This project is in part 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 as necessarily representing the official policies or endorsements, either expressed or implied, of the Department of Homeland Security or the US Government.

# DrawBridge 2.0:

## Bringing Software-Defined DDoS Defense To Practice

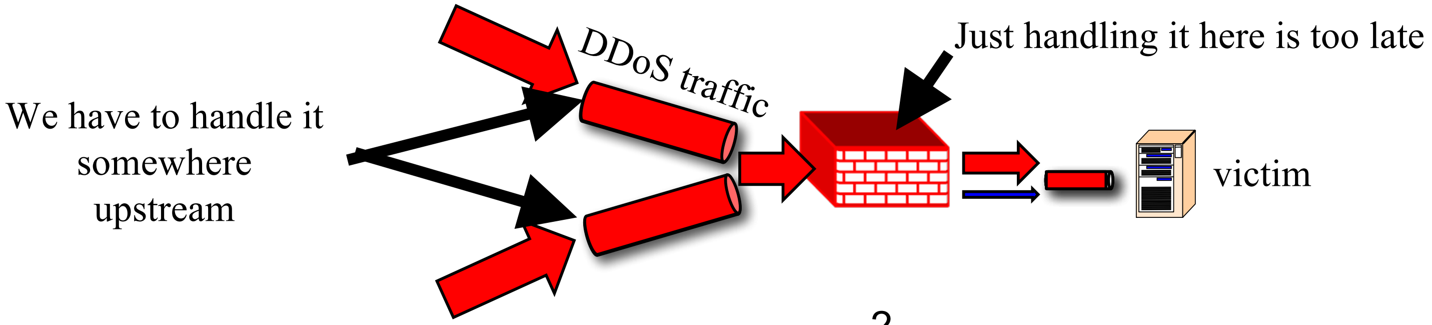
Jun Li
Professor, Computer and Information Science
Director, Center for Cyber Security and Privacy
University of Oregon

**Contact info:**

- Email: lijun@uoregon.edu
- Phone: 541-852-5580
- Skype: softlaser2

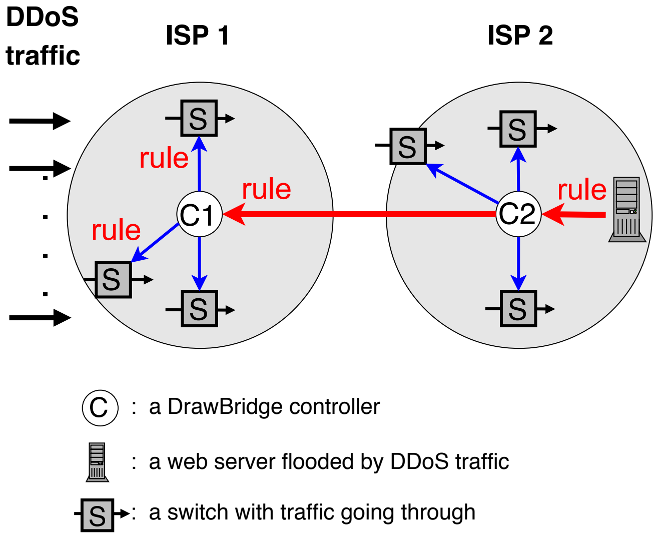
# Customer Need

- DDoS attacks continue to be devastating
- Victims are best able to determine which traffic should be delivered to them
- But least able to control that decision
- ISPs, on the other hand, are able to drop the DDoS packets but do not really know which traffic to drop


DDoS traffic
Just handling it here is too late
We have to handle it somewhere upstream
victim

# The DrawBridge Approach

- Our solution, DrawBridge, will enable its users to inform ISPs how to handle DDoS attacks
  - On attack, the user generates and sends DDoS-filtering rules to the DrawBridge controller at an upstream ISP
  - The controller verifies and deploys the rules at well-chosen switches or upstream ISPs to filter DDoS traffic
  - All communication uses the DrawBridge protocol to ensure efficiency and security
- DrawBridge is based on **software-defined networking** (SDN), which is well-suited for traffic handling tasks—including filtering traffic that meets specific rules or criteria


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

# Bringing DrawBridge To Practice

- We have developed a prototype of DrawBridge as well as demos of how DrawBridge works
- To further bring DrawBridge to practice, we will:
- Collect real-world input from potential DrawBridge adopters and subscribers
- Enhance DrawBridge code with more modules toward real settings
- Stress test DrawBridge on a designated subnet and GENI
- Test and improve user experience with UONet
- Experiment with DrawBridge and two ISPs—UONet and NERO
- Experiment with DrawBridge and multiple ISPs—UONet, NERO, Internet2, and others

- We will particularly need the following help:
- DrawBridge adopters to run DrawBridge service
- DrawBridge subscribers to sign up to be protected from DDoS
- Develop and execute a business plan
- Your feedback and comments

# Quad Chart for:

# Cybersecurity Research Acceleration Workshop and Showcase

October 18, 2017 | San Francisco, CA

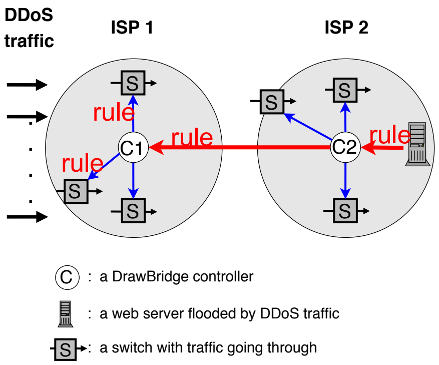
## Cybersecurity Transition To Practice (TTP) Acceleration (DrawBridge 2.0—Bringing Software-Defined DDoS Defense To Practice)

### Challenge:

Need many Internet service providers to adopt DrawBridge and build a collaborative defense of distributed denial-of-service (DDoS).

### Solution:

- Collect real-world input from potential DrawBridge adopters and subscribers
- Enhance DrawBridge code with more modules toward real settings
- Stress test DrawBridge on a designated subnet and GENI
- Test and improve user experience with UONet
- Experiment with DrawBridge and two ISPs—UONet and NERO
- Experiment with DrawBridge and multiple ISPs—UONet, NERO, Internet2, and others


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

### Value proposition:

- DrawBridge empowers DDoS victims to dictate what traffic can or cannot be delivered to them
- With a minimum number of highly effective rules generated on the fly by observing incoming DDoS traffic,
- And then placed at selected locations inside the DrawBridge network

### What we need to TTP

- DrawBridge adopters to run DrawBridge service
- DrawBridge subscribers to sign up to be protected from DDoS
- Develop and execute a business plan
- Your feedback and comments

### Contact us

- Email: lijun@uoregon.edu
- Phone: 541-852-5580
- Skype: softlaser2

UNIVERSITY OF OREGON