SENSS
Security Service for the Internet

Jelena Mirkovic (USC/ISI), Minlan Yu (USC), Ying Zhang (HP Labs), Sivaram Ramanathan (USC)
Attack Mitigation Today

• DDoS
  – Local device does traffic analysis, sometimes DPI (low-volume and application attacks; cannot handle high-volume or reflected traffic)
  – Cloud-based defense, traffic goes to cloud for scrubbing (high-volume attacks; takes time to set up, expensive, redirects traffic, special handling for encrypted traffic)

• BGP prefix hijacking
  – BGP anycast (distributes prefix presence; takes time to set up, expensive, needs content replication too)

• Most solutions focus on resource replication and withstand attacks
Our solution - SENSS

• Collaborative between victim and ISPs
• Enables victim to query its own ISP or remote ISPs about:
  – Its inbound traffic
  – Routes to its prefixes
• Enables victim to ask ISPs to:
  – Filter some of its inbound traffic (victim specifies header signature)
  – Demote a route that may contain a hijacker
• Secure, robust to misbehavior
• Works with existing ISP infrastructure
Operation

- **ISPs** run SENSST servers
- **Victim** identifies ISPs to interact with using public SENSST directory
  - Sends to each a query
  - **ISPs** authenticate prefix ownership, process query, charge the victim and return replies
- **Victim** decides which control actions to apply and where
  - Sends messages about this to chosen ISPs
  - **ISPs** authenticate prefix ownership, charge the victim, implement requested actions
SENSS APIs at ISPs

- Exposed as Web services
  - Leverage existing functionalities for robustness (replication), security (HTTPS), charging (e-commerce)

<table>
<thead>
<tr>
<th>Type</th>
<th>Fields</th>
<th>Action/Reply</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic query</td>
<td>Flow, dir, obs_time</td>
<td>List of &lt;tag, dir, volume&gt;</td>
</tr>
<tr>
<td>Traffic filter/allow</td>
<td>Flow, dir, tag, duration</td>
<td>Deploy filter/allow actions</td>
</tr>
<tr>
<td>Route query</td>
<td>Prefix</td>
<td>List of best paths to prefix</td>
</tr>
<tr>
<td>Route demote</td>
<td>Prefix, segment, duration</td>
<td>Demote routes with given segment</td>
</tr>
</tbody>
</table>

- Message authentication: Proof of authority for a prefix
  - Signed proof that owner of a given public key is authorized to speak for a set of prefixes in the SENSs messages
  - RPKI, extension of SSL certs, ...
  - ... or manually populate a DB of known customers and prefixes
- TLS for communication security
- Victim can delegate a proxy if it cannot communicate itself
Example: Isolated Deployment

V $\Rightarrow$ A: traffic_query
A $\Rightarrow$ V: 1 (D-A), 0.5 (E-A), 5 (F-A), 0.5 (C-A)

V $\Rightarrow$ A: traffic_filter(tag=F-A, dest=V)

V NATs all DNS traffic through VN, ports 1000-2000

V $\Rightarrow$ A: traffic_allow(dest=VN, sport=53, dport=(1000,2000))
V $\Rightarrow$ A: traffic_filter(dest=V, sport=53)
Example: ISP-Only Deployment

S periodically collects traffic reports from A,B,C,D,E,F,G,H
Analyzes traffic
Detects attack on V
Identifies E as ingress router, which sends most of the attack to V
Deploys blackholing at E for destination V
SENSS Components

- **@ISP: SENSS server** – Web application + scripts, which communicate with routers
- **@Victim or @ISP: SENSS client** – application, which sends messages to SENSS server, analyzes responses, decides on mitigation strategy
- **@Victim or @ISP: Attack detection module** – works on Netflow records to detect attacks, suggest filter rules to SENSS client
What SENSS Can Do For ISPs?

- Help you defend your customers from DDoS with existing infrastructure
- Automate DDoS handling within your ISP
- Help detect and diagnose attacks (separate module)
Integrating SENSS With ISP

• SENSS is a Web application, which can be ran on any Web server within your ISP:
  – Admin account requires 2-factor authentication
  – Use RPKI or set up DB for proof of authority for a prefix
  – Supply IP addresses of switches

• SENSS needs traffic/route observation and filtering:
  – For traffic observation: SDN or SNMP
  – For traffic filtering: SDN or Flowspec or ACLs
  – For route observation/filtering: interact with router software (Quagga)
Expected Performance

• SENSES should help mitigate most direct floods and 100% of reflector attacks

• SENSES server performance scales with # border routers and # concurrent requests from clients
  – Irrespective of attack volume or # attackers
  – Message processing under $\frac{1}{4}$ sec under heavy load

• One rule per SENSES message:
  – Modest consumption of TCAM space

• Fast-path packet handling

• Easy deployment: no separate hardware
Test drive SENSS in your network
Reach out
sunshine@isi.edu
http://steel.isi.edu/Projects/SENSS/

Jelena Mirkovic
Minlan Yu
Ying Zhang
Sivaram Ramanathan