


CS514: Intermediate Course in Computer Systems

Lecture 20: March 5, 2003

*Options for blocking Distributed
Denial of Service Attacks in the Net*



Question: What was the largest
Internet “break in” to date?



CS514

- Definition: “break in” means “ability to remotely login”
- Answer: Freeman and Mann describe this in their book @Large: The Strange Story of the World’s Biggest Internet Invasion. A teenager in Portland broke into thousands of machines!



Distributed Denial of Service Attacks

CS514

- How are they typically launched?
- Is there any simple pattern that characterizes the traffic?
- What can be done to defend against them
 - In a server?
 - At the firewall?
 - In the network itself?



DDoS Attacks: Many flavors

CS514

- There is no single approach!
- But there is a broad pattern
 1. Attacker gains control over multiple workstations
 - Perhaps by manually installing something on them, e.g. at a University
 - Perhaps using a virus or worm “exploit”
 - Surprisingly often, by finding lists of machines/logins on hacker web sites



Steps in DDoS attack

CS514

2. Attacker loads some predesigned software onto those nodes
 - The code could exploit some form of O/S weakness
 - Or it could just be a standard program
3. The code rests dormant waiting for a launch signal and target
 - Signal could come via email, or some other message. Or attack code could be designed to poll for instructions



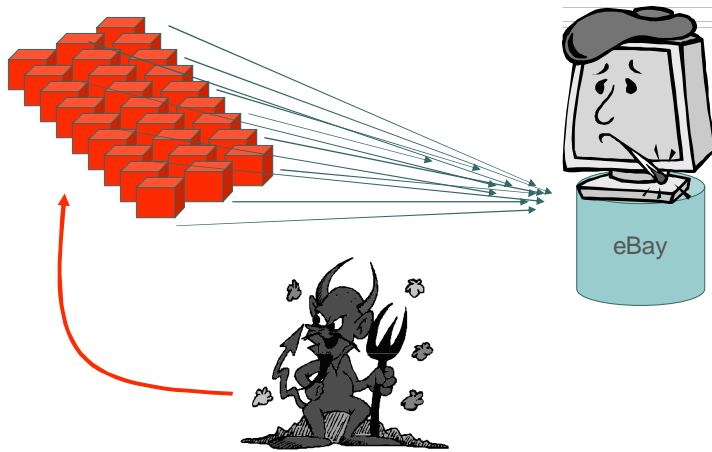
The big day arrives!

CS514

4. Hacker gets annoyed with some site
 - E.g. decides to take eBay down
5. Figures out IP address of the site and hands it/them to attack agents
 - By now, some may have been neutralized
6. The agents send a high volume of messages to the designated target
7. Target, overwhelmed, wastes tons of CPU or other resources and grinds to a halt

DDoS on the big day

CS514



Some common variants

CS514

- Worm or Virus may effectively mount a DDoS attack simply trying to infect lots of machine
 - Example: recent Worm infection of MS SQL Server (exploited a buffer overflow)
 - Here, load of infection attempts was what overwhelmed the network
- Or could try and knock out a shared critical resource
 - Example: Attack on root nodes of DNS



Side comment

CS514

- In fact, these are all different cases
 - The attacker who mounts an attack by commandeering other machines
 - The attacker who breaks into the target
 - The worm, which just tries to “get everywhere”
 - The virus, which normally does actual damage, theft of materials, etc
 - The insider threat
- Today, focus on the first “DDoS” scenario



Defending against attack

CS514

- Unchanging content is more easily defended, often right “at the server”
 - E.g. CNN.com or NYTimes.com
 - Here the data is actually hosted on large-scale web farms
 - Many IP addresses involved... too many to attack!
 - Attacker rarely has resources to go after more than two or three IP addresses at one time
 - Philosophy here is divide (many times) to defend!
- Server can also become paranoid when resource levels dip unexpectedly



Defending against attack

CS514

- Much harder to defend if
 - Attack exploits a legitimate category of requests (e.g. TCP SYN)
 - Attacker masks source IP address
 - So you can't just filter all such requests
 - Defender doesn't have option of spreading out
 - Volume is already high near firewall



Defender may have plenty of time to work on the problem...

CS514

- DDoS attacks sometimes go on for days or weeks!
 - Attacks can come and go and come back again!
 - Recent estimate: there are several DDoS attacks underway, per day, every day. And numbers are growing
- By some estimates, DDoS attacks are growing at an *exponential rate!*



Defending in the ISP

CS514

- Your friendly ISP is under attack too, if you are under attack
- And they may not be happy with all that traffic on their links
- Current trends favor
 - ISP-level firewalls
 - Close dialog between ISP and client
 - Companies like Arbor Networks and Mazur are in this space



Examples of ISP-level options?

CS514

- ISP can try to block incoming traffic at borders
 - Try to detect spoofed source address
 - E.g. says “rns.seoul.kr” but there are no current routes from korea via that gateway
 - This needs to be done semi-manually
 - After all, routes can change dramatically!
 - Studies have shown that > 80% of spoofed-source traffic is easily detectable



More ISP opportunities

CS514

- ISP can watch for unusual packet statistics
 - E.g. high rates of TCP SYN packets
 - But doing check is potentially very costly
- ISP wants the tools to enable such a mechanism without needing to do it all the time



Broad objective

CS514

- ISP ideally wants
 - Firewall at the periphery of the network
 - Ability to gather statistics during “peacetime”
 - Ability to compare “wartime” statistics with peacetime data
 - Help formulating a firewall policy that will catch the offending packets but let the normal stuff get through



More options

CS514

- ISP can help by changing the IP address of the attacked site
 - But DNS updates may be slow to reach real customer sites
 - Meanwhile, eBay will be offline
- Attackers know about the DNS too!
 - An attacker could insert corrupt DNS updates
 - Attacker's DNS itself could be compromised
 - DNSSec reduces risk of this
 - But Linux boxes (open source) increase risk!



VPN option

CS514

- Paul discussed *virtual private network* idea several times
- The basic idea works like this
 1. Distribute a shared key to the computers in some application
 2. They sign (or encrypt) communication with one-another
 3. On receipt, reject a packet if it isn't correctly signed



VPN variants

CS514

- VPN with membership information could accomplish this without shared keys
 - Security might be better
 - But costs would be higher and tracking membership can be tricky
- Or can use some form of login, at which time computer is given the key of the day
 - Kerberos works this way
 - Advantage is that you can use “weaker” keys



Could eBay use VPN ideas?

CS514

- Could use secure HTTP as a form of VPN...
 - In practice, eBay might find it too slow
- Also would struggle with
 - Fresh keys, in which case a user unable to get one is unable to use VPN
 - Long-lived keys, but these could be easier to compromise when intruder hacks a machine
- Some people think the long term future of the Internet will look like lots of VPNs



The future of the Internet?

CS514

- It will steadily grow faster
 - And larger
 - But not safer
- DDoS attacks will remain a big problem
- And there isn't much hope that the network will soon start to guarantee any form of reliability!



Critical Infrastructure

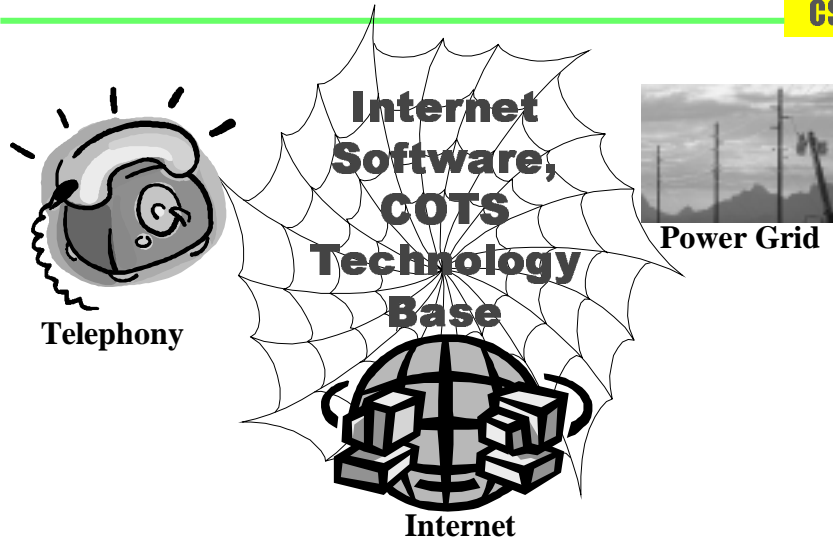
Rapidly Expanding Web of Dependency

CS514

- Massive rollout underway
 - Control of restructured power grid
 - New medical information systems link hospital to other providers, reach right into the home
 - Telephony infrastructure
 - Air traffic control systems
 - Financial systems: eMoney replaces cash!
 - Disaster response and coordination
- Future military will be extremely dependent on information resources and solutions

● ● ● | Tangled Interdependencies

CS514



● ● ● | Multiple Concerns

CS514

Infrastructure industries have been dangerously naïve about challenges of using Internet and computing technologies in critical ways

- Nationally critical information systems poorly protected, fragile, easily disrupted
 - Stems from pervasive use of COTS components
 - Vendors poorly motivated to address the issue
- Yet academic research is having little impact
 - No sense of “excitement” or importance
 - Few significant technology transition successes



Security: Often mistaken for the whole story

CS514

- Even today, most CIP work emphasizes security and denial of service attacks
- But critical applications must also work
 - *Correctly*
 - *When and where required*
 - *Even when components fail or are overloaded*
 - *Even when the network size grows or the application itself is used on a large scale*
 - *Even when the network is disrupted by failures*



Concrete Examples of Threats?

CS514

- Power system restructuring
 - Requires new generation of technology for buying/selling power, implementing load-following power contracts, preventing cascaded failures
 - Industry has no idea how to build this.
- California crisis only masks technical problems!
 - Although people *have* noticed that we don't know how to monitor for fairness...
 - ... they *haven't* noticed that we have no idea how to control a restructured, competitive power grid!



Concrete Examples of Threats?

CS514

- Telemedicine, “CHINs” coming soon
 - Patients want home care, insurance companies want online filing, hospitals want e-records
- Some components are already in use!
 - But security is totally inadequate
 - Reliability isn’t adequate for uses such as remote control of an insulin pump, remote monitoring, or computer-assisted surgery
 - Faster networks promote increased use without addressing either limitation



Concrete Examples of Threats?

CS514

- Vision: decision maker has information anytime, anywhere, at touch of a button
 - Scale will be orders of magnitude beyond anything ever done with Internet technologies
 - Air Force “JBI”, Navy “NCW”, Army “FCS”
- The military is betting we’ll have these
 - And that it can be done off-the-shelf
 - But the Internet just can’t do it
 - Commercial products are totally inadequate
- Situation recalls FAA’s AAS fiasco (lost \$6B!)

Vendor Perspective?

CS514

- Main focus is security... but
 - *"You have zero privacy anyway. Get over it."*
Scott McNealy, CEO Sun Microsystems; 1/99
 - Bill Gates recently suggested that MSFT needs to improve, but didn't point to Internet issues.
- Internet technology is adequate for the most commercially lucrative Web functions
 - But inadequate for CIP requirements
 - Issue is that market is the main driver for product evolution, and market for critical solutions is small

The real story?

CS514

- A pervasive need for secure, reliable, scalable communication
- But crippled by features of the Internet
 - Fundamentally weak on security
 - TCP features compromise any kind of reliability that involves timing guarantees
 - Depends on lines leased from an even less secure telephone network



Some legal ideas

CS514

- Could make it illegal to
 - Fake a return address on an email
 - Spoof a source address in an IP packet
 - Knowingly assist a sender of spam or DDoS attack data
- Could even require senders to mark unsolicited packets/email as such



Some *bad* legal ideas

CS514

- Recent legislation proposed that playing any role of any kind in moving purloined bytes would be illegal
- Why is this a bad idea?



Some *bad* legal ideas

CS514


- Recent legislation proposed that playing any role of any kind in moving purloined bytes would be illegal
- Why is this a bad idea?
 - How can the disk-driver tell?
 - Suppose a big image is fragmented into many small pieces (like TCP/IP). How can Internet recognize bad content
 - Suppose that "WhiteHouse.gif" is really a compressed copy of a Nora Jones song?
 - What if a researcher developing a new operating system initially omits the functionality?
 - What if a high-resolution digital image happens to *include* a picture of some object on which rights are held, such as a famous picture?




Ethics of hacking

CS514

- If I leave my door wide open, should it be illegal to look inside from outside in the street?
- Suppose someone sends a letter pointing out that my windows lack curtains and my doors aren't locked. Is it *now* my fault if intruders wander in?
- Should our bias view the Internet as a friendly, open space or a commercial one?



Should eBay have a right to do business on the Internet?



- Is everything permissible?
 - View of Internet as a giant intellectual commons welcoming all forms of activity and discourse
 - Why should Microsoft be the only software vendor?



Converse side



- In what ways are hackers different from terrorists?
 - What about the black-hat/gray-hat/white-hat distinction?
- Could there be cases where hacking would be a socially good thing?
 - What if a musical artist attacks a Napster-like site stealing her work?
 - How about disrupting Neo-Nazi sites?