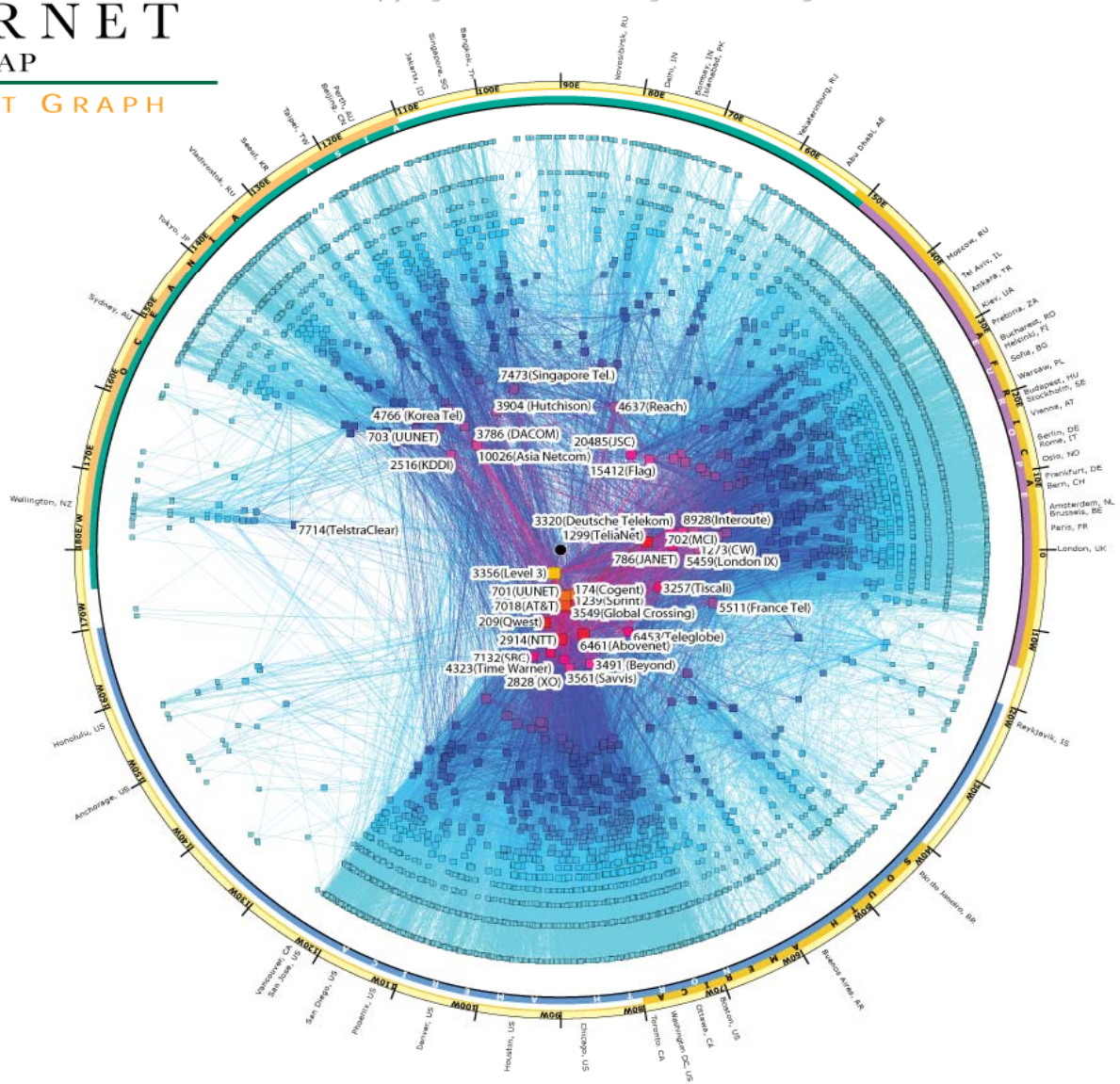
Best Practices With IP Security

Presented by Stuart Strong
s.strong@fecinc.com

IPv4 INTERNET
TOPOLOGY MAP
AS-level INTERNET GRAPH



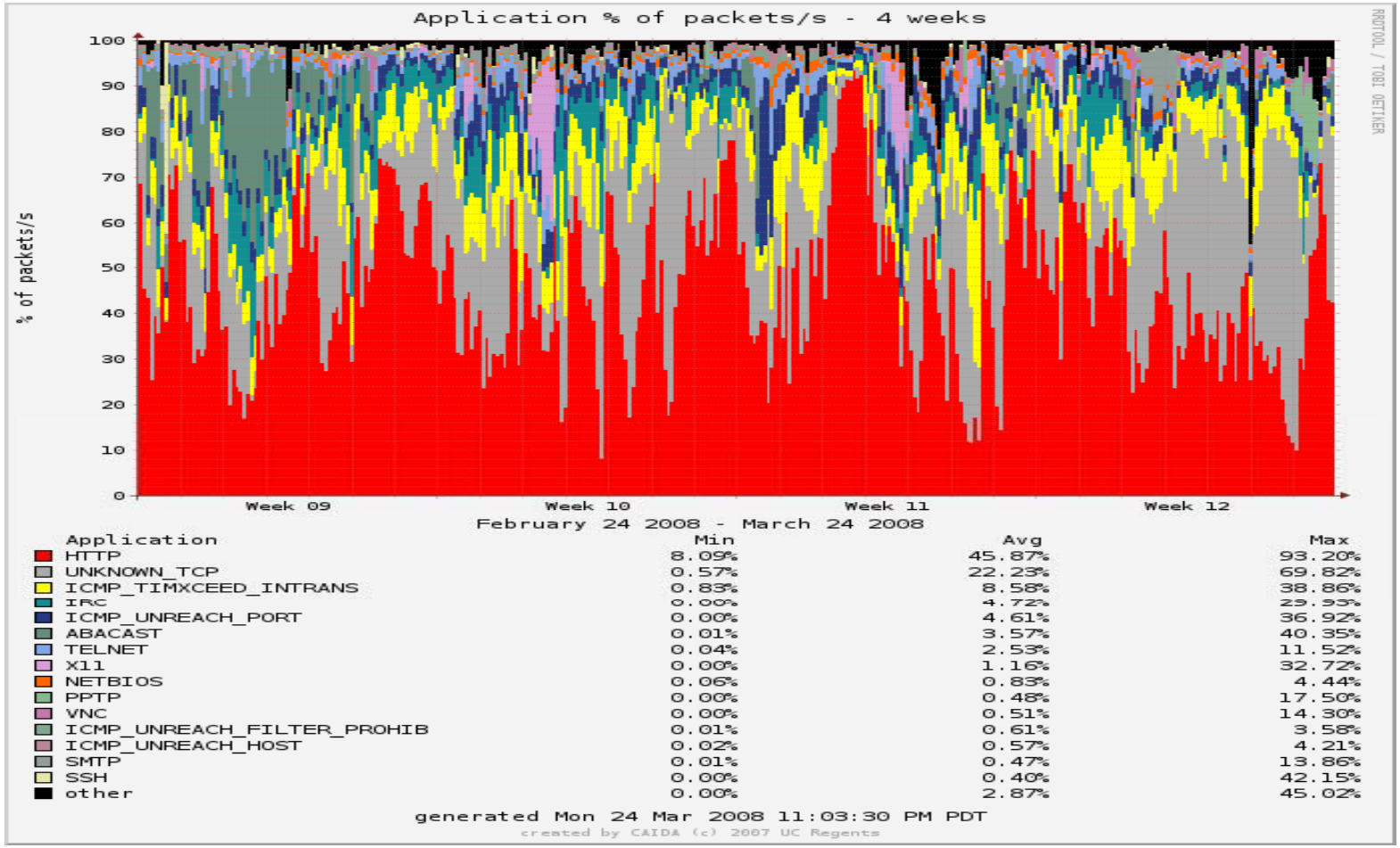
What are the threats?

- Know your enemy
- Network telescope research
  - Current measurement of network events
  - Represents at least 1/256th of illegitimate traffic
- “Among the visible events are various forms of flooding DoS attacks, infection of hosts by Internet worms, and network scanning.”
  - http://www.caida.org/research/security/telescope/

This work would not be possible without the cooperation of UCSD Network Operations and support from DARPA, NSF, Cisco Systems and Caida members. http://www.caida.org/research/security/telescope/

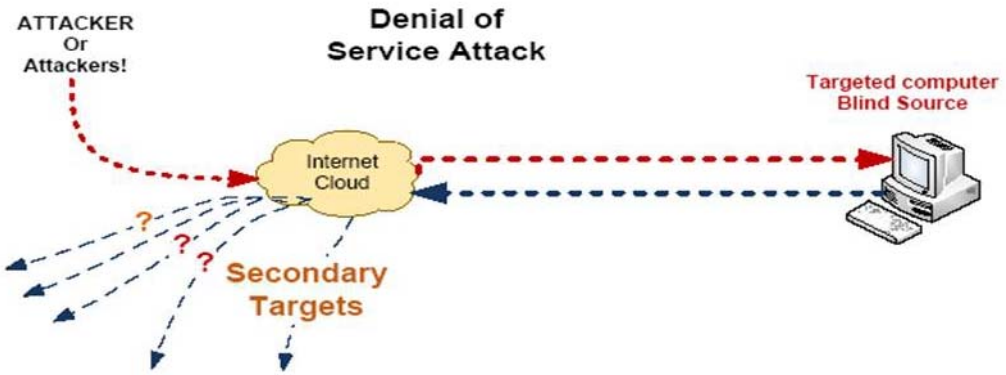
What are the risks?

- Risk = threat x vulnerability x cost



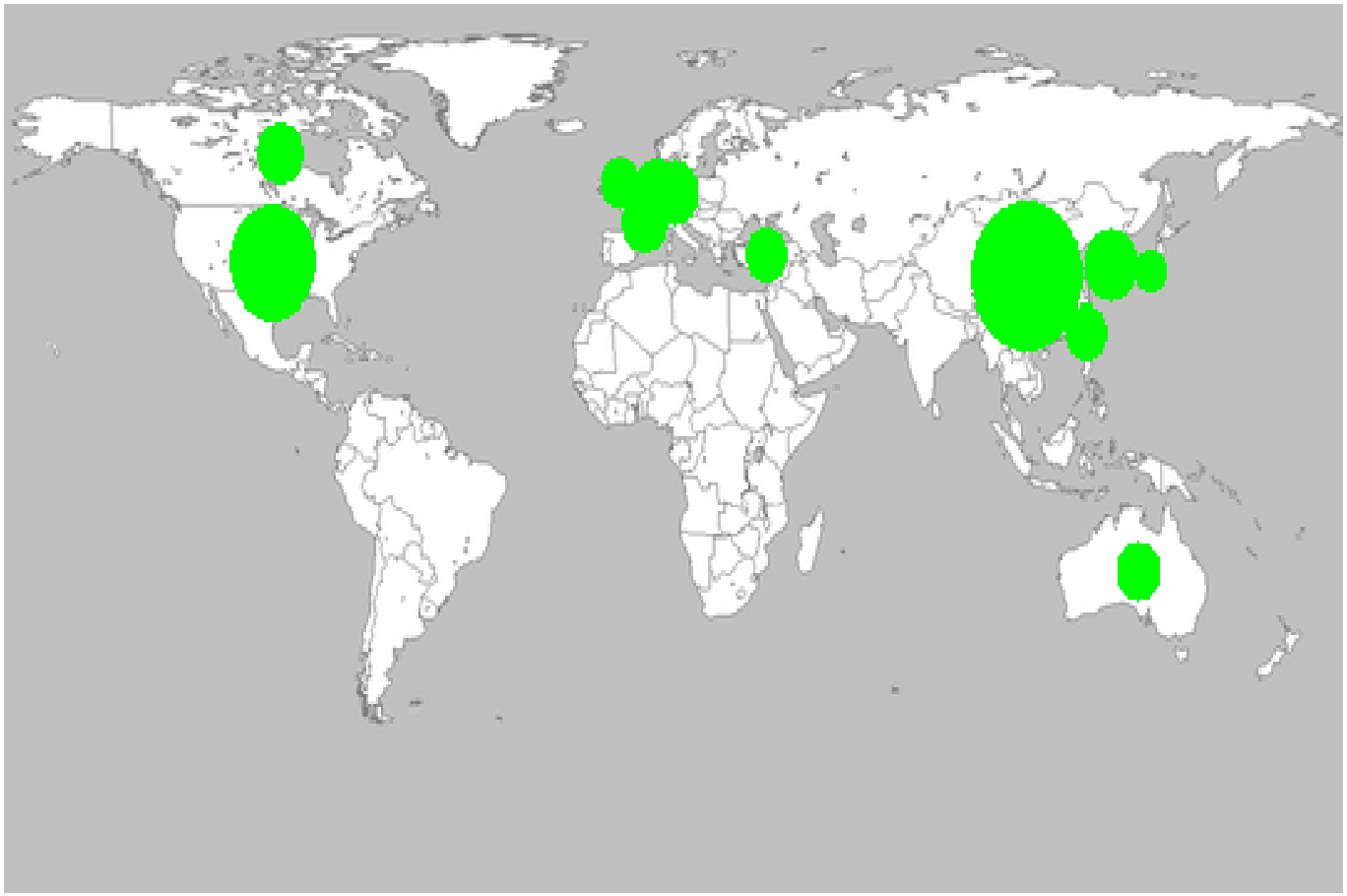
Network vulnerability

- DoS attacks



- Change the source address
  - To random IP address
  - Or to a secondary target
- Scanning is used to find resources to attack

Who is attacked?



- These are locations of attacked computers
- 4 week average of source of backscatter “dark” traffic

http://www.caida.org/data/realtime/telescope/?monitor=telescope_backscatter&row=timescales&col=sources&sources=src_country&graphs_sing=map&counters_sing=packets&timescales=672

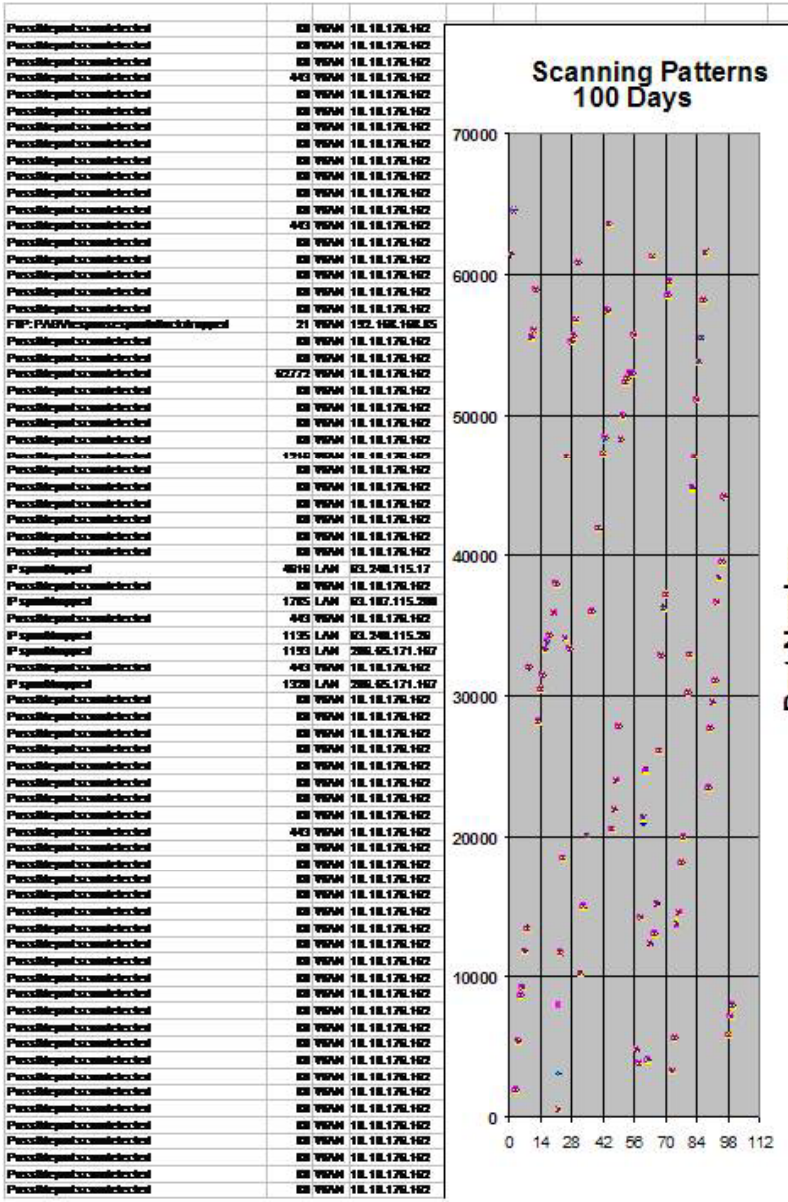
Network configuration vulnerability

Tracing route to customer-10-36-45-33.uninet.net.mx [10.36.45.33] over a maximum of 30 hops:

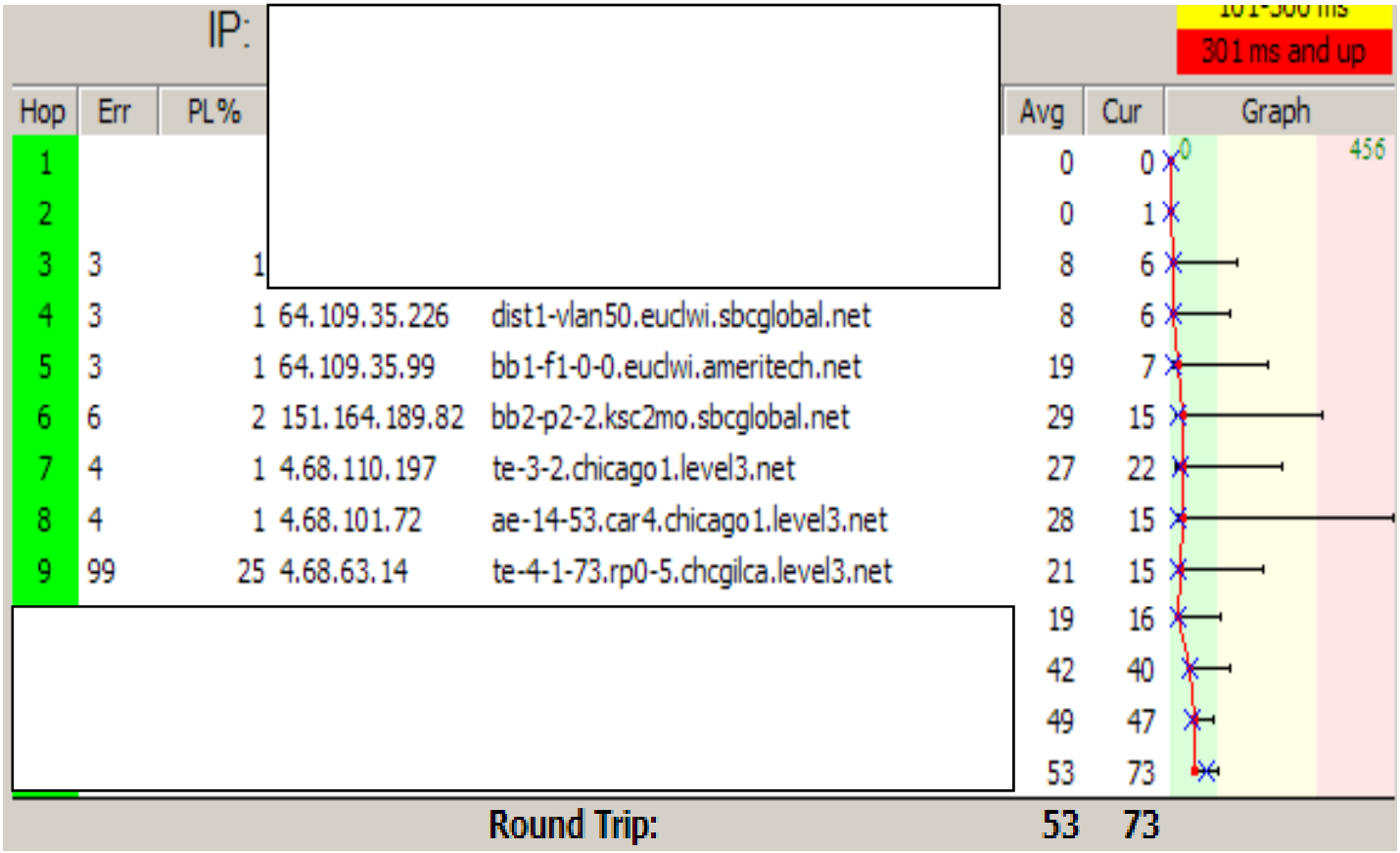
1 >>>11 137 ms 137 ms 137 ms wan-d34-0412-0009.uninet-ide.com.mx [10.134.176.237]
12 141 ms 141 ms 140 ms gw-bb-cun.cancun.com.mx [10.33.191.253]
13 137 ms 145 ms 137 ms noc.cancun.com.mx [10.33.188.5]
14 161 ms 157 ms 160 ms intercun-pya.cancun.com.mx [10.33.191.125]
15 170 ms 182 ms 197 ms ppp-190-129.cancun.com.mx [10.33.190.129]
16 198 ms 201 ms 265 ms intercun-pya.cancun.com.mx [10.33.191.125]
17 195 ms 196 ms 210 ms ppp-190-129.cancun.com.mx [10.33.190.129]
18 193 ms 201 ms 202 ms intercun-pya.cancun.com.mx [10.33.191.125]
19 244 ms 230 ms 209 ms ppp-190-129.cancun.com.mx [10.33.190.129]
20 231 ms 198 ms 230 ms intercun-pya.cancun.com.mx [10.33.191.125]
21 222 ms 223 ms 271 ms ppp-190-129.cancun.com.mx [10.33.190.129]
22 234 ms 252 ms 230 ms intercun-pya.cancun.com.mx [10.33.191.125]
23 262 ms 260 ms 256 ms ppp-190-129.cancun.com.mx [10.33.190.129]
24 259 ms 259 ms 262 ms intercun-pya.cancun.com.mx [10.33.191.125]
25 288 ms 247 ms 281 ms ppp-190-129.cancun.com.mx [10.33.190.129]
26 282 ms 257 ms 295 ms intercun-pya.cancun.com.mx [10.33.191.125]
27 292 ms 318 ms 305 ms ppp-190-129.cancun.com.mx [10.33.190.129]
28 320 ms 344 ms 290 ms intercun-pya.cancun.com.mx [10.33.191.125]
29 295 ms 304 ms 287 ms ppp-190-129.cancun.com.mx [10.33.190.129]
30 290 ms 307 ms 329 ms intercun-pya.cancun.com.mx [10.33.191.125]

Network Scanning

Sonic wall event logs, 100 days, all odd ports scanned



Network denial of service



Node traffic overload = Denial of Service
Compromising the routing table will create partitions in the network
Five percent of the internet cannot connect to the rest of the internet

Network costs

- Can you harden your critical applications and equipment?
- What is the price of convenience vs. cost of being compromised?
  - What is the cost your business integrity (*intangible asset*)?
  - What are the costs of your equipment (*tangible*)?
- What are the appropriate tactics and strategy?
- One of the first rules in security is access
  - Keys: physical and otherwise
  - Encryption
  - Doors: physical and otherwise
  - Restricted routes

Network strategies

- Identify your assumptions
  - Audit your network process
  - Who is trusted and why?
  - http://www.nanog.org/ispsecurity.html
- What has to be protected?
  - Your only as secure as your weakest link
  - Know your weaknesses
  - Remember human factors

Network strategies

- Secure access
  - Authentication: Who are you?
  - Authorization: Limit the scope of access
  - Accounting: Where have you been, and why?
- What are your company's policies?
  - Security must be pervasive and enforced
  - http://www.nanog.org/mtg-0310/kaeo.html

Network security tactics

- Control access
  - Use appropriate technology
    - Passwords: change them
    - Encryption of secrets
  - Use built in technology
    - Routers
    - Access lists
    - Source and destination limiting
    - Disable the ability to discover your network
    - Rate limiting commands
    - Disable easily compromised technologies
    - *SNMP vs.* SNMP v3: k*eep your secrets*

Network security tactics

- Switches
  - Be specific with trunk ports
  - Turn off Dynamic Trunking Protocol on all ports
  - Assign remaining ports to access VLANs
  - Use DHCP snooping

Best practices for IP security

- Application level attack
  - Intrusion detection systems
    - Snort
  - Use application layer gateway
    - Has the ability to open and close pinholes dynamically in firewalls
    - http://www.nanog.org/ispsecurity.html

Best practices for IP security

- Distributed Denial of Service
  - Maintain current patch levels
  - Install and maintain antivirus system
  - Use application-aware IDP systems
  - Establish policy-based security zones
  - Use VLANS to protect voice/video traffic from data network attacks

Best practices for IP security

- Eavesdropping
  - Isolate critical traffic on VLANS
  - Apply encryption selectively
- Viruses
- Worms