Technical University of Delft

Faculty of Technology Management and Engineering

Principals of Policy Analysis –

Economics of Cyber Security - Final individual assignment

Member of Group 4

Tzanakou, Eleni

Engineering and Policy Analysis

4417895

9th November, 2015

Abstract

DDoS attacks are one of the major threats in our world. Many security issues are caused by these attacks. The idea of this study is to focus in one certain issue, which is the unavailability of server, to explain the negative results from the different stakeholders after that to investigate what affects it. Thus, the main question of the research is if there is a relation between the packets transferred to the targets due to a DDoS attack and the duration of this attack. A quantitative analysis was conducted and the results show that there is a weak positive relationship between these two variables. We observed that nowadays there is a new trend characterized the DDoS attacks which are: *short attacks with high impact*.

Introduction

According to Stallings (1999) there are six basic principles that should be followed in order to provide the appropriate security into a network and an organization. Thus, a computer system should be satisfying the following principle: availability, confidentiality, integrity, authentication and interoperability in order to sustain secure against a DDoS attack.

Participants of a research conducted by the Ponemon Institute (2012) were asked to rank the security principles from 5 (highest priority) to 1 (lowest priority). The results of the research indicate that the availability of the system -the included information to those who need them, anytime they want them- is in the highest security priority of an organization (4.7%). For these reasons, in our research we decided focus in the principle of the availability of the system and how the duration and a volume of a DDoS attack can affect it.

When a DDoS attack launches into a network system many negative effects are taking place immediately. The security issue that we examine in this assignment is related to the negative consequences (i.e. packets transferred, traffic caused and server's unavailability etc.) into a system due to DDoS attacks. Our database contains information about many DDoS attacks from 2013 to 2015. Through literature research we try to define the direct and indirect losses that the owners of the autonomous systems (AS), which are mostly ISPs, and other related stakeholders like customers, infrastructures etc. face due to DDoS attack. By conducting a statistical analysis we want to give a better insight into this issue (e.g. how much time an attack lasts, which is the packet rate per attack and how much traffic is caused into the system).

Literature Review

Nowadays, DDoS attacks are one of the most serious threats. Many well-recognized firms like Pay Pal, Google, Microsoft, Apple and Visa etc. are already toppled by DDoS attacks (Alomari, Manickam, Gupta, Karuppayah & Alfaris, 2012). The first DDoS attack took place at the

University of Minnesota in August 1999 against the Relay chat server. The university's server was rendered unusable for two days and at least 214 systems were involved in this attack (Criscuolo, 2000).

A DDoS attack is characterized by the recruitment of several hosts over the Internet that attack either all together or in a coordinated manner. The goal of a DDoS attack is to attack targets systems' resources in order to make the systems deny service. Thus, a DDoS attack blocks the targeted networks and renders them unavailable to users (Kaur & Sachdeva, 2013).

If the system is down for a certain amount of time then the direct and indirect losses are many. According to the Jones (2006), when a DDoS attack takes place the internal processes into a system are decreasing and the system is not productive any more. Thus, because of the traffic that is causing into the system the ISPs are not able any more to protect the existing information into the system and to provide the appropriate internet services to their customers. Therefore, if the attack took the entire server for several hours the ISPs should find the quicker way to response in this situation as for example by hiring external experts and consultants.

Moreover, the customers that are affected by the attacks are unable to use the resources of the server and they might change to another ISP because they will not trust them anymore and possible future customers might be discouraged to choose its services. In addition, the customers that suffered by the unavailability of the online services could also file lawsuits against the ISPs.

As a result, the negative impacts of a DDoS attack could be (Ponemon, 2012):

- lost intellectual property
- reduction in productivity
- lost revenue
- legal pursuits and fines
- damage to reputation

Many several researches showed that last years the number and the damages of DDoS Attacks have increased and at the same time the duration of these attacks have declined (Corero, 2014). Also, a research conducted by Arbor Networks (2013), indicates that the duration of the largest DDoS attacks as reported by the majority participants of the survey last from 0 to 6 Hours with 48%. Less than the one-eighth (1/8) of the total sample of participants (11%) described that the duration of the attacks was between 7-12 Hours. And only the 5% of respondents conclude that the largest DDoS attacks last from 13-24 Hours.

Another research took place also in 2013, concluded almost in the same results as concerning the duration of the attacks. The majority of the attacks (87%) last less than an hour (Turner, 2014). Additionally, a report published by the Corero organization in the last quarter of 2014 presents that 96% of attacks targeting their customers lasted less than 30 minutes. At the same time, the negative consequences of the attack are inverse proportional to the duration. Thus, an attack that lasts for some minutes cause huge damages into the system and characterized as "high-risk attack". Thus, nowadays we should not focus any more in the high volume and long duration attacks as we did in the past but in the new trend of the DDoS attacks which are short attacks with high volume.

As we already mentioned, many researches are conducted concerning the duration of the attacks. On the other hand, researches that combine the volume and as a result the losses of the DDoS attacks with the duration of the attacks are limited. In this study we investigate if there is a relation between the duration of the DDoS attacks and the damage that cause into the system.

Research Question, Objective and Hypothesis

It is a fact that in recent years the continuous evolution of technology contributed significantly the DDoS attacks to become one of the most dangerous threats. This assignment aims to investigate if there is a relation between the duration of the attacks and the amount of packets that transferred in these attacks. Through this work we want to study the impact of a DDoS attack for the targets.

In order to describe, explore, explain and evaluate one or more characteristics of the given database, processing and analysis of quantitative data happened (Cohen & Manion, 1997). Therefore, a quantitative research, which shows us if there is a relation between the duration of the attacks and the packets that the attackers send to the targets is conducted.

The main research question that arises with the objectives of this research is:

- "Do the losses caused by a DDoS attack have any relation with the duration of the attack?"

More specifically in this study the following research question is examined:

- "Does the unavailability of server have a significant relation with the duration of this attack?"

To investigate the research question and achieve the goal of the study a literature and quantitative research was conducted.

The main negative consequence of DDoD attacks that we focused on this study is the high bandwidth consumption of the intended target during a DDoS attack. The feature that represents the bandwidth consumption is the packets that are transferred by the attacker. So, through this study it should be investigated we should investigate the duration of the attacks and the amount of transmitted packets of the attacks. It is expected that there is a positive relation between the packets and the duration.

Methodology (Research Design)

a. Data refinement

The first step of pre-processing was cleaning the data. In particular, we removed all the durations that had value 0 since they provide faulty information. Probably, they were milliseconds which rounded to zeros. After that, we observed that the variance of duration was really high. Therefore, a log transformation for duration was necessary. Other than that, since we focus on the relationship between duration and transferred packets we eliminated all features except for duration and packets. In addition, we created an extra feature, the packet rate. Packet rate is the speed at which packets traverse a network, measured in packets per second (pps).

b. Statistical analysis

Afterwards, we examined whether there is a significant correlation between the duration of an attack and the packets transmitted during this attack by performing Pearson's correlation.
Moreover, we plotted the distribution of log values of durations over the resulted histogram. A normal distribution is observed where most of the values are between 40 seconds and 10 minutes.

In addition, we divide the dataset into three classes.

- Low-duration, between 0 ~ 40 seconds
- Normal-duration, between 40 seconds ~ 10 minutes (most of the values fall into this category)
- High-duration, from 10 minutes ~ max value

After that, we plotted the boxplots of the log transformations of packet rates for these three different categories. Outliers were previously removed. We do this to check the different variations among the groups. In order to test the variations of groups means the ANOVA test was performed.

Results

At first, to check whether there is any relation between the duration and the packets transmitted in this duration we use Pearson's correlation coefficient test. Pearson's correlation results indicate a positive, weak, significant relation (significance 2.2e-16<0.05 and correlation coefficient equal to 0.35 - **Table 1**). H0 is thus rejected and a relation between duration and transmitted packets is observed.

Table 1 - Pearson's product-moment correlation

Pearson's product-moment correlation		
data: duration and packets		
t = 702.72	df = 3478000	**p-value < 2.2e-16**
H1 – alternative hypothesis: true correlation is not equal to H0		
95 percent confidence interval: 0.3516830 0.3535236 sample estimates: cor = 0.3526036		

Figure 1 indicates the scatter-plot of duration in seconds against packets. The red line in the plot illustrates the best fitted linear model for this dataset, which means that the next point that comes from a test set is more probable to be on this line.

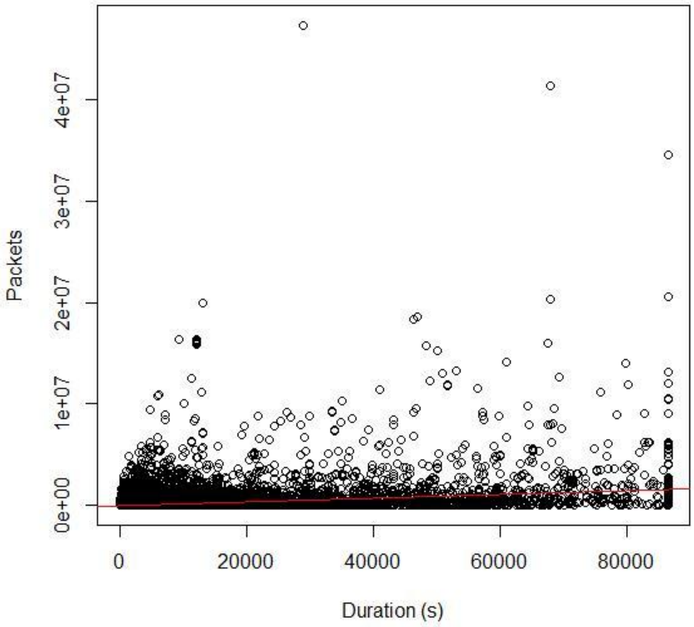

Figure 1 - Scatterplot of duration against packets

In addition, the Figure 2 illustrates, the histogram with the fitted normal distribution of the dataset was plotted where most of the values are between 40 seconds and 10 minutes.

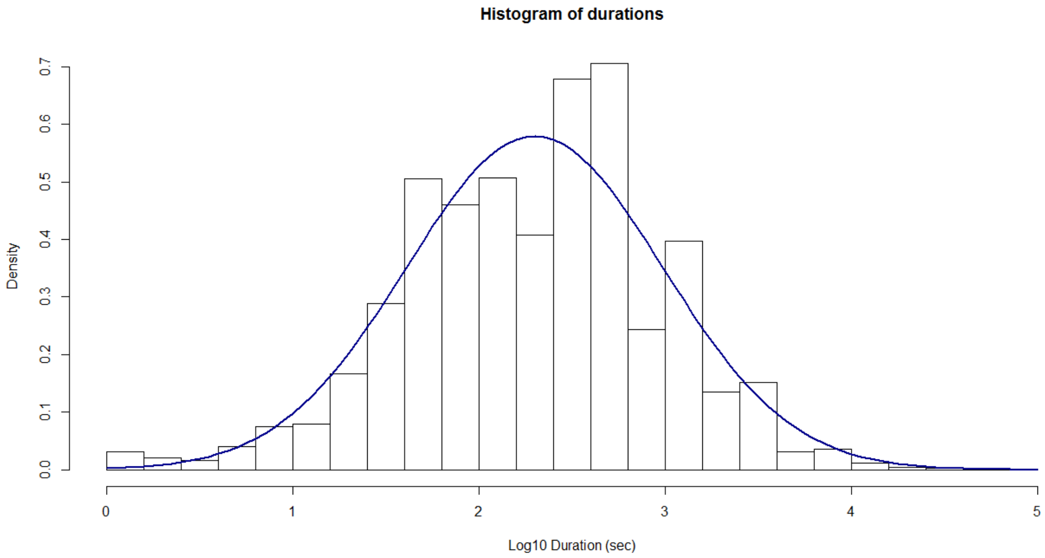

Figure 2 - Histogram and normal distribution of log of duration

We split the dataset into three groups depending on the duration and the density of the attacks. In **Figure 3**, the boxplots of packet rates for these groups are illustrated.

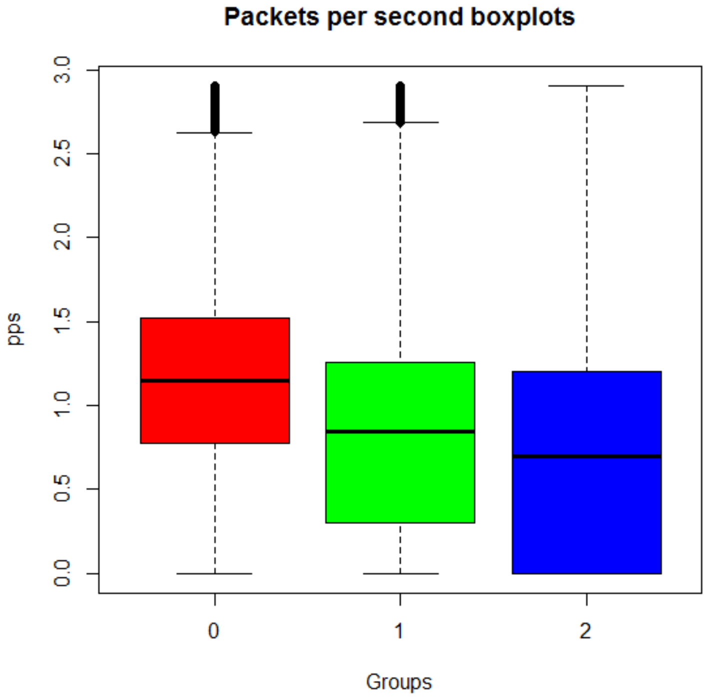

Figure 3 - Boxplot for packets rate in each groups

Surprisingly, the group 1 with the shorter durations has higher packet rates mean than the other two. To test whether the variations between the groups means are caused due to true differences about the populations means or just due to sampling variability we performed ANOVA test (**Table 2**).

Table 2 - ANOVA test

ANOVA test – Packet rates per Label (1, 2, 3)					
	Df	Sum Sq	Mean Sq	F value	Pr(>F)
Label	1	1.040e+08	104037754	**9984**	**<2e-16**
Residuals	3478019	3.624e+10	10420		

Since the F-value is high and the p-value is extremely low, the variation of packet rate means among different groups is much larger than the variation of packets per seconds within each group and this relation is significant (2e-16 < 0.05). Therefore, we accept the alternative hypothesis H1 that there is a significant relationship between groups and packet rates. This means that attacks with shorter durations are more intensive and stronger than the longer ones.

The higher density of attacks is observed between 40 seconds and 10 minutes (~55%). This comes to an agreement with previous studies where most of attacks last less than 30 minutes (Corero, 2014).

Even though the duration of an attack and the transmitted packets have a weak positive correlation, an increased packet rate is observed in the shorter duration attacks. The positive correlation between duration and packets is considered normal; as the duration is increasing the number of packets is also increasing in a degree. The second observation probably happens because of the technology improvements of recent years. This fact leads more sophisticated attacks that last less and are more efficient.

Limitations

To answer our research question we focused to a narrow set of features. It would probably be better to incorporate other data for example the targets of the attacks. In this way, we could have better insights about the losses for each server. However, it was difficult to do this in the current study since the number of unique target-ips in the dataset was more than 700.000.

Another limitation of the current study is the lack of information for the packet size. The damage that an attack causes depends mainly on two factors. Firstly, the packet rate and secondly, the packet size. So, this study could result into safer conclusions if data for packets' size were available.

Conclusion

As concluded, utilizing the results, which accrued from the analysis of the findings, it was observed that the most of the attacks have low duration. These results were expected because, as we already discussed in the literature review, all the surveys reported that nowadays the attacks last for a small amount of time and this fact happens because of the evolution of the technology.

Moreover, according to surveys of the literature we show that the duration of a DDoS attack does not play an important role in the damages that a DDoS attack can cause into a system. Last years, the new tendency is short attacks with high volume (Corero, 2014). From the above quantitative analysis we conclude almost in the same results. Even though there is a weak positive correlation between the duration and the number of packets, we indicated that the short attacks have stronger impact and thus cause more severe damage.

Finally, for securing an organization and a network against the DDoS attacks it is essential to retain the availability of the system because this is one of the most important factors (Zhang, & Parashar, 2006). Now, we investigated that the time that an attack lasts and the negative consequences that are caused into the system are almost independent. So, in order to reduce the direct and indirect losses of the attacks for the different stakeholders, there is a demand for stakeholders to be well-informed about the new technological achievements and to develop high-technology measurements that will get them one step in front of the attackers.

References

Alomari, E., Manickam, S., Gupta, B. B., Karuppayah, S., & Alfaris, R. (2012). Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. *arXiv preprint arXiv:1208.0403*.

Arbor Networks. (2013). Worldwide Infrastructure Security Report, *Volume IX*. Retrieved from: http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf

Cohen, L. & Manion, L. (1997). Research Methods in Education. *Routledge*: *London and New York*

Corero Network Security. (2014). DDoS Trends and Analysis Report, *Q4 Report*. Retrieved from: http://www.corero.com/resources/files/Reports/16803%20Corero%20Quarterly%20Report%20Q4%2014_FINAL.pdf

Criscuolo, P. J. (2000). *Distributed Denial of Service: Trin00, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht CIAC-2319* (No. CIAC-2319).

Jones, J. (2006). An introduction to factor analysis of information risk (fair).*Norwich Journal of Information Assurance*, *2*(1), 67.

Kaur, D., & Sachdeva, M. (2013). Study of Recent DDoS Attacks and Defense Evaluation Approaches‖. *International Journal of Emerging Technology and Advanced Engineering.*

Ponemon Institute LLC. (2012). Cyber Security on the Offense: A Study of IT Security Experts, Independently Conducted Research, *Ponemon Institute.* Retrieved from: http://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf

Stallings, W. (1999). Cryptography and Network Security: Principles and Practice, *2nd ed. Prentice Hall.*

Turner, R. (2014). Tackling the DDoS Threat to Banking in 2014. *White Paper of Alamai.*

Zhang, G., & Parashar, M. (2006). Cooperative defence against ddos attacks.*Journal of Research and Practice in Information Technology*, *38*(1), 69-84