Network Security War Stories

CS 161/194-1
Anthony D. Joseph
September 7, 2005

About Me

- Joined faculty in 1998
  - MIT SB, MS, PhD
- Contact info
  - adj @ cs.berkeley.edu
  - http://www.cs.berkeley.edu/~adj/
- Research Areas:
  - Mobile/wireless computing, network security, and security testbeds
- Office hours: 675 Soda Hall, M/Tu 1-2pm

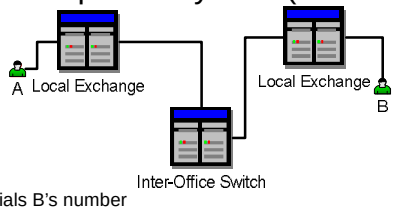
Outline

- War stories from the Telecom industry
- War stories from the Internet: Worms and Viruses
- Crackers: from prestige to profit
- Lessons to be learned

Phone System Hackers: Phreaks

- Earliest phone hackers?
- 1870's teenagers
- 1920's (first automated switchboards)
- Mid-1950's saw deployment of automated direct-dial long distance switches

US Telephone System (mid 1950's)



- A dials B's number
- Exchange collects digits, assigns inter-office trunk, and transfers digits using Single or Multi Frequency signaling
- Inter-office switch routes call to local exchange
- Local exchange rings B's phone

Early 1970's Phreaks

- John Draper (AKA "Captain Crunch")
  - Makes free long-distance calls by blowing a "precise" tone (2600Hz) into a telephone using a 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 long-distance calls
- But, not all systems use SF for dialing…

Blue Boxes: Free Long Distance Calls

- Once trunk thinks call is over, use a "blue box" to dial desired number
  - Emits MF signaling tones
- Builders included members of California's 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, …

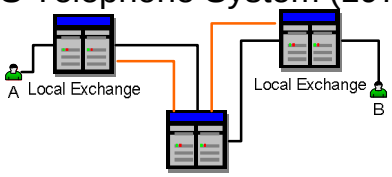
The Game is On

- 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?
  - In-band signaling!
  - Information channel used for both voice and signaling
  - Knowing "secret" protocol = you control the system

Signaling System #7

- "Ma Bell" deployed Signaling System #6 in late 1970's and SS#7 in 1980's
  - Uses Common Channel Signaling (CCS) to transmit 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
- False sense of security…
  - Single company that owned entire network
  - SS7 has no internal authentication or security

US Telephone System (1978-)



- A dials B's number
- Exchange collects digits and uses SS7 to query B's exchange and assign all inter-office trunks
- Local exchange rings B's phone
- SS7 monitors call and tears down trunks when either end hangs up

Cellular Telephony Phreaks

- Analog cellular systems deployed in the 1970's used in-band signaling
- Suffered same fraud problems as with fixed phones
  - Very easy over-the-air collection of "secret" identifiers
  - "Cloned" phones could make unlimited calls
- Not (mostly) solved until the deployment of digital 2nd generation systems in the 1990's

Today's Phone System Threats

- Deregulation in 1980's
  - Anyone can become a Competitive Local ExChange (CLEC) provider and get SS7 access
  - No authentication → can spoof any messages (think CallerID)…
- PC modem redirections (1999-)
  - Surf "free" gaming/porn site and download "playing/viewing sw
  - Software mutes speaker, hangs up modem, dials Albania
  - Charged $7/min until you turn off PC (repeats when turned on)
  - Telco "forced" to charge you because of international tariffs
- PBX hacking for free long-distance
  - Default voicemail configurations often allow outbound dialing for convenience
  - 1-800 social engineering ("Please connect me to x9011…")

Phreaking Summary

- In-band signaling enabled phreaks to compromise telephone system integrity
- Moving signaling out-of-band provides added security
- New economic models mean new threats
  - Not one big happy family, but bitter rivals
- End nodes are vulnerable
  - Beware of default configurations!
- Social engineering of network/end nodes

Outline

- War stories from the Telecom industry
- War stories from the Internet: Worms and Viruses
- Crackers: from prestige to profit
- Lessons to be learned

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

Morris Worm

- Written by Robert Morris while a Cornell graduate student (Nov 2-4, 1988)
  - Exploited debug mode bug in `sendmail`
  - Exploited bugs in `finger`, `rsh`, and `rexec`
  - Exploited weak passwords
- Infected DEC VAX (BSD) and Sun machines
  - 99 lines of C and >3200 lines of C library code

Morris Worm Behavior

- Bug in `finger` server
  - Allows code download and execution in place of a finger request
- `sendmail` server had debugging enabled by default
  - Allowed execution of a command interpreter and downloading of code
- Password guessing (dictionary attack)
  - Used `rexec` and `rsh` remote command interpreter services to attack hosts that share that account
- Next steps:
  - Copy over, compile and execute bootstrap
  - Bootstrap connects to local worm and copies over other files
  - Creates new remote worm and tries to propagate again

Morris Worm

- Network operators and FBI tracked down author
- First felony conviction under 1986 Computer Fraud and Abuse Act
- After appeals, was sentenced to:
  - 3 years probation
  - 400 hours of community service
  - Fine of more than $10,000
- Now a professor at MIT…

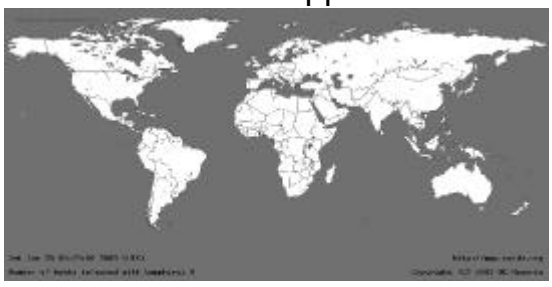
Internet Worms: Zero-Day Exploits

- Morris worm infected a small number of hosts in a few days (several thousand?)
  - But, Internet only had ~60,000 computers!
- What about today? ~320M computers
- Theoretical "zero-day" exploit worm
  - Rapidly propagating worm that exploits a common Windows vulnerability on the day it is exposed
  - Propagates faster than human intervention, infecting all vulnerable machines in minutes

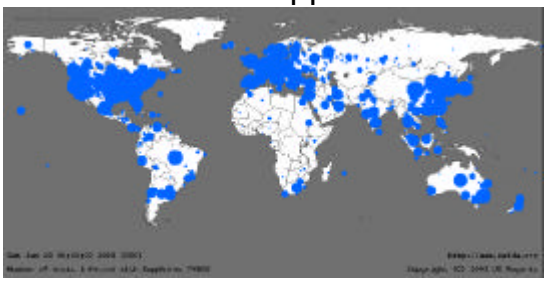
Sapphire (AKA Slammer) Worm

- 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

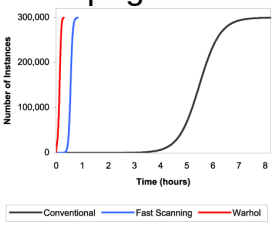
Before Sapphire



After Sapphire



Worm Propagation Behavior



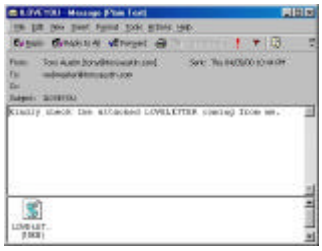
- More efficient scanning finds victims faster (< 1hr)
- Even faster propagation is possible if you cheat
  - Wasted effort scanning non-existent or non-vulnerable hosts
  - Warhol: seed worm with a "hit list" of vulnerable hosts (15 mins)

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 Windows 98/2000 installations
- 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 drives, including networked 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

- Default configurations are still a problem
  - Default passwords, services, …
- Worms are still 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 still a critical threat
  - FBI survey of 269 companies in 2004 found that viruses caused ~$55 million in damages
  - DIY toolkits proliferate on Internet

Outline

- War stories from the Telecom industry
- War stories from the Internet: Worms and Viruses
- Crackers: from prestige to profit
- Lessons to be learned

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

- 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, …

Evolution

- 1990's: Internet spreads around the world
  - Crackers proliferate in Eastern Europe
- Early 2000's Do-It-Yourself toolkits
  - Select propagation, infection, and payload on website for customized virus/worm
- 2001-
  - Profit motivation: very lucrative incentive!

Evolution (Circa 2001-)

- Cracking for profit, including organized crime
  - But, 50% of viruses still contain the names of crackers or the groups that are supposedly behind viruses
- 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…

Zotab Virus Goal (August 2005)

- Infect 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…

Some Observations/Lessons

- We still rely on "in-band" signaling in the Internet
  - Makes authentication hard
  - What's wrong with: https://www.ebay.com/ ?
- Bad default, "out-of-the-box" software configs
  - Wireless access point passwords?
- We'll click on any e-mail we get
  - This is why spam continues to grow…