CS 194-1 (CS 161) Computer Security

Lecture 3

Network security war stories and networking background

September 6, 2006
Prof. Anthony D. Joseph
http://cs161.org/

Review: Security Evaluation

- Identify the security goals
  - What are we trying to protect?
- Perform a threat assessment
  - What threats does the system need to protect against?
- Do a security analysis
  - Can we envision any feasible attack that would violate the security goals?
  - May be very technical
- Use same process for new system design
  - Easier to ensure security when you know the security goals and threats
  - Security analysis helps refine system design

Goals for Today

- War stories:
  - Telecom industry
  - Internet: Worms and Viruses
- Motivation: Crackers – from prestige to profit
- Lessons to be learned
- Communications Network Taxonomy
  - Packet Networks
- The Internet
  - Transport Layer: UDP/IP, TCP/IP
- Network Service Examples

Many networking slides courtesy of EE 122 (Stoica/Katz)

Phone System Hackers: Phreaks

- Earliest phone hackers?
  - 1870's teenagers
- 1920's (first automated switchboards)
- Mid-1950's deployment of automated direct-dial long distance switches
  - Dialed digits transferred using Single or Multi Frequency signaling

Early 1970's Phreaks: Free LD Calls

- John Draper (AKA "Captain Crunch")
  - Blows "precise" 2600Hz tone into telephone using whistle from a cereal box…
  - Tone indicates caller has hung up → stops billing!
  - Then, whistle digits one-by-one
- "2600" magazine help phreaks make free LD calls
- But, not all systems use SF for dialing…
  - Once trunk thinks call is over, use a "blue box" to dial desired number using MF signaling tones
- Builders included members of Homebrew Computer Club:
  - Steve Jobs (AKA Berkeley Blue)
  - Steve Wozniak (AKA Oak Toebark)
- Red boxes, white boxes, pink boxes, …
  - Variants for pay phones, incoming calls, …

The Game is On

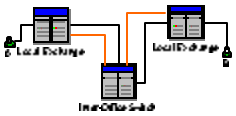
- Cat and mouse game between telcos and phreaks
- Telcos can't add filters to every phone switch
- Telcos monitor maintenance logs for "idle" trunks
- Phreaks switch to emulating coin drop in pay phones
- Telcos add auto-mute function
- Phreaks place operator assisted calls (disables mute)
- Telcos add tone filters to handset mics
- …

The Phone System's Fatal Flaw?

- It uses in-band signaling!
- Information channel used for both voice and signaling
- Knowing "secret" protocol = you control the system
- What's the solution?

Signaling System #6 and #7 (1978-)

- Transmits out-of-band signaling information
  - Completely separate packet data network used to setup, route, and supervise calls
  - Not completely deployed until 1990's for some rural areas (equal access)
- But, false sense of security…
  - Single company that owned entire network
  - No authentication
  - 1980's deregulation – any telco can gain SS7 access and spoof any msgs (think CallerID)…



Phreaking Summary

- In-band signaling enabled phreaks to compromise telephone system integrity
- Moving signaling out-of-band provides added security
  - But, what's out-of-band for wireless?
    - » Think, analog cellular…
    - » Need strong crypto – authentication, encryption
- New economic models mean new threats
  - Not one big happy family, but bitter rivals

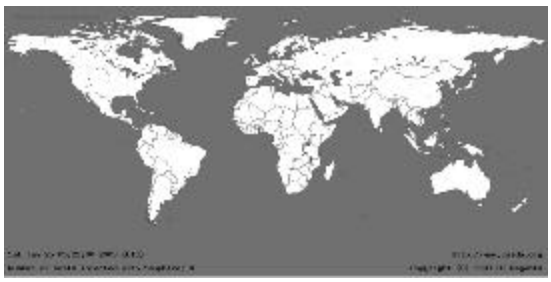
Internet Worms

- Self-replicating, self-propagating code and data
- Use network to find potential victims
- Typically exploit vulnerabilities in an application running on a machine or the machine's operating system to gain a foothold
- Then search the network for new victims

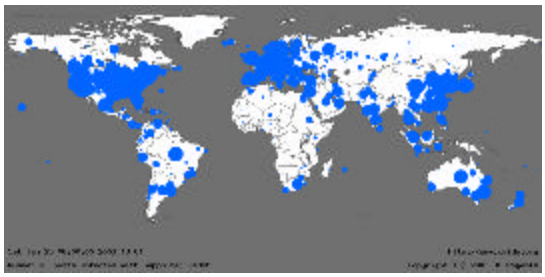
Sapphire (AKA Slammer) Worm

- January 25, 2003
- Fastest computer worm in history
  - Used MS SQL Server buffer overflow vulnerability
  - Doubled in size every 8.5 seconds, 55M scans/sec
  - Infected >90% of vulnerable hosts within 10 mins
  - Infected at least 75,000 hosts
  - Caused network outages, canceled airline flights, elections problems, interrupted E911 service, and caused ATM failures

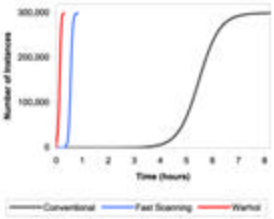
Before Sapphire



After Sapphire



Worm Propagation Behavior



- More efficient scanning finds victims faster (< 1hr)
- Even faster propagation is possible if you cheat
  - Wasted effort scanning non-existent or non-vulnerable hosts
  - Warhol: seed worm with a "hit list" of vulnerable hosts (15 mins)

Administrivia

- Your 3 late days can only be used for projects
  - Not homeworks
- My office hours: Mon/Tue 3-4pm
  - No office hours next week
- Final exam conflict solution is in the works
  - More details on Monday

Internet Viruses

- Self-replicating code and data
- Typically requires human interaction before exploiting an application vulnerability
  - Running an e-mail attachment
  - Clicking on a link in an e-mail
  - Inserting/connecting "infected" media to a PC
- Then search for files to infect or sends out e-mail with an infected file

LoveLetter Virus (May 2000)

- E-mail message with VBScript (simplified Visual Basic)
- Relies on Windows Scripting Host
  - Enabled by default in Win98/2000
- User clicks on attachment
  - ➔ infected!

What LoveLetter Does

- E-mails itself to everyone in Outlook address book
  - Also everyone in any IRC channels you visit using mIRC
- Replaces files with extensions with a copy of itself
  - vbs, vbe, js, jse, css, wsh, sct, hta, jpg, jpeg, mp3, mp2
- Searches all mapped and network drives
- Attempts to download a file called WIN-BUGSFIX.exe
  - Password cracking program
  - Finds as many passwords as it can from your machine/network and e-mails them to the virus' author in the Phillipines
- Tries to set the user's Internet Explorer start page to a Web site registered in Quezon, Philippines

LoveLetter's Impact

- Approx 60 – 80% of US companies infected by the "ILOVEYOU" virus
- Several US gov. agencies and the Senate were hit
- > 100,000 servers in Europe
- Substantial lost data from replacement of files with virus code
  - Backups anyone?
- Could have been worse – not all viruses require opening of attachments…

Worm/Virus Summary

- Worms are a critical threat
  - More than 100 companies, including Financial Times, ABCNews and CNN, were hit by the Zotob Windows 2000 worm in August 2005
- Viruses are a critical threat
  - FBI survey of 269 companies in 2004 found that viruses caused ~$55 million in damages
  - DIY toolkits proliferate on Internet
- We'll revisit worms and viruses in more detail later in the semester

Cracker Evolution

- Cracker = malicious hacker
- John Vranesevich's taxonomy:
  - Communal hacker: prestige, like graffiti artist
  - Technological hacker: exploits defects to force advancements in sw/hw development
  - Political hacker: targets press/govn't
  - Economical hacker: fraud for personal gain
  - Government hacker: terrorists?

Cracker Profile

- 1990's: Internet spreads around the world
  - Crackers proliferate in Eastern Europe
- FBI Profiles (circa 1999)
  - Nerd, teen whiz kid, anti-social underachiever, social guru
- Later survey
  - Avg age 16 – 19, 90% male, 70% live in US
  - Spend avg 57 hrs/week online, 98% believe won't be caught
- Most motivated by prestige
  - Finding bugs, mass infections, …

Changing Incentives (2001-)

- Cracking for profit, including organized crime
  - 50% of viruses still contain names of crackers or groups that created them
- Goal: create massive botnets
  - 10-50,000+ machines infected
  - Each machine sets up encrypted, authenticated connection to central point (IRC server) and waits for commands
- Rented for pennies per machine per hour for:
  - Overloading/attacking websites, pay-per-click scams, sending spam/phishing e-mail, or hosting phishing websites…

Example: Zotob Virus (August 2005)

- Financially-driven motive
- Process:
  - Infected machines and set IE security to low (enables pop-up website ads)
  - Revenue from ads that now appear
  - User may remove virus, but IE settings will likely remain set to low
  - Continued revenue from ads…
- Creators arrested August 25th
  - Farid Essebar was arrested in Morocco and Atilla Ekici was detained by police in Turkey
- 16 others arrested in Turkey
  - Used variants of Zotob for credit card fraud

Computer Networks

- Need to understand computer networks to understand vulnerabilities and potential attacks
- What are the vulnerabilities of networks?
- How do crackers leverage networks to attack computers?
- How does the network "limit" crackers?
- How do crackers exploit network design and services?
- How can we harden networks, computers, and services?

What is a Communication Network? (End-system Centric View)

- Network offers one basic service: move info
  - Bird, fire, runner, telegraph, phone, Internet, …
- What distinguish different types of networks?
  - The services they provide, security, …
- What distinguish the services?
  - Latency, Bandwidth, Loss rate, size, Service interface (how to invoke the service?)
  - Others
    - » Reliability, unicast vs. multicast, real-time...
- What are the security issues?
  - Authentication, privacy, anonymity, integrity, …

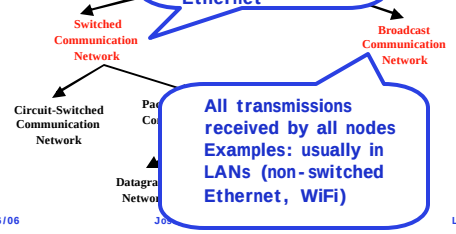
What is a Communication Network? (Infrastructure Centric View)

- Communication medium: electron, photon
- Network components:
  - Links – carry bits from 1 place to 1 or more: fiber, copper, wireless,…
  - Interfaces – attach devices to links
  - Switches/routers – interconnect links: electronic/optic, crossbar/Banyan
  - Hosts – comm. endpoints: PCs, PDAs, cell phones, toasters
- Protocols – rules governing comm. between nodes
  - TCP/IP, ATM, MPLS, SONET, Ethernet, X.25
- Applications: Web browser, X Windows, FTP, ...
- Low-level security issues:
  - Authentication, privacy, integrity, …

Taxonomy of Communication Networks

- Communicat… d based on the way information

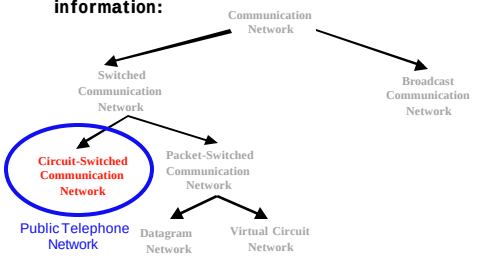
Info sent to subset of nodes Examples: WANs (Telephony Network, Internet), switched Ethernet



All transmissions received by all nodes Examples: usually in LANs (non-switched Ethernet, WiFi)

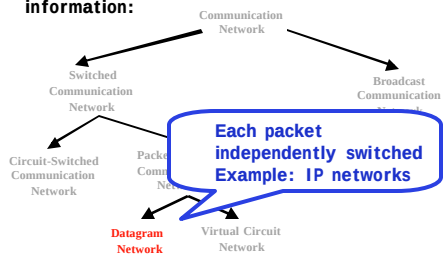
Taxonomy of Communication Networks

- Communication networks can be classified based on the way in which the nodes exchange information:



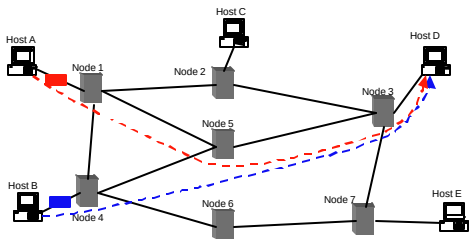
Taxonomy of Communication Networks

- Communication networks can be classified based on the way in which the nodes exchange information:



Each packet independently switched Example: IP networks

Datagram Packet Switching

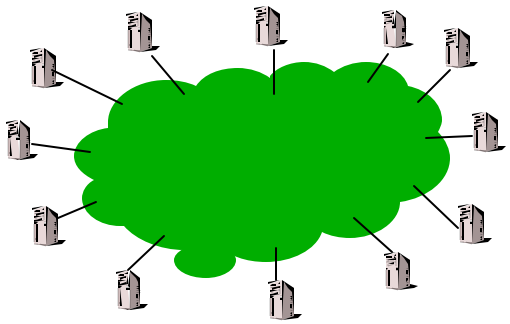


BREAK

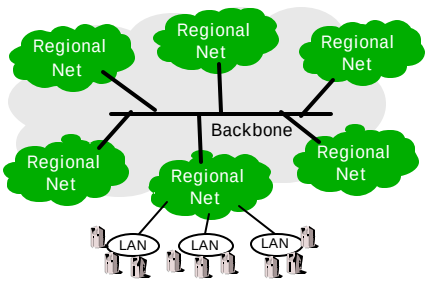
The Internet

- Global scale, general purpose, public, heterogeneous-technologies,computer network
- Internet Protocol: Open standard
  - Internet Engineering Task Force (IETF)
  - Technical basis for other nets: Intranets
- History of the Internet
  - 68-70's: started as a *research project*, 56 kbps, initially 4 nodes (UCLA, UCSB, SRI, Utah)
  - 85-86: NSF builds NSFNET as backbone, links 6 Supercomputer centers, 1.5 Mbps, 10,000 nodes
  - 94: NSF backbone dismantled, multiple private backbones; Introduction of Commercial Internet
  - Today: backbones run at 10 Gbps, close to 320M computers in 150 countries

Network "Cloud"

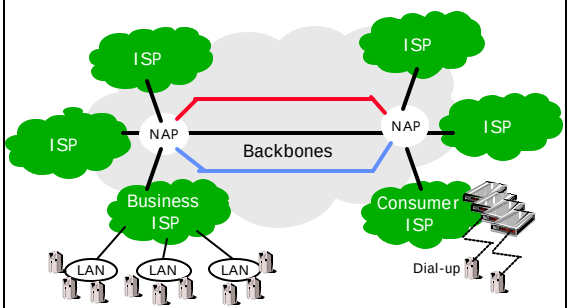


Regional Nets + Backbone



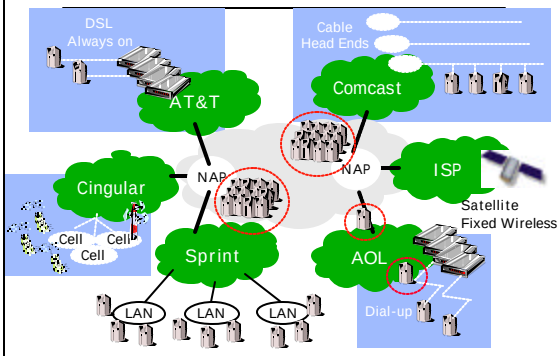
LAN: Local Area Network

Backbones + NAPs + ISPs



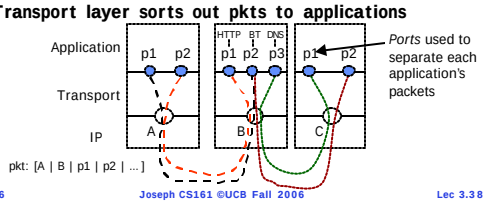
ISP: Internet Service Provider
NAP: Network Access Point

Access Networks + Nodes In the Core

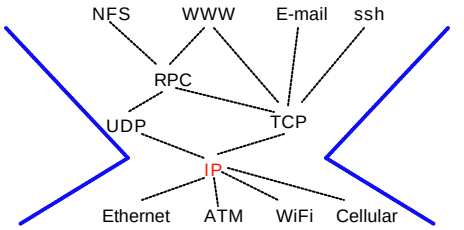


Internet Service

- "Best-Effort" service "between friends"
  - No guarantees about packet delivery or authenticity
  - Hosts must handle loss, delay, reordering, duplication
- Why not guarantee no loss and low delay?
- IP packets are addressed to a host (67.114.133.15)
  - Network routes packets to address
- Transport layer sorts out pkts to applications



Internet Protocol Layers



- Many different network technologies
- IP was invented to glue them together
  - n translations, not n x n!
  - Minimal requirements (datagram)
  - "IP over everything"

Services Provided over the Internet

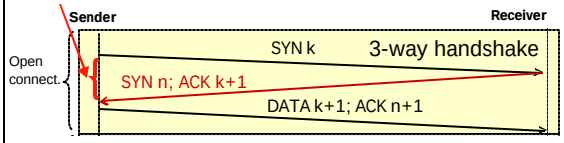
- Shared access to computing resources
  - telnet (1970's), ssh (1990's)
- Shared access to data/files
  - FTP, NFS, AFS (1980's), CIFS (late 90's)
- Communication medium over which people interact
  - email (1980's), on-line chat rooms, instant messaging (1990's)
  - audio, video, Voice-over-IP (1990's, early 00's)
    - » replacing telephone network?
- Medium for information dissemination
  - USENET (1980's)
  - WWW (1990's)
    - » replacing newspaper, magazine?
  - Audio, video (late 90's, early 00's)
    - » replacing radio, TV?
  - File sharing (late 90's, early 00's)

Common Transport Protocols

- User Datagram Protocol (UDP)
  - Minimalist transport protocol
  - Same best-effort service model as IP
  - Messages up to 64KB
  - "Fire and Forget"
  - Provides multiplexing/demultiplexing to IP
  - Does not provide flow and congestion control
  - Application examples: video/audio streaming, VoIP
- Transmission Control Protocol (TCP)
  - Reliable, in-order, and at most once delivery
  - Messages can be of arbitrary length
  - Provides multiplexing/demultiplexing to IP
  - Provides congestion control and avoidance
  - Application examples: file transfer, chat, P2P

TCP Timing Diagram

1 RTT delay – limits rate of new connections

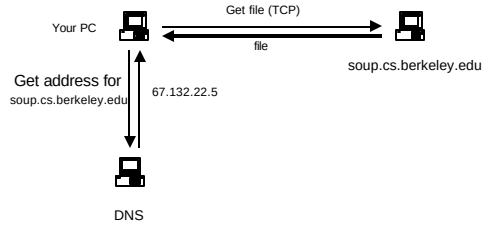


Example Svc: Domain Name Service (DNS)

- Humans/applications use machine names
  - e.g., www.cs.berkeley.edu
- Network (IP) uses IP addresses
  - e.g., 67.114.112.23
- DNS translates between the two
  - An overlay service in its own right
  - Global distribution of name-to-IP address mappings—a kind of content distribution system as well
  - Unsung hero of the Internet

Ex: File Transfer (FTP, SCP, etc.)

Get file from soup.cs.berkeley.edu



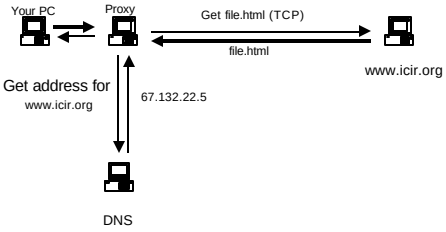
Email

Email message exchange is similar to previous example, except

- Exchange is between mail servers
- DNS gives the name of mail server for a domain

Web

Get www.icir.org/file.html



Summary

- If you build it, someone will try to crack it
  - And probably will succeed…
- Changing incentives from prestige to profit increases the worm/virus threat
- Internet designed in a friendly era/environ
  - What's wrong with: https://www.ebay.com/ ?
- Internet relies on "in-band" signaling
  - Makes authentication hard
- Using TCP limits connection rate
  - Slows worm/virus propagation
  - But UDP allows fast "fire and forget"…