Overview

- An Brief Overview of Ethernet
- Ethane Overview
- Ethane Protocol Assumptions
- Ethane Switches and Controller
- Configuration
- Flow Process
- Experimental Data
- Strengths and Weaknesses
- Questions

Overview of Ethernet Routing Strategy

- Routers control traffic flow
  - Use ARP/BGP style protocols to determine best routes through network
  - No one router understands the whole network
  - Autonomous
    - Each router makes own decisions about packets
  - No Authentication
    - In general, communication is permitted
      - firewall knows IPs, ports, protocols
    - No knowledge of network users
  - Failure-resistant
    - Reroutes around failed hardware automatically

Ethernet Switches

- Independent
  - Follow their own rules
  - Determine their own routes
  - stores 100,000s of routes
  - Responsible for NAT, VLAN and other services
  - Communicate route information with their peers
Overview of Ethane

- Centralized Network Control
  - Network rules enforced by network controller
  - Controller monitors and approves all traffic
    - Allows for complete policy-based control of the network
  - Controller responsible for damage-routing
  - Access Controls Built In
    - Network understands users, hardware, topology, and policies

Ethane’s Assumptions

- Policy determines packet flow
  - Network should maintain a strong connection between users and traffic
  - Policy should be simple to implement
  - Incremental Deployability
    - Should work with ethernet
    - Bake security into network policy

Ethane Switches

- Dependent
  - Requires connection to controller to route new traffic
  - Communicates with Controller over a secure channel
- Simple
  - Minimal On-Board Logic
    - “Flow” table lookup only
      - Only stores active flows
    - No understanding of network topology
    - No NAT knowledge
    - No VLAN support

The Ethane Controller

- Switches report network topology to Controller
  - Controller uses this to create flow rules
  - Controls all routes between hosts
    - Allows for prioritization
    - Controller handles congestion
    - Can restrict client movement
  - Handles Authentication
    - Users, Devices, Switches
      - Understands where a user is physically connected to the network
The Ethane Controller
(Continued)

- Informed of link failures and updates flow rules
- Can cut off misbehaving hosts at the switch, completely denying network access
- Supports Resource Limits on Clients
- Allows for very detailed network usage logs
- Useful for failure post-mortems
- Presents something of a privacy risk
- Acts on network broadcast requests

Ethane Configuration: Pol-Eth

- The Configuration language for Ethane
  - Compiled into controller
  - Individual rules are ANDs of simple statements
  - Allows for user-based rules
  - Rules priority determined by order in file
  - Very human-readable

Flow Setup Process

1. User A tries to connect to User B
2. User A to User B flow isn’t in Switch 1’s Flow Table, so the packet is forwarded to the Controller
3. Controller either approves or denies route
4. If approved, Switch 1 and Switch 2 establish a flow from User A to User B

Experimental Setup

- Used 3 custom-built Ethane switches
  - Wireless G access point
  - NetFPGA-based Gigabit switch
    - Based on 7000 lines of verilog
    - x86 Linux-based switch
    - Ethane implemented in software
  - Deployed over department’s network
    - 300 total hosts
    - 120 active hosts at a time
    - Reimplemented existing rules in Pol-Eth

# Groups

desktops = ["griffin", "reo", "zer"],
laptops = ["laptop", "laptop"],
phones = ["phone", "phone"],
server = ["http_server", "telx_server"],
private = ["desktops", "laptops"],
computers = ["private", "server"],
students = ["bob", "bill", "pete"],
profs = ["plum"],
group = ["students", "profs"],
wap = ["wap1", "wap2"],
0:0

# Rules

match dst-port(int(80)) { [htc=ht(int"server") & (htl=ht(int"private"))] : deny;
# Do not allow phones and private computers to communicate
[htc=ht(int"phones") & (htl=ht(int"computers"))] : deny;
[htc=ht(int"computers") & (htl=ht(int"phones"))] : deny;
# NAT-like protection for laptops
[htc=ht(int"laptops")]: outbound-only;
# No restrictions on desktops communicating with each other
[htc=ht(int"desktops") & (htl=ht(int"desktops"))]: allow;
# For wireless, non-group members can use http through
# a proxy. Group members have unrestricted access.
[(aproc=ht(int"wap") & (user=ht(int"group")))]: allow;
[(aproc=ht(int"wap") & (protocol= protocol=mip))]: waypoint( http-proxy "http-proxy");
[(aproc=ht(int"wap"))]: deny;
}: allow; # Default-on: by default allow flows

[C+5]
Experimental Results

- Hardware Prototypes
  - Wireless Access Point
    - Ethane Speed Equivalent to Ethernet
  - Gigabit FPGA board
    - Forwarded minimum-size packets in full-duplex at a line rate of 1Gb/s
  - x86 Linux Desktop
    - Forwarding Performance drops with packet size
      - 100 byte packets lower speed to 16Mb/s
  - Implemented previous firewall rules in 132 lines of Pol-Eth
  - Controller could handle an estimated 11,000 new flows/sec
    - Allows 25,000 hosts

- Forwarding Performance drops with packet size
  - 100 byte packets lower speed to 16Mb/s

- Controller could handle an estimated 11,000 new flows/sec
  - Allows 25,000 hosts

Strengths

- Implementation and Testing
  - Actually used their software defined testing in a real-world environment and it worked
  - Tested various failure scenarios
    - Provide solutions for some expected scenarios
  - Understood and explained weaknesses
  - Provide strong paths for future research

Weaknesses

- Not compatible with all network uses
  - Broadcast services have to be implemented in Ethane Controller
- Policies relatively easy to work around
  - Application level routing
  - Service Identification done by port
- Current implementation requires relinking for new ruleset
  - Even very short (132 line) rule files create large (4500+ line) compiled policy
- Networking partition can result in entire arms of the network failing
  - Without access to the controller, switches cannot add flows, even if the rest of the network is available

References

Questions?