Enterprise Security Management

Today

- Difficult to express policies [Wool04]
  - Meaningless identifiers, Distributed rule sets

- Policies easily broken/subverted [Maltz04]
  - Filtering and forwarding at odds, rules encode topology
Why Not Manage Network With …

- Central policy
  (not distributed over many components)
- Over high-level names
  (not low-level addresses)
- Enforced robustly
  (not easily subverted)

Challenge: High-Level Names

Requirement: map “nancy” -> n
- Jen can forge Nancy’s name -> IP bindings
- Jen can forge source to be n
- Nancy’s IP may be reallocated (dhcp)

Problems:
- Bindings unauthenticated
- Address bindings/allocation separate

Payroll

Nancy
IP: n
Challenge: Network Enforcement

"Nancy's web traffic must use proxy"
- Where will Nancy's traffic go?

Problem:
- No control of routes

Consequence:
- Must place security at physical choke points
- Adding or moving equipment is dangerous

Our Goal: Improve Security Management through Policy Support

v Claim: Difficult with current architecture

v Proposal: Redesign to support policy management
**Design Principles**

**Principle 1: Unification through Centralization**
- Name/address bindings and allocation
- Policy declaration
- Routing and filtering

**Principle 2: Authenticate all bindings**

**Principle 3: “Default Off”**
- Require permission check for every flow

---

**Issues with Centralization**

- **Attack target**
  -Resource controls
- **Scaling**
  - Single PC for 20k host network
  - Simple replication for throughput
- **Resiliency**
  - Simple replication for redundancy
Ethane:
First Packet = Path Setup

Switches are Flow Tables

✓ Check flow-table
✓ If entry exists, apply corresponding action
  • Forward (or drop)
  • Rate limit
  • Change MAC addresses (Source obfuscation)
  • Place in specific queue (isolation)
✓ If no entry, send to Controller
Ethane Properties

- High-level names
  - Securely bound
  - Fully independent of topology
  - Support arbitrary policy language
- Enforce in network
  - Enforced at every switch (defense in depth)
  - Adding switch = better network (Not Less secure)
- Semi backwards compatible
  - No modification to end hosts
  - Interoperate with existing switches

Ethane Details

- Protecting the Controller
- Policy language
- Bootstrapping
- Supporting debugging and diagnostics
- Revocation
- Replicating the Controller
  - Redundancy
  - Load balancing
- Limitations
Is Ethane Practical?

Prototype

- Built 3 switches
  - Software 100Mb/1Gig platform
  - Embedded wireless
  - Hardware in Verilog
- Controller
  - Standard PC (1.5Ghz Celeron)
  - Authentication, Permission check, forwarding, resource limits
Deployment

- 9 Wired switches
- 7 Wireless switches
- 2 Residential users
- ~300 Hosts in broadcast domain
  - VOIP phones
  - Printers
  - Servers
  - Workstations (Windows, Linux, Solaris, Mac OS X)
  - Laptops
- Integrated with Stanford authentication system

The “Real” World ...

- Integrating with VLANs
- Obscure protocols
- Dealing with broadcast/service discovery
- Proxy-ARP breaks symmetry
Switch Performance

Software
- PC development platform
  - MTU size packets = 1Gb/s
  - 100-byte packets = 16Mb/s
- Embedded, wireless = 23Mb/s (266MHz MIPS chip)
  (equivalent to native Linux bridging module)

Hardware

<table>
<thead>
<tr>
<th>Packet Size</th>
<th>64b</th>
<th>65b</th>
<th>100b</th>
<th>1518b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measured</td>
<td>1524Mbps</td>
<td>1529Mbps</td>
<td>1677Mbps</td>
<td>1974Mbps</td>
</tr>
</tbody>
</table>

Tested with Ixia 1600T traffic generator

Controller Performance

DNS RTT at residential network
- Stanford, 22,000 IPs
- LBL, 8,000 IPs

DNS RTT on Campus

Load (flows/s)
Ethane Summary

- Current networks insecure and difficult to manage
  - Useless namespace
  - Topology encoded in configurations

- Ethane addresses this through architectural changes
  - Centralized
  - Authenticated bindings
  - "default-off"

- Ethane provides strong guarantees and is practical
  - Support network of 20k hosts from single PC
  - Switches are simple and run at line speeds

Related Work

- SANE
  [Casado06]

- 4D Architecture
  [Yan07],[Greenberg05],[Rexford04]

- Distributed Firewalls
  [Bellovin99],[Ioannidis00],[Keromytis03]

- Hard LANs
  [Weaver05]
Questions?