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.

The Need for Security

Functions of Information Security

- Protects the organization’s ability to function
- Enables the safe operation of applications implemented on the organization’s IT systems
- Protects the data the organization collects and uses
- Safeguards the technology assets in use at the organization

Why We Need Information Security?

- Because there are threats

Why We Need Information Security?

Threats

- A threat is an object, person, or other entity that represents a constant danger to an asset
- Threat agent

Threats

- The 2007 CSI survey
  - 494 computer security practitioners
  - 46% suffered security incidents
  - 29% reported to law enforcement
  - Average annual loss $350,424
  - 1/5 suffered ‘targeted attack’
  - The source of the greatest financial losses?
  - Most prevalent security problem
    - Insider abuse of network access
    - Email

Threat Categories

- Acts of human error or failure
- Compromises to intellectual property
- Deliberate acts of espionage or trespass
- Deliberate acts of information extortion
- Deliberate acts of sabotage or vandalism
- Deliberate acts of theft
- Deliberate software attack
- Forces of nature
- Deviations in quality of service
- Technical hardware failures or errors
- Technical software failures or errors
- Technological obsolesce
Acts of Human Error or Failure

- Includes acts done without malicious intent
- Caused by:
  - Inexperience
  - Improper training
  - Incorrect assumptions
  - Other circumstances
- Employees are greatest threats to information security

Employee mistakes can easily lead to the following:
- Revelation of classified data
- Entry of erroneous data
- Accidental deletion or modification of data
- Storage of data in unprotected areas
- Failure to protect information
- Many of these threats can be prevented with controls

Deliberate Acts of Theft

- Illegal taking of another’s property - physical, electronic, or intellectual
- The value of information suffers when it is copied and taken away without the owner’s knowledge
- Physical theft can be controlled
  - A wide variety of measures used from locked doors to guards or alarm systems
- Electronic theft is a more complex problem to manage and control
  - Organizations may not even know it has occurred

Deviations in Quality of Service by Service Providers

- Situations of product or services not delivered as expected
- Information system depends on many inter-dependent support systems
- Three sets of service issues that dramatically affect the availability of information and systems are
  - Internet service
  - Communications
  - Power irregularities

Internet Service Issues

- Loss of Internet service can lead to considerable loss in the availability of information
  - Organizations have sales staff and telecommuters working at remote locations
- When an organization outsource its web servers, the outsourcer assumes responsibility for
  - All Internet Services
  - The hardware and operating system software used to operate the web site
Power Irregularities

Voltage levels can increase, decrease, or cease:
- spike – momentary increase
- surge – prolonged increase
- sag – momentary low voltage
- brownout – prolonged drop
- fault – momentary loss of power
- blackout – prolonged loss

Electronic equipment is susceptible to fluctuations, controls can be applied to manage power quality
- Surge protector
- UPS

Communications and Other Services

Other utility services have potential impact
- Among these are
  - telephone
  - water & wastewater
  - trash pickup
  - cable television
  - natural or propane gas
  - custodial services
- The threat of loss of services can lead to inability to function properly

Forces of Nature

Forces of nature, or acts of God are dangerous because they are unexpected and can occur with very little warning
- Can disrupt not only the lives of individuals, but also the storage, transmission, and use of information
- Include fire, flood, earthquake, and lightning as well as volcanic eruption and insect infestation
- Since it is not possible to avoid many of these threats, management must implement controls to limit damage and also prepare contingency plans for continued operations

Compromises to Intellectual Property

“The ownership of ideas and control over the tangible or virtual representation of those ideas”
- Many organizations are in business to create intellectual property
  - trade secrets
  - Copyrights
  - trademarks
  - Patents

Trade Secret

- Definition
  - any valuable business information that is not generally known and is subject to reasonable efforts to preserve confidentiality
- Protected from exploitation by
  - those who either obtain access through improper means
  - those who obtain the information from one who they know or should have known gained access through improper means
  - those who breach a promise to keep the information confidential
- Fragile

Uniform Trade Secret Act

- Drafted by the National Conference of Commissioners on Uniform State Laws in 1970
- Amended in 1985
- Recent case
Copyright

- Definition
  - a form of intellectual property protection that granted by the federal government
  - a copyright is provided to the authors of “original works of authorship”
    - regardless of whether the work has been published
    - regardless of whether the work has been registered

- Work protected
  - Literature
  - Music
  - Dramatic
  - Pantomimes or choreography
  - Pictorial, graphical or sculptural
  - Motion picture and audiovisual
  - Sound recording
  - Architectural
  - A copyright protects only the form of expression

- Laws and regulations
  - Digital Millennium Copyright Act

- Recent case

- Exemption
  - http://www.securityfocus.com/brief/365

Trademarks

- Definition
  - A “trademark” (which relates to goods) and a “service mark” (which relates to services) can be any word, name, symbol, or device, or any combination, used, or intended to be used, in commerce.

- To acquire federal trademark rights
  - start using the slogan, name or logo in commerce (i.e., some kind of commercial use) and then subsequently file a trademark application
  - or
  - file an intent to use application which will lock in your filing date but which does not require immediate use

- Laws
  - U.S. Trademark Law

- Case
  - http://cyber.law.harvard.edu/property00/domain/SportyShort.html

Patents

- Definition
  - A patent is a proprietary right granted by the Federal government to an inventor who files a patent application with the United States Patent Office.

- Three types of patents
  - Utility patent
    - covers the functional aspects of products and processes
  - Design patent
    - covers the ornamental design of useful objects
  - Plant patent
    - covers a new variety of living plant

- Protect inventions and methods that exhibit patentable subject matter
  - http://www.pcmag.com/article2/0,1895,2125974,00.asp
Software Piracy

- Most common IP breaches involve software piracy
- Watchdog organizations investigate:
  - Software & Information Industry Association (SIIA)
  - Business Software Alliance (BSA)
- Enforcement of copyright has been attempted with technical security mechanisms

Compromise to Intellectual Property

- Copyright reminder

Compromise to Intellectual Property

- License Agreement Window

Espionage/Trespass

- Broad category of activities that breach confidentiality
- Unauthorized accessing of information
- Competitive intelligence vs. espionage
- Shoulder surfing, hidden camera, etc
- Controls implemented to mark the boundaries of an organization’s virtual territory giving notice to trespassers that they are encroaching on the organization’s cyberspace
Espionage/Trespass

- **What is a hacker?**
  - a person who illegally gains access to and sometimes tampers with information in a computer system
  - an expert at programming and solving problems with a computer

- Generally two skill levels among hackers:
  - **Expert hacker**
    - develops software scripts and codes exploits
    - usually a master of many skills
    - will often create attack software and share with others
  - **Script kiddies**
    - hackers of limited skill
    - use expert-written software to exploit a system
    - do not usually fully understand the systems they hack

- Other terms for system rule breakers:
  - **Cracker** - an individual who “cracks” or removes protection designed to prevent unauthorized duplication
  - **Phreaker** - hacks the public telephone network

Information Extortion

- Information extortion is an attacker or formerly trusted insider stealing information from a computer system and demanding compensation for its return or non-use

- Extortion found in credit card number theft

Technical Hardware Failures or Errors

- Technical hardware failures or errors occur when a manufacturer distributes to users equipment containing flaws
  - Intel Pentium II processor
  - These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability
  - Some errors are terminal, in that they result in the unrecoverable loss of the equipment
  - Some errors are intermittent, in that they only periodically manifest themselves, resulting in faults that are not easily repeated

Technical Software Failures or Errors

- This category of threats comes from purchasing software with unrevealed faults
  - Large quantities of computer code are written, debugged, published, and sold only to determine that not all bugs were resolved
  - Sometimes, unique combinations of certain software and hardware reveal new bugs
  - Sometimes, these items aren’t errors, but are purposeful shortcuts left by programmers for honest or dishonest reasons

Technological Obsolescence

- When the infrastructure becomes antiquated or outdated, it leads to unreliable and untrustworthy systems
  - Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity to threats and attacks
  - Ideally, proper planning by management should prevent the risks from technology obsolesce, but when obsolescence is identified, management must take action
Deliberate Act of Sabotage or Vandalism

- Individual or group who want to deliberately sabotage the operations of a computer system or business, or perform acts of vandalism to either destroy an asset or damage the image of the organization
- These threats can range from petty vandalism to organized sabotage
- Organizations rely on image so Web defacing can lead to dropping consumer confidence and sales
- Rising threat of hacktivist or cyber-activist operations – the most extreme version is cyber-terrorism

Deliberate Software Attacks

- When an individual or group designs software to attack systems, they create malicious code/software called malware
  - Designed to damage, destroy, or deny service to the target systems
- Mainly targeting Windows OS
  - http://stason.org/TULARC/os/linux.virus.html

Deliberate Software Attack

- Includes:
  - macro virus
  - boot virus
  - worms
  - Trojan horses
  - logic bombs
  - back door or trap door
  - denial-of-service attacks
  - polymorphic
  - hoaxes

Virus

- A virus is a computer program that copies itself from file to file and typically performs malicious or nuisance attacks on the infected system
  - Upon activation, copies its code into one or more larger programs
  - Hard to detect as well as hard to destroy or deactivate

Symptoms of Virus

- Computer runs slower then usual
- Computer no longer boots up
- Screen sometimes flicker
- PC speaker beeps periodically
- System crashes for no reason
- Files/directories sometimes disappear
- Denial of Service (DoS)
- Display some strange message on the screen

HI Virus

The HI virus was submitted in August, 1992. It is originally from Eastern Europe. HI is a memory resident infect of .EXE programs. When the first HI infected program is executed, the HI virus will install itself memory resident at the top of system memory but below the 640K DOS boundary, moving interrupt 12’s return. Total system and available free memory, as indicated by the DOS CHKDSK program, will have decreased by 1,024 bytes. Interrupt 21 will be hooked by the virus. Once the HI virus is memory resident, it will infect. EXE programs when they are executed. Infected programs will have a file length increase of 460 bytes with the virus being located at the end of the file. The program’s date and time in the DOS disk directory listing will have been updated to the current system date and time when infection occurred. The following text string can be found near the end of all infected programs: “HI”
Worms

- Spread over network connection
- Worms replicate
- First worm released on the Internet was called Morris worm, it was released on Nov 2, 1988.

Worms

- **Bubbleboy**
  - **Discovery Date:** 11/8/1999
  - **Origin:** Argentina (?)
  - **Length:** 4992
  - **Type:** Worm/Macro
  - **SubType:** VbScript
  - **Risk Assessment:** Low
  - **Category:** Stealth/Companion

- **How Bubbleboy works**
  - Bubbleboy is embedded within an email message of HTML format.
  - A VbScript while the user views a HTML page
  - A file named “Update.hta” is placed in the start up directory
  - Upon reboot Bubbleboy executes

- **How Bubbleboy works**
  - Changes the registered owner/organization
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RegisteredOwner = “Bubble Boy”
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RegisteredOrganization = “Vandalay Industry”
  - Using the Outlook MAPI address book it sends itself to each entry
  - Marks itself in the registry
    - HKEY_LOCAL_MACHINE\Software\Outlook\bubbleboy = “OUTLOOK.Bubbleboy1.0 by Zulu”

Trojan Horse

- A Trojan Horse is any program in which malicious or harmful code is contained inside of what appears to be a harmless program
- Malicious intent
  - Edit programs even registry information
  - Delete files
  - Set the computer as an FTP server
  - Obtain password
  - Spy
- Usually doesn’t reproduce
Trojan Horse

About Back Orifice
- requires Windows to work
- distributed by “Cult of the Dead Cow”
- similar to PC Anywhere, Carbon Copy software
- allows remote access and control of other computers
- install a reference in the registry
- once infected, runs in the background
- by default uses UDP port 54320
  TCP port 54321
- In Australia 72% of 92 ISP surveyed were infected with Back Orifice

Macro

Specific to certain applications
- Comprise a high percentage of the viruses
- Usually made in WordBasic and Visual Basic for Applications (VBA)
- Microsoft shipped “Concept”, the first macro virus, on a CD ROM called “Windows 95 Software Compatibility Test” in 1995

Melissa

Discovery Date: 3/26/1999
Origin: Newsgroup Posting
Length: varies depending on variant
Type: Macro/Worm
Subtype: Macro
Risk Assessment: High
Category: Companion
Macro

Melissa
- requires WSL, Outlook or Outlook Express Word 97 SR1 or Office 2000
- 105 lines of code (original variant)
- received either as an infected template or email attachment
- lowers computer defenses to future macro virus attacks
- may cause DoS
- infects template files with its own macro code
- 80% of the 150 Fortune 1000 companies were affected

Macro

How Melissa works
- the virus is activated through a MS word document
- document displays reference to pornographic websites while macro runs
- 1st lowers the macro protection security setting for future attacks
- checks to see if it has run in current session before
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Office\Melissa = "by Kwyjibo"
- propagates itself using the Outlook MAPI address book (emails sent to the first 50 addresses)

Macro

How Melissa works
- infects the Normal dot template file with its own code
- Lastly if the minutes of the hour match up to the date the macro inserts a quote by Bart Simpson into the current document
  - “Twenty two points, plus triple word score, plus fifty points for using all my letters. Game’s over. I’m outta here.”

Back Door/Trap Door

Payload of virus, worm, Trojan horse
- Allow the attacker to access the system at will with special privileges
- Back Orifice and Subseven

Polymorphism

Boot Virus

- Most difficult to remove
Logical Bomb

- “explosion” based on “logic”

Spyware: what is it?

- spyware is programming that is put in your computer to “spy” on you
- adware pushes ads, track Internet habits and performs other sneaky tricks

Spyware: how do you know when you have it?

- Computers slow down to a crawl
- Annoying Pop-ups appear
- Browser Start Page changes
- Unwanted toolbars, tray programs
- New programs are installed on your PC and show up on the desktop

Cases of Spyware Infection

Spybot in action
MALWARE BASED ATTACK

How bad guys get malware onto your computer?
How does malware spread from one computer to the whole network?

Web Browsing
- Attacker makes all Web content files infectious, so that users who browse to those pages become infected

Email

Network Space
- Unprotected share
- Public file server

P-2-P Download
- Attractive names
- Avril_latest_album.exe, …
W32/Netsky.p@MM

- Email propagation
  - The worm exploits the Incorrect MIME Header Can Cause IE to Execute E-Mail Attachment vulnerability in Microsoft Internet Explorer (ver 5.01 or 5.5 without SP2), to automatically execute the virus on vulnerable systems.
- P2P propagation
  - Emule, edonkey, kazaa, icq
  - Copy to the directory
    - 1001 Sex and more.rtf.exe, 3D Studio Max 6 3dsmax.exe, ACDSee 10.exe, Adobe Photoshop 10 crack.exe, Adobe Photoshop 10 full.exe, Ahead Nero 8.exe, Atkins Diet.doc.exe, American Idol.doc.exe, Arnold Schwarzenegger.jpg.exe, Best Matrix Screensaver new.scr, Britney sex xxx.jpg.exe, ...

Virus and Worm Hoaxes

A More Creative Way


Password-related Attacks

- Password Crack - Attempting to reverse calculate a password
- Brute Force - The application of computing and network resources to try every possible combination of options of a password
- Dictionary - The dictionary password attack narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords (the dictionary) to guide guesses

Brute Force Attack

Dictionary Attack
Spam

- Spam - unsolicited commercial e-mail - while many consider spam a nuisance rather than an attack, it is emerging as a vector for some attacks
- http://technology.timesonline.co.uk/tol/news/tech_and_web/article5598661.ece

Spam

- Spam - the number of spam emails MSN says it blocks daily
- $100bn: cost of computer repairs and lost productivity this year
- 71%: of email users filter spam
- 51%: of internet users say they have lost trust in email because of spam
- $5.5m: the amount MySpace won from TheGlobe.com in spam compensation in February

Spoofing

- Spoofing - technique used to gain unauthorized access whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host

DoS

- Denial-of-service (DoS) —
  - Attacks that prevent the system from processing or responding to legitimate traffic or requests from resources and objects
  - Most common form
    - attacker sends a large number of data packets to a target
    - Server cannot process them all
  - Other forms
    - exploiting a known fault or vulnerability in an operating system or application
    - often result in a system crash, or 100% CPU utilization

Possible consequences

- System crashes
- System reboots
- Data corruption
- Blockage of services

No known means by which DoS attack can be prevented

Normally impossible to trace back to the origin
DoS (Cont’d)

- Mail-bombing - an attacker routes large quantities of e-mail to the target

Example on How to Launch a DOS Attack

DDoS (Distributed Denial of Service)

- An attack in which a coordinated stream of requests is launched against a target from many locations at the same time

DRDoS (Distributed Reflective Denial of Service)

- Take advantage of the normal operation mechanisms of key Internet services
  - DNS, router update protocols, etc
- Used by the infamous “Mafia Boy” who took down cnn.com, yahoo.com, amazon.com and ebay.com

Other Forms of DoS

- Error in operating systems, services, and applications.
One Example of DoS Attack

- SYN flood attack

![Diagram of SYN flood attack]

Sniffer

- A program and/or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information from a network.

![Sniffer image]

Man-in-the-Middle Attack

- Man-in-the-Middle - an attacker sniffs packets from the network, modifies them, and inserts them back into the network.

![Diagram of Man-in-the-Middle Attack]

Attack Descriptions

- Buffer Overflow:
  - Application error occurs when more data is sent to a buffer than it can handle.
  - When the buffer overflows, the attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure.

![Diagram of Buffer Overflow]
Social Engineering

- The process of using social skills to convince people to reveal access credentials or other valuable information to the attacker

Attack Descriptions

- “People are the weakest link”

Phishing in Action (HSBC)
Pharming Out-Scams Phishing

First came Phishing, in which con artists hooked unwary Internet users one by one into compromising their personal data

Pharmers
can scoop up many victims
in a single pass

What is Pharming?

New use for a relatively old concept: domain spoofing

Pharmers
simply redirect as many users as possible from legitimate commercial websites to malicious ones

Pharming most alarming threat

DNS poisoning
Large group of users to be silently shuttled to a bogus website even when typing in the correct URL
You no longer have to click a URL link to hand over your information to identity thieves

Certificate Mismatch

Industry Approach - Phishing

- Based on social engineering – Self defense relies on common sense of the user
- The automated detection of new Phishing fraud is very difficult
- Only an extensive forensic analysis by law enforcement can prove the evidence of Phishing
- Try to mitigate by
  - URL blocking of known URLs of Phishing websites
  - Spam blocking of emails of Phishing scams that are sent en mass
Industry Approach - Pharming

- Browsers that could authenticate website identity. (CardSpace, OpenID)
- Browser toolbars displaying the true physical location of a website's host (e.g. Russia)
- Some financial institutions are experimenting with "multi-factor authentication" logins, including:
  - single-use passwords (e.g. tokens)
  - automatic telephone call-backs

Security Recommendations

- Do not open e-mail attachments unless you know the source and are expecting the attachment
- Do not reply to the e-mail from an unknown source
- Do not click on entrusted hyperlinks to the Internet
- Do not download unapproved software from the Internet
- Do not respond or visit the website indicated by an instant message or e-mail
- Do not give out personal information over the Internet
- Before revealing any identifying information, ask how it will be used and secured.

Brick Attack

- “People are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything.” — Kevin Mitnick

Timing Attack

- Timing Attack –
  - relatively new
  - works by exploring the contents of a web browser's cache
  - can allow collection of information on access to password-protected sites
  - another attack by the same name involves attempting to intercept cryptographic elements to determine keys and encryption algorithms

Legal Attack

- Attacks that use the legal system
- Persuade a judge and jury that there could be a flaw in the system.