

# Architectural Support for Security Management in Enterprise Networks

Martin Casado  
Stanford University

With: Michael Freedman, Justin Pettit, Jianying  
Luo, Scott Shenker, Nick McKeown

ACM Sigcomm  
2007

August, 2007



Stanford University

## 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

August, 2007



Stanford University

## Why Not Manage Network With ...

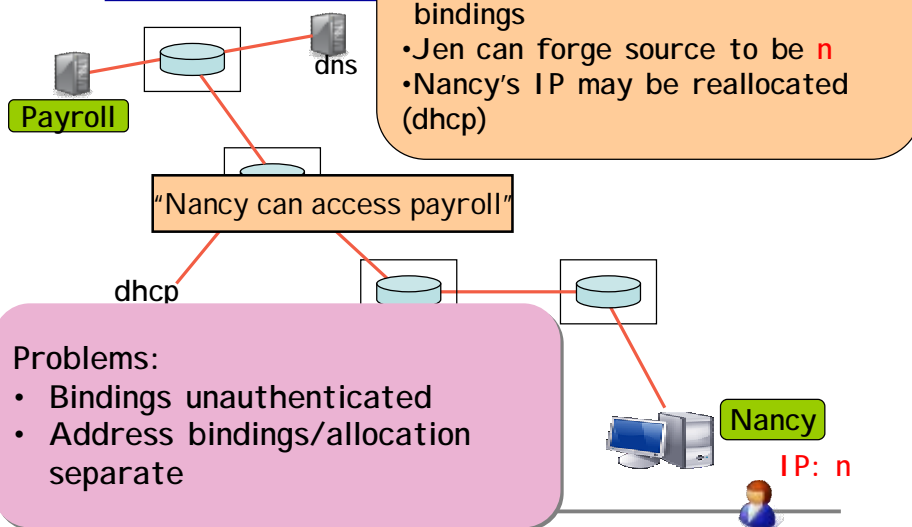
- ✓ Central policy  
(not distributed over many components)
- ✓ Over high-level names  
(not low-level addresses)
- ✓ Enforced robustly  
(not easily subverted)

August, 2007



Stanford University

## Challenge: H

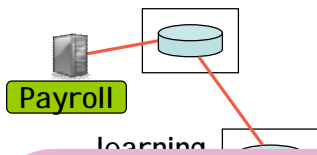


August, 2007



Stanford University

## Challenge: Network Enforcement



"Nancy's web traffic must use proxy"

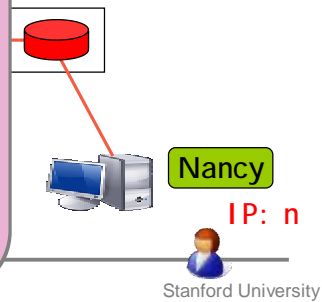
- Where will Nancy's traffic go?

### Problem:

- No control of routes

### Consequence:

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



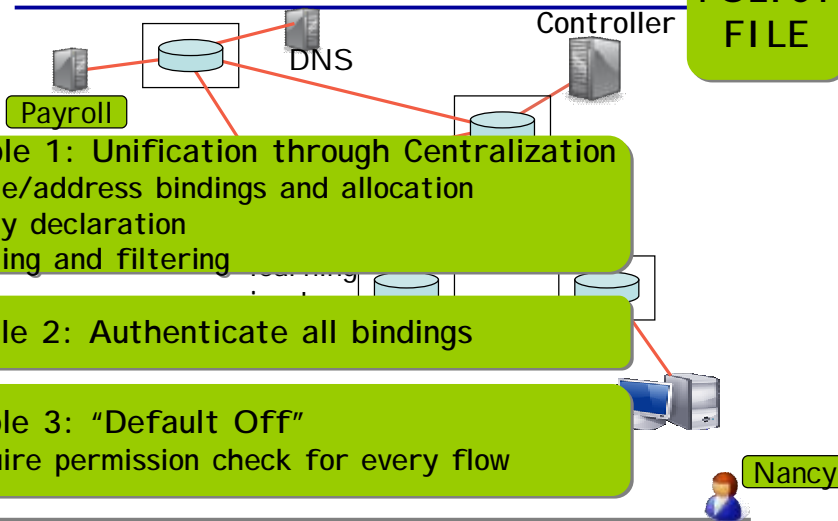
## Our Goal: Improve Security Management through Policy Support

✓ Claim: Difficult with current architecture

✓ 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

August, 2007



Stanford University

# Issues with Centralization

## ✓ Attack target

- ∅ Resource controls

## ✓ Scaling

- ∅ Single PC for 20k host network
- ∅ Simple replication for throughput

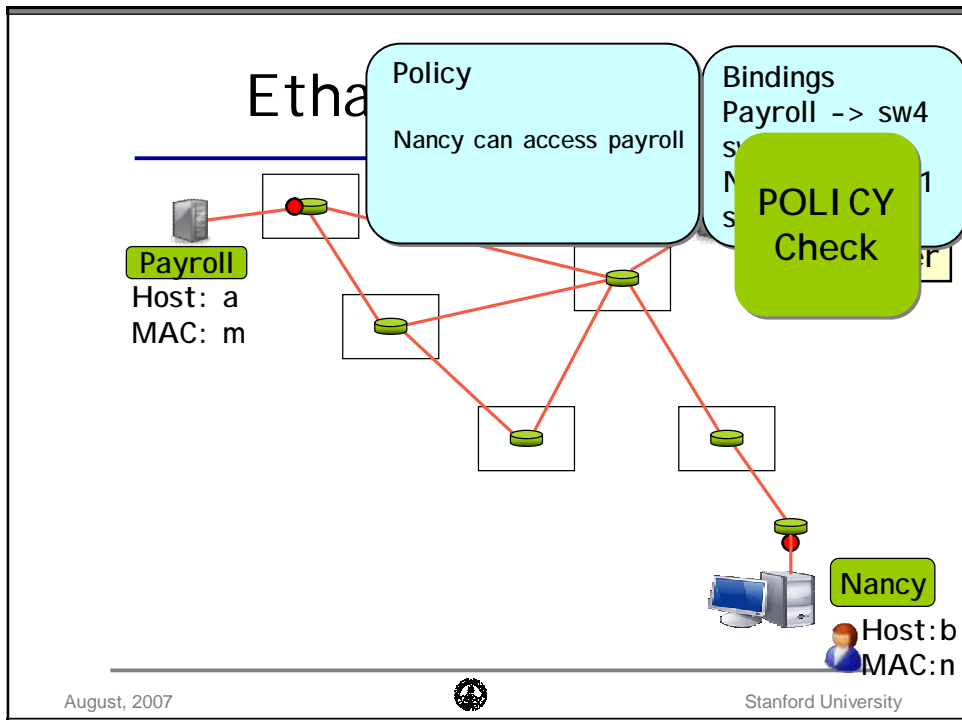
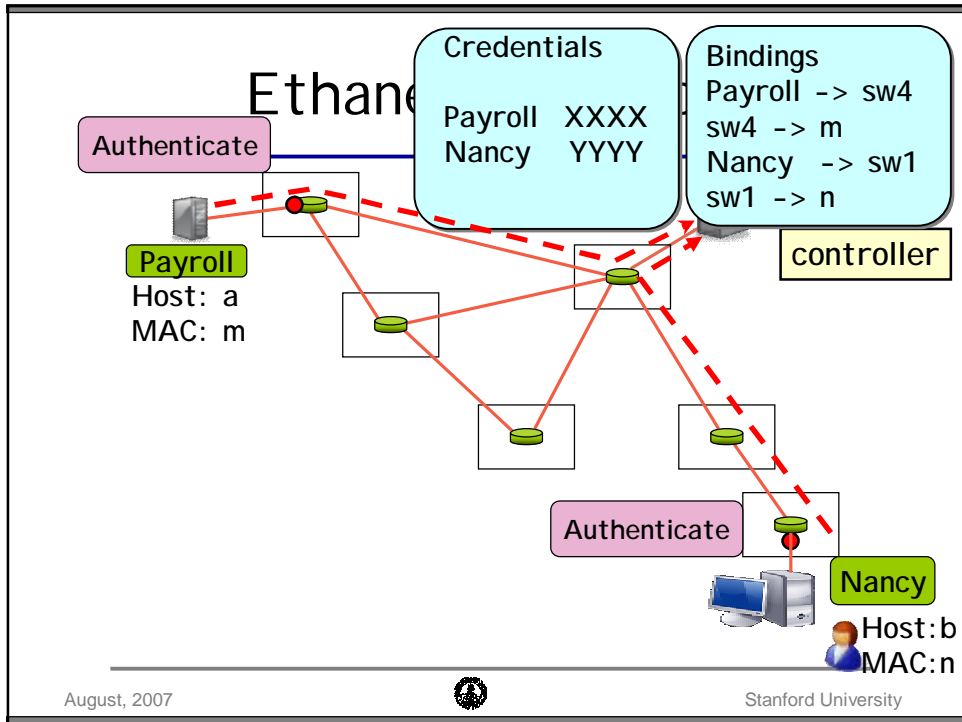
## ✓ Resiliency

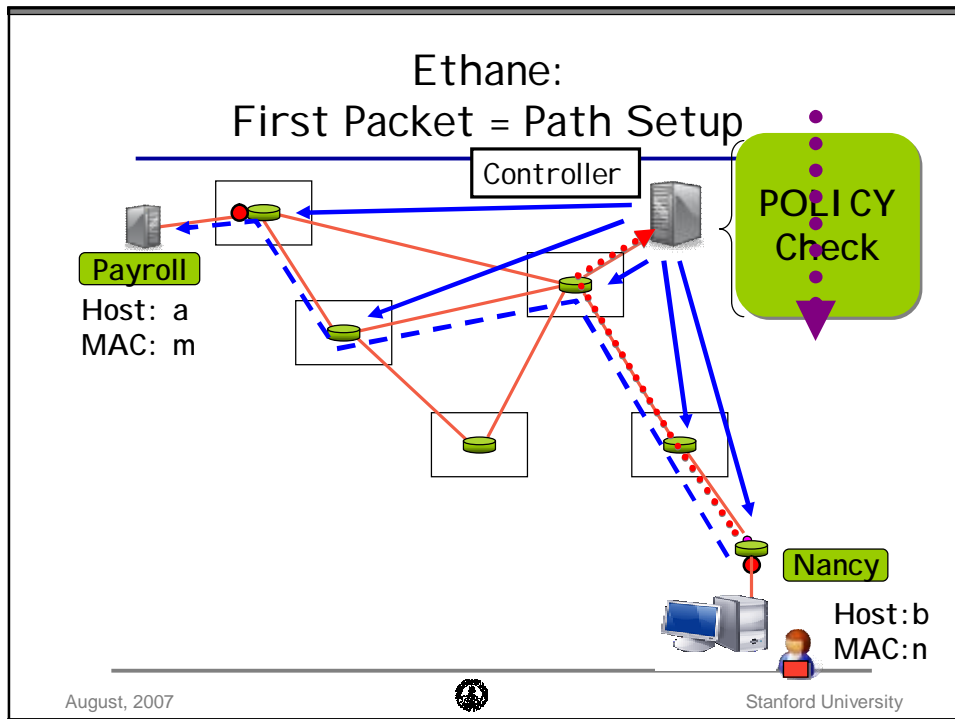
- ∅ Simple replication for redundancy

August, 2007



Stanford University





## 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

---

August, 2007



Stanford University

# Ethane Details

---

- ✓ Protecting the Controller
- ✓ Policy language
- ✓ Bootstrapping
- ✓ Supporting debugging and diagnostics
- ✓ Revocation
- ✓ Replicating the Controller
  - ∅ Redundancy
  - ∅ Load balancing
- ✓ Limitations

---

August, 2007



Stanford University

# Is Ethane Practical?

---

August, 2007



Stanford University

## Prototype

---

### ✓ Built 3 switches

- Ø Software 100Mb/1Gig platform
- Ø Embedded wireless
- Ø Hardware in Verilog



### ✓ Controller

- Ø Standard PC (1.5Ghz Celeron)
- Ø Authentication, Permission check, forwarding, resource limits

August, 2007



Stanford University

## Deployment

---

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

---

August, 2007



Stanford University

## The "Real" World ...

---

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

---

August, 2007



Stanford University



# 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

---

August, 2007



Stanford University

# Related Work

---

- ✓ SANE  
[Casado06]
- ✓ 4D Architecture  
[Yan07],[Greenberg05],[Rexford04]
- ✓ Distributed Firewalls  
[Bellovin99],[Ioannidis00],[Keromytis03]
- ✓ Hard LANs  
[Weaver05]

---

August, 2007



Stanford University

# Questions?

---

