DrawBridge—Software-Defined DDoS-Resistant Traffic Engineering

Jun Li
University of Oregon
Eugene, OR, USA
lijun@cs.uoregon.edu

Skyler Berg
University of Oregon
Eugene, OR, USA
skylerb@uoregon.edu

Mingwei Zhang
University of Oregon
Eugene, OR, USA
mingwei@cs.uoregon.edu

Peter Reiher
University of California
Los Angeles, CA, USA
reiher@cs.ucla.edu

Tao Wei
University of California
Berkeley, CA, USA
lenx.wei@gmail.com

ABSTRACT

End hosts in today's Internet have the best knowledge of the type of traffic they should receive, but they play no active role in traffic engineering. Traffic engineering is conducted by ISPs, which unfortunately are blind to specific user needs. End hosts are therefore subject to unwanted traffic, particularly from Distributed Denial of Service (DDoS) attacks. This research proposes a new system called **DrawBridge** to address this traffic engineering dilemma. By realizing the potential of software-defined networking (SDN), in this research we investigate a solution that enables end hosts to use their knowledge of desired traffic to improve traffic engineering during DDoS attacks.

Categories and Subject Descriptors

C.2.3 [**Computer-Communication Networks**]: Network Operations—*network management, network monitoring*; C.2.0 [**Computer-Communication Networks**]: General—*security and protection*; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design

General Terms

Design, Management, Security

Keywords

Traffic engineering; Software-defined networking; DDoS

1. PROBLEM STATEMENT

End hosts on today's Internet do not play an active role in traffic engineering. They have no means to control what traffic can be forwarded to them, how much traffic should be forwarded to them, and when traffic should be forwarded to them. Traffic engineering is totally the responsibility of their Internet Service Providers (ISPs).

An ISP must consider many factors when conducting traffic engineering, including the highly dynamic and unpredictable nature of Internet traffic, its resource capacity, its policy agreements with other ISPs, its service agreements with its customers, as well as its own desire to handle as much traffic as possible to make money. While many studies have addressed these factors, an ISP still faces a troubling dilemma: ISPs want to avoid possibly upsetting a customer's by dropping their traffic, however, much of the traffic may be unwanted by the customer.

This dilemma leads to problems familiar to end hosts, especially handling Distributed Denial of Service (DDoS) attack traffic that clogs the bandwidth or processing units of the end hosts, and sometimes impacts the ISP itself. For example, the DDoS against Spamhaus in March 2013—which may have been the largest DDoS to date—generated over 300 Gbps of attack traffic [1], enough to bring down almost any running service on the Internet that does not aggressively overprovision. More recently, in February 2014, an NTP-based DDoS generated over 400 Gbps of traffic [2], Many other similarly powerful attacks are feasible, posing a significant threaten to most hosts on today's Internet [3].

The recent rise of DDoS is in large part due to the use of a particularly potent breed of DDoS: the Distributed Reflective Denial of Service (DRDoS) attack. A DDoS is considered *reflective* if an attacker sends messages to so called *reflector* nodes with a spoofed IP address (the address of the desired victim), which in turn send response messages to the victim. With enough traffic from reflectors, the victims bandwidth will become saturated. Furthermore, the responses sent by the reflectors can be much larger than the queries sent by the attacker. This is referred to as *bandwidth amplification* because the attacker can use a small amount of attack bandwidth to generate a large amount of traffic.

In general, end hosts can determine if certain traffic is desired or not, but they are unable to inform upstream ISPs. ISPs can attempt to filter malicious traffic, but this is done blind to specific user needs. So end hosts can receive large volumes of traffic they know they do not want, ISPs could filter that traffic if they knew it was unwanted, but there is no effective communication between the party who knows what to do and the party that can do it.

SIGCOMM'14, August 17–22, 2014, Chicago, IL, USA.
ACM 978-1-4503-2836-4/14/08.
http://dx.doi.org/10.1145/2619239.2631469.

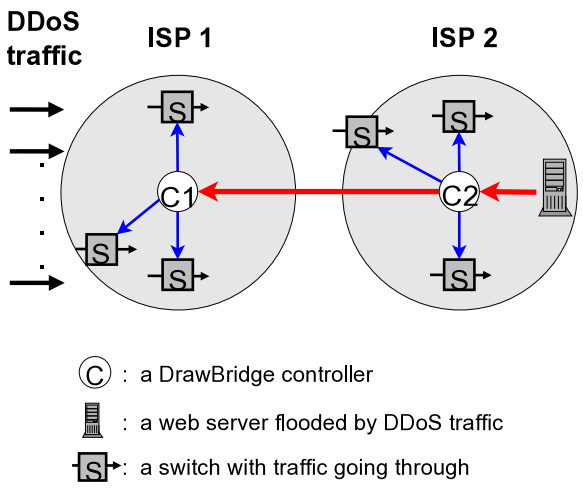

Figure 1: An example of DrawBridge throttling DDoS traffic. A DrawBridge subscriber informs its DrawBridge controller what traffic to filter (red arrows), which then informs SDN switches to act on traffic filtering as instructed (blue arrows). Note in this example the web server is a subscriber of DrawBridge controller C2, and C2 is a subscriber of C1.

2. DRAWBRIDGE ARCHITECTURE

Software-defined networking (SDN) has the potential to address the traffic engineering dilemma described in Section 1, through protocols such as OpenFlow [4]. We enhance SDN to perform the demanding task of handling high volume DDoS traffic. In particular, we devise an approach to blocking unwanted traffic while still letting desired traffic through. Due to its functional similarities to a castle's drawbridge, we call our approach **DrawBridge**.

DrawBridge enables an end host from within an ISP to act as a **subscriber** to express its traffic engineering rules and send them to a DrawBridge-enabled SDN controller in the ISP, referred to as a **DrawBridge controller**. The DrawBridge controller can further push such rules to the ISP's SDN switches where traffic will be filtered according to these rules, or another DrawBridge controller in an ISP upstream. In the latter case, the downstream controller will act as a subscriber to the upstream DrawBridge controller. Figure 1 shows how a potential victim can use DrawBridge to prevent itself from being flooded.

DrawBridge's architecture allows users, end hosts, or another ISP to subscribe to the traffic engineering service that an ISP's DrawBridge controller provides, and enables a DrawBridge subscriber to establish traffic engineering rules at the controller. This paradigm fundamentally changes the current paradigm of "blind" traffic engineering done by ISPs, enabling end hosts to express their needs and enabling ISPs to make informed traffic engineering decisions.

The primary function of a DrawBridge controller is to process and deploy traffic engineering rules. Upon receipt of new rules to deploy, a controller can verify the validity of rules, check if the rules can be aggregated with other rules, determine whether to deploy rules locally at switches of its own ISP, or push rules to ISPs upstream. It can further determine which local switches or upstream ISPs to deploy rules.

DrawBridge also supports a subscriber to be adaptive in dealing with traffic floods. Based on the traffic dynamics, a subscriber can decide on the fly what rules to establish at a DrawBridge controller. It can choose to receive all the traffic itself, or only a restricted set of traffic, or even nothing. Furthermore, if current rules do not seem effective in throttling DDoS traffic, the subscriber can adapt the rules and make them more restrictive. Not only can a subscriber express its rules when there is no DDoS, it can also do so when it is under stress.

3. OPEN ISSUES AND FUTURE WORK

Clearly, DrawBridge needs to support scalable handling of a potentially very large number of rules, speedy deployment of new rules, and secure handling of all operations. While still a research in progress, in our future work we will demonstrate how effective DrawBridge is in handling DDoS traffic. We will first apply DrawBridge to DRDoS traffic, and then use our experiences with DRDoS to expand DrawBridge's ability to handle more general DDoS traffic. We will also investigate security and deployment issues. In particular, we will consider what attackers can do to circumvent DrawBridge. We will design attacks which focus on attaining a high amplification and which cannot be easily blocked by the intended victim. After designing the attacks we will launch them against our networks to test both the success of the attack and the capabilities of the defense.

4. CONCLUSIONS

This research enhances SDN using an architectural design that allows users, end hosts, or another ISP to subscribe to the traffic engineering service that an ISP's controller provides, and enables a subscriber to establish traffic engineering rules at the controller. It further allows a controller to verify and process the traffic engineering rules, and deploy them at switches or upstream ISPs with the best location for filtering traffic. DrawBridge aims to handle these demanding traffic engineering tasks even when numerous victims are under high stress from DDoS traffic. It is designed to be scalable and efficient with high performance, as well as secure and easy to deploy with low cost. In our future work we will fully implement and comprehensively evaluate the DrawBridge architecture.

5. REFERENCES

[1] "Answers about recent DDoS attack on Spamhaus," http://www.spamhaus.org/news/article/695, Spamhaus, 2013.

[2] "Technical details behind a 400Gbps NTP amplification DDoS attack," http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack.

[3] C. Rossow, "Amplification hell: Revisiting network protocols for DDoS abuse," in *the 21th Annual Network & Distributed System Security Symposium (NDSS)*, 2014, pp. 1–15.

[4] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.