NSF Campus Cyberinfrastructure PI and Cybersecurity Innovation for Cyberinfrastructure

PI Workshop September 24-25| Minneapolis, Minnesota

NSF Program: CICI **Award Number:** 1739034

Program Area: Resilient Security Architecture for Research Cyberinfrastructure

Project: CICI: RSARC: DDoS Defense In Depth for DNS (DDIDD)

https://ant.isi.edu/ddidd/

PI: John Heidemann
johnh@isi.edu

co-PIs: Jelena Mirkovic
mirkovic@isi.edu

Wes Hardaker
hardaker@isi.edu

University of Southern California / Information Sciences Institute

NSF Campus Cyberinfrastructure PI and
Cybersecurity Innovation for Cyberinfrastructure PI Workshop
September 2019 | Minneapolis, MN

Quad Chart for: DDoS Defense In Depth for DNS (DDIDD)

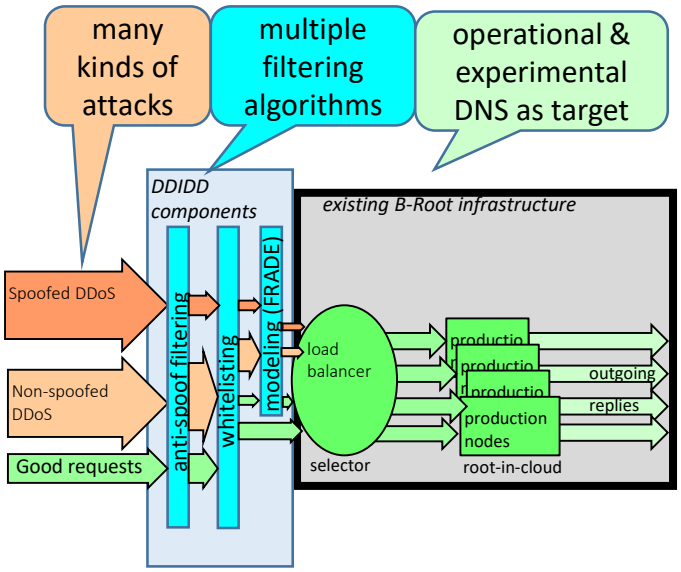
Challenges

- Many kinds of DDoS attacks
  - Spoofed traffic
  - Direct, non-spoofed bogus traffic
  - Legitimate-like requests from new sources
  - Legitimate-like requests from established sources
- How can we defend against all?

Insight and Approach

- No *single* method efficiently addresses all threats
- We need *multiple* methods: **Defense in Depth**
- Planned approaches:
  - Anti-spoof filtering
  - Off-loading bogus query responses
  - Whitelisting known good clients
  - Modeling known good clients
  - Dynamically scaling infrastructure

DDIDD concepts



Status as of Sept. 2019

- key ideas have been tested
- multiple filters (hop count, known-good sources, response code, query name) under evaluation at B-Root and in testbed
- automatic filter choice system evaluated (ISI tech report "Dynamically Selecting Defenses to DDoS for DNS" by Rizvi, Heidmeann, and Mirkovic)

Broader Impacts

- Initial tests on B-Root, one of the 13 root nameservers for the Internet
- Open source releases for all
- Technology transfer from prior NSF projects (CNS #1319215, FRADE)
- Leverage our prior work
  - Oikonomou and Mirkovic. Modeling Human Behavior for Defense Against Flash Crowd Attacks. IEEE ICC, 2009. 10.1109/ICC.2009.5199191
  - Moura, Schmidt, Heidemann, de Vries, Müller, Wei, and Hesselman. Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event. 10.1145/2987443.2987446

About Us

- PIs: John Heidemann, Jelena Mirkovic, Wes Hardaker (USC/ISI)
- Joint work of researchers and B-Root operators at ISI
- https://ant.isi.edu/ddidd/
- Mid-term project, started October 2017