2017 Cyber Security R&D Showcase and Technical Workshop

July 11 - 13, 2017 | Washington, D.C.
DDoS Defense for a Community of Peers (3DCoP)

Jem Berkes | Galois, Inc.
July 12, 2017
Team Profile

Galois specializes in the research and development of new technologies that solve the most difficult problems in computer science and cybersecurity.

Our solutions – built for DHS, DoD, DoE, NASA, the IC, and private clients – ensure that the systems you depend on work as intended, and only as intended.
Need for DDoS Protection

- Distributed Denial of Service (DDoS) kills internet connectivity
- Medium-sized organizations can’t withstand large attacks
- Attacks are too large even for ISPs to handle, > 1 Terabit/s
Our Approach

Organization’s Network

Our Approach

3DCoP

- Anomalies
- Request to block attacks

Firewall & router rules

Internet

Organization’s border routers

LAN(s)

Organization’s Network
Approach: Challenges

- We are working with Internet Protocol (IP), layer 3
- How to process large volumes of traffic?
  - Use “flow” (NetFlow, IPFIX) representation
- How to communicate among peers?
  - We use IPFS, a decentralized P2P layer: [http://ipfs.io](http://ipfs.io)
- How to analyze huge attacks?
  - A rules-based engine for distributed analysis
  - Used models of large attacks to test 3DCoP
Approach: Design for large attacks

Simulated attack we created for development:
1.23 Tbps traffic from over 175,000 sources
Benefits of 3DCoP

- Organizations retain control and autonomy of their networks – the way the Internet is supposed to be
- Built to handle the largest attacks
- 3DCoP works with existing equipment
  - Most routers already support NetFlow/IPFIX
- Easy to deploy
  - No structural changes to your network
  - No re-routing, tunneling, or new IP announcements
# Competition

<table>
<thead>
<tr>
<th>Dimension</th>
<th>3DCoP</th>
<th>Competition: Scrubbers and hosted services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost $</td>
<td>Minimal – PC hardware</td>
<td>Packet scrubbers are expensive</td>
</tr>
<tr>
<td>Autonomy</td>
<td>Retain full control</td>
<td>Hosted = loss of control</td>
</tr>
<tr>
<td>Deployment</td>
<td>Works with your routers, stays on premises, keep existing setup</td>
<td>Lots of migration tools to shift workloads to hosted services</td>
</tr>
<tr>
<td>Phasing in</td>
<td>Non-destructive</td>
<td>Hosted = change all services</td>
</tr>
<tr>
<td>Knowledge</td>
<td>New defensive knowledge</td>
<td>Hosted = outsourced, learn nothing</td>
</tr>
</tbody>
</table>
Current Status

- All project milestones completed on schedule
- Successfully evaluated system for 1 Tbps attacks
  - DHS Program Goal
- Pilot programs in progress
Current Status: Pilots

- The International Gaming Association (non-profit)
  - Approached us with interest in early adoption
  - 3DCoP is running there right now
- Galois
  - Eat your own dog food
- More partnership discussions in progress
Current Status: Technical Work

- Evaluated 1 Tbps attack
  - Used ddosflowgen, our high data rate simulation tool
- Tested with DHS IMPACT datasets
- Evaluated scalability of peer-to-peer network
- Synthesized large scale attacks
- Collaborating with Spamhaus
  - Analyzing new botnet attacks (Mirai, etc)
  - Review and critique of 3DCoP design
Places We’ve Talked About 3DCoP

- FloCon 2016 and 2017
- BSides PDX 2016
- Northwest Academic Computing Consortium (NWACC)
- DHS Science and Technology (S&T) Cyber Seminar
- University of Oregon
- IEEE section at University of Manitoba
- Intel
Transition Activities

- We have two active pilot programs
- Currently in discussions with
  - Universities and network hardware vendors
  - Looking for other organizations to partner with
Technical Lessons Learned

- Real-world attack data is hard to find
  - DHS IMPACT datasets are useful
- Available data is often heavily obfuscated
- In-house simulation is essential for this kind of work
Contact Info

Jem Berkes
PI, DDoS Defense

Team: Jem Berkes, Erin Chapman, Adam Wick
Galois, Inc.
ddos@galois.com
503.626.6616
Twitter: @galois