# Leveraging Software-Defined Networking for DDoS Defense

Peter Reiher | UCLA

October 24, 2019

Homeland Security

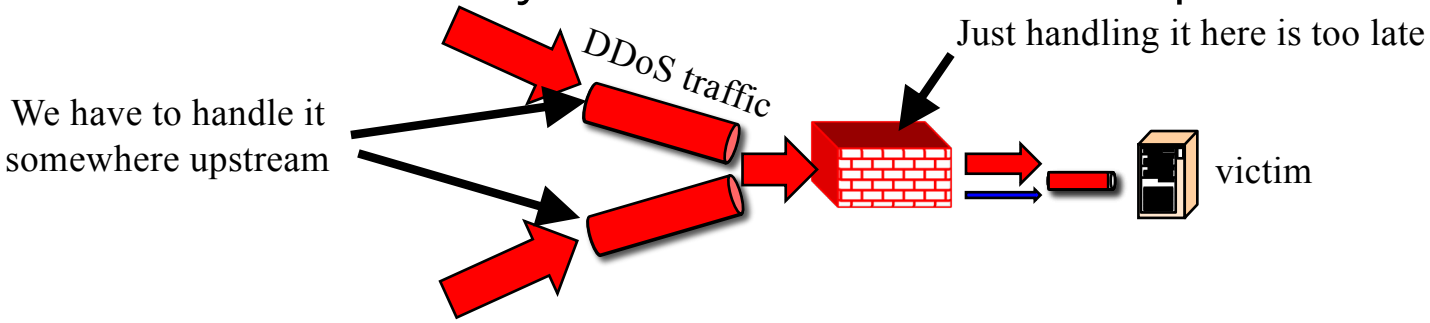
Science and Technology

# Team Profile

- Jun Li, Ph.D., Professor, Director of Center for Cyber Security and Privacy, University of Oregon (UO)
- Peter Reiher, Adjunct Professor, UCLA
- Ph.D. students: Devkishen Sisodia, Yebo Feng, Sam Mergendahl, Lumin Shi


# Customer Need

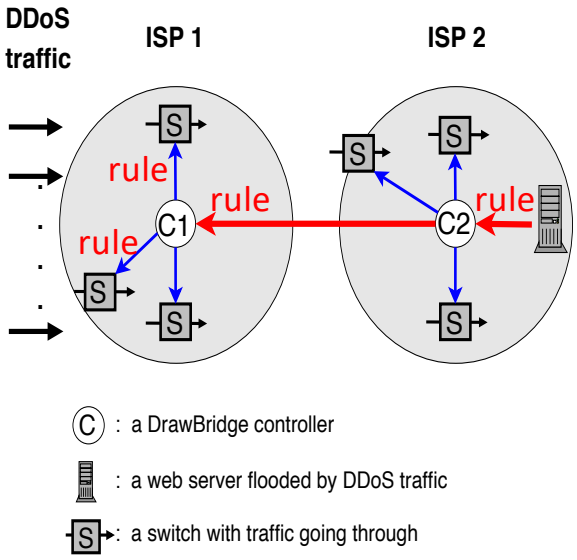
- DDoS attacks continue to be devastating
- Victims are best able to determine which traffic should be delivered to them
- But least able to control that decision
- ISPs, on the other hand, are able to drop the DDoS packets but do not really know which traffic to drop



# Approach

- Basic Idea
- Architecture
- Rule Generation
- Rule Placement

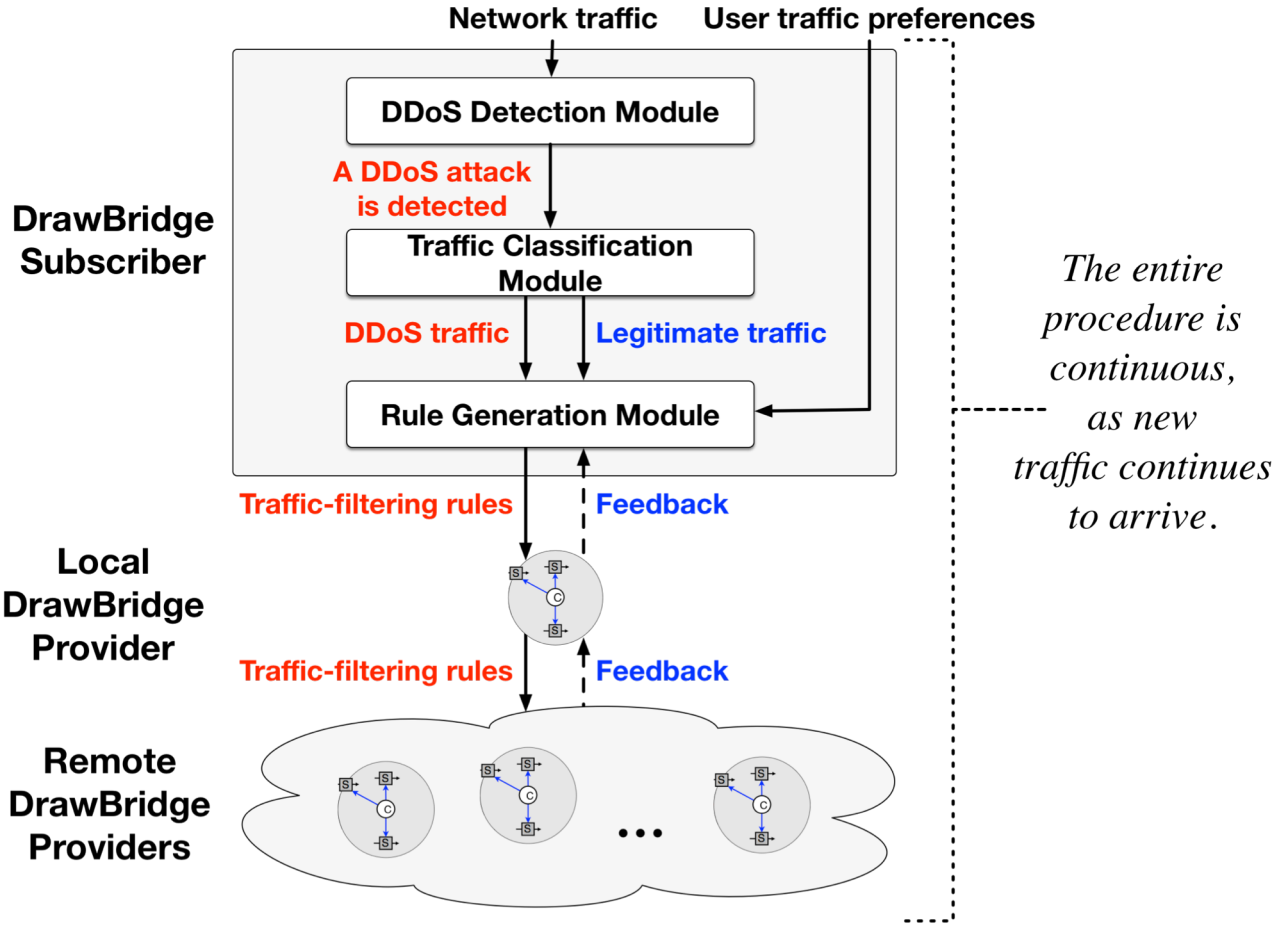
# Approach: Basic Idea




- DrawBridge allows users to tell 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 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

# Approach: Architecture – Subscriber's POV

- DrawBridge nodes request/acknowledge rule deployment
  - filtering rules and their metadata
- A DrawBridge network composed of subscriber-provider links
  - and communication via the network



# Approach: Rule Generation

- Generate small number of effective rules on-the-fly by observing incoming DDoS traffic
- With maximal possible coverage of DDoS traffic
- With minimal collateral damage
  - Dropping minimal “good” or “unknown” traffic
- A multi-objective optimization problem
  - Handled using well-known optimization methods
- Evaluate the rules’ effectiveness by observing DDoS traffic after deploying the rules
- If necessary, generate and deploy a new, more aggressive set of rules, then re-evaluate

# Approach: Rule Placement

- Determine which Drawbridge nodes should host the chosen rules
- **PathFinder:** A log-based approach to discovering autonomous system (AS) paths of traffic to a victim that is fast, efficient, and deployable
- **Optimal Placement:** choose ISPs and switches with:
  - maximal filtering of DDoS traffic
  - furthest possible distance from the victim
  - with the rule space constraints
  - an NP-hard problem which we solve with a rule placement algorithm

# Benefits

- DrawBridge enables the victims of DDoS attacks to play an **active** role in responding to the attack
  - They can specify exactly what they do and do not want delivered on the fly
- DrawBridge enables ISPs upstream to make informed traffic decisions
  - Thus changing the current paradigm of “blind” traffic engineering performed by ISPs

# Competition

- Classic DDoS defense solutions
  - AITF, Mayday, SOS, NetFence, FireCol, Dward, Defcon
- Leading industry DDoS defense solutions
  - DDoS protection service: Cloudflare, AWS Shield
  - DDoS Open Threat Signaling (dots)
- SDN-based DDoS defense solutions

# Current Status (Part 1)

- Current month of the project: 51 (October 2019)

| Milestone | Description | Done? |
|---|---|---|
| 1 (12 mo.) | DrawBridge architecture designed | ✓ |
| 2 (12 mo.) | DrawBridge subscriber can generate static rules successfully | ✓ |
| 3 (27 mo.) | DrawBridge subscriber can generate dynamic rules successfully | ✓ |
| 4 (27 mo.) | DrawBridge controller can successfully process and dispatch rules | ✓ |
| 5 (33 mo.) | DrawBridge controller equipped with a full set of rule-related functions | ✓ |
| 6 (33 mo.) | DrawBridge subscriber can distinguish DDoS traffic | ✓ |
| 7 (39 mo.) | Some classic DDoS solutions added to DrawBridge | ✓ |

| Deliverable | Description | Done? |
|---|---|---|
| 1 (12 mo.) | DrawBridge code with basic architecture implemented | ✓ |
| 2 (12 mo.) | Preliminary evaluation report | ✓ |
| 2.1 (30 mo.) | Additional efforts from the extended Option Period 1 | ✓ |
| 3 (33 mo.) | DrawBridge code with all rule-related functions implemented | ✓ |
| 4 (33 mo.) | Midterm evaluation report | ✓ |
| 5 (39 mo.) | Complete DrawBridge code | ✓ |
| 6 (39 mo.) | DrawBridge deployment and transition plan | ✓ |
| 7 (53 mo.) | Complete evaluation report | |
| 8 (53 mo.) | A full-fledged demonstration of DrawBridge, incl. its deployability | |

# Current Status (Part 2)

- Two major demos:
  1. Via simulated environment with real-time visualization, showing that DrawBridge effectively filters a replayed real-world DDoS attack
     - 5,000+ unique attack sources from 1,000+ different ASes over an inferred Internet AS topology
  2. Via the GENI testbed, showing how a video streaming service under DDoS attack is protected by Drawbridge
     - Real traffic on a real network
  - Video versions of both demos are both available.

# Current Status (Part 3)

- Major preparations for Drawbridge pilot deployment
  - Solidifying the code base
  - Testing for performance and functionality
  - Improvements in recognizing and characterizing traffic
- Working on finalizing deployment plans for pilot test of Drawbridge in real ISPs
  - Using mirror of real traffic to evaluate system effectiveness
  - Processing new data format of the traffic
  - Instrumenting the code for data collection and analysis

# Current Status (Part 4)

- Also investigated other interesting aspects of Drawbridge:
  - ISP incentives based on game theory
  - Modeling of in-network DDoS defense
  - GENI experimentation tools
  - Rule placement optimization and evaluation

# Transition/Completion Activities

- Finish Drawbridge evaluation
  - Performance
  - Efficacy against a range of attacks
  - Security of the system
  - Further comparison to other defense approaches
- Pilot deployment of Drawbridge
  - Details of deployment being worked out now
  - Plan is to deploy at three real ISPs

# Lessons Learned (Part 1)

- What went well:
  - Our clear statement of work guided us well
  - We stuck to the time line for milestones and deliverables
  - Identified key research topics while designing and developing the system
  - Had good communications with POs (Dan & Ann) and contract officers (Eric & Tracy)
  - DHS/DDoSD meetings were helpful

# Lessons Learned (Continued, Part 2)

- Technical challenges/issues:
  - SDN deployment rate is still low
  - Making DrawBridge work in non-SDN environment
  - Rule generation and placement are both NP-hard problems
    - We designed heuristics and evaluated them
  - Lack of enough real DDoS traces
    - We used what we could get

# Contact Info

**Peter Reiher**
UCLA
reiher@cs.ucla.edu
(310) 825-8332

Jun Li
University of Oregon
lijun@uoregon.edu
541.346.4424
Twitter handle: ccspuo