DrawBridge: A New Approach to DDoS Defense

Presenter: Lumin Shi & Gautam Sondur
Intro

● What is DDoS?

● What are the approaches being implemented in the industry?

● What is SDN and what are its advantages?
Software-Defined Networking

What if we can allocate a new path for these cars?
Software-Defined Networking

Basic SDN architecture
(opennetworking.org)
Basic Structure of DrawBridge
DrawBridge Defense Mechanism
#FromWhatWeKnowSoFar

- Application specific defense
  - e.g. NTP DDoS attack
  - Filter the traffic by port or protocol

- Deep packet inspection required defense
  - Reroute traffic via a VNF-enabled entity
    - think it as a tollbooth
  - VNF-enabled entity can do the inspection
DrawBridge Defense Mechanism

#FromWhatWeKnowSoFar

Virtual network function forwarding graph
(opennetworking.org)
Problems

- Find the right place to install rules
- How can ISPs push/receive rules
- Most importantly, how to get ISPs involved
Thank you!

Questions?
**Motivation**

- Distributed denial-of-service attack (DDoS) has become more severe.
- DDoS traffic against Spamhaus in 2013 was 300 Gbps, and DDoS against CloudFlare in 2014 was 400 Gbps, enough to bring down almost any running service on the Internet that does not aggressively over provision.
- End hosts on today’s Internet have no means to control what traffic, when traffic, and how much traffic can be forwarded to them.
- Internet service providers (ISPs) on today’s Internet conducts “blind” traffic engineering since they are not informed by traffic recipients.

**Objectives**

- To enable a subscriber, such as an end host or a customer ISP, to express its traffic engineering rules and send them to a DrawBridge-enabled SDN controller.
- To enable a DrawBridge controller to push such rules to SDN switches in the same ISP where traffic will be filtered according to these rules.
- The primary function of DrawBridge is to leverage SDN infrastructure to generate, process, and deploy traffic engineering rules that can stop DDoS traffic without mislabeling legitimate traffic.

**Example**

<table>
<thead>
<tr>
<th>at&amp;t</th>
<th>Verizon</th>
<th>Other AS</th>
</tr>
</thead>
</table>

**Technologies**

- OpenFlow
- ONOS
- Java
- Ubuntu

**Open Issues**

- Must support scalable handling of potentially a very large number of rules.
- Must be secure in handling all the operations.
- Must be able to deploy rules speedily.
- Must demonstrate the efficacy of DrawBridge design.

**Other Potential Parts:**

- Distributed hash table
- Web server for RESTFUL API

**DrawBridge**

Leveraging Software-Defined Networking for DDoS Defense