DrawBridge—Software-Defined DDoS-Resistant Traffic Engineering

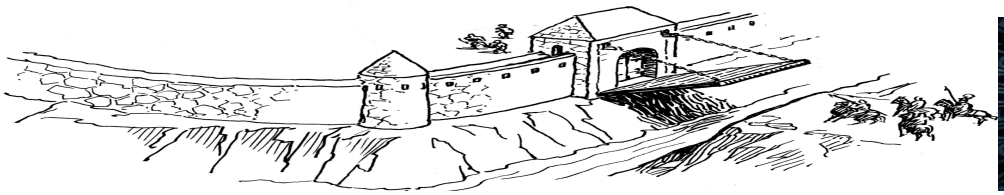
Jun Li
University of Oregon
Eugene, OR, USA
lijun@cs.uoregon.edu

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



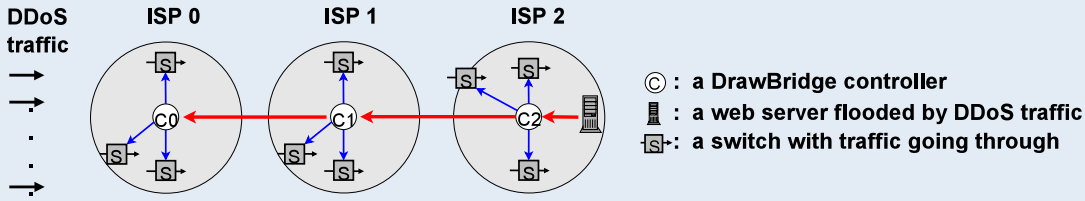
MOTIVATION

- 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 overprovision.
- 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



OPEN ISSUES AND FUTURE WORK

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

OREGON

SIGCOMM CHICAGO 2014