Assignment Block 4 Group 4

Reviewed by group 1 28-10-2015

Summary

This paper is about countermeasures for DDOS attacks and factors that influence a metric related to DDOS attacks. Countermeasure are defined for three actors (Autonomous System' owners, non-critical users and critical users) related to DDOS. For all of those countermeasures costs and benefits are given, the incentives of the actors are analysed and the role of externalities are discussed. Critical-users and AS owners have more incentive to take countermeasures than non-critical users. Besides the analysis of the countermeasures, factors that influence the variance in the used dataset are analysed too. First, the percentage of population online is determined using the average attack intensity of each AS registered to a certain country and also by using the attack frequency per country. After that the influence of the Gross Domestic Product is determined for both, the attack intensity and attack count. Finally, those results are used to do a multivariate analysis.

Strengths of the assignment

- Clear written paper.
- Many references are used to support your paper.
- Nice presentation of the results of your statistical analysis.

Major issues

Section: Introduction

- You should have repeated your security issue in this paper too, since the countermeasures you define influence your security issue.

Section: Owners of autonomous systems

- Costs vs. benefits
  - You do not mention indirect costs, but there will be indirect costs. For example: The productivity costs when installing and preparing infrastructure and more repair costs due to higher probability of hardware failures.

Section: Non-critical users of autonomous systems

- No major issues

Section: Critical users of autonomous systems

- No major issues

Section: Factor analysis

- "The type of actor that is visible in the metric is the Autonomous System". What metric did you mean?
- It is shown multiple times that you used R to calculate the correlation between two values. This calculation is never included though.

Section: Conclusion

- No major issues

Minor issues

Section: Introduction

- You did not explain where AS stands for

- You say that strategies are defined in this paper, but you actually defined them in the previous paper

Section: Owners of autonomous systems

- Concrete countermeasure
- Costs vs. benefits
    - Another benefit for the AS Owner may be more customers, since it is a more reliable party.
- Analysis of incentives
    - You only take the benefits into account, but what if the costs are extremely high, will the AS Owner still have incentive?
- Externalities
    - What about companies who sell hardware? Their income may rise, so they may be an externality too.

Section: Non-critical users of autonomous systems

- Concrete countermeasure
    - It is not totally clear what the concrete countermeasure is. The idea behind the countermeasure is clear but you could be more specific on the details.
- Costs vs. benefits
    - Attackers may also have indirect costs.
- Analysis of incentives
    - Here, you did not take the moral benefit into account, why not? There may be users who do have incentive for this, since they want to "improve the world".
    - Aside from moral benefits, you might want to take into consideration that users want to avoid legal issues when their system is being used for DDOS purposes. They might also fear countermeasures by third parties like their IP being blocked.
    - You did not explain if the attackers have incentive.
- Externalities
    - Antivirus program developers and sellers may benefit from this countermeasure too, since the sale will increase when people have incentive to this countermeasure.

Section: Critical users of autonomous systems

- Concrete countermeasure
    - A critical infrastructure system will never be definitely secure, reference is missing.
- Costs vs. benefits
    - Critical AS users have also indirect costs such as the costs of employees not working on other projects.
- Analysis of incentives
    - You could have mentioned the incentives of the other two actors too.
- Externalities
    - Here you also could have mentioned other countries, since critical infrastructures are most of the time connected beyond borders.

Section: Factor analysis

- Percentage of population online
    - "We cleaned the data from the UN", the reference is missing.
    - The figures do not have a name or a number and is not referenced to.
- Gross Domestic Product
    - The figures do not have a name or a number and is not referenced to.
- Multivariate analysis
    - You could have mentioned what you see as economic factors and socio-economic factors.
    - The tables do not have a name or number.

Section: Conclusion

- The conclusion sounds like a list of statements. Although that is the point of a conclusion, it is easier to read if you make a coherent story from these statements.