SANE: A Protection Architecture for Enterprise Networks

Martin Casado, Tal Garfinkel, Aditya Akella, Michael J. Freedman
Dan Boneh, Nick McKeown, Scott Shenker
Enterprise Network

• no losses of data

• no exposition of private information

• no losses of system availability
Current Techniques

- Complexity of Mechanism
- Proliferation of Trust
- Proliferation of Information
Enterprise Network Special

- carefully engineered and centrally administered

- clients use predictable set of local services

- hosts and principals are authenticated

- quickly adopt a new protection architecture
Threat Environment

- insider threats authenticated users, or switches

- outsider threats
  attacker plugging into a network jack
Design Goal

• Allow natural policies that are simple yet powerful

• Enforcement should be at the link layer, to prevent lower layers from undermining it

• Hide information about topology and services from those without permission to see them

• Have only one trusted component
SANE Overview

Step 1
Publish B.http
Allow A access

Step 2
Request capability
to B.http

Step 0
Authenticate with DC

Step 3
Use returned capability
to communicate with B
Domain Controller

- central component in SANE network
- Authentication Service
- Network Service Directory (NSD)
- Protection Layer Controller
Network Service Directory

- a hierarchy of directories and services
- access control list for each of them
- privilege to view, access, publish services
Protection Layer Controller

• capability (encrypted source route) in SANE header in data packets

| Ethernet | SANE header | IP header | data |

• symmetric key for encryption
  DC <--> switches and hosts

• Learn whole topology and establish key pairs by link-state update
SANE Overview
Protection Layer

• Communication with the DC

✓ Minimum Spanning Tree as default connectivity to DC

✓ Construct request capabilities along the path
Protection Layer

• Communication with the DC
  Minimum Spanning Tree

http://en.wikipedia.org/wiki/Minimum_spanning_tree
# Protection Layer

- **Point-to-Point Communication**
  
  ✓ SANE names & connection identifier
  
  ✓ DC construct capability by client's name, location, service's location, and path between them
  
  ✓ Use FORWARD packets

<table>
<thead>
<tr>
<th>FORWARD</th>
<th>Cap-ID</th>
<th>Cap-Exp</th>
<th>Capability</th>
<th>Payload</th>
</tr>
</thead>
</table>
Protection Layer

• Point-to-Point Communication

1. Initialize:
   \[ \text{CAPABILITY} \leftarrow E_{K_{\text{server-name}}} \left( \text{client-name}, \text{client-ID}, \text{server-ID}, \text{last-hop} \right) \]

2. Recurse: For each node on the path, starting from the last node, do:
   \[ \text{CAPABILITY} \leftarrow E_{K_{\text{switch-name}}} \left( \text{switch-name}, \text{next-hop}, \text{prev-hop}, \text{CAPABILITY} \right) \]

3. Finalize:
   \[ \text{CAPABILITY} \leftarrow E_{K_{\text{client-name}}} \left( \text{client-name}, \text{client-ID}, \text{first-hop}, \text{CAPABILITY} \right), \ \text{IV} \]
Protection Layer

• Revoking Access

✓ revoke capability for misuse

✓ victim requests, DC verifies, sends REVOKE packet

✓ switch records this capability, drops packets, forwards request
Fault Tolerance

• Replicating the Domain Controller
  DC physically replicated for scalability and fault tolerance

• Recovering from Nework Failure
Interoperability

- SANE used by unmodified end-hosts
  - Translation Proxies
  - Gateways
  - Broadcast
  - Service Publication
Additional Features

- Middleboxes and Proxies
- Mobility
- Anti-mobility
- Centralized Logging
Attack Resistance

• Mechanism

✓ Access control List

✓ Encrypted, authenticated source-routes and link-state updates

✓ Authenticated network components
Attack Resistance

• Resource Exhaustion

✓ Flooding

✓ Revocation state exhaustion
  refresh switch
  limit revocation requests of senders
Attack Resistance

• Tolerating Malicious Switches

✓ Sabotaging MST Discovery
  falsy advertising distance in MST construction

✓ Bad Link-State Advertisement
  falsifying connectivity information in link-state updates
Attack Resistance

• Tolerating a Malicious DC

distribute trust among DCs using threshold cryptography
Conclusion

• Enterprise Network is special

✓ Consistent policies
✓ Centralized control
✓ Restricted Access
✓ Least possible privilege and knowledge