This report is divided into the following steps: First, the security issue is defined with concrete specifications. Based on defined security issue, ideal measurements as well as existing metrics are presented and discussed. Building on present theories and practices, we then try to create meaningful security metrics and implement them with the given AmpPot DDoS attack dataset. Finally, we discuss the results and conclude with the findings.

2 Security Issue

Security metrics are indirect measurements of the security level. The metrics are used to transform data into meaningful information, which provides specific actors with insights for defining new policies or means for specific issues. Baldwin (1997) defined the concept of security in terms of several specifications. In this assignment, the following three basic specifications are selected and discussed:

1. *Security for whom?* - or, who the "problem owner" of the security issue is. This can be the individual, the state, the international system, etc.
2. *Security for which values?* - which is the "objective" of the defined problem owner. Individuals, states, and other social actors have many values: e.g. physical safety, economic welfare, autonomy, etc, which lead the actor to its specific goal of security issue.
3. *From what threat?* - or the particular kinds of threats that the problem owner is facing in these issues.

Below we define the three specifications for the given issue for this assignment:

2.1 Security for whom?

DDoS attacks are malicious attempts against a targeted server, service or network that cause a "traffic jam" clogging up with highway, preventing regular traffic from arriving at its desired destination. Among the types of victims, service hosting providers - or more specifically, Internet Service Providers (ISPs) and web hosts - are one of the most influenced actors in terms of DDoS attacks. These service hosting providers strive to have their servers available at all times against the disruption of abnormal Internet traffics brought by DDoS attacks; in other words, DDoS attacks form a major threat to the core business of service hosting providers. Therefore, in this assignment the focus will be on the security for server hosting providers.

2.2 Security for which values?

The second part of security is a "value" that should be secured. In the case of DDoS attacks this value is the availability of services. 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.

2.3 From what threat?

The third and last part of security is from whom this value of availability should be protected. In the case of DDoS attacks, the "attacker" can be anyone who has an incentive to break down the availability of a service and also has (indirect) access to a large number of infected computers that are needed to perform the attack. This could be a rival company that wants to take over the market, but also vandalism.

In summary, in this assignment the focus will be on the security issue for service hosting providers, who are threatened by DDoS attacks that potentially lead to disruptions of their services and thereby losses of fortune.

3 Ideal Metrics

The security issue in this assignment is defined for service hosting providers, who are facing threats of service disruptions brought by DDoS attacks. A common practice to secure themselves from the threats is security investments on, for instance, strengthening their service infrastructure. The key question for the service hosting providers in management of information security is then whether this money is being spent well (Böhme, 2010). An ideal metric to "measure" this is the Return On Security Investment (ROSI) (Böhme, 2010; Purser, 2004; Böhme & Moore, 2009). We further discuss this metric using the notion of security production function (Böhme, 2010), as shown in Figure 1.

3.1 Controls

ROSI exists of the ratio between the investments in security and the received benefits. In the scheme of possible computer security metrics, the security investments would be placed under the control flag, as the investments translate to different actions put in place to keep attackers out. This could be, for example, investing in dynamic IP addresses. Probably, the investments will not cover all existing threats, as not all threats are known beforehand. Therefore, ROSI should include the "costs" of vulnerabilities (also found in the security metrics scheme, Figure 2). Ideally the place and size of each of the vulnerabilities are known, which means a straightforward height of costs can be calculated by multiplying the probability of an incident (happens in the security metric scheme if a vulnerability gets exposed and used) with the effect that this incident would have.

3.2 Benefits

The benefits part of ROSI can be found at the other end of the security metrics scale - the part of prevented losses. In an ideal situation, all uncertainty of the possible attacks would be non-existent. Ideally, the losses that were prevented by the controls in place are completely known, which means also ROSI can be calculated without uncertainty. Prevented losses could for example exist of keeping a strong reputation or losing no customers due to the prevention of any unavailability. Ideally, these rather qualitative prevented losses can be translated into a monetary value easily. This would lead to a simple decision on the height of the investment by decision makers, leading to a certain level of prevented losses.

3.3 Security level

Before the attack takes place, it would also be helpful if decision makers would know all existing reasons for a potential DDoS attack on their organization. This would make them able to pinpoint potential attackers and try to remove the corresponding reasons. If removing this incentive is not possible, the information could also predict potential attacks in the near future, making it easier to take the right steps at the right time.

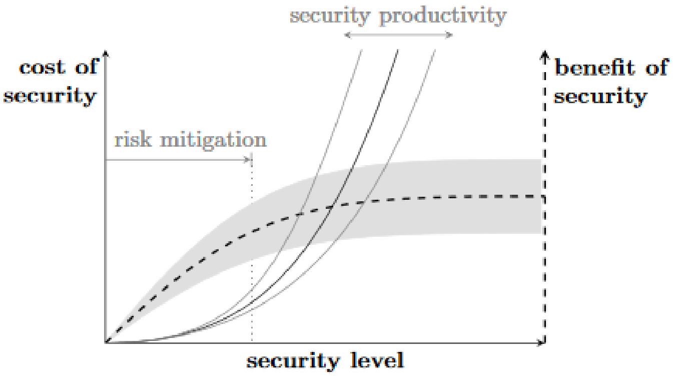


Fig. 1: The security production function (Böhme, 2011)

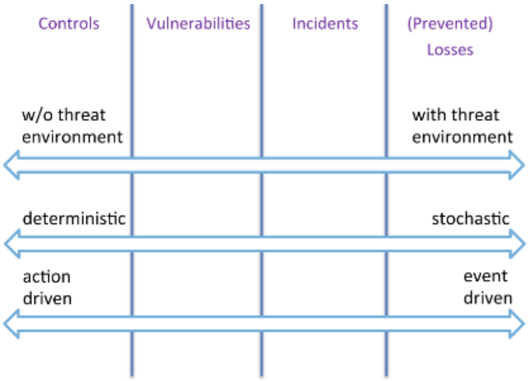


Fig. 2: Security metrics scheme (Noroozian et al., 2016)

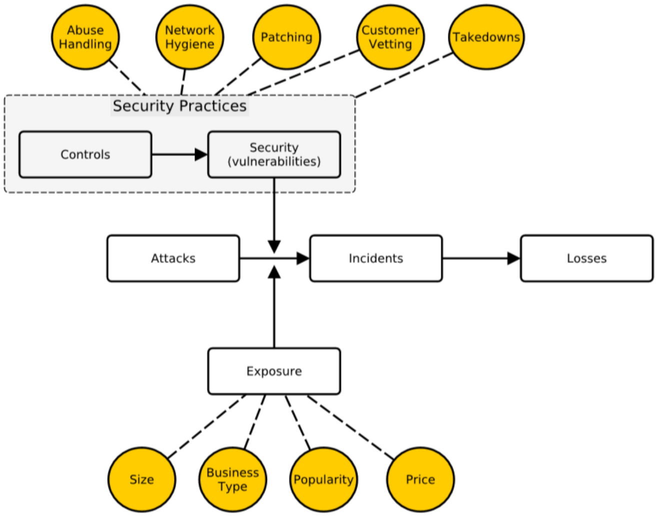


Fig. 3: Causality model incidents and the corresponding four types of security metrics (Noroozian et al., 2017)

4 Existing Metrics

To get more insights into the current practices of actors regarding security against DDoS attacks, an overview is made of existing security metrics. By reviewing literature and industrial reports, a list of current metrics can be established. In the scientific literature, the basis can be found for the security metrics that can be extracted from the available data, which will be elaborated on in the next chapter. The industrial reports show the incentives of businesses to report certain security metrics, and thus show commonly used security metrics.

4.1 Scientific literature

When looking for an overview of DDoS attacks, an impact analysis can be very insightful. The impact analysis of Arora et al. (2011) reveals the enormous financial costs of DDoS attacks on companies (Arora et al., 2011). Looking at the security metrics scheme (Figure 2), this type of metric can be seen as one under the "losses" flag. In this paper the technique to attack, botnet size, and attack traffic are the most important metrics that where analysed. A financial report on damages caused by fraudulent behavior on the internet in 2007 shows that DDoS caused around $2,8 billion in damages (Richardson, 2007). This is also an important metric for companies, since it shows how important securing against a loss of availability is for the revenue of a company. In their paper, Buchanan et al. (Buchanan, Flandrin, Macfarlane, & Graves, 2011) proposed a methodology of evaluating DDoS attacks using a framework based on their research. As a result, the paper distinguishes between three types of metrics to evaluate DDoS attacks: response, impact and resource metrics. To put these metrics into perspective, the security metric framework (Figure 2) is used. A column was added to the table of Buchanan et al. that shows in which of the categories (according to the metric types of Noorozian (2017)) each of the metrics can be placed.

Table 1: Evaluation Metrics from Buchanan (2011)

Category	Name of Metric	Description	Metric type
Response metric	Packets lost by source	Rate legitimate packets lost	Incidents
	Packets lost by destination	Overall packets lost	Losses
Impact metric	Available Bandwidth	Rate of maximum traffic that could pass through the DUT	Controls
	Latency	Time spent for a packet to cross the DUT	Vulnerabilities
	Data Throughput Since Intervention (DTSI)	Number of packets before the DUT responds to the threat	Vulnerabilities
	Reliability	Time without a system error	Vulnerabilities
Resources metric	CPU Load	Percentage of CPU load	Controls
	Memory Load	Percentage of memory load	Controls

4.2 Industrial reports

When looking at the reports written by the security industry, a tendency is to articulate the preparedness of a network to withstand DDoS attacks. Although not mentioned in the industry, these kinds of metrics can be placed in the control part of the security metrics scheme (Figure 2) Furthermore, the industry uses metrics to show the minimized or negated damages caused by loss of availability of services whilst offering the least amount of infrastructural costs. A few examples from the industry reveal these metrics.

The first paper shows the growth of the use of DDoS Prevention Systems (DPS) such as CloudFlare by businesses by a factor 1.24x (Jonker, Sperotto, van Rijswijk-Deij, Sadre, & Pras, 2016). In the paper, the most important metric that comes up is the amount of diverted traffic (from a DDoS attempt).
In a paper showing the effectiveness of Software-defined Networking (SDN), the metrics are defined as "An effective DDoS attack detection system requires the ability to rapidly respond to increasing malware traffic. This type of metric can be seen as an incident metric (Figure 2) as it measures the severity of a potential attack. Furthermore, customizability and ease of management in application of rules for detection and prevention against DDoS attacks is also required." (Bawany, Shamsi, & Salah, 2017). Compared to the ideal metrics established in the previous chapter, there can be stated that the existing metrics are relatively far away from the ideal metrics. Although the costs that DDoS attacks invoke can actually be calculated, the relation between investments and and these costs is absent.

5 Security metrics for DDoS attacks

The DDoS dataset that is used for this assignment is AmpPot dataset (Kaspersky.com, 2015). The dataset contains victim data gathered from eight amplifier honeypots with a measurement period of two years (2014-2015). While empirical data can help focus the security level on the threat environment, Noroozian et al. (2017) mentions four problems measuring security performances in empirical data.

5.1 Problems of abuse dataset

Firstly, noisiness of data is an issue in the dataset. To categorize hosting organizations, a classification algorithm was created with a false-positive/true-positive rate of 0.17/0.74 (Noroozian et al., 2016). Misattribution of organizations can give wrong conclusions specific to the type.

Secondly, considering the completeness and bias of data the Japanese based honeypots only measured between 01-01-2014 and 31-12-2015, with support for specific protocols. The dataset therefore does not contain attacks excluding Japanese IP ranges, different protocols, or long-term trends of DDoS amplifier attacks.

Thirdly, datasets are often very heterogeneous in measurements, therefore each dataset will measure their own perception of reality. While there is one AmpPot dataset, this consists of data from multiple honeypots. Figure 4 shows that there are differences between the types of attacks and the honeypots. For example, *sensor002* does not include any services except for DNS which could lead to an overestimation of DNS-service attacks. It is clear that *sensor008* was added at a later date as it has less records of attacks but it biases the dataset with an temporal aspect towards new trends. *Sensor003* and *sensor004* also has more attacks recorded with the snmp-service, whereas the other sensors score low.

Fourthly, multi-causality makes it difficult to establish the security performance. A wide variety of factors can affect the DDoS attacks unrelated to the security level, for example the motivation of attackers are factors that cannot be easily measured (de Bruijne, van Eeten, Gañán, & Pieters, 2017).

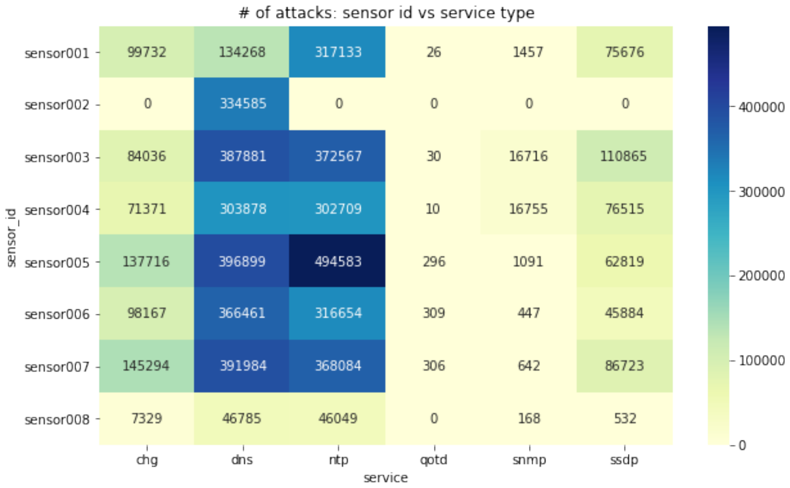
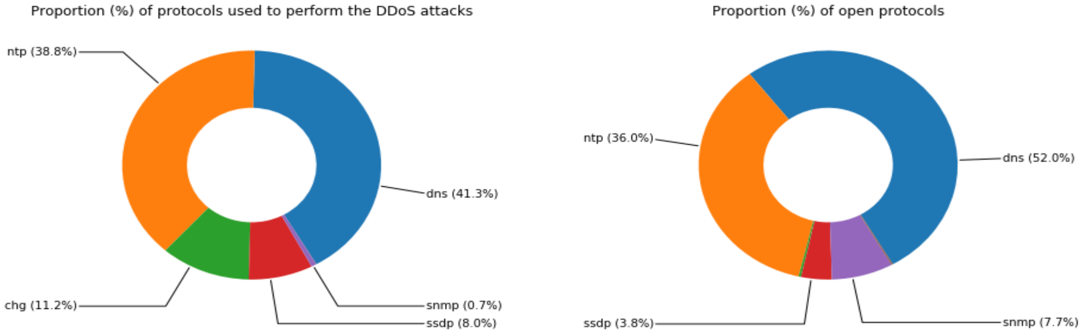


Fig. 4: Observed number of DDoS attacks: per protocol type and deployed AmpPot honeypot

5.2 Present and evaluation of metrics

Before we will go into specific metrics that can be extracted from the dataset, we will show a general overview of the dataset. From this point on, we will work towards metrics that are more useful step by step. Showing this process is useful in understanding what the metrics show. There are $5,721,431$ records of attacks across IP-addresses associated with 216 (raw) countries. Figure 5 shows the percentages of the services of the DDoS attacks compared to the percentages of open protocols. The data for open protocols is gathered from Shodan.io. Open protocols are commonly used for reflector attacks as they are easily abused. This figure shows that attacks performed by CharGen are from a limited number of open services with the CharGen protocol. It seems that the DNS and NTP protocols are popular as a means of amplification services, the majority of attacks also have the most open services.

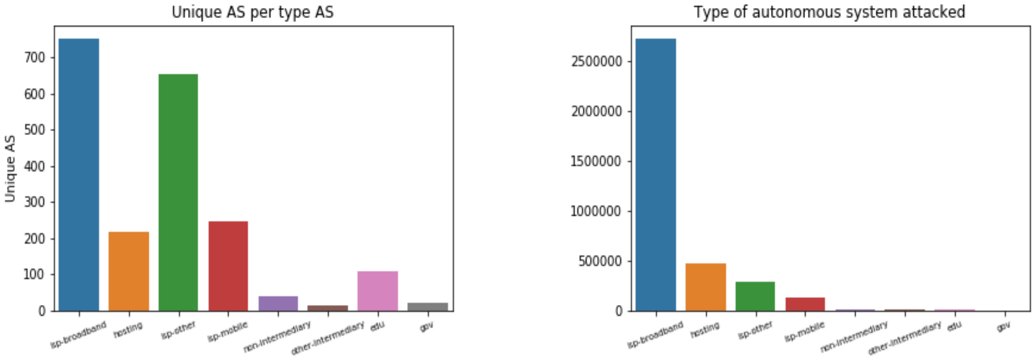


(a) Percentage protocols used in DDoS attacks

(b) Percentage open protocols

Fig. 5: Number of attacks over unique AS and type autonomous system

Figure 6 shows more information regarding who gets attacked accounting for the size of certain autonomous system sectors. Broadband ISP take the majority of the DDoS attacks on their systems. Hosting providers are ranked second in number of attacks despite being ranked 4th in unique autonomous systems. This discrepancy was also shown in Noroozian et al. (2016) however it is important to show that the high number of attacks on hosting providers are due to other factors than size.

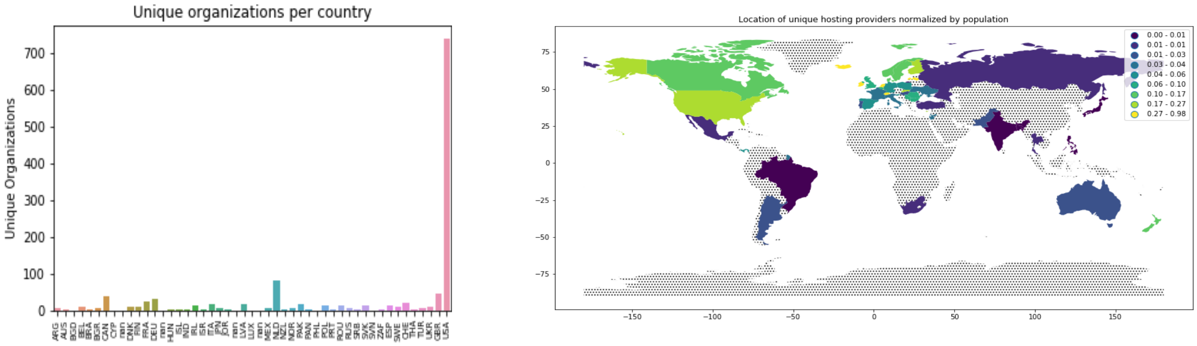


(a) Unique AS

(b) Type autonomous systems

Fig. 6: Number of attacks over unique AS and type autonomous system

Figure 7 shows the unique organizations in a country which are classified as a hosting provider. The top five locations where hosting providers are attacked: United States, Netherlands, United Kingdom, Canada, and Germany. However, this might be due to the number of organizations in a country. As a way to normalize for this effect they unique organizations are divided by the population in the country. Compared to the not normalized metric, taking into account the population shows that the problem is the biggest in Iceland, followed by Latvia and the Netherlands. This has limits on its own because these hosting providers are not limited to the population but rather infrastructure and availability of a country.



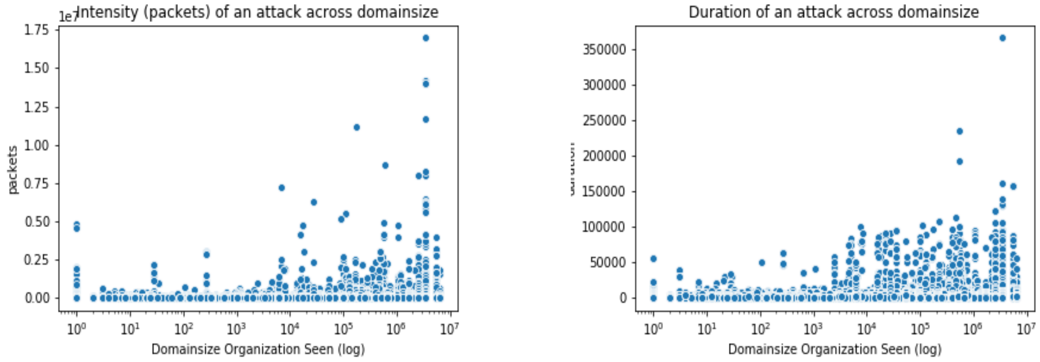
(a) Unique organizations

(b) Unique organizations normalized per population

Fig. 7: Unique organizations classified as hosting providers

Figure 8 showcases the intensity and duration of the DDoS attacks across domain size of hosting organizations. As hosting providers host multiple domains it relates to the size of the organization. Bigger organizations would most-likely attract bigger attacks. Possible other reasons not related to size for this are evaluated by Noroozian et al. (2016) as they mention that popularity and type of hosting providers are important. Due to the limited resources of this project, other reasons are not further declared.

These metrics have focused on the size of services (protocols), the uniqueness and type of AS, location of hosting providers, and the strength of DDoS attacks across hosting providers. While these metrics are useful for an explanatory overview, the security level of the issue is difficult to determine. The security level is a latent construct that is not directly observed. The current metrics help reflect on different aspects of the security level, but have not yet resulted in a multi-factor analysis to measure security level. They help to compare the problem of DDoS attacks in different organizations and countries, but do not suffice in comparing the actual costs as a result of the attacks, or the effectiveness of different ways to deal with the problem.



(a) Packets

(b) Duration

Fig. 8: Packets and duration of a DDoS attack across domain sizes of hosting providers

6 Conclusion

Distributed Denial of Service (DDoS) attacks can harm service hosting providers in their core business of having servers available at all times. This availability should be protected against any individual or organization that has an incentive to break it down.

In order to measure how well the availability is protected from these potential attackers, it is important to have complete and useful metrics in place. Although it is close to impossible to ever reach the ideal metrics that were discussed in this paper, it is important to keep these in mind when thinking about metrics that can actually be used in the reflecting on security against DDoS attacks. Literature showed that multiple researchers have attempted to pinpoint useful metrics on DDoS attacks. It turns out that calculating the total costs for companies can be achieved, which relates to the ideal metrics. However, what the influence of investment in controls against DDoS attacks is precisely, did not show up in any literature or industry metrics.

The metrics calculated from the data set are even further away from the ideal metrics defined in this paper, as we were limited to the existing columns in the dataset. The focus was on the geographical location where DDoS attacks form the biggest problem. In this, we took into account the size of the different countries, considering their populations to create a normalized value that shows how bad the problem is in different countries. This showed that the most victims are located in Iceland, followed by Latvia and the Netherlands. Although it is now still unclear why these countries perform worst, it can perhaps be stated that protection measures should be higher on the agenda in these countries.

Another metric extracted from the dataset is the positive correlation between the size of an organization and the number of attacks that take place against the organization. This shows that the focus in protection should perhaps be proportional to the size of an organization.

These identified and created metrics are only a start for achieving a complete and useful set of metrics. In the future, more data from the dataset and other datasets should be processed into a set of metrics that can clearly show the location of the problem of DDoS attacks, as well as the size of the problem and the performance of different protection measures. Examples would be the actual time that a server was not available or the number of customers that could not use the server due to the unavailability. Metrics like these can be translated to costs, which would lead to metrics closer to the ideal metrics found in this paper, leading to a better understanding of the system by the security decision makers, which would lead to policies that perform better.

In summary, it is hard to find and calculate metrics that are useful, even though the focus should be one these useful metrics rather than of those easily obtainable. This paper showed that even with a limited amount of data, still useful metrics can be created. However, there are multiple limitations to these metrics and time should be invested further to make more useful metrics achievable. This will then improve the way service hosting providers can protect the availability of their servers from DDoS attackers.

References

Arora, K., Kumar, K., & Sachdeva, M. (2011). Impact analysis of recent ddos attacks. *International Journal on Computer Science and Engineering*, *3*(2), 877–883.

Baldwin, D. A. (1997). The concept of security. *Review of international studies*, *23*(1), 5–26.

Bawany, N. Z., Shamsi, J. A., & Salah, K. (2017). Ddos attack detection and mitigation using sdn: methods, practices, and solutions. *Arabian Journal for Science and Engineering*, *42*(2), 425–441.

Böhme, R. (2010). Security metrics and security investment models. In *International workshop on security* (pp. 10–24).

Böhme, R., & Moore, T. (2009). The iterated weakest link model of adaptive security investment. *Journal of Information Security*, *7*(02), 81.

Buchanan, B., Flandrin, F., Macfarlane, R., & Graves, J. (2011). A methodology to evaluate rate-based intrusion prevention system against distributed denial-of-service (ddos). *Cyberforensics 2011*.

de Bruijne, M., van Eeten, M., Gañán, C. H., & Pieters, W. (2017). Towards a new cyber threat actor typology. *Delft University of Technology*.

Jonker, M., Sperotto, A., van Rijswijk-Deij, R., Sadre, R., & Pras, A. (2016). Measuring the adoption of ddos protection services. In *Proceedings of the 2016 internet measurement conference* (pp. 279–285).

Kaspersky.com. (2015). *Smbs lose around* $38,000$ *in every cyber-attack.* Retrieved 2019-09-16, from `https://www.kaspersky.com/about/press-releases/2015_smbs-lose-around--38000-in-every-cyber-attack`

Krämer, L., Krupp, J., Makita, D., Nishizoe, T., Koide, T., Yoshioka, K., & Rossow, C. (2015). Amppot: Monitoring and defending against amplification ddos attacks. In *International symposium on recent advances in intrusion detection* (pp. 615–636).

Noroozian, A., Ciere, M., Korczynski, M., Tajalizadehkhoob, S., & Van Eeten, M. (2017). Inferring the security performance of providers from noisy and heterogenous abuse datasets. In *16th workshop on the economics of information security. http://weis2017. econinfosec. org/wp-content/uploads/sites/3/2017/05/weis_2017_paper_60. pdf.*

Noroozian, A., Korczynski, M., Hernandez Ganan, C., Makita, D., Yoshioka, K., & van Eeten, M. (2016). Who gets the boot? analyzing victimization by ddos-as-a-service. In *Proceedings of the international symposium on research in attacks, intrusions, and defenses, raid 2016.* Springer.

Purser, S. A. (2004). Improving the roi of the security management process. *Computers & Security*, *23*(7), 542–546.

Richardson, R. (2007). The 12th annual computer crime and security survey, 2007. *Retrieved on September*, *18*.