Cyber Security: Threats and Challenges

R. Sekar
sekar@cs.sunysb.edu

Alarming Trends in Cyber Attacks

- Large increases in Cybersecurity spending
  - Factor of 10+ increase in the past ten years
- Yet, security incidents continue to skyrocket
  - Incidents reported by CERT Coordination Center increased by a factor of 120 in the past decade
  - 97% of participants in 2003 FBI/CSI survey reported attacks
  - Malicious attacks cost companies tens of billions to clean up [Computer Economics, Trend Micro]
  - Many small/medium businesses are victims of cyber extortion
    - 17% of companies surveyed by CMU and Information Week

Evolution of Threats

- World War II and earlier
  - Break secret messages during transmission
  - Primarily the domain of nation states
  - Modern cryptography has all but eliminated this threat
- Modern era
  - Focus shifts from altering messages to breaking end-systems that store and process these messages

Evolution of Modern Threats

- First generation
  - break into high-value systems (e.g., banks) through proprietary networks
  - criminal elements as well as rogue nations
- Second generation
  - Malware that spreads due to information sharing
    - Viruses and worms
    - Perpetrated by hackers as a “hobby”
- Third generation
  - Malware that spreads via the Internet
  - Email viruses and Internet worms
  - Still, no evidence of organized or criminal elements
Traditional Threats - Examples

- **1989**
  - Hackers in West Germany broke into US government and corporate computers and selling operating system source code to the Soviet KGB

- **1994**
  - Russian crackers siphoned $10 million from Citibank and transferred the money to bank accounts around the world

Current Threats (Fourth generation)

- **Steal confidential information**
  - Credit-card/bank account #s, passwords, …
  - Trade secrets and other proprietary information
  - Security-sensitive information
    - Useful for breaching physical world security
- **Establish base for future operations**
  - Conduit for future attacks
- **Surveillance**
  - Capture keystrokes, microphone or camera input
  - Reveal information about software installed
  - Snoop on web sites visited

Current Threats (Continued)

- **Driven by commercialization of Malware**
  - Thriving black-market for exploits
  - Zero-day exploits have arrived
  - “Bot”-centric model for cyber crime
    - Relay spam (e-mail scam, phishing)
    - Extortion (using DDoS or targeted attacks)
    - Focus on desktop (rather than server) vulnerabilities
- **Profit-driven adware and spyware**
  - Customer-profiling, niche-marketing
  - IP protection (digital rights management)
  - Aggressive installation, stealth (rootkits, spyware)

Current Threats (Continued)

- **Specialization and commoditization**
  - Exploit tools and techniques
    - Compromise
    - Payload
  - Targeting information
  - Botnet management and leasing
  - Brokers
  - Employment of botnets
  - Cash-out
    - The step that most closely relates to things outside the cyber world
Modern Threats: Enablers

- High connectivity
  - Home users with always-on broadband connectivity
  - Increasing adoption of the Net in day-to-day activities
- Software homogeneity
  - Find single bug, own millions of computers!
- Inherent complexity of modern software
- Short-term thinking by vendors
  - “Feature obsession” and cost-cutting
    - Shoddy software quality + code bloat
  - Result: security bugs are all over the place and easy to find!
- Lack of user awareness
  - Find millions of trusting users and own their computers!
- Lack of traceability and attribution
  - Conduct your attack and disappear!

Modern Threats: A Glance

- Viruses
- Worms
- DDoS and Botnet
- Spyware
- Spam
- Phishing
- Online extortion

Computer Virus

- Properties
  - Replicates itself
  - Attaches to other non-malicious code
- Examples
  - Boot sector virus (difficult on OS with memory protection)
  - Other OS level virus
  - Virus that attaches to programs, scripts, libraries
  - Macro virus
  - Mail attachments / active web content

Well-Known Computer Viruses

- 1982, Elk Cloner
  - First virus in the wild
  - Targeting Apple II
- 1986, (c)Brain
  - First virus for IBM PC
  - A boot sector virus
- 1995, Concept virus
  - First Macro virus
- 1998, CIH
  - One of the most harmful widely circulated viruses
  - Overwrites both hard disks (data loss) and Flash BIOS (hardware damage)
**Macro Virus**
- Written in a macro language.
- Macros can perform operations that the software can do.
- To date, only Microsoft Office products are vulnerable to this kind of virus.
- Simple solution: turning off the macro feature

**CIH Virus**
- Spreads via Portable Executable files under Windows 95/98/Me.
- Damages:
  - Overwriting the first 1024KB of the hard drive with zeroes ➔
  - Loss of data on the entire hard drive
  - Overwriting the Flash BIOS with junk code ➔
  - Computers cannot boot any more
- Activated in the public eye on April 26, 1999
- An untold number of computers worldwide were affected, much in Asia

**Melissa**
- Found on March 26, 1999
- Targetting Microsoft Word and Outlook-based systems, and creating considerable network traffic
- Shut down many Internal mail systems
  - That got clogged with infected e-mails propagating from the worm
- Inside a file called “List.DOC”
- Can mass-mail itself from email client Microsoft Outlook 97 or Outlook 98.
- Attempts to mass mail itself once an infected Word document is opened.

**ILOVEYOU**
- First appeared on May 3, 2000
- Caused widespread e-mail outages, an estimated $10 billion in economic damage
- Written in VBScript
- E-mail
  - Subject: “ILOVEYOU”
  - Attachment “LOVE-LETTER-FOR-YOU.TXT.vbs”
- Overwrote important files with a copy of itself
- Sent out itself to everyone in a user’s contact list
Computer Worm

- Replicates over the network (usually by itself)
  - First worm appeared at Xerox PARC in 1978
- What a worm can do?
  - Replicates itself, and thus consumes network bandwidth
  - Deletes files on a host system
  - Sends documents via e-mail
  - Carries other executables as a payload
    - Installs a backdoor in an infected computer (zombie computer)
- Modern worms
  - Large scale infection
  - Fast spread rate
    - spread over the Internet within a second

Timeline of Notable Worms (1)

- Nov 1988, Morris worm
  - First well-known worm
- March 1999, Melissa (E-mail worm)
  - Targeting Microsoft Word & Outlook-based systems
- May 2000, VBS/Loveletter or ILOVEYOU (E-mail worm)
  - Caused an estimated $10 billion in economic damage
- July 2001, Code Red (Exploited IIS bugs)
  - Considerably slowed down Internet traffic
- Jan 2003, SQL Slammer (Exploited MS SQL Server bugs)
  - Very fast: infected most of its 75,000 victims within ten minutes
  - Amazingly small, only 376 bytes

Timeline of Notable Worms (2)

- Aug 2003, Blaster, Welchia (Nachi), SoBig
  - Blaster (Exploited DCOM RPC bugs)
    - Coded to start a SYN flood on Aug 15 against windowsupdate.com
  - Welchia (Nachi)
    - A goodwill worm to remove Blaster and patch Windows
  - SoBig (E-mail worm)
    - Infected millions of Windows computers in Aug 2003
    - Microsoft wanted information of the worm creator for $250,000
- Apr 2004, Sasser (Exploited LSASS bugs)
  - Affected:

Code Red

- Released on July 13, 2001
- Considerably slowed down the Internet traffic
- Details:
  - Attacked computers running Microsoft's IIS web server
  - Defaced the affected web site
  - Tried to spread itself by looking for more IIS servers on the Internet
  - Waited 20-27 days after it was installed to launch DoS attacks on several fixed IP addresses, including White House.
  - Exploited a buffer overflow vulnerability in IIS;
    - Used illegal GET requests to trigger the vulnerability
**SLAMMER**
- January 2003
- Caused DoS on some Internet hosts and dramatically slowed down general Internet traffic
- Fast
  - Infect most of its 75,000 victims within ten minutes
- A buffer overflow based attack targeting Microsoft SQL Server
- Amazingly small, only 376 bytes
- Generate random IP addresses and send itself out to those addresses.
- If the selected address happens to belong to a host that is running an unpatched copy of Microsoft SQL Server, the host immediately becomes infected and begin spraying the Internet with more copies of the worm program.
- Only stays in memory.

**Blaster**
- Spread during August 2003 (first noticed on August 11, peaked on August 13)
- Programmed to start a SYN flood on August 15 against port 80 of windowsupdate.com.
- Exploited a buffer overflow in the DCOM RPC service on the affected Windows operating systems

**Welchia (Nachi)**
- Welchia (Nachi), a worm that tries to remove the Blaster worm and patch Windows
  - Discovered in August 18, 2003
- Not good
  - Create vast amount of network traffic, thereby slowing down the Internet
  - Make the system unstable (e.g. reboot after patching)
  - Without user’s explicit consent

**SoBig**
- Consequences:
  - Infected millions of Microsoft Windows computers in August 2003
  - Microsoft wanted information of the worm creator for $250,000
- Details:
  - Appear as an e-mail with one of the following subjects:
    - Re: Approved
    - Re: Details
    - Re: Thank you
  - Contain the text: “See the attached file for details” or the like
  - Contain an attachment by one of the following names:
    - application.pif
    - details.pif
    - thank_you.pif
- Infection and spreading:
  - Infect a host computer once the attachment is opened
  - Replicate by sending out the above-mentioned emails
  - E-mail addresses are gathered from files on the host computer
MyDoom
- One of the fastest spreading e-mail worms
- Details
  - Primarily transmitted via e-mail, appearing as a transmission error
  - Subject lines including “Error”, “Mail Delivery System”, “Test” or “Mail Transaction Failed”
  - Contains a malicious attachment
- Infection and Spreading
  - Resend the worm to e-mail addresses found in local files once the attachment is opened.
  - Copies itself to the “shared folder” of KaZaA (a P2P file-sharing app)
- Backdoor
  - Installs a backdoor on port 3127/tcp to allow remote control of the subverted PC
  - A DoS attack against SCO Group, Microsoft, and antivirus sites

Sasser
- First noticed in April 2004. Affected:
- Can spread without the help of the user.
  - Exploit a buffer overflow in LSASS (Local Security Authority Subsystem Service)
  - Scan different ranges of IP addresses and connect to victims’ computers primarily through TCP port 445.
- Can be easily stopped by a properly configured firewall, or by downloading patches

Distributed Denial-of-Service (DDoS)
- DoS
  - An attack on a computer system or network that causes a loss of service to users
- Methods
  - Consumption of computational resources, such as bandwidth, disk space, or CPU time
  - Disruption of configuration information, such as routing information
  - Disruption of physical network components
- DDoS
  - Use of multiple hosts (often through Botnet) in a DoS

Botnet
- What is a Botnet?
  - A collection of compromised computers
  - The computers are implanted with backdoor programs
    - Usually by worms, viruses
  - The programs are under a common control infrastructure
  - Botnet’s originator can control the group remotely
    - Usually through a means such as IRC
- Purpose
  - DDoS
  - SMTP mail relays for SPAM
  - Theft of sensitive information
    - E.g. login IDs, credit card numbers, application serial numbers
### Rootkit

- **Stealthy backdoor programs**
- **Intended to maintain “invisibility” of intruders**
  - Intercepts data from terminals, network connections, and the keyboard
  - Conceals logins, running processes, files, logs, or other system data
- **Origins of “rootkit”**
  - Originally referred to such kind of programs in Unix systems (root – the administrator)

### SonyBMG DRM Rootkit (2005)

- **Extended Copy Protection (XCP) DRM for CD copy protection**
  - User is required to install XCP software contained in the CD to play XCP-protected CD on a Windows system.
  - XCP intercepts all accesses of the CD drive and only allows XCP-bundled media player to access music tracks on the CD
  - XCP conceals itself from the user by installing a patch to the Windows operating system. This patch stops ordinary system tools from displaying processes, registry entries, or files who names begin with $sys$.
- About 4.7 million XCP-CDs shipped, 2.1 million sold [New York Times]

### Spyware

- **Properties**
  - Intercept or take partial control of computer’s operation
  - Without the informed consent of that computer’s legitimate user.
  - Does not usually self-replicate.
- **Purpose**
  - Delivery of unsolicited pop-up advertisements
  - Theft of personal information
  - Monitoring of Web-browsing activity for marketing purposes
  - Routing of HTTP request to advertising sites
Spam

- Properties
  - Sending of *unsolicited* (commercial) emails
  - Sending nearly identical messages to thousands (or millions) of recipients
- Spamming in different media
  - E-mail spam, Messaging spam, Newsgroup spam and Forum spam, Mobile phone spam, Internet telephony spam, Blog, wiki, guestbook, and referrer spam, etc

- Cost USA organizations alone more than $10 billion in 2004 [California legislature]

Phishing

- Uses social engineering techniques
  - Masquerading as a trustworthy person or business in an apparently official electronic communication
  - Attempts to fraudulently acquire sensitive information
    - Such as passwords and credit card details

Online DDoS Extortion

- Extortion: you pay us or you will be attacked

- [CMU and Information Week, 2004]
  - 17% of companies surveyed are victims of online extortion.

- [Alan Paller, SANS Institute, 2004]
  - 6 or 7 thousand organizations are paying extortion
  - Every online gambling site is paying extortion

Underlying Causes

- Untrusted software
  - Malware, including viruses, worms, bots, …
- Configuration errors
  - Default passwords, permissive firewall rules, …
- Human element
  - Insider threats, operator mistakes, social engineering
- Vulnerabilities in trusted software
  - These may be the result of errors in
    - Threat modeling
    - Design/logic
    - Implementation
    - Testing
Threats Due to Untrusted Code

- Metamorphic viruses
  - Viruses that use complex transformations that elude signature-based techniques
- Rootkits
- Trojan software
  - Will likely evolve into stealthy forms
- Need proactive (rather than reactive) solutions

The Human Element

- Insider attacks
- Growing system complexity contributes to more operator errors
  - Misconfigured systems
  - Especially problematic in settings where many components interact
- Intentionally introduced vulnerabilities
  - Infiltration into key proprietary or open-source software development teams
- Social engineering attacks

Software vulnerabilities

- Most vulnerabilities are due to software bugs
  - 97% of vulnerabilities reported in CVE
  - The rest are configuration errors
- These vulnerabilities may be exploited in attacks to obtain unauthorized or unintended capabilities
- Most vulnerabilities are due to simple programming errors
  - Bounds-checking
  - Input validation
  - Error-handling

CVE Vulnerabilities, 2003 and 2004

- Memory errors 24%
- Command injection 14%
- SQL injection 2%
- Cross-site scripting 4%
- Directory traversal 7%
- Other injection 4%
- Logic errors 19%
- Unknown 4%
- Format string 4%
- Crash 7%
- Loop 4%
- Config error 3%
- Known 3%
- Symlink attacks 4%
- Other 4%

Secure Systems Laboratory
Example: SQL Injection

- **Attacker-provided data** used in SQL queries
  
  ```php
  $cmd = "SELECT price FROM products WHERE name='" . $name . "'
  ... Use cmd as an SQL query
  
  - **Attacker-provided name**: xyz
    
    ```sql
    UPDATE products SET price=0 WHERE name='xyz';
    ```
  
  - **Resulting query**
    
    ```sql
    SELECT price FROM products WHERE name='xyz';
    UPDATE products SET price=0 WHERE name='OneCaratDiamondRing';
    ```