Mitigating DDoS Attacks Using OpenFlow-Based Software Defined Networking

Mattijs Jonker, Anna Sperotto

Mitigating DDoS Attacks using OpenFlow-based Software Defined Networking

Mattijs Jonker and Anna Sperotto

Design and Analysis of Communication Systems (DACS)
Centre for Telematics and Information Technology (CTIT)
University of Twente, Enschede, The Netherlands
{m.jonker, a.sperotto}@utwente.nl

Abstract. Over the last years, Distributed Denial-of-Service (DDoS) attacks have become an increasing threat on the Internet, with recent attacks reaching traffic volumes of up to *500 Gbps*. To make matters worse, web-based facilities that offer "DDoS-as-a-service" (i.e., *Booters*) allow for the layman to launch attacks in the order of tens of *Gbps* in exchange for only a few euros. A recent development in networking is the principle of Software Defined Networking (SDN), and related technologies such as OpenFlow. In SDN, the control plane and data plane of the network are decoupled. This has several advantages, such as centralized control over forwarding decisions, dynamic updating of forwarding rules, and easier and more flexible network configuration. Given these advantages, we expect SDN to be well-suited for DDoS attack mitigation. Typical mitigation solutions, however, are not built using SDN. In this paper we propose to design and to develop an OpenFlow-based mitigation architecture for DDoS attacks. The research involves looking at the applicability of OpenFlow, as well as studying existing solutions built on other technologies. The research is as yet in its beginning phase and will contribute towards a Ph.D. thesis after four years.

1 Introduction

While Distributed Denial-of-Service (DDoS) attacks have been long noted in the literature, it was not until a large group of attacks referred to as *"operation payback"* in 2010 by WikiLeaks supporters that the general public better understood the power of such attacks. As part of this group of attacks, the websites of *MasterCard* and *Visa* were brought down entirely, and *PayPal*'s website was notably disrupted [1,2]. Ever since, we have seen a rapid increase in DDoS attacks in occurrence and magnitude. The *"Spamhaus attack"* is a notorious example [3]. While its *300 Gbps* traffic peak created the largest-ever-seen DDoS attack at the time, it has since been surpassed by attacks up to sheer volumes of *500 Gbps* [4,5]. These types of attacks use core parts of the Internet infrastructure to amplify traffic (e.g., the *Domain Name System (DNS)*) and can be launched without an underlying botnet. As they operate at the network and transport layers [6], they are nearly impossible to mitigate with strictly on-premise solutions. To make matters worse, the ability to launch such attacks is

nowadays no longer limited to people with advanced technical skills. Contrarily, "DDoS-as-a-Service" providers, i.e., *Booters* [7], allow anyone to perform attacks in the order of tens of Gbps in exchange for only a few euros. As a result of the increased threat of DDoS attacks, a market for mitigation solutions was created, which gave rise to DDoS Protection Service (DPS) providers such as *Akamai Prolexic* [8], *CloudFlare* [9] and *Verisign* [10].

A recent development in networking technology that has attracted a lot of attention from the research community is the Software Defined Networking (SDN) principle [11, 12]. In SDN, the control plane and data plane of the network are decoupled. This decoupling has many advantages, such as centralized control over forwarding decisions, dynamic updating of forwarding rules, and easier and more flexible network configuration. OpenFlow [13] is the most commonly deployed SDN technology. Considering the characteristics of SDN, we expect it to be well-suited for DDoS attack mitigation [14].

Despite SDN's potential for DDoS attack mitigation [15], we observe that existing solutions rely on other techniques. For example, solutions offered by 'cloud-based' DPS providers rely on DNS anycast and Border Gateway Protocol (BGP) announcements. Moreover, there are challenges when it comes to SDN itself, such as the performance of programmable devices, and its susceptibility to attacks [16,17]. The aim of this research, therefore, is to investigate the applicability of OpenFlow-enabled SDN for DDoS attack mitigation, and to propose and develop an architecture to this end.

The remainder of this paper is organized as follows. In Section 2 the research questions and approach for this work are detailed. Some of the preliminary steps taken are presented in Section 3, and in Section 4 we conclude this paper.

2 Goal, Research Questions and Approach

The goal of this research is to evaluate OpenFlow for use in DDoS attack mitigation, and to design and to develop a mitigation architecture. By using the advantages of OpenFlow, such an architecture is expected to allow for attacks to be mitigated in an early stage, i.e., closer to the Internet backbone and further away from the target, in a flexible and scalable manner. In addition, an OpenFlow-based architecture may allow, to some extent, the protected entity to control routing, which could have benefits. In support of achieving this goal we have defined the following main research question.

> ***RQ*$_M$:** Can we use OpenFlow in a DDoS attack mitigation architecture, and how will such an architecture operate?

Our approach to answering RQ_M is primarily measurement-based, in which measurements are first focussed on assessing the applicability of OpenFlow-enabled devices for DDoS mitigation, and later shift towards the architecture operation. In the subsections to follow we will divide the main research question in sub-questions, and discuss, for every sub-question, the envisioned approach.

2.1 The Applicability of OpenFlow-based SDN

In the context of researching the applicability of OpenFlow-based SDN for a mitigation architecture, the following sub-questions are defined.

> ***$RQ_{M.1}$* : What do DDoS attack mitigation solutions based on technologies other than SDN look like, and how do they operate?** The purpose of this research question is to thoroughly study other solutions, and investigate where OpenFlow-based SDN can excell, and where it may fall short in comparison. Typical solutions based on BGP and DNS anycast, for example, re-route all traffic at the network layer (L3) through 'scrubbing centers', i.e., data centers where traffic is cleansed. This way of operating needs to be studied for comparative purposes.
> ***$RQ_{M.2}$* : How applicable is OpenFlow to the end of DDoS attack mitigation, in terms of flexibility, performance, and scalability?** The specification of OpenFlow may be different from the performance and scalability actually offered by OpenFlow implementations. This question serves to quantify the flexibility, performance, and scalability of OpenFlow.

To approach $RQ_{M.1}$, we will study mitigation solutions offered by DPS providers; solutions deployed at backbone providers, ISPs, and National Research and Education Networks (NREN); and other type of solutions, such as traditional firewalls or vendor-specific solutions. Part of this study will include large-scale measurements using DNS, which will reveal statistics about which domains use (or migrate to) cloud-based DPS providers. Furthermore, using DNS we can study how parts of DPS architectures based on DNS anycast (e.g., *CloudFlare*) operate and behave. We will also perform comparative benchmarks between transport layer (L4) filtering with OpenFlow and traditional firewalls or vendor-specific implementations, such those based on [18]. We will also perform measurements to study if re-routing everything at L3 is efficient. Our approach for $RQ_{M.2}$ will include benchmarks of specific OpenFlow-enabled device implementations, for example to see how well forwarding devices behave when rules are frequently dynamically modified. This type of benchmarks will be done in lab settings, as well as in production networks.

2.2 Architecture Requirements

In the context of architecture requirements, the following sub-question is defined.

> ***$RQ_{M.3}$* : What are the requirements of an OpenFlow-based mitigation architecture for DDoS attacks?** This research question serves to get a thorough technical understanding of how an architecture needs to operate, what its performance requirements are, and how it can be scalable and be flexible. Its design should also account for the notion that multiple organisations are likely to be involved, which will give rise to legal and ethical questions, such as about net neutrality.

The approach we will take to answer $RQ_{M.3}$ involves interviewing operators of software defined networks [12] to reveal how current SDN topologies are deployed, what the challenges are, if and how control over routing is currently realized, and under which conditions dynamic routing allows for DDoS attack mitigation. Non-technical issues (e.g., ethical and legal) can also be identified this way. The approach also involves measurements of preliminary architecture setups in a lab setting to measure how different parts interact. This will allow us to benchmark architecture designs, review requirements, and steer architecture design choices.

The overall approach, as identified in the preceding sections, will be iterative. This is due to several reasons. First, the consequences of design choices may affect architecture scalability and performance. Second, results from one research question may lead to revisiting others.

3 Preliminary steps

This section briefly describes some preliminary steps taken to achieve the goal of the proposed research. We recently deployed a large-scale measurement framework based on DNS. It uses the full *.com*, *.net* and *.org* zones to perform DNS queries for about *142* million domain names daily. Given that several record types are of interest, billions of queries are performed per day. The measurement framework is used for different research efforts, but in the context of this work it is used as follows. By mapping address responses of domains, i.e. `A` and `AAAA` to Autonomous System (AS) numbers, the use of DPS providers (e.g., *CloudFlare*) can be identified. Name Server (`NS`) responses can be used to the same end. This type of analysis allows us to evaluate statistics on the use of, and migration over time to, DPS providers.

4 Final considerations

During the first four months of this Ph.D research, the preliminary steps presented in Section 3 were taken. The main goal of this work (as described in Section 2) should be achieved within a period of four years, as part of a Ph.D thesis. During this time, this research is expected to benefit from the network of contacts the University of Twente (UT) has, such as those in the context of EU FP7 FLAMINGO NoE.

Acknowledgments

This research is funded by FLAMINGO, a Network of Excellence project (318488) supported by the European Commission under its Seventh Framework Programme and by the NWO Project D3.

References

1. Esther Addley and Josh Halliday: WikiLeaks supporters disrupt Visa and MasterCard sites in 'Operation Payback's. http://www.theguardian.com/world/2010/dec/08/wikileaks-visa-mastercard-operation-payback/ Accessed on January 13th, 2015.
2. Andry Greenberg: WikiLeaks Supporters Aim Cyberattacks At PayPal. http://www.forbes.com/sites/andygreenberg/2010/12/06/wikileaks-supporters-aim-cyberattacks-at-paypal/ Accessed on January 13th, 2015.
3. John Markoff and Nicole Pelroth: Firm Is Accused of Sending Spam, and Fight Jams Internet. http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?_r=0 Accessed on January 13th, 2015.
4. Steven Musil: Record-breaking DDoS attack in Europe hits 400Gbps. http://www.cnet.com/news/record-breaking-ddos-attack-in-europe-hits-400gbps/ Accessed on January 13th, 2015.
5. Parmy Olson: The Largest Cyber Attack In History Has Been Hitting Hong Kong Sites. http://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/ Accessed on January 13th, 2015.
6. Zimmermann, H.: OSI reference model–The ISO model of architecture for open systems interconnection. IEEE Transactions on Communications **28**(4) (1980) 425–432
7. Karami, M., McCoy, D.: Understanding the Emerging Threat of DDoS-as-a-Service. In: Proceedings of the 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats, LEET'13. (2013)
8. Prolexic, A.: Prolexic: DDoS Protection and Mitigation. http://www.prolexic.com/ Accessed on January 13th, 2015.
9. CloudFlare: CloudFlare: The web performance & security company. http://www.cloudflare.com/ Accessed on January 13th, 2015.
10. Verisign: Verisign: Internet Security and Web Domain Names. http://www.verisigninc.com/ Accessed on January 13th, 2015.
11. Shenker, S., Casado, M., Koponen, T., McKeown, N.: The future of networking, and the past of protocols, Presented at the Open Networking Summit (2011)
12. Bezerra, J.A.: Migrating AmLight from legacy to SDN: Challenges, Results and Next Step, Presented at NANOG 63 (2015)
13. McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., Turner, J.: OpenFlow: enabling innovation in campus network. ACM SIGCOMM Computer Communication Review **38**(2) (2008) 69–74
14. François, J., Dolberg, L., Festor, O., Engel, T.: Network Security through Software Defined Networking: a Survey. In: Proceedings of the 7th ACM conference on Principles, Systems and Applications of IP Telecommunications, IPTComm'14. (2014)
15. Vizváry, M., Vykopal, J.: Future of DDoS Attacks Mitigation in Software Defined Networks. In: Proceedings of the 8th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS'14. (2014)
16. Sezer, S., Scott-Hayward, S., Kaur, P.C., Fraser, B., Lake, D., Finnegan, J., Viljoen, N., Miller, M., Roa, N.: Are We Ready for SDN? Implementation Challenges for Software-Defined Networks. ACM SIGCOMM Computer Communication Review **51**(7) (2013) 36–43

17. Kreutz, D., Ramos, F., Verissimo, P.: Towards secure and dependable software-defined networks. In: Proceedings of the 2nd ACM SIGCOMM workshop on Hot topics in software defined networking. (2013)
18. Juniper: Junos OS: Network operating system for routing, switching, and security. http://www.juniper.net/us/en/products-services/nos/junos/ Accessed on January 22nd, 2015.