EE 8084
Cyber Security

The Need for Security

Our bad neighbor makes us early stirrers,

which is both healthful and good husbandry.

WILLIAM SHAKESPEARE (1564–1616),
KING HENRY, IN *HENRY V*, ACT 4, SC. 1, L. 6-7.

Learning Objectives

- Appreciate the need for Cyber Security
- Understand that an organization's general management and IT management are responsible for a successful information security program
- Have a good understanding of threats and attacks
- Overview of antivirus and patch

By Kevin Kwang
@KevinKwangCNA

20 Jul 2018 05:29PM
(Updated: 20 Jul 2018 08:00PM)

228 shares

Bookmark

Singapore

Singapore health system hit by 'most serious breach of personal data' in cyberattack; PM Lee's data targeted

A total of 1.5 million SingHealth patients' non-medical personal data were stolen, while 160,000 of those had their dispensed medicines' records taken too, according to MCI and MOH.

Among those affected was Prime Minister Lee Hsien Loong, with the attackers "specifically and repeatedly targeting" his personal particulars and information of his outpatient dispensed medicines, the ministries said in a joint release on Friday (Jul 20).

The personal data taken from the 1.5 million patients include their names, NRIC numbers, address, gender, race and date of birth, the release said, adding that the hackers did not amend or delete the records.

Patients' medical records, including past diagnosis, doctors' notes and health scans, were not affected.

"Singaporeans lost more than $500,000 to cybercrime last year: security report"

Published Nov 24, 2015, 12:00 pm SGT
The Strait Times, SPH Website

http://www.straitstimes.com/singapore/singaporeans-lost-more-than-500000-to-cybercrime-says-security-report

Introduction

- The primary aim of an information security program is to ensure the safety and usefulness of information assets (information and the systems that house the information)

- Resources could be used to improve systems that contain, use, and transmit information if there is no threat

- However, threats and attacks are constant concerns

Business Needs First

Information security performs four important functions

– Protecting the functionality of an organization

– Protecting data and information an organization collects and uses

– Enabling the safe operation of applications running on the organization's IT systems

– Safeguarding the organization's technology assets

Protecting the Functionality of an Organization

- Management (general and IT) is responsible for facilitating security program

- Implementing information security is more a management issue than technology

- Information security should be addressed in terms of business impact and the cost of business interruption.

Protecting Data That Organizations Collect and Use

- When an organization loses its data, it also loses its record of transactions and ability to deliver value to customers.

- A critical aspect of information security is to protect data in transmission, in processing, and at rest (storage)

Enabling the Safe Operation of Applications

- Organization needs an environment that safeguard the operation of applications
- Management must continue to oversee infrastructure once in place—not relegate to IT department.

Safeguarding Technology Assets in Organizations

- Secure infrastructure hardware must be appropriate to the size and scope of the organisation

- Additional security services may be needed as the organization grows.

- More robust solutions should replace security programs when the organization has outgrown its capacity

Threats

- Threat: a potential risk to an asset's loss of value
- Management must be informed about the various threats to an organization's people, applications, data, and information systems.
- Overall security is improving, so is the number of potential hackers
- The 2010–2011 CSI/FBI survey found
  - 67.1 percent of organizations had malware infections.
  - 11 percent indicated system penetration by an outsider.

Type of attack or misuse	2010/11	2008	2006	2004	2002	2000
Malware infection (revised after 2008)	67%	50%	65%	78%	85%	85%
Being fraudulently represented as sender of phishing message	39%	31%	(new category)			
Laptop/mobile hardware theft/loss	34%	42%	47%	49%	55%	60%
Bots/zombies in organization	29%	20%	(new category)			
Insider abuse of Internet access or e-mail	25%	44%	42%	59%	78%	79%
Denial of service	17%	21%	25%	39%	40%	27%
Unauthorized access or privilege escalation by insider	13%	15%	(revised category)			
Password sniffing	11%	9%	(new category)			
System penetration by outsider	11%		(revised category)			
Exploit of client Web browser	10%		(new category)			
Attack/misuse categories with less than 10% responses (listed in decreasing order):						
Financial fraud						
Web site defacement						
Exploit of wireless network						
Other exploit of public-facing Web site						
Theft of or unauthorized access to PII or PHI due to all other causes						
Instant Messaging misuse						
Theft of or unauthorized access to IP due to all other causes						
Exploit of user's social network profile						
Theft of or unauthorized access to IP due to mobile device theft/loss						
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss						
Exploit of DNS server						
Extortion or blackmail associated with threat of attack or release of stolen data						

Table 2-1   CSI Survey Results for Types of Attack or Misuse (2000–2011)[5]

Category of threat	Attack examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in quality of service	Internet service provider (ISP), power, or WAN service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes, lightning
Human error or failure	Accidents, employee mistakes
Information extortion	Blackmail, information disclosure
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial-of-service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

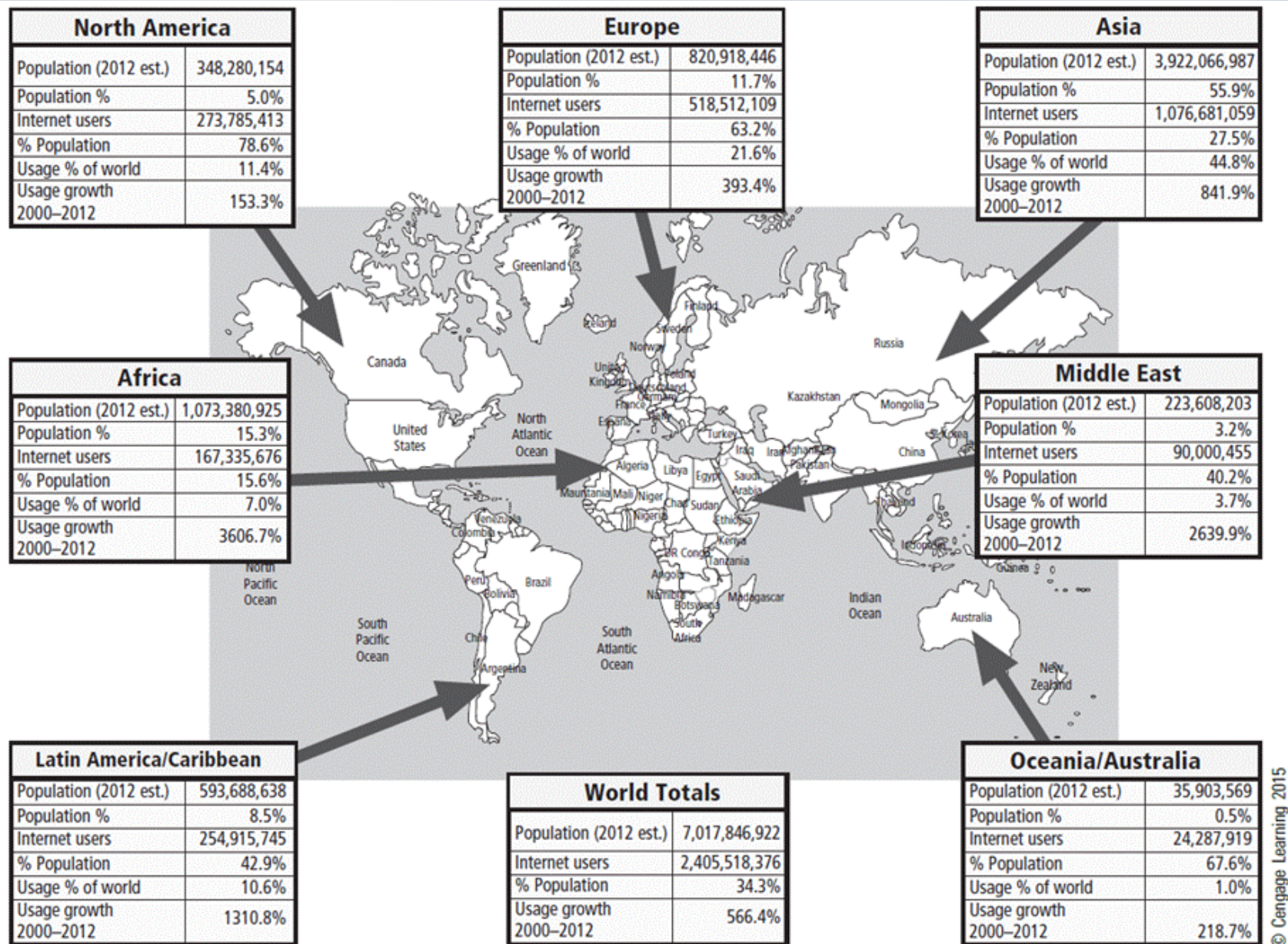**Table 2-2** The 12 Categories of Threats to Information Security[7]

North America

Population (2012 est.)	348,280,154
Population %	5.0%
Internet users	273,785,413
% Population	78.6%
Usage % of world	11.4%
Usage growth 2000–2012	153.3%

Europe

Population (2012 est.)	820,918,446
Population %	11.7%
Internet users	518,512,109
% Population	63.2%
Usage % of world	21.6%
Usage growth 2000–2012	393.4%

Asia

Population (2012 est.)	3,922,066,987
Population %	55.9%
Internet users	1,076,681,059
% Population	27.5%
Usage % of world	44.8%
Usage growth 2000–2012	841.9%

Africa

Population (2012 est.)	1,073,380,925
Population %	15.3%
Internet users	167,335,676
% Population	15.6%
Usage % of world	7.0%
Usage growth 2000–2012	3606.7%

Middle East

Population (2012 est.)	223,608,203
Population %	3.2%
Internet users	90,000,455
% Population	40.2%
Usage % of world	3.7%
Usage growth 2000–2012	2639.9%

Latin America/Caribbean

Population (2012 est.)	593,688,638
Population %	8.5%
Internet users	254,915,745
% Population	42.9%
Usage % of world	10.6%
Usage growth 2000–2012	1310.8%

World Totals

Population (2012 est.)	7,017,846,922
Internet users	2,405,518,376
% Population	34.3%
Usage growth 2000–2012	566.4%

Oceania/Australia

Population (2012 est.)	35,903,569
Population %	0.5%
Internet users	24,287,919
% Population	67.6%
Usage % of world	1.0%
Usage growth 2000–2012	218.7%

Figure 2-1 World Internet usage[3]

© Cengage Learning 2015

Intellectual Property Breach

- Intellectual property (IP) refers to the creation, ownership, and control of original ideas as well as the representation of those ideas
- Software privacy is the most common IP breaches
- Two watchdog organizations investigate software abuse:
  - Software & Information Industry Association (SIIA)
  - Business Software Alliance (BSA)
- The Intellectual Property Office of Singapore (IPOS)

Quality of Service (1)

- Depends on the successful operation of many interdependent support systems.

- Availability of information and systems are greatly affected by the internet service, communications, and power irregularities

Quality of Service (2)

- Internet service issues
  - Internet service provider (ISP) failures can adversely affect the availability of information.
  - Outsourced Web hosting provider is responsible for all Internet services as well as for the hardware and Web site operating system software.
- Communications and other service provider issues
  - Other utility services affect organizations: telephone, water, wastewater, trash pickup.
  - Loss of these services can affect organization's ability to function.

Quality of Service (3)

- Power irregularities
  - Commonplace
  - Lead to fluctuations such as power excesses, power shortages, and power losses
  - Sensitive electronic equipment vulnerable to and easily damaged/destroyed by fluctuations
  - Controls can be applied to manage power quality.

Espionage or Trespass (1)

- Unauthorized access of protected information
- Competitive intelligence (legal) versus industrial espionage (illegal)
- Shoulder surfing can occur anywhere a person accesses confidential information.
- Controls let trespassers know they are encroaching on organization's system
- Hackers use skill, guile, or fraud to bypass such controls
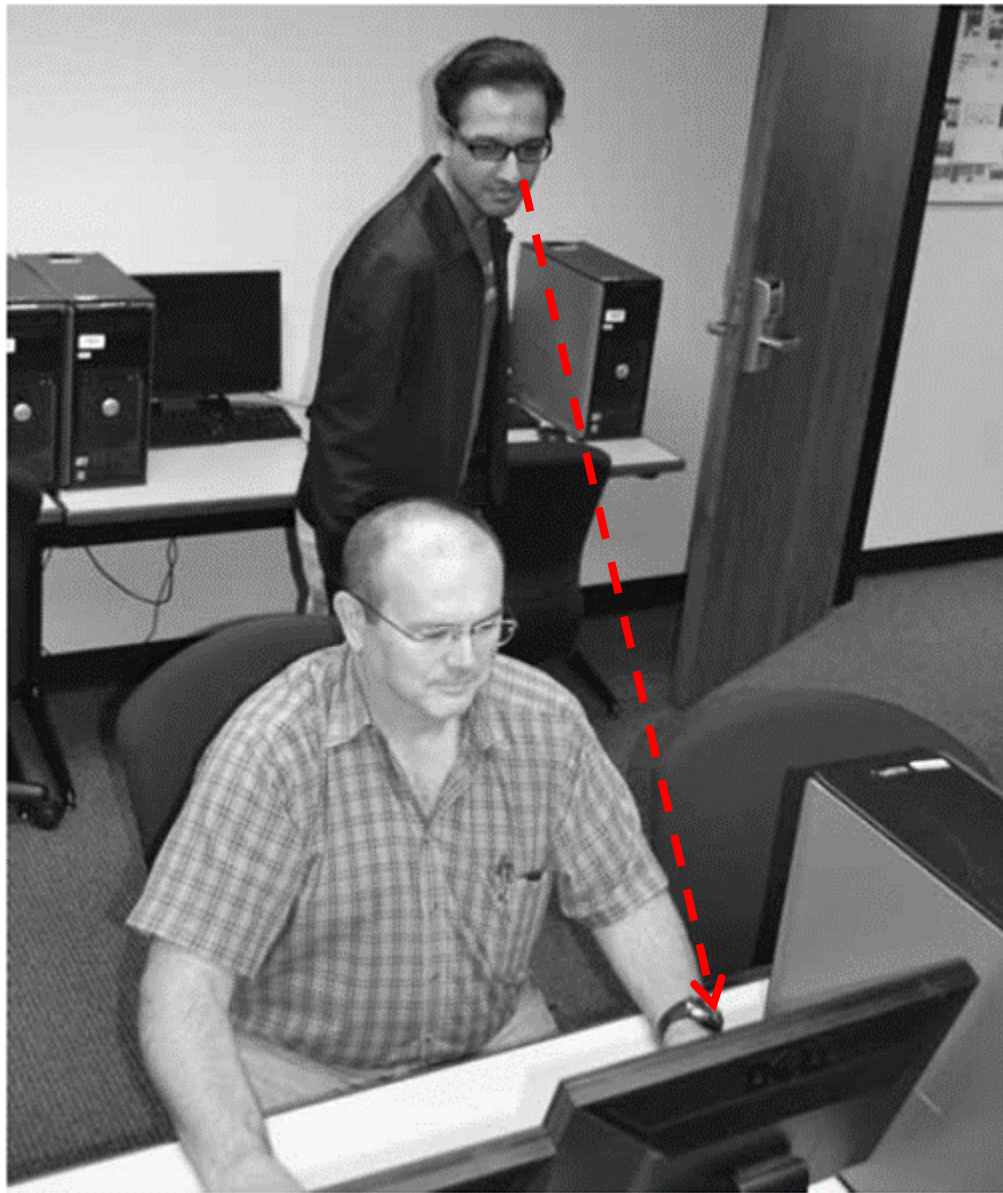
Figure 2-6 Shoulder surfing

Espionage or Trespass (2)

- Expert hacker
  - Develops software scripts and program exploits
  - A master of many skills, especially in programming
  - Create attack software (malware) and share with others
- Unskilled hacker (script kiddies)
  - Many more unskilled hackers than expert hackers
  - Use expertly written software to exploit a system
  - Do not usually fully understand the systems they hack

Figure 2-7 Contemporary hacker profile

Espionage or Trespass (3)

- Other terms for system rule breakers:
  - Cracker: "cracks" or removes software protection designed to prevent unauthorized duplication
  - Phreaker: hacks the public telephone system to make free calls or disrupt services
- Password attacks
  - Cracking
  - Brute force
  - Dictionary
  - Rainbow tables
  - Social engineering

Case-Insensitive Passwords Using a Standard Alphabet Set (No Numbers or Special Characters)

Password length	Odds of cracking: 1 in (based on number of characters ^ password length):	Estimated time to crack*
8	208,827,064,576	1.9 seconds
9	5,429,503,678,976	50.8 seconds
10	141,167,095,653,376	22.0 minutes
11	3,670,344,486,987,780	11.1 hours
12	95,428,956,661,682,200	10.3 days
13	2,481,152,873,203,740,000	268.6 days
14	64,509,974,703,297,200,000	19.1 years
15	1,677,259,342,285,730,000,000	497.4 years
16	43,608,742,899,428,900,000,000	12,932.8 years

Case-Sensitive Passwords Using a Standard Alphabet Set with Numbers and 20 Special Characters

Password length	Odds of cracking: 1 in (based on number of characters ^ password length):	Estimated time to crack*
8	2,044,140,858,654,980	5.2 hours
9	167,619,550,409,708,000	18.14 days
10	13,744,803,133,596,100,000	4.1 years
11	1,127,073,856,954,880,000,000	334.3 years
12	92,420,056,270,299,900,000,000	27,408.5 years
13	7,578,444,614,164,590,000,000,000	2,247,492.6 years
14	621,432,458,361,496,000,000,000,000	184,294,395.9 years
15	50,957,461,585,642,700,000,000,000,000	15,112,140,463.3 years
16	4,178,511,850,022,700,000,000,000,000,000	1,239,195,517,993.3 years

Table 2-3   Password Power

*Estimated Time to Crack is based on an average 2013-era Intel i7 PC (3770K) chip performing 109,924 Dhrystone MIPS (million instructions per second) at 3.9 GHz.

Forces of Nature

- Some of the most dangerous threats come from the forces of nature

- They disrupt not only individual lives, but also storage, transmission, and use of information

- Controls must be implemented to limit damage and prepare contingency plans for continued operations

Human Error or Failure (1)

- Acts performed by employees without malicious intent or in ignorance
- Causes:
  - Inexperience
  - Improper training
  - Incorrect assumptions
- Hence employees are potentially one of the greatest threats to an organization's data.

Human Error or Failure (2)

- Potential damages
  - Revelation of classified data
  - Entry of erroneous data
  - Accidental data deletion or modification
  - Data storage in unprotected areas
  - Failure to protect information
- Can be prevented with training, ongoing awareness activities, and controls.
- Social engineering uses social skills (trickery) to convince people to reveal access credentials or other valuable information to an attacker.

Social Engineering (1)

- "People are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee."—Kevin Mitnick

- Advance-fee fraud: indicates recipient is due money and small advance fee/personal banking information required to facilitate transfer

- Phishing: attempt to gain personal/confidential information; apparent legitimate communication hides embedded code that redirects user to third-party site

Social Engineering (2)

- Social engineering is a network intrusion technique based on **trickery**.

- Hackers use it to fool someone into revealing access codes, passwords, or other confidential information and break into a system.

- It's an elaborate term for **fraudulently obtaining information to gain access.**

- **Telephone no, job responsibilities and email addresses** **used as password, userid**

- **Work best if people don't know one another very well and/or there is a high staff turn over**

- **Manipulate human tendencies: greed and trust**

Social Engineering
The Key is Manipulation

Example: Social Engineering in NTU

Virus Detected

Nanyang Technological University [noreply@upgrade.com]

Extra line breaks in this message were removed.

Sent: Mon 4/4/2011 9:04 AM
To: info@upgrade.com

The Web management discovered some Virus in your mail account and in order to clean this virus from your mail account, you will need to upgrade your Web account Reconfirming to us the below details of your account.

We need the following for your email profile upgrade:

UserID:
Password:
Reconfirm Password:
Date of Birth:

You have limited time to supply the above details for effective services by replying to this email.

Warning: failure to provide the following details of your account or incorrect username or password, may cause our server to automatically deactivate you from our database in order not to spread this Virus.

Regards,
Web Administrator.

Information Extortion

- Steals information from a computer system and then demands compensation for its return or nondisclosure.

- Also known as cyberextortion.

- Use in credit card number theft

Sabotage or Vandalism

- Range from petty vandalism, web site defacing to organized sabotage.

- Web site defacing can erode consumer confidence, diminishing organization's sales, net worth, and reputation.

- Threat of hacktivist or cyberactivist operations is rising.

- Cyberterrorism/Cyberwarfare is a much more sinister form of hacking

Figure 2-14 Cyberactivists wanted

Software Attacks (1)

- Malicious software (malware) is used to overwhelm the processing capabilities of a system or to gain access to protected systems

- Software attacks occur when an individual or a group designs and deploys malwares to attack a system.

Software Attacks (2)

Malwares include the viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information

- Virus: Code segments that attach to existing program and take control of access to the targeted computer.

- Worms: Replicate themselves until they completely fill available resources such as memory and hard drive space.

- Trojan horses: Disguised as helpful, interesting, or necessary pieces of software

Virus - overview

- A program that piggybacks on other executable programs
- Not structured to exist by itself
- When the host program is executed, the virus code also executes and performs its action
- Typically, actions may be
  - Spreading itself to other programs or disks
  - Delete files
  - Cause systems to become unusable

3 ways for viruses to get into your computer

1. On contaminated media (floppy, USB drive, or CDROM)

2. Through email and peer-to-peer sites

3. Part of another program

Types of viruses

- Armored virus
- Companion virus
- Macro virus
- Multipartite virus
- Phage virus
- Polymorphic virus
- Retrovirus
- Stealth virus

Armored Virus

- It is designed to make itself difficult to detect or analyze

- Cover themselves with a protective code that stop debuggers or disassemblies from examining critical elements of the virus

- Some part of the code may also act as a decoy to distract analysis

- Need to identify them quickly!

Companion Virus

- Attaches itself to legitimate program and then creates a program with a different filename extension
- When a user types the name of the legitimate program, the companion virus executes instead of the real program
- Or make changes to program pointers in the registry so that they point to the infected program
- The infected program perform its dirty deed and then starts the real program

Macro Virus

- It exploits the enhancements made to many applications

- Example: Microsoft Word supports a mini-BASIC programming language that allows files to be manipulated automatically (eg., automatically spell-check your documents when opens). These programs are called macros.

- Macro virus infects such macros such that the related documents are infected and can spread to other systems via attached documents in an email

Multipartite Virus

- Attacks your system in multiple ways

- May infects your boot sector, all your executable files and destroy your application files (eg., MS word documents) at the same time

- The key is that you won't be able to correct all the problems and will allow infestation to continue.

Phage Virus

- It modifies other programs and databases
- Require reinstallation of programs or databases to remove virus

Polymorphic Virus

- The virus changes form in order to avoid detection
- Attempt to hide from your antivirus program by
  - encrypting itself
  - mutation
- Change its signature to fool the antivirus program

Retrovirus

- It bypasses the antivirus program
- May directly attack the antivirus program
- Destroy the virus definition database file
- May leave you with a false sense of security

Stealth Virus

- Hide from antivirus program by masking itself from application

- May attach itself to the boot sector

- Redirects commands to avoid detection

- Report a different file size

- Move around from file to file, eg., from file A (not yet scanned) to file B (already scanned) during a virus scan

Virus Transmission

- Some viruses destroy the target system immediately
- Some uses the victim system as a carrier to infect other servers, shared files and other resources in a network. It then eventually infects the original victim system and destroy it completely

Worm

- A program that crawls itself from system to system without any assistance of its victims

- Spreads on its own and replicates on its own

- Creator of a worm seek out system vulnerabilities to get the worm started

- The Internet may have to be shut down due to a infestation of a worm

Trojan Horse

- A program that hides its malicious nature behind the façade of something useful or interesting

- It is a complete and self-contained program that is designed to perform some malicious actions

- Disguise itself as a new capability or as an email that is attractive or interesting to read

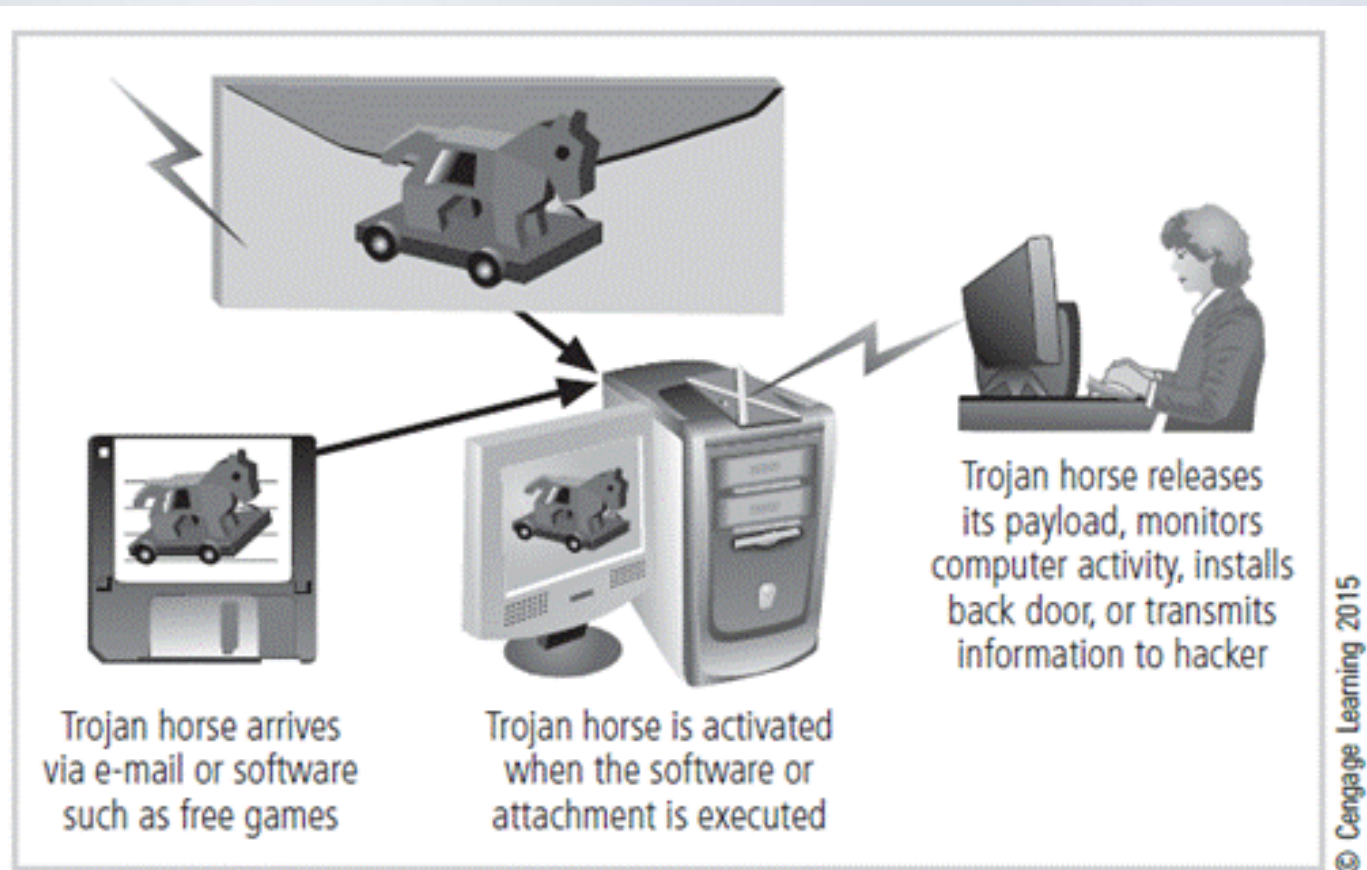- It may contain mechanism to spread itself

Trojan horse arrives via e-mail or software such as free games

Trojan horse is activated when the software or attachment is executed

Trojan horse releases its payload, monitors computer activity, installs back door, or transmits information to hacker

© Cengage Learning 2015

Figure 2-17 Trojan horse attacks

Malware	Type	Year	Estimated number of systems infected	Estimated financial damage
MyDoom	Worm	2004	2 million	$38 billion
Klez (and variants)	Virus	2001	7.2% of Internet	$19.8 billion
ILOVEYOU	Virus	2000	10% of Internet	$5.5 billion
Sobig F	Worm	2003	1 million	$3 billion
Code Red (and CR II)	Worm	2001	400,000 servers	$2.6 billion
SQL Slammer, a.k.a. Sapphire	Worm	2003	75,000	$950 million to $1.2 billion
Melissa	Macro virus	1999	Unknown	$300 million to $600 million
CIH, a.k.a. Chernobyl	Memory-resident virus	1998	Unknown	$250 million
Storm Worm	Trojan horse virus	2006	10 million	Unknown
Conficker	Worm	2009	15 million	Unknown
Nimda	Multivector worm	2001	Unknown	Unknown
Sasser	Worm	2004	500,000 to 700,000	Unknown
Nesky	Virus	2004	Under 100,000	Unknown
Leap-A/Oompa-A	Virus	2006	Unknown (Apple)	Unknown

Table 2-4   The Most Dangerous Malware Attacks to Date[36,37]

© Cengage Learning 2015

Melissa: both virus and worm

- The worm part enabled it to travel from system to system.

- The virus part replicated itself on local systems and did the damage.

- Creator-author, David Smith, was sentenced to 20 months in prison and fined $5,000 for releasing it.

Logic Bomb

- Program or snippet of codes that execute when a certain predefined events occurs

- Events could also be based on a certain date (eg, Christmas) or set of circumstances (certain employee has being sacked)

- It could send a message back to the attacker or launch an attack such as DDoS, or grant access to the victim system at attacker choice of time

Software Attacks (3)

- Polymorphic threat: actually evolves to elude detection
- Virus and worm hoaxes: nonexistent malware that employees waste time spreading awareness about
  - Check with CERT for hoaxes before forwarding
    http://www.cert.org/
- Back door: gaining access to system or network using known or previously unknown/newly discovered access mechanism

Software Attacks (4)

- Denial-of-service (DoS): An attacker sends a large number of connection or information requests to a target.
  - The target system becomes overloaded and cannot respond to legitimate requests for service.
  - It may result in system crash or inability to perform ordinary functions.
- Distributed denial-of-service (DDoS): A coordinated stream of requests is launched against a target from many locations simultaneously.
- Code Red and Nimda viruses caused extensive damage to businesses worldwide by causing DoS attacks that caused over $3 billion in damages.

In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software, and then remotely activated by the hacker to conduct a coordinated attack.
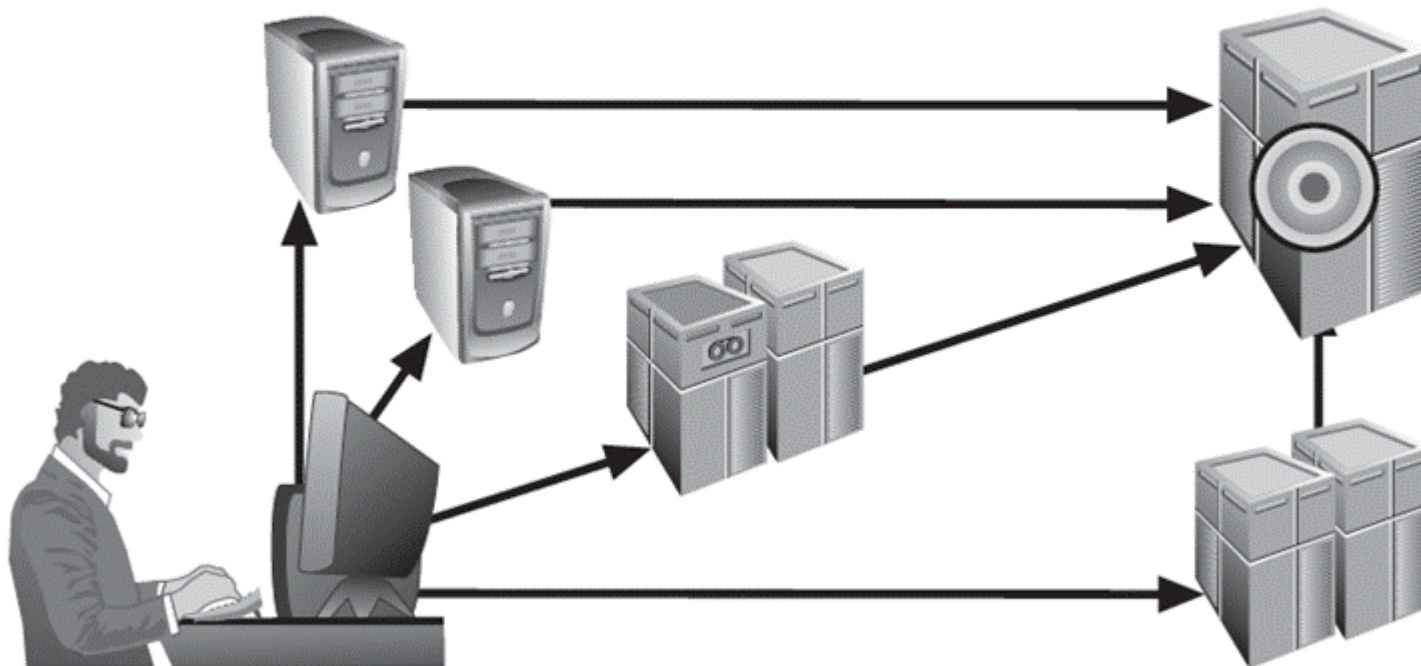

© Cengage Learning 2015

Figure 2-18 Denial-of-service attack

Software Attacks (5)

- Mail bombing (also a DoS): An attacker routes large quantities of e-mail to target to overwhelm the receiver.
- Spam (unsolicited commercial e-mail): It is considered more a nuisance than an attack, though is emerging as a vector for some attacks.
- Packet sniffer: It monitors data traveling over network; it can be used both for legitimate management purposes and for stealing information from a network.
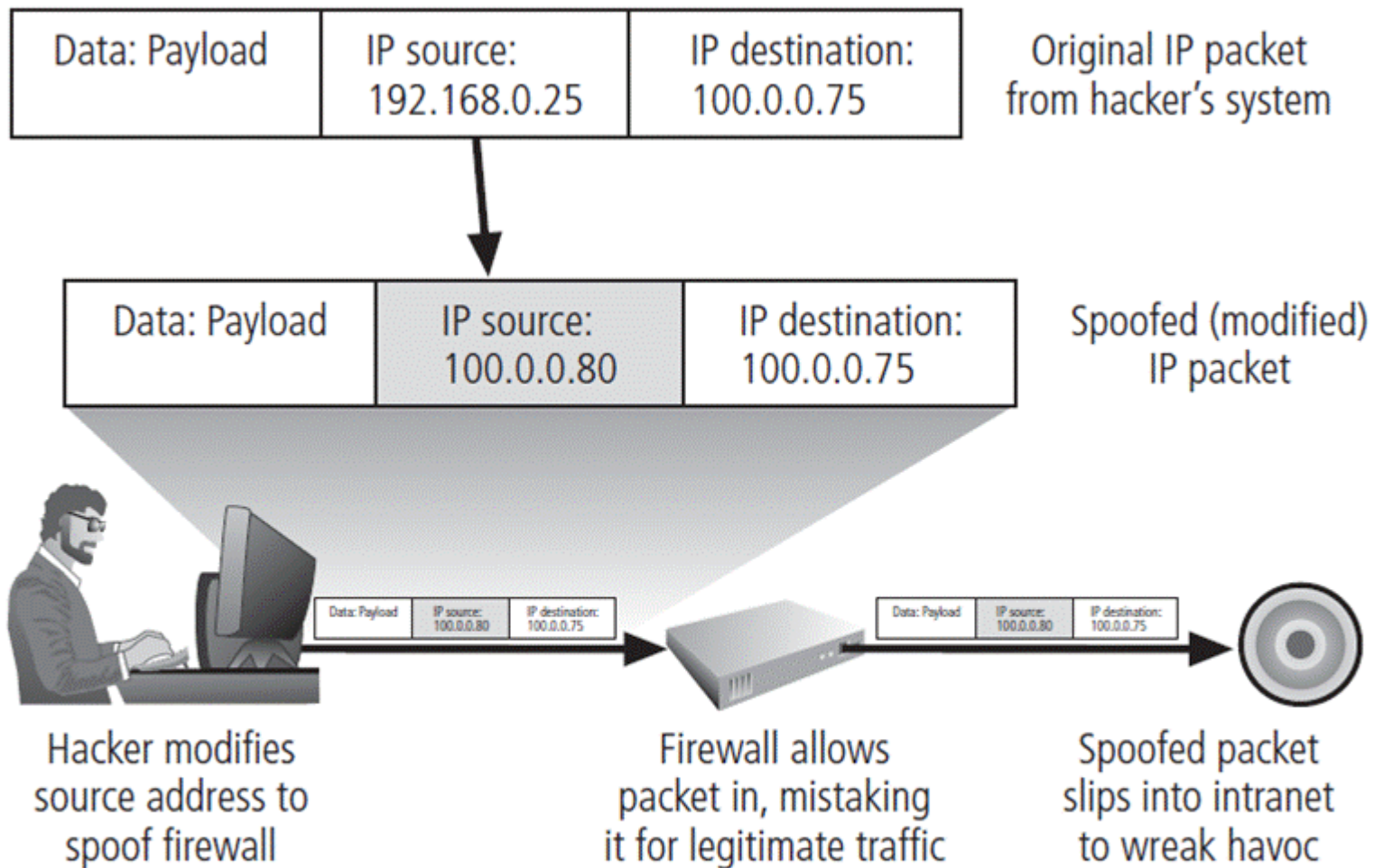- Spoofing: A technique used to gain unauthorized access; intruder assumes a trusted IP address.

Figure 2-19 IP spoofing attack

Software Attacks (6)

- Pharming: It attacks a browser's address bar to redirect users to an illegitimate site for the purpose of obtaining private information.

- Man-in-the-middle: An attacker monitors the network packets, modifies them, and inserts them back into the network.
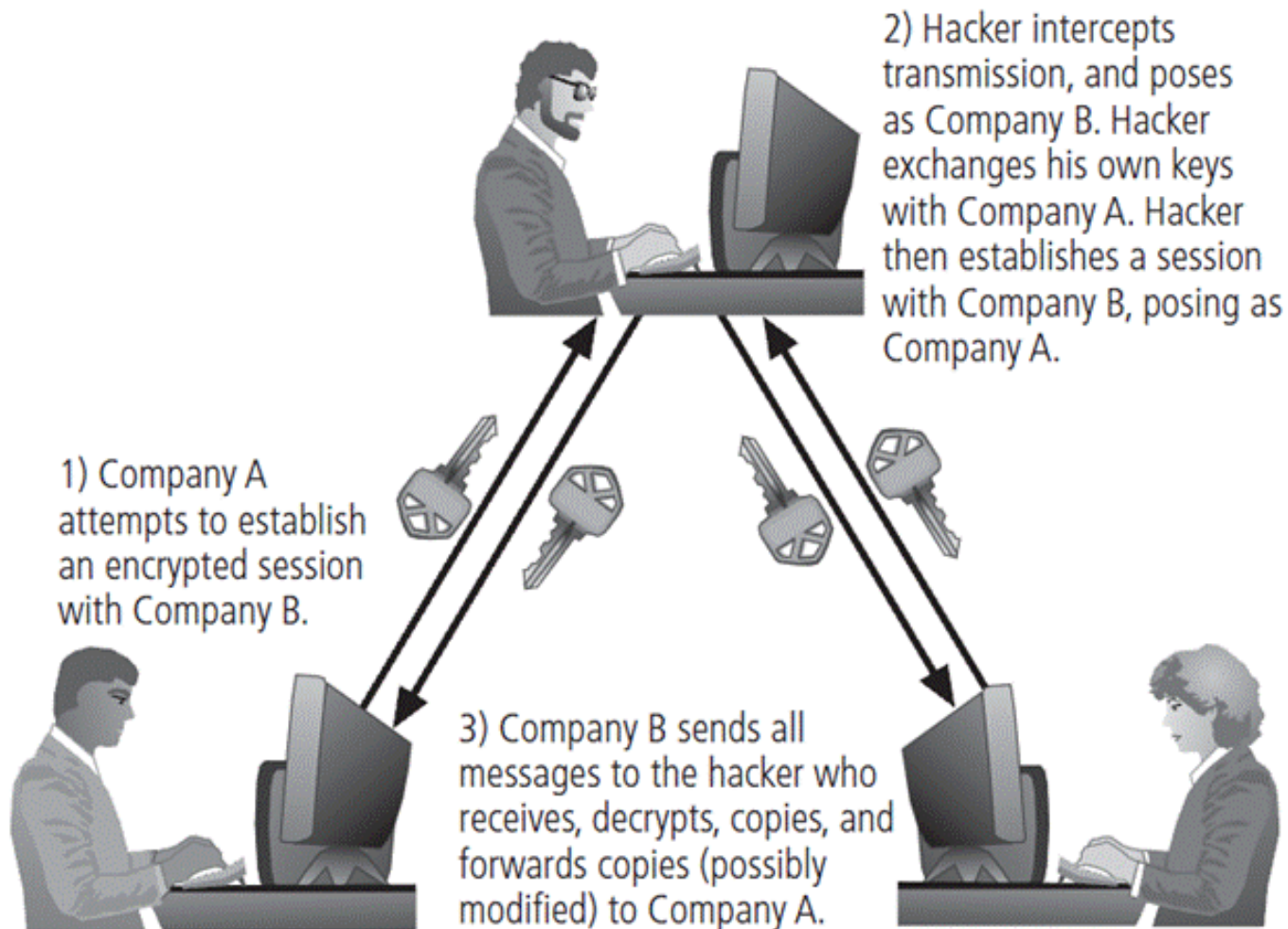
2) Hacker intercepts transmission, and poses as Company B. Hacker exchanges his own keys with Company A. Hacker then establishes a session with Company B, posing as Company A.

1) Company A attempts to establish an encrypted session with Company B.

3) Company B sends all messages to the hacker who receives, decrypts, copies, and forwards copies (possibly modified) to Company A.

© Cengage Learning 2015

Figure 2-20 Man-in-the-middle attack

Technical Hardware Failures or Errors

- Occur when a manufacturer distributes equipment containing a known or unknown flaw.

- Can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability.

- Some errors are terminal and some are intermittent.

- CPU failure

- Mean time between failure measures the amount of time between hardware failures.

Technical Software Failures or Errors

- Large quantities of computer code are written, debugged, published, and sold before all bugs are detected and resolved.

- Combinations of certain software and hardware can reveal new software bugs.

- Open Web Application Security Project (OWASP) is dedicated to helping organizations create/operate trustworthy software and publishes a list of top security risks.

  https://www.owasp.org/index.php/Main_Page

Software Vulnerability

- The developer creates software containing a vulnerability
- The attacker finds the vulnerability before the developer finds or fix it
  - Or is aware of but has neglected, e.g., due to an internal assessment of the threat's potential damage costs being lower than the costs of developing a fix
  - Or has been unable to fix it
- The attacker writes/uses/distributes an exploit, eg, a virus
- The developer or the public becomes aware of the exploited vulnerability and the developer is forced to start working on a fix, if not already working on one
- The developer releases the fix (or "patch")

Install Patches ASAP

- Zero-day (or zero-hour or day zero) attack
  - The developers had zero day to patch
- Once a patch is available, it is no longer a "zero-day exploit"
  - Install patches as soon as possible

From: EEE NOC Hotline   Sent: 14/5/2013 (周二) 8:55 AM

To: ⊞ **EEE Staff;** ⊞ **EEE Research Staff;** ⊞ **EEE Laboratories**

Cc:

Subject: FW: Fix Release - [ZERO-DAY] Microsoft Internet Explorer Unspecified Use-After-Free Vulnerability

Dear all,

Microsoft had release an emergency fix to the reported IE zero day vulnerability :

http://blogs.technet.com/b/srd/archive/2013/05/08/microsoft-quot-fix-it-quot-available-to-mitigate-internet-explorer-8-vulnerability.aspx

The workaround, which Microsoft calls a one-click Fix it tool, can be used to block attacks leveraging the Internet Explorer 8 (IE8) vulnerability described in Security Advisory 2847140.
Microsoft once again confirmed that the bug only affects IE version 8: IE 6, 7, 9, and 10 are not affected.

Note: The "Fix it" solution will apply only for the x86 versions of Internet Explorer 8 that have applied MS13-028: Cumulative Security Update for Internet Explorer: April 9, 2013

For your information and necessary actions where required.

Regards,

See more about: EEE NOC Hotline.

Two kingpins of Russian computer crime – Hackers (1)

- Alexey Ivanov and Vasily Gorshkov were found guilty of breaking into U.S. corporate information systems.

- They attacked through a known *vulnerability in Windows NT*.

  - First they would steal sensitive data.

  - Then email company executives demanding payment in exchange for not exposing confidential customer data or destroying financial records.

Two kingpins of Russian computer crime – Hackers (2)

- To carry out their attacks and extortion demands and hide their identities, they used various *Hotmail* email accounts, or hacked company accounts.

- Prior to being arrested by FBI in Nov. 2000, they had:

  - broken into >38 companies

  - stolen data from 2 banks

  - stolen data from 300,000 credit cards from CD Universe's Website and 15,700 credit cards from Western Union's Website.

Software patches not installed (1)

- Afterwards, it was learned that the victimized companies had not installed the *patch* that might have protected them from these intrusions.

  - There are some who would hold these companies accountable for failing to protect against the hackers' exploits (Lawyer action).

  - Even in Aug. 2003, many companies were hit by SoBig because they had not installed patches.

Software patches not installed (2)

However, Installing software patches is risky.

– Patches cannot be installed without first verifying that the "fix" won't cause more damage than hackers.

– Patches can destroy important computer applications.

Vulnerability Window (1)

- By one estimate, the average vulnerability window of a zero-day exploit is about 10 months
  - Can be much longer, e.g., in 2008 Microsoft confirmed a vulnerability in Internet Explorer which affected versions released in 2001
- Reverse engineering patches
  - By analyzing the patch just released, attackers can more easily figure out how to exploit the underlying vulnerability, and attack the systems that have not yet been patched

Vulnerability Window (2)

- Some vulnerability windows may never be closed
  - Hardwired in a device, requiring its replacement or the installation of additional hardware
  - Microsoft is warning users that, after it discontinues support for Windows XP starting on April 8, 2014, users running Windows XP will take risk of 'zero-day forever' because of reverse engineered security patches for newer Windows versions

Common failures in Software Development (1)

- Buffer overruns
- Command injection
- Cross-site scripting (XSS)
- Failure to handle errors
- Failure to protect network traffic
- Failure to store and protect data securely
- Failure to use cryptographically strong random numbers

Common failures in Software Development (2)

- Format string problems
- Neglecting change control
- Improper file access
- Improper use of SSL
- Information leakage
- Integer bugs (overflows/underflows)
- Race conditions
- SQL injection

Problem areas in Software Development

- Trusting network address resolution
- Unauthenticated key exchange
- Use of magic URLs and hidden forms
- Use of weak password-based systems
- Poor usability

Spyware

- Definition: gathering information about a person or organization without their knowledge
  - May send information to another entity without consent
  - May asserts control over a computer without the owner's knowledge
  - 4 types: system monitors (e.g., keyloggers), trojans, adware, and tracking cookies (owner's movements on the Internet)
- Spyware legally used or made by governments
  - Govware: Germany, Switzerland, ~ 2007
  - Policeware: installed to suspects' computers

Computer and Network Surveillance

- Definition: monitoring of computer activity, data stored on a hard drive, or data being transferred over computer networks such as the Internet, corporate networks, and phone networks
  - recognize and monitor threats
  - maintain social stability
  - prevent and investigate criminal activity
- Possible data analysis
  - Public data: Social networks, e.g., facebook, twitter
  - Privacy issues: Emails, SMS, GPS locations, phone calls

Browser Hijacking

- Definition: the modification of a web browser's settings without the user's permission
  - A browser hijacker may replace the existing home page, error page, or search page with its own
- Some browser hijacking can be easily reversed, while other instances may be difficult to reverse
  - Various software packages exist to prevent such modification and remove browser hijackers
- Most installers will give users the opportunity to accept or decline an offer to install a hijacker
  - however, declining the offer is often ignored

Theft

- Illegal taking of another's physical, electronic, or intellectual property

- Physical theft is controlled relatively easily.

- Electronic theft is a more complex problem; the evidence of crime is not readily apparent.

Antivirus Software (1)

- 2 common methods for virus and worm detection
  - Signature: a unique string of program that cannot be found in other legitimate programs
    - Protected only from viruses/worms in the antivirus signature list in their most recent virus/worm definition update
    - Update your antivirus software!
    - Not protected from new viruses/worms (e.g., zero day attack)
  - Heuristic algorithms based on common virus/worm behaviors
    - False positives can be disruptive, especially in a commercial environment

Antivirus Software (2)

- Option of antivirus (AV) software once the AV discovers a virus
  - If possible, cleaning the virus from the file without damaging the file (ideal!)
  - quarantining the infected file
  - If impossible to clean the virus from the file without damaging the file, deleting the file that contains the virus (you loss the file!)

Backup !

- *Regular backups* of *data* on *different media*
  - As often as you care to loss your data ☹
- If you have time, back up your whole system (operating system, application software, etc)
  - Create a cloned disk, a disk image
  - Restore system to the disk image if the whole system is infected

Technological Obsolescence

- Antiquated/outdated infrastructure can lead to unreliable, untrustworthy systems.

- Proper managerial planning should prevent technology obsolescence.

- IT plays a large role.

Summary

- Main aim is to ensure information stay the way they are
- There is a need for security
- Management must play its roles in Information Security
- 4 important functions of Information Security
- Threats and attacks
  - Software and hardware threat
  - Forces of nature
  - Social engineering
  - Malwares: virus, worm and Trojan horses
  - Others
- Antivirus and patch