DrawBridge—Leveraging Software-Defined Networking for DDoS Defense

University of Oregon

Center for Cyber Security and Privacy (CCSP)

Jun Li, **Mingwei Zhang,** Lumin Shi, Devkishen Sisodia, Elizabeth Fuller,
Peter Reiher (UCLA)

UNIVERSITY
OF OREGON

CCSP@UO

UCLA

Acknowledgment

This project is the result of funding provided by the Science and Technology Directorate of the United States Department of Homeland Security under contract number D15PC00204. The views and conclusions contained herein are those of the authors and should not be interpreted necessarily representing the official policies or endorsements, either expressed or implied, of the Department of Homeland Security or the US Government.

Homeland
Security

Science and Technology

Problem Statement

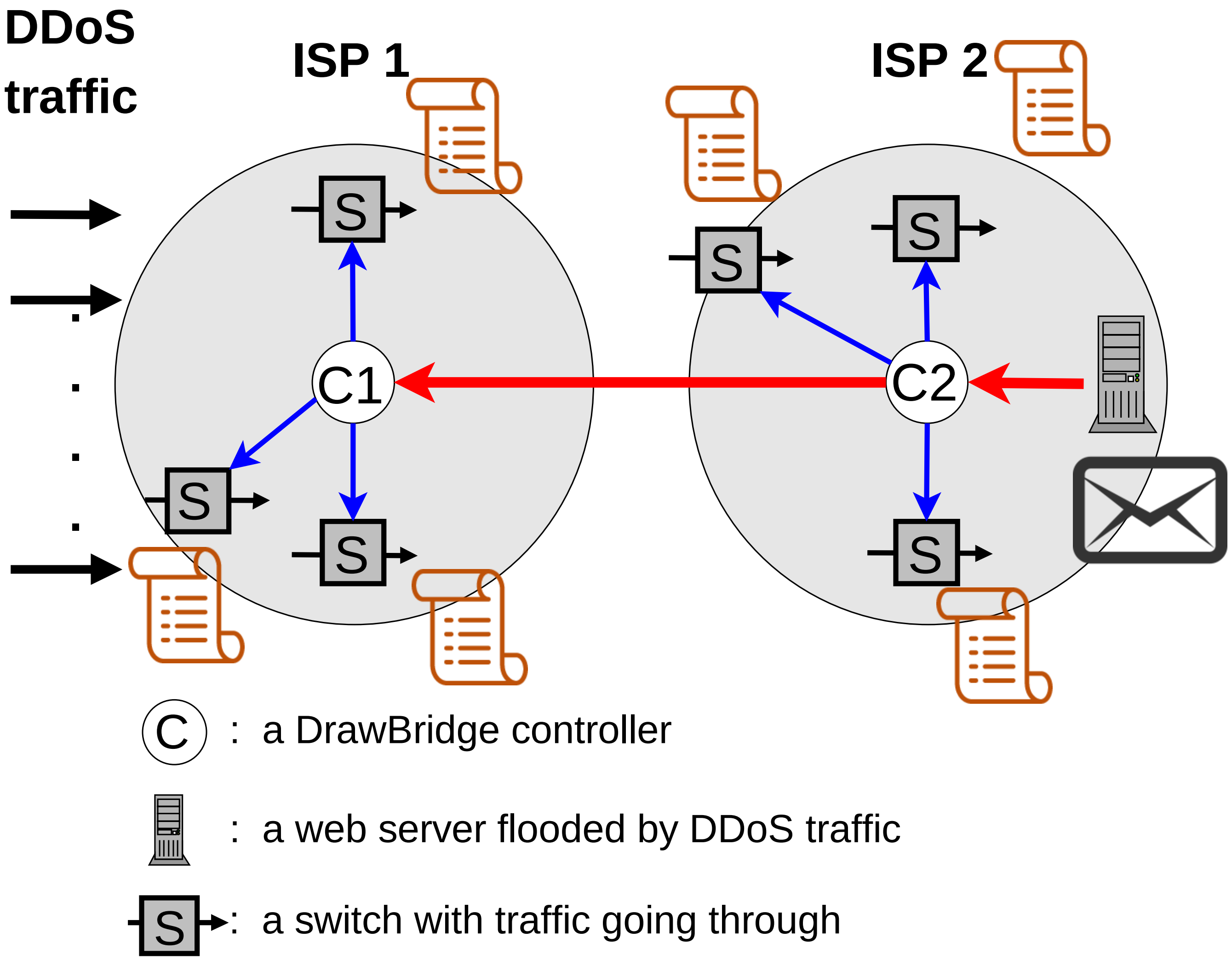
- Distributed denial-of-service (DDoS) attacks cause serious damage to network-based services and their users.
- DDoS attacks are performed by sending large volumes of garbage packets to their targets.
- Small- and medium-sized organizations lack the resources to withstand a very large DDoS attack.
- The end users have the best knowledge of which packets they want and which should be dropped.
- But the ISPs are the ones who might be able to drop the DDoS packets.
- **The dilemma – how do we effectively get the customer knowledge to the ISPs who can act on it?**

Basic Idea of DrawBridge

- Our solution, DrawBridge, enables users to inform ISPs how to handle DDoS attacks.
- Drawbridge is based on Software-Defined Networking (SDN)
  - SDN is perfectly well-suited for traffic handling tasks—including filtering traffic meeting specific rules or criteria
- Drawbridge will change the current paradigm of traffic engineering performed by ISPs.
- DrawBridge enables the propagation of the DDoS filtering rules from customers to ISPs and between ISPs.

Leveraging SDN

- Users, end hosts, or ISPs can subscribe to the Drawbridge service that an ISP's controller provides.
- On attack, the customer sends traffic filtering rules to the controller.
- The controller verifies and processes the traffic engineering rules.
- And deploys the rules at well-chosen Drawbridge switches or upstream ISPs to filter the DDoS traffic.


DDoS traffic
ISP 1
ISP 2
S
S
S
S
S
S
S
C1
C2
C
: a DrawBridge controller
: a web server flooded by DDoS traffic
S
: a switch with traffic going through

Current Research Topics

- Identification of the best strategies for ISP collaboration
- Discovery of best locations for deploying DDoS filtering rules
- Optimization of rule space throughout DrawBridge nodes
- Incentive of ISPs to run DrawBridge

Conclusion

- This project allows the traffic recipients who are hurt by DDoS attacks to play an active role in responding to them.
    - They can choose exactly what they do and do not want receive.
- Drawbridge changes the current paradigm of traffic engineering performed by ISPs, enabling end hosts or downstream ISPs to express their needs and enabling ISPs to make informed traffic engineering decisions.
- DrawBridge enables active AS-level collaboration on DDoS defense, and can potentially stop the DDoS traffic close to the attack sources.

Contact Us

- We seek the interests and collaboration from NANOG attendants on this project, including testing and deploying DrawBridge.

Jun Li
University of Oregon
netsec@cs.uoregon.edu
541.346.4424
Twitter: @ccspuo

UNIVERSITY
OF OREGON