

Workshop on Infrastructure Security and Operational Challenges of Service Provider Networks

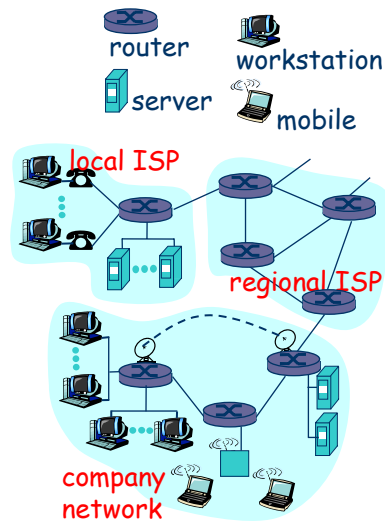
Farnam Jahanian
University of Michigan and Arbor Networks

IFIP Working Group 10.4
June 29-30, 2006



What's the Internet: "nuts and bolts" view

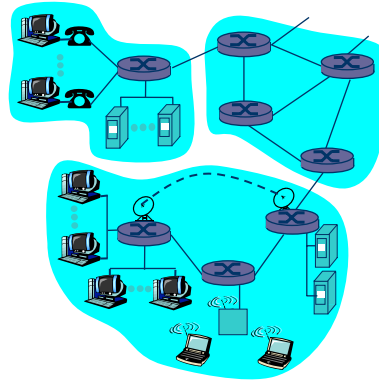
- millions of connected computing devices: *hosts, end-systems*
 - PCs workstations, servers
 - PDAs phones, toastersrunning *network apps*
- *communication links*
 - fiber, copper, radio, satellite
 - transmission rate = *bandwidth*
- *routers*: forward packets (chunks of data)





What's the Internet: "nuts and bolts" view

- **communication infrastructure** enables distributed applications:
 - Web, email, games, e-commerce, database., voting, file (MP3) sharing
- **communication services provided to apps:**
 - connectionless
 - connection-oriented

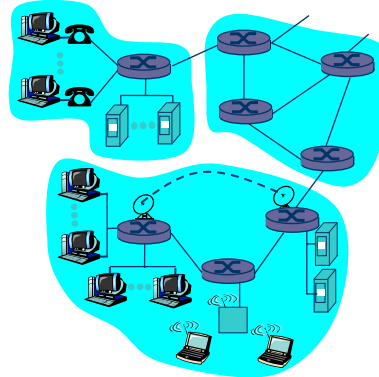


- 3 -



What's the Internet: a service view

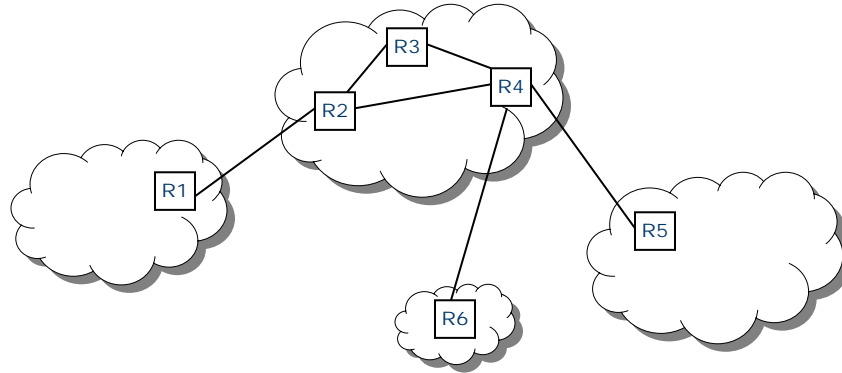
- **communication infrastructure** enables distributed applications:
 - Web, email, games, e-commerce, database., voting, file (MP3) sharing
- **communication services provided to apps:**
 - connectionless
 - connection-oriented



- 4 -



Autonomous Systems (AS)



- The Internet is a collection of autonomous systems.
- AS: A set of routers and networks under the same administrative control.
- Inter-domain vs. intra-domain routing.

- 5 -



Internet design – End-to-End Principle

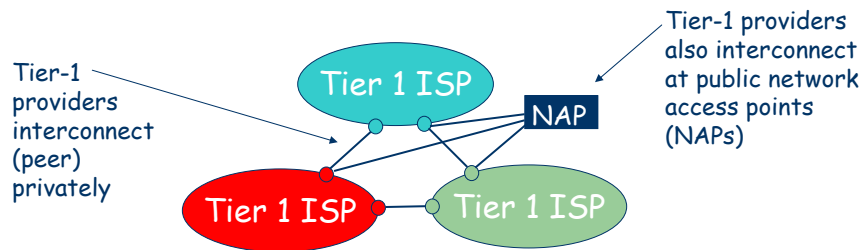
- Put the intelligence in the end hosts and keep the network simple
 - Packet switched instead of circuit switched
 - Best effort delivery
 - Force transport layer to deal with delay and loss
- Dynamic routing in the face of failures
 - No session state on routers
 - Allows routers to be added and removed without causing large disturbances

- 6 -



Internet structure: network of networks

- roughly hierarchical
- **at center: "tier-1" ISPs** (e.g., AT&T, Verizon, Sprint), national/international coverage
 - treat each other as equals

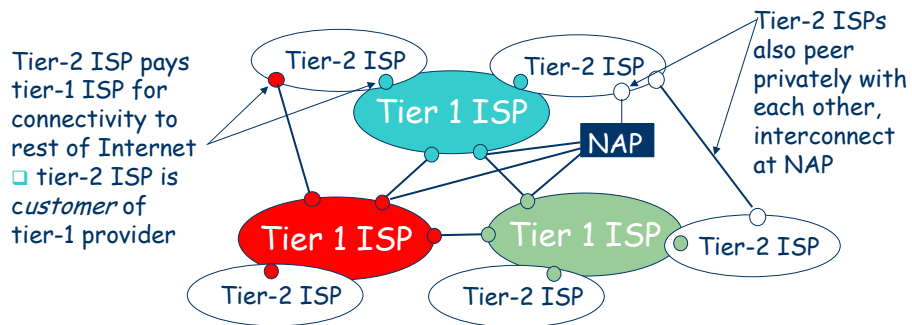


- 7 -



Internet structure: network of networks

- **"Tier-2" ISPs: smaller (often regional) ISPs**
 - Connect to one or more tier-1 ISPs, possibly other tier-2 ISPs

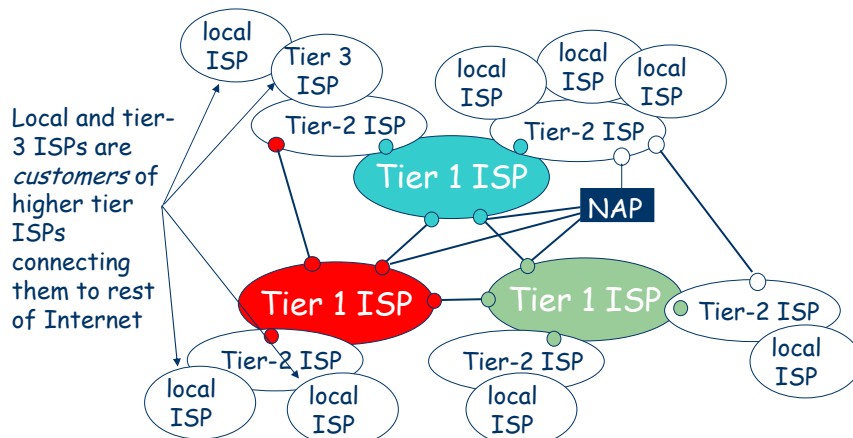


- 8 -



Internet structure: network of networks

- “Tier-3” ISPs and local ISPs
 - last hop (“access”) network (closest to end systems)

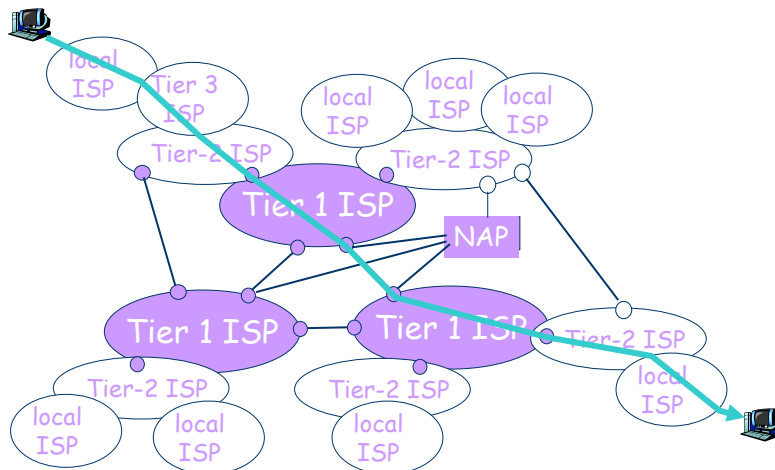


- 9 -

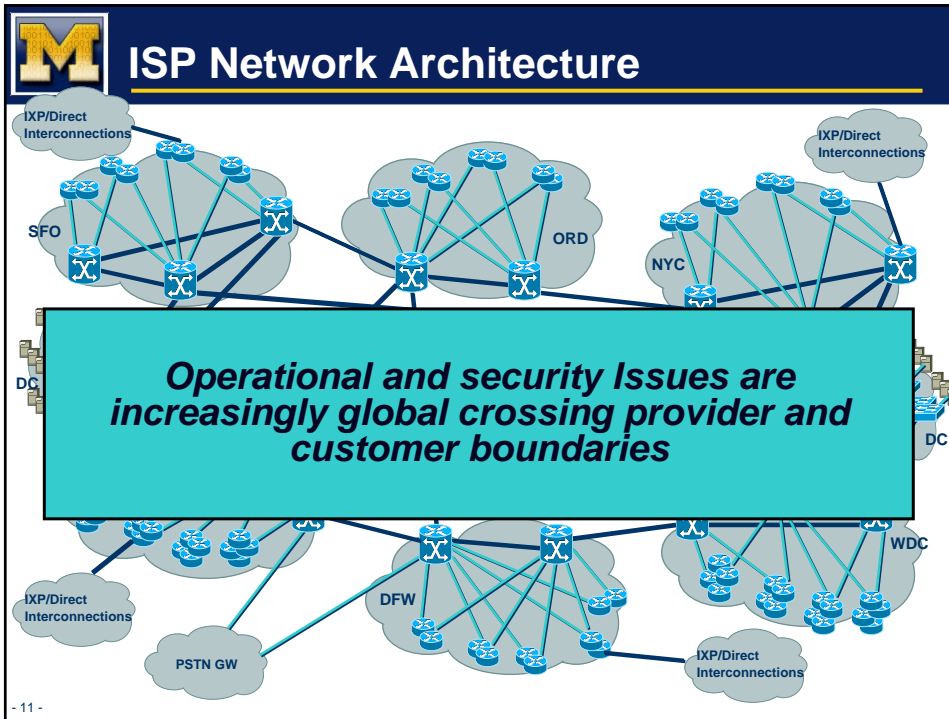


Internet structure: network of networks

- a packet passes through many networks!



- 10 -



-
- M** **WHY IS IT HARD?**
- Requirements of emerging Internet applications
 - VoIP, IPTV, groupware, content delivery & DRM
 - Predictable, reliable and secure services
 - Diverse and complex building blocks
 - 10,000 of network elements in a large network
 - Provider edge, customer edge, POP, backbone
 - Fragile and vulnerable IP control infrastructure
 - IP is a best-effort service, end-to-end principle
 - Scalability achieved thru highly decentralized protocols/services
 - Evolution of security attacks
 - DDoS, worms, botnets, phishing, ...
 - Crumbling network perimeter
 - Evolving regulatory and legal issues
- 12 -



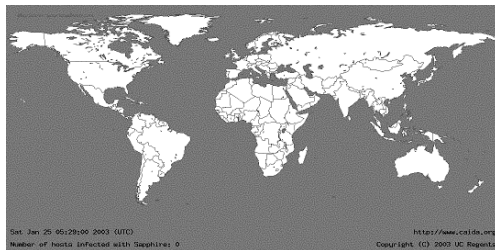
Trends in Internet Security Threats

- **Globally scoped**, respecting no geographic or topological boundaries.
 - At peak, 5 Billion infection attempts per day during Nimda including significant numbers of sources from Korea, China, Germany, and the US. [Arbor Networks, Sep. 2001]
- Exceptionally **virulent**, propagating to the entire vulnerable population in the Internet in a matter of minutes.
 - During Slammer, 75K hosts infected in 30 min. [Moore et al, NANOG February, 2003]
- **Zero-day** threats, exploiting vulnerabilities for which no signature or patch has been developed.
 - In Witty, "victims were compromised via their firewall software the day after a vulnerability in that software was publicized"

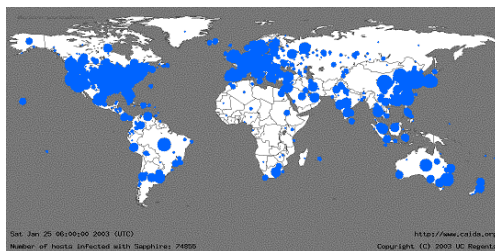
- 13 -



SQL Slammer Attack Propagation



0 hosts infected at the start



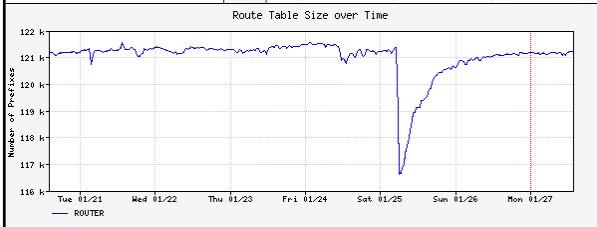
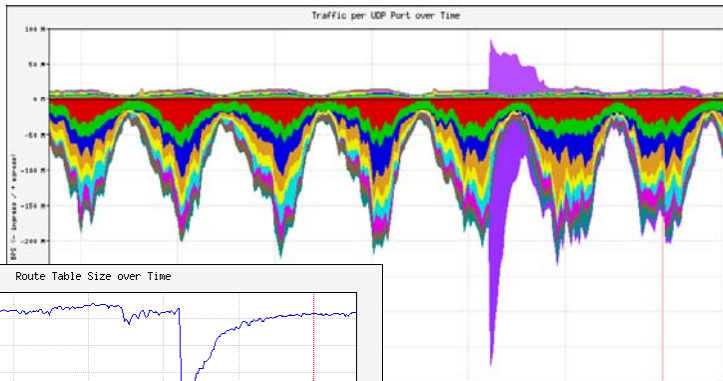
75,000 hosts infected in 30 min.
Infections doubled every 8.5 sec.
Spread 100X faster than Code Red
At peak, scanned 55M hosts per sec.

[Moore, Paxson, et al; NANOG February, 2003]

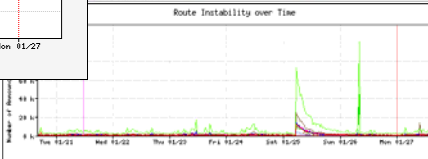


Impact of Slammer on the Internet

No DoS payload!



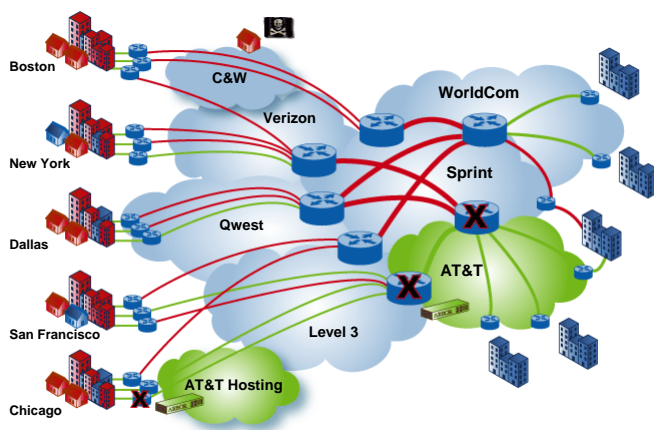
Loss of several thousand routes, mostly /24s



- 15 -



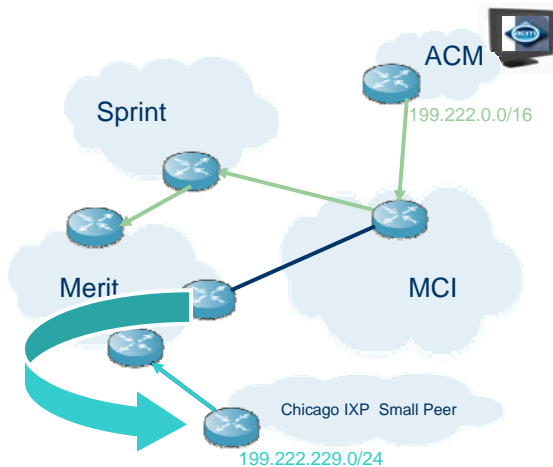
Distributed Denial-of-Service



- 16 -



BGP Address Hijacking



- Though providers filter customer BGP announcements, few filter peers
 - Memory, line-card limitations
 - Maintenance problem
- More specific announcements wins
- Injection attack requires compromised commercial or PC-based router
 - man-in-middle session attacks rare

- 17 -



... Availability Attacks

washingtonpost.com Sign In | Register Now PRINT EDITION | Subscribe to

NEWS OPINION SPORTS ARTS & LIVING Discussions Photos & Video

SEARCH: News Web

washingtonpost.com > Technology > Tech Policy > Security

Worms

Attack On Internet Called Largest Ever

By David McGuire and Brian Krebs
washingtonpost.com Staff Writers
Tuesday, October 22, 2002; 5:40 PM

The heart of the Internet sustained its largest, most sophisticated attack ever, starting late Monday and lasting through Tuesday, according to officials at key online backbone organizations.

These attacks disrupt infrastructure

DoS

Viruses

February 8, 2000

Yahoo Attributes a Lengthy Service Failure to an Attack

By MATT RICHTER

SAN FRANCISCO, Feb. 7 -- Yahoo Inc. blamed a "planned" attack by computer hackers for a service failure that lasted nearly three hours today, in a rare interruption of one of the most popular and best performing sites on the World Wide Web.

BusinessWeek EPIDEMIC

BBC NEWS UK EDITOR

Bookies suffer online

Technology News Online investigation.

Home Site Index Site Search Forums Archives Marketplace

- 18 -



A Dramatic Transformation and Escalation

Anti-Phishing Working Group (APWG) logo and text: "Anti-Phishing Working Group Committed to wiping out Internet scams and fraud"

Reported Phishing Sites by Week October 2004-January 2005

Week Ending	Reported Phishing Sites
10/25/2004	82
11/01/2004	304
11/08/2004	380
11/15/2004	416
11/22/2004	438
11/29/2004	471
12/06/2004	515
12/13/2004	595
12/20/2004	626
12/27/2004	630
01/03/2005	423
01/10/2005	545
01/17/2005	582
01/24/2005	833
01/31/2005	848

Headlines: "18 Arrested In Israeli Probe Of Computer Espionage", "Phishing", "These attacks rely on taking control", "Zombie PCs: Silent, Growing", "'Phishing' e-mails widespread, survey finds", "SPAM", "Spyware"

Footer: - 19 -



Threat Evolution

The evolution of malicious Internet activities primarily motivated by *economic incentives*

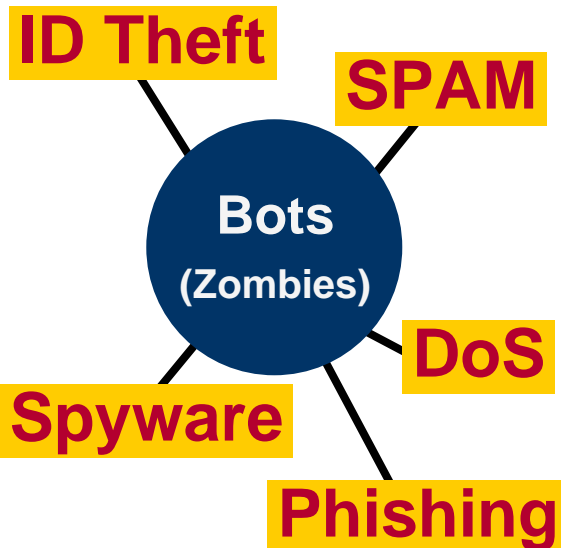
- DoS Extortion
- Identity Theft
- Phishing
- SPAM
- Spyware

Attackers have learned:

1. A compromised system provides anonymity
2. Network of compromised hosts provides a powerful delivery platform
3. A compromised system is more useful alive than dead!



Lurking in the darkness... Bots



How many bots?

- Almost 1 million *bot* infected systems [IEEE04]
- Reports of botnets with 100,000 *Zombies!* [CERT03]
- 1000's of new *bots* each day [Symantec05]

- 21 -



Network Managements & Traffic Engineering

- Inter-domain Traffic Engineering
- Transit / Peering Management
- Backbone Engineering
- Capacity Planning / Provisioning
- Root-cause Analysis / Failure Diagnosis
- Traffic / Routing Anomalies
- Abuse and Misuse

- 22 -



WHY IS IT HARD?

- Requirements of emerging Internet applications
 - VoIP, IPTV, groupware, content delivery & DRM
 - Predictable, reliable and secure services
- Diverse and complex building blocks
 - 10,000 of network elements in a large network
 - Provider edge, customer edge, POP, backbone
- Fragile and vulnerable IP control infrastructure
 - IP is a best-effort service, end-to-end principle
 - Scalability achieved thru highly decentralized protocols/services
- Evolution of security attacks
 - DDoS, worms, botnets, phishing, ...
 - Crumbling network perimeter
- Evolving regulatory and legal issues