A Brief History of the World
Network Security

Lecture 10
Why and Who Attack Networks?

- Challenge: Hackers
- Money: Espionage
- Money: Organized Crime
- Ideology: Hacktivists/Cyberterrorists
- Revenge: Insiders
Challenge: Hackers

- Examples
  - Cult of the Dead Cow: demonstrate weaknesses to strengthen security

- Details
  - Few discover new vulnerabilities
  - Most simply try known problems on new systems
  - Motivated by thrill of access and status
  - Hacking community a strong meritocracy
  - Status is determined by level of competence
Money : Espionage

- Examples
  - 2002: Princeton snoops on admission decisions at Yale
  - Obtain information on competing companies

- Details
  - Intellectual property
  - CSI/FBI survey in 2005
    - IP loss estimated to $31 million
    - $350,000 per incident
Money : Organized Crime

- Examples
  - October 2004: Shadowcrest
    - 28 people 7 countries (8 US states)
    - 1.5 million stolen credit card and bank numbers
  - January 2006: Jeanson James Ancheta
    - Infected 400,000 computers and rented them for use

- Details
  - Criminal hackers usually have specific targets
  - Once penetrated act quickly and get out
Ideology: Hacktivism/Cyberterror

- Example
  - Code Red worm

- Details:
  - Hacktivism
    - Web site defacements/parodies, redirects, denial-of-service attacks, information theft, ...
  - Cyberterrorism
    - Use Internet based attacks in terrorist activities
    - Acts of deliberate, large-scale disruption of computer networks
Revenge: Insiders

Examples

- Terry Childs – sysadmin in San Francisco
  - Changed passwd for FiberWAN – traffic for city govt
  - 4 years of prison

- Roger Duronio – employee at UBS PainWebber
  - Placed logic bomb took down 2000 computers
  - Company couldn’t trade for weeks, $3.1 million losses

- Wikileaks, Snowden, Bradley/Chelsey Manning
  - Access to DoD’s Secret Internet Protocol Router Network and passed it to Wikileaks
  - ~750,000 classified, or unclassified but sensitive, military and diplomatic documents
Revenge: Insiders (cont’d)

- Details
  - Difficult to detect and prevent
  - Employees have access & systems knowledge

- Insiders can
  - Capture data and give it to new employer/competitor
  - Place trojan horses and trapdoors to allow future access
  - Place logic bombs to harm company at a later time
Intrusion Techniques

- Reconnaissance
- Eavesdropping and Wiretapping
- Impersonation
- Message confidentiality threats
- Web site vulnerabilities
- DOS and DDOS
Reconnaissance

- Port scan
  - For a given address find which ports respond
- OS and application fingerprinting
  - Certain features and lack thereof can give away OS/apps manufacturer and versions
  - Nmap: guess of the OS and version, what services are offered
Reconnaissance (cont’d)

- Social engineering
  - Use social skills
  - Pretend to be someone else and ask for details
  - Run ipconfig - all

- Intelligence
  - Dumpster diving
  - Eavesdropping
  - Blackmail

- Bulletin boards and Chats
Social Problems

- People can be just as dangerous as unprotected computer systems
- People can be manipulated to give up valuable information
  - Bribed, threatened, harmed, tortured
Social Engineering

- Pretexting
- Phishing
- Baiting
- Quid Pro Quo
- Tailgating
Pretexting

- **Example 1:**
  - “Hi, I’m your AT&T rep, I’m stuck on a pole. I need you to punch a bunch of buttons for me”
Pretexting

- Example 2: Call in the middle of the night
  - “Have you been calling Egypt for the last six hours?”
  - “No”
  - “Well, we have a call that’s actually active right now, it’s on your calling card and it’s to Egypt and as a matter of fact, you’ve got about $2000 worth of charges on your card and ... read off your AT&T card number and PIN and then I’ll get rid of the charge for you”
Phishing

- **E-mail**
  - Appears to come from a legitimate business
  - Requests "verification" of information
    - Home address
    - Password, PIN, SSN, credit card number
  - Dire consequences if not provided
  - Contains a link to a fraudulent web page that seems legitimate—with company logos and content
Baiting

- Physical world Trojan horse/Virus
- Attacker leaves a malware infected CD, flash drive in public space
- Write something appealing on front
  - "Executive Salary Summary Q1 2016"
- Exploit finder curiosity
Intrusion Techniques

- Reconnaissance
- Eavesdropping and Wiretapping
- Impersonation
- Message confidentiality threats
- Web site vulnerabilities
- DOS and DDOS
Wiretapping

- Cable
  - *Packet sniffers*
  - Inductance/radiation emitted, Cutting the cable
- Satellite
  - Easily intercepted over large areas
- Optical fiber
  - Harder to wiretap
  - Repeaters, splices and taps are vulnerable
- Wireless
  - Easy to intercept, steal service and disrupt/interfere
Packet Sniffing

- Recall how Ethernet works ...
- When someone wants to send a packet to someone else
  - Put the bits on the wire with the destination MAC address
- Other hosts are listening on the wire to detect for collisions ...
- It couldn’t get any easier to figure out what data is being transmitted over the network!
Packet Sniffing (cont’d)

- This works for wireless too!
  - In fact, it works for any broadcast-based medium
- What kind of data is of interest
- Answer:
  - Anything in plain text
  - *Passwords are the most popular*
Intrusion Techniques

- Reconnaissance
- Eavesdropping and Wiretapping
- Impersonation
- Message confidentiality threats
- Web site vulnerabilities
- DOS and DDOS
Impersonation

- Access the system by pretending to be an authenticated user
  - Password guessing/capture
  - Spoofing
Password Guessing

- Very common attack
- Attacker knows a login (from email/web page etc)
- Attempts to guess password for it
  - Defaults, short passwords, common word searches
  - User info (variations on names, birthday, phone, common words/interests)
    - Exhaustively searching all possible passwords
- Check by login or against stolen password file
- Success depends on password chosen by user
  - *Surveys show many users choose poorly*
Password Capture

- Watch over shoulder as password is entered
- Use a trojan program to collect
- Monitor an insecure network login
  - E.g. telnet, FTP, web, email
Password Capture using Sniffing

- Monitor an insecure network login
- **Example:** Microsoft LAN Manager
  - Hash of passwd was transmitted, not passwd
  - At most 14 characters
  - *Split in blocks of 7 chars, each with a different hash!*
  - If 7 chars or less, second hash is of nulls
  - If 8 chars, second hash is of single char
  - Vulnerable to brute force attacks
Password Collection Protection

- SSH, not Telnet
  - Many people still use Telnet and send their password in the clear (use PuTTY instead!)
  - Now that I have told you this, please do not exploit this information
  - Packet sniffing is, by the way, prohibited by Computing Services
- HTTP over SSL
  - Especially when making purchases with credit cards!
- SFTP, not FTP
  - Unless you really don’t care about the password or data
- IPSec
  - Provides network-layer confidentiality
Spoofing

- Pretend to be someone else
  - Masquerade
  - Session Hijacking
  - Man-In-the-Middle-Attack
Masquerade

- One host pretends to be someone else
- Easy to confuse names or mistype
- Example: BlueBank vs Blue-Bank (masquerade)
  1. Blue-Bank copies web page of BlueBank
  2. Attracts customers of BlueBank
     - Phishing, Ads, Spam, etc ...
  3. Ask customer to enter account name and passwd
  4. Optional: redirect connection to BlueBank
- Try https://www.sonicwall.com/phishing/ to test your phishing nose
Session Hijack vs. MitMA

- *Intercept and carry on session begun by another entity*

- **Example:**
  - Administrator uses telnet to login to privileged account
  - Attacker intrudes in the communication and passes commands as if on behalf of admin

- *Man-In-The-Middle Attack*
  - Similar, but...
  - Attacker needs to participate since session start
Intrusion Techniques

- Reconnaissance
- Eavesdropping and Wiretapping
- Impersonation
- Message confidentiality threats
- Web site vulnerabilities
- DOS and DDOS
Message Confidentiality Threats

- **Misdelivery**
  - Mistyping the destination address

- **Exposure**
  - Packets are exposed over wires and in buffers at
    - Switches, gateways, routers, ...

- **Traffic Flow Analysis**
  - The existence of communication may help infer information
Intrusion Techniques

- Reconnaissance
- Eavesdropping and Wiretapping
- Impersonation
- Message confidentiality threats
- Web site vulnerabilities
- DOS and DDOS
Web Site Vulnerabilities

- Anyone has access to the code of a web page
  - Also the order in which pages are accessed
- Example vulnerabilities:
  - Web site defacement
  - Buffer overflows
Web Site Defacement

- Attack on a website that changes the visual appearance of the site

United Nations website 😊
Buffer Overflows

- Work exactly like standard buffer overflows
  - Feed web site program more data than expected
  - Overflow into neighboring code and data
Intrusion Techniques

- Reconnaissance
- Eavesdropping and Wiretapping
- Impersonation
- Message confidentiality threats
- Web site vulnerabilities
- DOS and DDOS
Denial of Service

- Make a network service unusable, usually by overloading the server or network

- Many different kinds of DoS attacks
  - SYN flooding
  - SMURF
  - Distributed attacks
TCP Three Way Handshake

- **SYN**: Client sends a SYN to the server
  - The segment sequence number is a random value $A$

- **SYN-ACK**: Server replies with a SYN-ACK.
  - The acknowledgment number is set to one more than the received sequence number ($A + 1$)
  - The sequence number that the server chooses for the packet is another random number $B$

- **ACK**: Client sends an ACK back to the server.
  - The acknowledgement number is set to one more than the received sequence number $B + 1$
  - The sequence number is set to the received acknowledgement value $A + 1$
SYN Flooding Attack

- Send SYN packets with fake source address
  - Why?
- Server responds with SYN+ACK and keeps state about TCP half-open connection
  - Eventually, server memory exhausted with state
- Fake source address: packets are hard to trace
- Solution: use “SYN cookies”
SYN Cookies

- In response to a SYN, create a special “cookie” for the connection, and forget everything else

- Let:
  - $t = $ timestamp
  - $m = $ maximum segment size (MSS) value that the server would have stored in the SYN queue entry
  - $s = H_K(t, IP_{srv}, port_{srv}, IP_{cli}, port_{cli})$

- SYN Cookie: initial sequence number $B$
  - First 5 bits: $t \mod 32$
  - Next 3 bits: an encoded value representing $m$
  - Final 24 bits: $s \mod$ (some prime of 24 bits)
SYN Cookies

- **ACK**: Client sends an ACK back to the server.
  - The acknowledgement number is set to one more than the received sequence number \( N = B + 1 \)

- The server performs the following operations:
  - Break \( N-1 \) into \( t, m, s \) fields (by length)
  - Check the value \( t \) against the current time to see if the connection is **expired**
  - Compare \( s = H_K(t, IP_{srv}, port_{srv}, IP_{cli}, port_{cli}) \) ?
  - Decode \( m \) from the 3-bit encoding in the SYN Cookie
    - Reconstruct the SYN queue entry
Smurf Attack

Honey! I think our network is having another Smurf attack!
Smurf Attack

- **ICMP echo request (ping) traffic to IP broadcast address**
  - Source IP address of a broadcast ping is spoofed - victim
- Large number of machines respond back to victim, overloading it
Smurf Attack - ICMP

- ICMP echo (spoofed source address of victim)
  Sent to IP broadcast address
- ICMP echo reply

Diagram:
- Internet
- Perpetrator
- Victim
- Smurf Attack - ICMP
Smurf Attack Defenses

1. Configure individual hosts and routers not to respond to ping requests or broadcasts.

2. Configure routers not to forward packets directed to broadcast addresses.
Distributed Denial of Service (DDoS)

- Same as regular DoS, but on a larger scale
- Example: Sub7Server Trojan and IRC bots
  - Infect a large number of machines with a “zombie” program
  - Zombie program logs into an IRC (Internet Relay Chat) channel and awaits commands
    - Bot command: !p4 207.71.92.193
    - Result: runs ping.exe 207.71.92.193 -l 65500 -n 10000
    - Sends 10,000 64k packets to the host (655MB!)
Mini Case Study – Code Red

- **July 19, 2001**: over 359,000 computers infected with Code-Red in less than 14 hours
- Used a known buffer exploit in Microsoft IIS
  - Internet Information Server – webserver
- **Damages estimated in excess of $2.6 billion**
- Launched a DDOS attack against [www1.whitehouse.gov](http://www1.whitehouse.gov) from the 20th to the 28th of every month!
- Spent the rest of its time infecting other hosts
Defenses against DDoS

- Intrusion Detection
- Blacklisting and Firewalls
- CloudFlare
No CloudFlare

When visitor types allen.com
- Browser contacts DNS
- Gets back 1.1.1.1
- Sends request to 1.1.1.1

Without CloudFlare

Visitor

Crawlers and bots

Attacker

allen.com
server IP: 1.1.1.1
With CloudFlare

CloudFlare: sits between the visitor and the website it protects
CloudFlare

- Has (collaborates with) data centers around the world
- For the initial DNS request: route the request to the data center closest to visitor
  - The result: IP in the CloudFlare data center closest to visitor
  - Not 1.1.1.1, but 99.99.99.99
  - Visitor makes request to 99.99.99.99 (not 1.1.1.1)
CloudFlare

- CloudFlare edge servers (IP 99.99.99.99 address)
  - Receive the request for the protected website
- Analyze the traffic before sending to protected website
- Verify if the visitor appears to be a threat based on
  - The visitor's IP address (blacklisting/firewall)
  - Requested resources
  - Payload posted (malware, buffer overflow, SQL injection, etc)
  - Frequency of requests
CloudFlare Caching

- Speed up the response time
- Cache parts of websites that are static in CloudFlare servers
  - Images, CSS, and JavaScript
  - Do not cache HTML (to not mess up dynamic pages)
CloudFlare Request Handling

- If the visitor is not a threat
- Front server checks the request against the cache
- Serve from cache if found
- Otherwise, request page (from IP 99.99.99.99 to the original webpage (1.1.1.1))
CloudFlare Advantage

- Only CloudFlare knows the IP of webserver (1.1.1.1)
- CloudFlare protects multiple clients (webservers)
- Sees many attacks and attackers
- Can build more efficient blacklists
- Can use machine learning to detect existing and new attacks (similar to intrusion detection systems)