<Title>

René Boschma
University of Twente
r.boschma@student.utwente.nl

ABSTRACT

[COMMENT: The structure of an average abstract should have the (i) context, (ii) problem, (iii) proposal, and your most astonishing (iv) finding. Your goal is to meet ±100 words. The "context" part describes what your reader should know to understand your research. The "problem" part describes why your research need to be don; why it is interesting; and why someone needs to spend time reading your work. The "proposal" part describes what your approach has different from others. Finally, your "finding" part surprises your reader, make him VERY interested to read your paper. In a proposal you "findings" part describes what do you expect to be the most astonishing achievement of your research.]

1. INTRODUCTION

a Denial of Service (DoS) attack is an attack that aims to disable the service a target supplies. There are two main types of DoS attacks: *Vulnerability DoS* and *Flood DoS* [0]. A Vulnerability DoS aims to exploit a vulnerability of the target system to reduce performance or render it useless. An example of such an attack is to send a malformed messages to the target machines which can not deal with this message and as a result crashes. A Flood DoS attack on the other hand tries to exhaust the resources of the target. An example of such an attack is to fill the entire bandwidth of the target with messages of the attacker. The attacker can accomplish such speeds by using multiple machines to produces traffic. When multiple machines are used in the attack, the attack is called a Distributed Denial of Service (DDoS) attack.

Intrusion Detection Systems (IDS) is a system that monitors a network or system for malicious and/or suspicious activities within a network or system. Two main cattogories of IDSs are present: *host-based* and *network-based* [0]. A Host-based IDS (HIDS) is only for a single machine. A Network-based IDS (NIDS) is for an entire network. A NIDS usually scans the incoming and outgoing traffic of a network endpoint. Based on the detection methods of IDSs, again two categories can be identified: *Anomaly-based* and *Signature-based* [0]. An Anomaly-based IDS (AIDS) bases its detection on a constructed baseline and detects deviations from this baseline. A Signature-based IDS (SIDS) bases its detection on signatures. An AIDS has as benefit that it can detect unknown attacks but with the weakness that it has a low accuracy and difficulty to trigger alerts in the right time. A SIDS has as benefit that it has a high accuracy but with the weakness that it is ineffective in detecting unknown attacks and it is hard to maintain an up to date signature list [0].

DoS attacks are increasing in power. In 2011 the peak attack was measured at 60 Gb/s, in 2015 500 Gb/s and in 2016 1.1 Tb/s [0]. Also the frequency of the attacks are increasing: in the last quartile of 2016 more than 5000 attacks where observed, whereas 200 in 2012 [0]. An explanation for this increase in frequency could be the rise of *booters*. A booter, also called stressers, are websites that offer DoS attacks via a website. Booters eliminate the need for any technical knowledge to launch an attack. Clients of booters only need to pay a couple of dollars to launch an attack.

As the number of attacks are increasing and downtime costs are exceeding on average $300K per hour [1] a need for an efficient and effective mitigation method becomes bigger. We believe that SIDSs are promising systems that can fulfil these requirements when the major downside of keeping and up to date signature list is tackled. That is why in this paper we propose an automatic method to generate signatures for the SIDS Bro[1].

[COMMENT: The Introduction section has more or less the same structure as your abstract. The difference is that in the abstract each part is one statement/phrase, while in the introduction each part is a paragraph. So, (i) context, (ii) problem, (iii) proposal, and your most astonishing (iv) finding. Of course in the Introduction section you can give far more details than in the abstract. Avoid to copy and paste statements, re-write with different words.]

[COMMENT: In addition to the structure that you already know you should include your *research ques-*

[1] https://www.bro.org/

***tions* between the "proposal" paragraph and the "findings". The statement that precede the RQ is something like the following:]**

"To pursue our goal, we have defined the following research questions (RQ) as the basis of our research:

- **RQ1:** What are the current developments in automatic rule generation for Signature-based Intrusion Detection Systems (SIDS)?
- **RQ2:** How to ... ?
- **RQ3:** How to ...?

"

[COMMENT: Please, avoid "yes or no" questions. Make questions that your reader are not able to answer immediately. Usually the questions depend on each other, it means that to answer one question you must answer the one before.]

[COMMENT: Before a little bit of your most astonishing findings you must to introduce the structure of your paper/proposal. Usually the text looks like the following.]

"The remainder of this paper/proposal is organized as follows. Section 2 will discuss the approaches expected for answering each research question. After that, we present a preliminary planning for the research questions in Section 3. Finally, we conclude with a proposal and planning for the thesis structure in Section 4."

2. RELATED WORK

Go to Google scholar and search using keywords related to your research. Then, download some paper that the title immediately show similarities with your research. You must be able to judge the strong and weak-points of each paper. Also, you can extend your literature study by looking the related work section of each downloaded paper. In addition to that, you can look who cited the papers that you decided to include (till this moment) on your research (google scholar shows this information for you). This step is important because the papers that cited the paper that you decide to include on your research are potential papers to include on your section. Note that the final goal of this section is a table that summarizes the characteristics of each paper and your critical analysis to highlight the existing gaps of research.

3. PROPOSAL

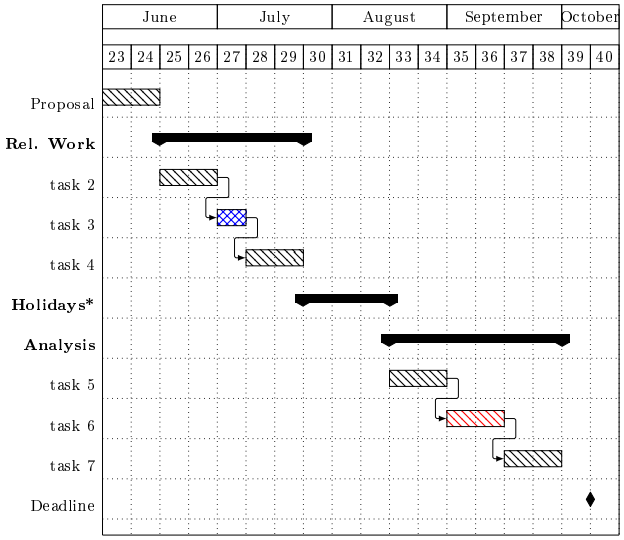
In this part I would like you to add a conceptual figure with your idea (if possible). On this, I must say that Figures MUST be in pdf format (I like to use Inkscape to create my figures, then I export to pdf) [ask me how, for help].

Figure 1: Example of Figure.

4. PLANNING TASKS

In this section we will shortly discuss the planning of the study. The study has been split into six parts, as can be seen in the table below. Note that this planning is merely meant as a guideline, and is not set in stone.

More examples on how to do a planning table you can see in http://www.martin-kumm.de/wiki/doku.php?id=Projects:A_LaTeX_package_for_gantt_plots



The research topics part consists solely of a literature study that focuses on ... All relevant information learned from this will be integrated in a survey that will form the first part of the thesis.

Following the research topics are each of the research questions, with time allotted at the end of each research question to integrate the results into the thesis.

5. REFERENCES

[1] Cost of hourly downtime soars: 81% of enterprises say it exceeds $300k on average. http://itic-corp.com/blog/2016/08/cost-of-hourly-downtime-soars-81-of-enterprises-say-it-exceeds-300k-on-average/. Accessed: 2018-03-21.

[2] J. Cardoso de Santanna. Ddos-as-a-service: Investigating booter websites, 11 2017. CTIT Ph.D. thesis Series No. 17-448, ISSN 1381-3617.

[3] N. Fallahi and A. Sami. Automated Flow-based Rule Generation for Network Intrusion Detection Systems. pages 1948–1953, 2016.

[4] A. G. Fragkiadakis, V. A. Siris, N. E. Petroulakis, and A. P. Traganitis. Anomaly-based intrusion detection of jamming attacks, local versus collaborative detection. *Wireless Communications and Mobile Computing*, 15(2):276–294, 2013.

[5] H. J. Liao, C. H. Richard Lin, Y. C. Lin, and K. Y. Tung. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1):16–24, 2013.

[6] D. Lin. Network Intrusion Detection and Mitigation against Denial of Service Attack. *WPE-II Written Report*, (January):1–28, 2013.