Assignment Block 2 Group 4

Reviewed by group 1 28-09-2015

Summary

The topic of this paper is DDoS attacks and their economic consequences. With this type of attack, an online service is overwhelmed with a lot of traffic, which results in an unavailable online service. A security issue of a DDoS attack is the economic loss of the Owner of the Autonomous Systems due to the effects of these DDoS attacks. The dataset used to measure this issue contains information about DDoS attackers targeted at autonomous systems. Ideally, the amount of money lost because of a DDoS attack should be measured using the time lost, direct costs, indirect costs and total costs, but this is not possible using this dataset. So, new metrics were created, namely: the average impact per month and the average intensity of attacks in each country and their Internet infrastructure development. According to those metrics an uptrend in the impact of DDoS attacks was observed. Besides the defined metrics, some metrics that exist in practice were described on the basis of three papers.

Strengths of the assignment

- The used dataset is described extensively;
- Multiple papers are used to show existing metrics;
- Additional datasets are used to get better results;
- The evaluation also contains advantages, disadvantages and a comparison.

Major issues

Section: Security Issue

- There is no explanation given for the security issue. It is useful to know why the group chose this specific issue.

Section: Ideal metrics

- No major issues.

Section: Existing metrics

- No major issues.

Section: Defined metrics

- In the evaluation you evaluate a metric about the longest DDoS attacks, but this metric is not described in this section;
- You did not mention what the contribution is to the security issue for this metric: the average intensity of attacks in each country and their Internet infrastructure development;
- You are not concrete about what the metrics are, instead of using the word ‘relates’, you should be specific in what the metrics are. In the two sections before, you wrote the metrics down as a list with clear explanations beneath them. Why not write them in the same fashion in this section? Overall you could have elaborated more on the definitions to make them clearer.
    - You actually mention 3 metrics in the first part, but what is the actual metric? Not all of them can be found in the evaluation:
        - The time owners of autonomous systems lose because of DDoS attacks per month.
        - The total attack strength each AS has per month.
        - The average impact per month.

Section: Evaluation

- The results are evaluated but it is not clearly explained what the graphs and tables represent. For example:
    - Appendix A: How is the average impact calculated? What does the number on the y-axis represent?
    - Appendix B: Again, how is the impact calculated here?
- The graphs of Appendix C are not evaluated in this section.

Minor issues

Section: Security Issue

- Maybe it would be better to add an introduction in which the DDoS attack is explained, instead of adding it to the section security issue;
- The term Owner of the Autonomous Systems mentioned in the security issue is not explained before;
- In the paper ISP's are seen as owner of the Autonomous Systems, but the ISP's are not always the owner. So, maybe it would be better if 'Owner of the Autonomous Systems' in the security issue was replaced with 'ISP's'.

Section: Ideal metrics

- Your ideal metric, the amount of money lost because of a DDoS attack, does not say on which systems the attack occur. Since you described above that you focus on autonomous systems, I would suggest to add this directly to the metric, so: the amount of money lost because of a DDoS attack on an autonomous system.

Section: Existing Metrics

- You could have mentioned why you analysed those papers. Especially for the paper that is from 2004.

Section: Definition of metrics

- A dataset from Caida is being used in addition to the given dataset. However, it is not explained what this additional dataset contains or how it can be used;

Section: Evaluation

- You say that the table in Appendix B should show the 10 longest DDoS attacks, but there are only five of them in the table;
- In the evaluation you are talking about the longest attacks, but Appendix B says something about the worst impact cases. The longest attack may not always have the largest impact.