How to Automatically Generate DDOS Attack Signatures?

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

1. PROPOSAL

A Denial of Service (DoS) attack is an attack that aims to disable services of a target system. There are two main types of DoS attacks: *vulnerability DoS* and *flood DoS* [10]. In one hand, a vulnerability DoS aims to exploit a vulnerability of a target system to reduce its performance or render it useless. An example of such an attack is to send a malformed message to the target machine which can not deal with this message and as a result stops working. On the other hand, a flood DoS attack 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 bandwidth flood by using multiple machines to produce traffic. When multiple machines are used in the attack, it is called a Distributed Denial of Service (DDoS) attack.

DDoS attacks have increased in power and frequency. In 2011, the peak attack was measured at 60 Gb/s [11], in 2015, 500 Gb/s and in 2016 1.1 Tb/s [3]. In the third quartile of 2016 more than 5000 attacks where observed, whereas 200 in the entire 2012 [2]. As the number of attacks increase and downtime costs are exceeding on average $300K per hour [1] a need for an efficient and effective mitigation method has become crucial. The first task before the mitigation is the detection of an attack. Intrusion Detection Systems (IDS) are such systems that can fulfill this task. An IDS is a system that monitors a system or network for malicious and/or suspicious activities. Based on the detection methods of IDSs, two categories can be identified: *Anomaly-based* and *Signature-based* [7]. 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 key characteristic of an attack for which predefined signatures are known. An AIDS has as benefit that it can detect unknown attacks but with the weaknesses that it has a low accuracy, needs time to learn a baseline of a system and has difficulties to trigger alerts before an attack scales up. A SIDS has as benefit that it has a high accuracy but with the weaknesses that it is ineffective in detecting unknown attacks and it is hard to maintain an up to date signature list [9].

Our hypothesis is that due to the high accuracy a SIDS is a suitable system that can fulfill the requirement of successfully and efficiently detecting DDoS attacks when the major downside of keeping an up to date signature list is tackled. The solution for this problem is to generate signatures for new attacks. This can be done either manually or automatically. As a manual approach requires significant amount of manual effort [10], we propose an automatic method. For this research we generate signatures from extracted features of DDoS attacks for the Bro SIDS[1]. Bro is an open source network security monitor that offers the functionality of a SIDS. The features of DDoS attacks are extracted by a different research of DDoSDB[2].

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

- **RQ1:** What are the current developments in automatic signature generation for SIDSs?
- **RQ2:** What is the performance of automatic signature generation against a DDoS attack for the Bro SIDS?
- **RQ3:** What is the accuracy and efficiency for Bro automatic generated signatures when applied on an ongoing DDoS attack?

The first RQ will be answered by analyzing various IDSs and inspecting various signature generation methods. The second RQ will be answered by building a proof of concept that generates signatures based on a given stream of features of DDoS attacks. The third and last RQ will be answered by replaying an attack for which a signature was generated and analyze what the performance of Bro is with these signatures implemented.

The remainder of this proposal is organized as follows. Section 2 discusses the related work identified. In

[1] `https://www.bro.org/`
[2] `http://ddosdb.org/`

Section 3 we conclude with a planning for the proposed research.

2. RELATED WORK

Fallahi et. al. [5] implemented automatic rule generation for the SIDS Snort. They used two data mining algorithms called Ripper and C5.0. They investigated five types of attacks and tested it on the ISCX 2012 dataset. Rather than looking to individual packets, they looked at the flow of data. From the flow 17 features were selected to generate rules. Fallahi et. al. applied this approach to a single dataset which contained various attacks, rather than focusing on DDoS attacks. Furthermore, by looking at the flow of data, the payload is discarded. The payload of messages are for some DDoS attacks a crucial for identification.

Fouda [6] proposes a payload based signature generation specific for DDoS attacks. Various pattern matching algorithms are tested to find the amount of similarity between incoming traffic and traffic that is associated with a DDoS attack. It was found that Smith-Waterman and Longest Common Substring algorithms yielded the highest accuracy. A problem, for example, apparent in this approach is that it tends to become slow. In 2003, a simmilar approach could only cope with up to 200 Mbps of traffic [8]. Furthermore, not all attacks lend themselves to be accurately identified by their payload.

Chimetseren et. al [4] proposes signature based generation method using Discrete Fourier Transform. In this method the payload between client and server are regarded as discrete waveform. They create a spectrum for normal, known attack and unknown attack sessions. This approach is tested on the Kyoto2006+ dataset[3]. By also generating a spectrum for normal sessions, they are able to detect unknown attacks. However, this does yield a 5% false positive in the selected dataset.

3. PLANNING TASKS

In this section, we will briefly discuss the planning of the research. Figure 1 pictures the intended planning. The first 7 weeks are planned for writing the proposal. This period knows two deadlines at the end of week 14 and 16. The first deadline is the deadline for the draft proposal and the second the deadline for the final proposal. During this period not that much time can be spent on the actual research due to other obligations.

The remaining of the time the actual research will be carried out. During this period, more time can be spent per week in comparison to the proposal period. The research period is defined in time per RQ. The first and last RQs are more theory based and therefore probably cost less time than RQ 2 which is more practical. During RQ 3 there is also a holiday planned where no time will be spent on this research.

Finally, a week to finalize the entire research is planned. This period is intended as a buffer in case some parts of the research are going less prosperous than intended.

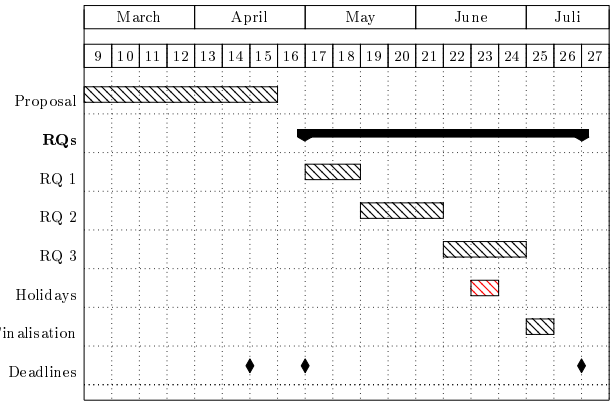

Figure 1: Planning of this research.

[3] http://www.takakura.com/Kyoto_data/

4. 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] Akamai. State of the Internet/Security (Q3/2017). page 40, 2016.

[3] Akamai. State of the Internet/Security (Q1/2017). 2017.

[4] E. Chimetseren, K. Iwai, H. Tanaka, and T. Kurokawa. A Study of IDS using Discrete Fourier Transform. pages 463–466, 2014.

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

[6] K. M. I. A. Fouda. Payload Based Signature Generation for DDoS Attacks. 2017.

[7] 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.

[8] H. Lai, S. Cai, H. Huang, J. Xie, and H. Li. A parallel intrusion detection system for high-speed networks. *Applied Cryptography and Network Security*, pages 439–451, 2004.

[9] 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.

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

[11] A. Networks and A. Networks. Arbor Networks 9th Annual Worldwide Infrastructure Security Report. 2014.