Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Enlightening Technical Minds Estd. 1998
An Autonomous Institution
(Since 2011)

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Affiliated to Anna University, Chennai; Approved by AICTE ; Accredited by NAAC with Grade 'A++'
Accredited by NBA - Tier1 (Mech, Auto, Civil, EEE, ECE, E&I and CSE)
Udumalai Road, Pollachi - 642 003. Tel: 04259-236030/40/50 Fax: 04259-236070 www.mcet.in

19ITOC1004 – Cyber Law and Information Security

Unit V -Security Investigation

CO5: Explain the secure application development using information security

LO1:Explain about the need for security.

SO1: Identify the business needs in information security.

Prepared by

G. Keerthika

AP/IT

Unit V -Security Investigation

Need for Security - Business Needs - Threats - Secure Software Development – Law and Ethical in Information Security - International Laws and Laws Bodies - Ethics and Information Security

Need for Security

- The primary mission of an information security program is to ensure that systems and their contents remain the same.
- Organizations expend hundreds of thousands of dollars and thousands of man-hours to maintain their information systems.
- If threats to information and systems didn't exist, these resources could be used to improve the systems that support the information.
- However, attacks on information systems are a daily occurrence, and the need for information security grows along with the sophistication of such attacks.
- Organizations must understand the environment in which information systems operate so that their information security programs can address actual and potential problems

Business Needs

Information security performs four important functions for an organization:

1. Protecting the organization's ability to function

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

3. Protecting the data that the organization collects and uses

4. Safeguarding the organization's technology assets

Protecting the organization's ability to function

- Both general management and IT management are responsible for implementing information security that protects the organization's ability to function.
- Although many business and government managers shy away from addressing information security because they perceive it to be a technically complex task, in fact, implementing information security has more to do with management than with technology.
- Just as managing payroll has more to do with management than with mathematical wage computations, managing information security has more to do with policy and its enforcement than with the technology of its implementation.
- Each of an organization's communities of interest must address information security in terms of business impact and the cost of business interruption, rather than isolating security as a technical problem.

Enabling the safe operation of applications

- Today's organizations are under immense pressure to acquire and operate integrated, efficient, and capable applications.
- A modern organization needs to create an environment that safeguards these applications, particularly those that are important elements of the organization's infrastructure—operating system platforms, electronic mail (e-mail), and instant messaging (IM) applications.
- Organizations acquire these elements from a service provider or they build their own.
- Once an organization's infrastructure is in place, management must continue to oversee it, and not relegate its management to the IT department.

Protecting the data that the organization collects and uses

- Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers.
- Any business, educational institution, or government agency operating within the modern context of connected and responsive services relies on information systems.
- Even when transactions are not online, information systems and the data they process enable the creation and movement of goods and services.
- Therefore, protecting *data in motion* and *data at rest* are both critical aspects of information security. The value of data motivates attackers to steal, sabotage, or corrupt it.
- An effective information security program implemented by management protects the integrity and value of the organization's data.

Safeguarding the organization's technology assets

- To perform effectively, organizations must employ secure infrastructure services appropriate to the size and scope of the enterprise.
- For instance, a small business may get by using an e-mail service provided by an ISP and augmented with a personal encryption tool.
- When an organization grows, it must develop additional security services.
- For example, organizational growth could lead to the need for public key infrastructure (PKI), an integrated system of software, encryption methodologies, and legal agreements that can be used to support the entire information infrastructure.

Safeguarding the organization's technology assets

- PKI involves the use of digital certificates to ensure the confidentiality of Internet communications and transactions.
- Into each of these digital certificates, a certificate authority embeds an individual's or an organization's public encryption key, along with other identifying information.
- Then cryptographically signs the certificate with a tamper-proof seal, thus verifying the integrity of the data within the certificate and validating its use.

References

Text Book(s): Michael E Whitman and Herbert J Mattord, —Principles of Information Security||, Cengage Learning, 2018. (Unit IV, V)

Reference Book(s):

Matt Bishop, —"Computer Security Art and Science", Pearson/PHI, 2018.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Enlightening Technical Minds Estd. 1998
An Autonomous Institution
(Since 2011)

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Affiliated to Anna University, Chennai; Approved by AICTE ; Accredited by NAAC with Grade 'A++'
Accredited by NBA - Tier1 (Mech, Auto, Civil, EEE, ECE, E&I and CSE)
Udumalai Road, Pollachi - 642 003. Tel: 04259-236030/40/50 Fax: 04259-236070 www.mcet.in

19ITOC1004 – Cyber Law and Information Security

Unit V -Security Investigation

CO5: Explain the secure application development using information security

LO1:Explain about the need for security.

SO2:Explain about threats.

Prepared by

G. Keerthika

AP/IT

Unit V -Security Investigation

Need for Security - Business Needs - Threats - Secure Software Development – Law and Ethical in Information Security - International Laws and Laws Bodies - Ethics and Information Security

Threat

A threat is an object, person, or other entity that presents an ongoing danger to an asset.

	Category of Threat	Examples
1.	Compromises to intellectual property	Piracy, copyright infringement
2.	Software attacks	Viruses, worms, macros, denial of service
3.	Deviations in quality of service	ISP, power, or WAN service issues from service providers
4.	Espionage or trespass	Unauthorized access and/or data collection
5.	Forces of nature	Fire, flood, earthquake, lightning
6.	Human error or failure	Accidents, employee mistakes
7.	Information extortion	Blackmail, information disclosure
8.	Missing, inadequate, or incomplete	Loss of access to information systems due to disk drive failure without proper backup and recovery plan organizational policy or planning in place
9.	Missing, inadequate, or incomplete controls	Network compromised because no firewall security controls
10.	Sabotage or vandalism	Destruction of systems or information
11.	Theft	Illegal confiscation of equipment or information
12.	Technical hardware failures or errors	Equipment failure
13.	Technical software failures or errors	Bugs, code problems, unknown loopholes
14.	Technological obsolescence	Antiquated or outdated technologies

Compromises to Intellectual Property

- Intellectual property is defined as “the ownership of ideas and control over the tangible or virtual representation of those ideas.
- Use of another person’s intellectual property may or may not involve royalty payments or permission, but should always include proper credit to the source.
- Intellectual property can be trade secrets, copyrights, trademarks, and patents.
- The unauthorized appropriation of IP constitutes a threat to information security.
- Employees may have access privileges to the various types of IP, and may be required to use the IP to conduct day-to-day business.
- Organizations often purchase or lease the IP of other organizations, and must abide by the purchase or licensing agreement for its fair and responsible use.
- The most common IP breach is the unlawful use or duplication of software-based intellectual property, more commonly known as software piracy.

Deliberate Software Attacks

- Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. Most of this software is referred to as **malicious code** or **malicious software**,or sometimes **malware.**
- These software components or programs are designed to damage, destroy, or deny service to the target systems.
- Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic bombs, and back doors.

Virus:

- A computer **virus** consists of segments of code that perform malicious actions.
- The code attaches itself to an existing program and takes control of that program's access to the targeted computer.
- The virus-controlled target program then carries out the virus's plan by replicating itself into additional targeted systems.
- Opening infected e-mail or some other seemingly trivial action can cause anything from random messages popping up on a user's screen to the complete destruction of entire hard drives of data.
- Among the most common types of information system viruses are the **macro virus**, which is embedded in automatically executing macro code used by word processors, spread sheets, and database applications, and the boot virus, which infects the key operating system files located in a computer's boot sector.

Worms

- **worm** is a malicious program that replicates itself constantly, without requiring another program environment.
- Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.
- Code Red, Sircam, Nimda and Klez are examples of a class of worms that combines multiple modes of attack into a single package.
- The complex behavior of worms can be initiated with or without the user downloading or executing the file. Once the worm has infected a computer, it can redistribute itself to all e-mail addresses found on the infected system.
- Furthermore, a worm can deposit copies of itself onto all Web servers that the infected system can reach, so that users who subsequently visit those sites become infected.

Trojan horses

- Trojan horses are software programs that hide their true nature and reveal their designed behavior only when activated.
- Trojan horses are frequently disguised as helpful, interesting, or necessary pieces of software, such as readme.exe files often included with shareware or freeware packages.
- once Trojan horses are brought into a system, they become activated and can wreak havoc on the unsuspecting user.

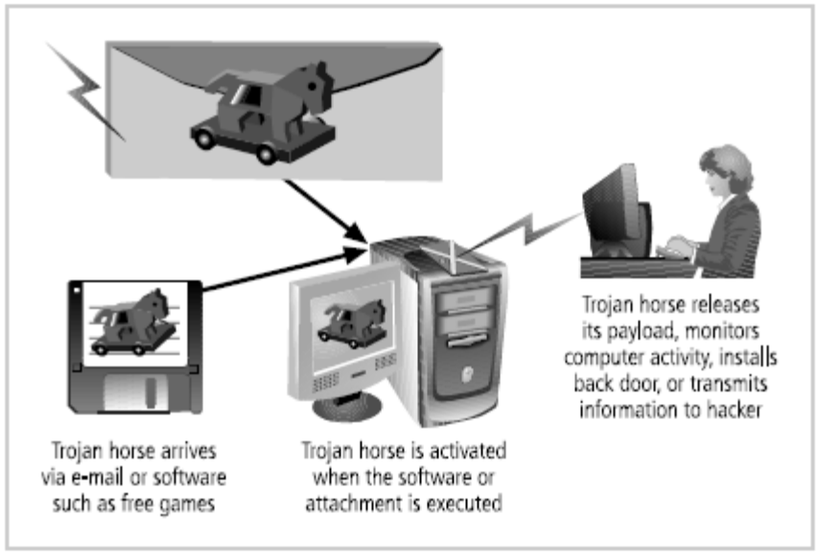


Figure 2-4 Trojan Horse Attack

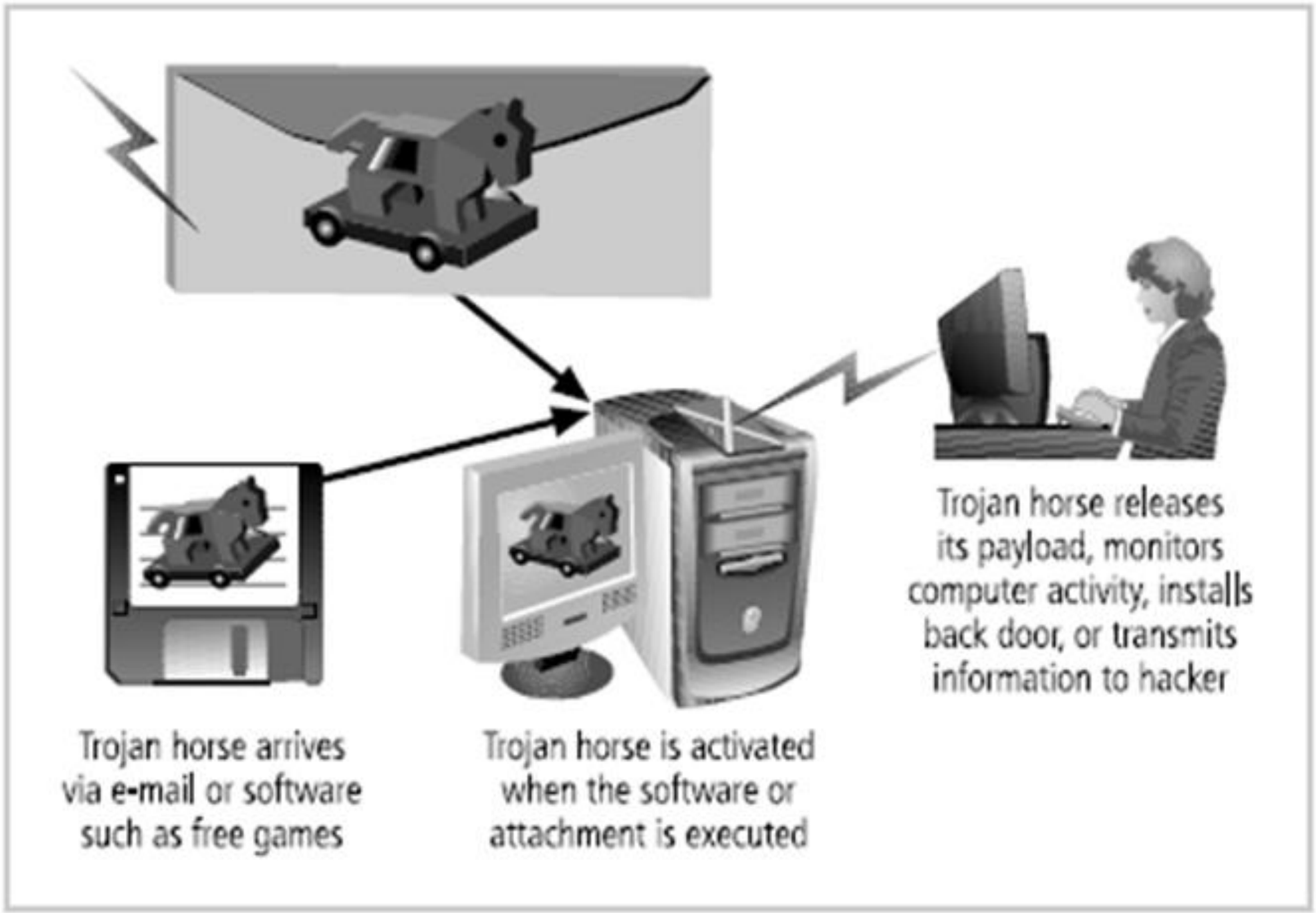


Figure 2-4 Trojan Horse Attack

Back Door or Trap Door:

- A virus or worm can have a payload that installs a **back door** or **trap door** component in a system, which allows the attacker to access the system at will with special privileges.
- Examples of these kinds of payloads include Sub seven and Back Orifice.

Polymorphic Threats :

- One of the biggest challenges to fighting viruses and worms has been the emergence of polymorphic threats.
- A **polymorphic threat** is one that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures.
- These viruses and worms actually evolve, changing their size and other external file characteristics to elude detection by antivirus software programs.

Virus and Worm Hoaxes

- As frustrating as viruses and worms are, perhaps more time and money is spent on resolving virus hoaxes.
- Well-meaning people can disrupt the harmony and flow of an organization when they send group e-mails warning of supposedly dangerous viruses that don't exist.
- When people fail to follow virus-reporting procedures, the network becomes overloaded, and much time and energy is wasted as users forward the warning message to everyone they know, post the message on bulletin boards, and try to update their antivirus protection software.

Deviations in Quality of Services

- An organization's information system depends on the successful operation of many interdependent support systems, including power grids, telecom networks, parts suppliers, service vendors, and even the janitorial staff and garbage haulers.
- Irregularities in Internet service, communications, and power supplies can dramatically affect the availability of information and systems.

Internet Service Issues:

- In organizations that rely heavily on the Internet and the World Wide Web to support continued operations, Internet service provider failures can considerably undermine the availability of information.
- Many organizations have sales staff and telecommuters working at remote locations. When these offsite employees cannot contact the host systems, they must use manual procedures to continue operations.

- The Web hosting services are usually arranged with an agreement providing minimum service levels known as a **Service Level Agreement (SLA)**.
- When a service provider fails to meet the SLA, the provider may accrue fines to cover losses incurred by the client, but these payments seldom cover the losses generated by the outage.

Communications and Other Service Provider Issues

- Other utility services can affect organizations as well. Among these are telephone, water, wastewater, trash pickup, cable television, natural or propane gas, and custodial services.
- The loss of these services can impair the ability of an organization to function.

Power Irregularities

- When voltage levels spike (experience a momentary increase), or surge (experience a prolonged increase), the extra voltage can severely damage or destroy equipment.
- A momentary low voltage or sag, or a more prolonged drop in voltage, known as a brownout, can cause systems to shut down or reset, or otherwise disrupt availability.
- Complete loss of power for a moment is known as a fault, and a more lengthy loss as a blackout.
- The more expensive uninterruptible power supply (UPS) can protect against spikes and surges as well as against sags and even blackouts of limited duration.

Espionage or Trespass

Espionage or trespass is a well-known and broad category of electronic and human activities that can breach the confidentiality of information.

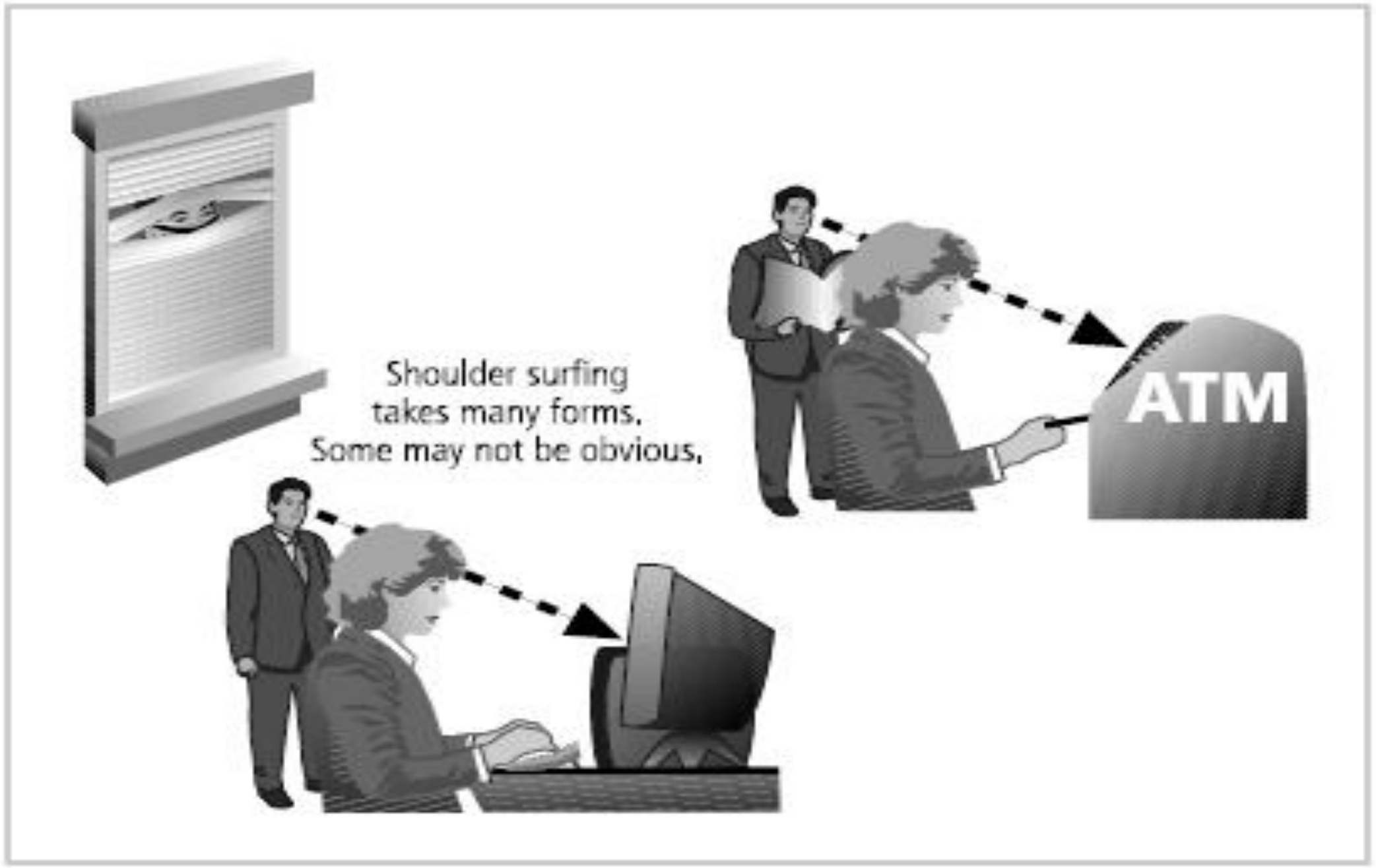
When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as espionage or trespass.

Attackers can use many different methods to access the information stored in an information system. Some information gathering techniques are quite legal, for example, using a Web browser to perform market research.

These legal techniques are called, collectively, competitive intelligence. When information gatherers employ techniques that cross the threshold of what is legal or ethical, they are conducting industrial espionage.

Espionage or Trespass(contd…)

- One example is shoulder surfing



Forces of Nature

- Fire
- Flood
- Earthquake
- Lightning
- Landslide or Mudslide
- Tornado or severe windstrome
- Hurricane or typhoon
- Tsunami
- Electrostatic Discharge
- Dust Contamination

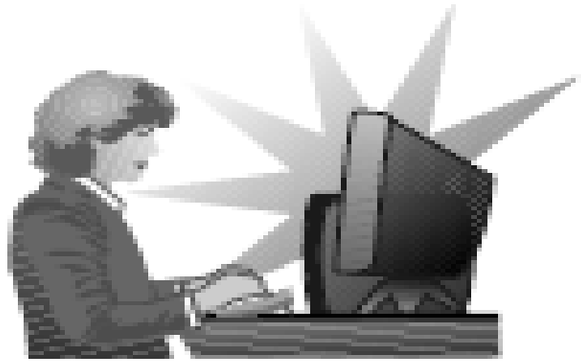
Human error or Failure

- This category includes acts performed without intent or malicious purpose by an authorized user. When people use information systems, mistakes happen.
- Inexperience, improper training, and the incorrect assumptions are just a few things that can cause these misadventures.
- Regardless of the cause, even innocuous mistakes can produce extensive damage.
- One of the greatest threats to an organization's information security is the organization's own employees. Employees are the threat agents closest to the organizational data.
- Because employees use data in everyday activities to conduct the organization's business, their mistakes represent a serious threat to the confidentiality, integrity, and availability of data

Who is the biggest threat to your organization?

Tom Twostory
convicted burglar

Dick Davis a.k.a.
"wannabe amateur hacker"



Harriet Allthumbs
employee
accidentally
deleted the one copy
of a critical report

Figure 2-8 Acts of Human Error or Failure

Information extortion

- Information extortion occurs when an attacker or trusted insider steals information from a computer system and demands compensation for its return or for an agreement not to disclose it.
- Extortion is common in credit card number theft.
- The culprit was a Russian hacker named Maxus, who hacked the online vendor and stole several hundred thousand credit card numbers.
- When the company refused to pay the $100,000 blackmail, he posted the card numbers to a Web site, offering them to the criminal community.

Missing, Inadequate, or Incomplete Controls

- Missing, inadequate, or incomplete controls—that is, security safeguards and information asset protection controls that are missing, misconfigured, antiquated, or poorly designed or managed—make an organization more likely to suffer losses when other threats lead to attacks.
- For example, if a small organization installs its first network using small office/home office (SOHO) equipment and fails to upgrade its network equipment as it becomes larger, the increased traffic can affect performance and cause information loss.
- Routine security audits to assess the current levels of protection help to ensure the continuous protection of organization's assets.

Sabotage or Vandalism

- This category of threat involves the deliberate sabotage of a computer system or business, or acts of vandalism to either destroy an asset or damage the image of an organization.
- These acts can range from petty vandalism by employees to organized sabotage against an organization.
- Although not necessarily financially devastating, attacks on the image of an organization are serious.
- Vandalism to a Web site can erode consumer confidence, thus diminishing an organization's sales and net worth, as well as its reputation.
- Compared to Web site defacement, vandalism within a network is more malicious in intent and less public.
- Today, security experts are noticing a rise in another form of online vandalism, hacktivist or cyberactivist operations, which interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency.
- Cyberterrorists hack systems to conduct terrorist activities via network or Internet pathways.
- The United States and other governments are developing security measures intended to protect the critical computing and communications networks as well as the physical and power utility infrastructures.

Theft

- The threat of theft—the illegal taking of another's property, which can be **physical, electronic, or intellectual**—is a constant.
- The value of information is diminished when it is copied without the owner's knowledge.
- Physical theft can be controlled quite easily by means of a wide variety of measures, from locked doors to trained security personnel and the installation of alarm systems.
- Electronic theft, however, is a more complex problem to manage and control.
- When someone steals a physical object, the loss is easily detected; if it has any importance at all, its absence is noted.

Technical Hardware Failures or Errors

- Technical hardware failures or errors occur when a manufacturer distributes equipment containing a known or unknown flaw. These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability.
- Some errors are terminal—that is, 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, and thus, equipment can sometimes stop working, or work in unexpected ways.

Technical Software Failures or Errors

- Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved.
- Sometimes, combinations of certain software and hardware reveal new bugs. These failures range from bugs to untested failure conditions.
- Sometimes these bugs are not errors, but rather purposeful shortcuts left by programmers for benign or malign reasons.
- Collectively, shortcut access routes into programs that bypass security checks are called trap doors and can cause serious security breaches.
- Software bugs are so commonplace that entire Web sites are dedicated to documenting them.
- Among the most often used is Bugtraq, found at www.securityfocus.com, which provides up-to-the-minute information on the latest security vulnerabilities, as well as a very thorough archive of past bugs.

Technological Obsolescence

- Antiquated or outdated infrastructure can lead to unreliable and untrustworthy systems.
- Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity from attacks.
- Management's strategic planning should always include an analysis of the technology currently in use.
- Recently, the software vendor Symantec retired support for a legacy version of its popular antivirus software, and organizations interested in continued product support were obliged to upgrade immediately to a different antivirus control software.

References

Text Book(s): Michael E Whitman and Herbert J Mattord, —Principles of Information Security||, Cengage Learning, 2018. (Unit IV, V)

Reference Book(s):

Matt Bishop, —"Computer Security Art and Science", Pearson/PHI, 2018.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Enlightening Technical Minds Estd. 1998
An Autonomous Institution
(Since 2011)

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Affiliated to Anna University, Chennai; Approved by AICTE ; Accredited by NAAC with Grade 'A++'
Accredited by NBA - Tier1 (Mech, Auto, Civil, EEE, ECE, E&I and CSE)
Udumalai Road, Pollachi - 642 003. Tel: 04259-236030/40/50 Fax: 04259-236070 www.mcet.in

19ITOC1004 – Cyber Law and Information Security

Unit V -Security Investigation

CO5: Explain the secure application development using information security

LO1:Explain about the need for security.

SO3:Explain about secure software development

Prepared by

G. Keerthika

AP/IT

Unit V -Security Investigation

Need for Security - Business Needs - Threats - Secure Software Development – Law and Ethical in Information Security - International Laws and Laws Bodies - Ethics and Information Security

Secure Software Development

- Systems consist of hardware, software, networks, data, procedures, and people using the system.
- Many of the information security issues have their root cause in the software elements of the system. Secure systems require secure, or at least securable, software.
- The development of systems and the software they use is often accomplished using a methodology, such as the systems development life cycle (SDLC).
- Many organizations recognize the need to include planning for security objectives in the SDLC they use to create systems, and have put in place procedures to create software that is more able to be deployed in a secure fashion.
- This approach to software development is known as software assurance, or SA.

Software Assurance and the SA Common Body of Knowledge

A working group drawn from industry, government, and academia was formed to examine two key questions:

1. What are the engineering activities or aspects of activities that are relevant to achieving

secure software?

2. What knowledge is needed to perform these activities or aspects?

Software Assurance and the SA Common Body of Knowledge

The SwA CBK(Secure Software Assurance (SwA) Common Body of Knowledge), which is a work in progress, contains the following sections:

- Nature of Dangers
- Fundamental Concepts and Principles
- Ethics, Law, and Governance
- Secure Software Requirements
- Secure Software Design
- Secure Software Construction
- Secure Software Verification, Validation, and Evaluation
- Secure Software Tools and Methods
- Secure Software Processes
- Secure Software Project Management
- Acquisition of Secure Software
- Secure Software Sustainment

Software Design Principles

- Good software development should result in a finished product that meets all of its designspecifications.
- Information security considerations are a critical component of those specifications, though that has not always been true.

security principles:

Economy of mechanism: Keep the design as simple and small as possible.

Fail-safe defaults: Base access decisions on permission rather than exclusion.

Complete mediation: Every access to every object must be checked for authority.

Open design: The design should not be secret, but rather depend on the possession of keys or passwords.

Security principles

- **Separation of privilege:** Where feasible, a protection mechanism should require two keys to unlock, rather than one.
- **Least privilege:** Every program and every user of the system should operate using the least set of privileges necessary to complete the job.
- **Least common mechanism:** Minimize mechanisms (or shared variables) common to more than one user and depended on by all users.
- **Psychological acceptability:** It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

Buffer Overruns

- Buffers are used to manage mismatches in the processing rates between two entities involved in a communication process.
- A buffer overrun (or buffer overflow) is an application error that occurs when more data is sent to a program buffer than it is designed to handle.
- During a buffer overrun, an attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure.
- Sometimes this is limited to a denial-of-service attack. In any case, data on the attacked system loses integrity.

Command Injection

- Command injection problems occur when user input is passed directly to a compiler or interpreter.
- The underlying issue is the developer's failure to ensure that command input is validated before it is used in the program.
- Perhaps the simplest example involves the Windows command shell:

```
@echo off
set /p myVar="Enter the string>"
set someVar=%myVar%
echo %somevar%
```

Cross-site Scripting

- Cross site scripting (or XSS) occurs when an application running on a Web server gathers data from a user in order to steal it.
- An attacker can use weaknesses in the Web server environment to insert commands into a user's browser session, so that users ostensibly connected to a friendly Web server are, in fact, sending information to a hostile server.
- This allows the attacker to acquire valuable information, such as account credentials, account numbers, or other critical data.
- Often an attacker encodes a malicious link and places it in the target server, making it look less suspicious.
- After the data is collected by the hostile application, it sends what appears to be a valid response from the intended server.

Failure to Handle Errors

- What happens when a system or application encounters an scenario that it is not prepared to handle?
- Does it attempt to complete the operation (reading or writing data or performing calculations)?
- Does it issue a cryptic message that only a programmer could understand?
- Does it simply stop functioning?
- Failure to handle errors can cause a variety of unexpected system behaviors.
- Programmers are expected to anticipate problems and prepare their application code to handle them.

Failure to Protect Network Traffic

- With the growing popularity of wireless networking comes a corresponding increase in the risk that wirelessly transmitted data will be intercepted.
- Most wireless networks are installed and operated with little or no protection for the information that is broadcast between the client and the network wireless access point.
- This is especially true of public networks found in coffee shops, bookstores, and hotels. Without appropriate encryption (such as that afforded by WPA), attackers can intercept and view your data.
- Traffic on a wired network is also vulnerable to interception in some situations. On networks using hubs instead of switches, any user can install a packet sniffer and collect communications to and from users on that network.
- Periodic scans for unauthorized packet sniffers, unauthorized connections to the network, and general awareness of the threat can mitigate this problem.

Failure to Store and Protect Data Securely

- Storing and protecting data securely is a large enough issue to be the core subject of this entire text.
- Programmers are responsible for integrating access controls into, and keeping secret information out of, programs.
- Access controls, the subject of later chapters, regulate who, what, when, where, and how individuals and systems interact with data.
- Failure to properly implement sufficiently strong access controls makes the data vulnerable.
- Overly strict access controls hinder business users in the performance of their duties, and as a result the controls may be administratively removed or bypassed.

Failure to Use Cryptographically Strong Random Numbers

- Most modern cryptosystems, like many other computer systems, use random number generators.
- However, a decision support system using random and pseudo-random numbers for Monte Carlo method forecasting does not require the same degree of rigor and the same need for true randomness as a system that seeks to implement cryptographic procedures.
- These “random” number generators use a mathematical algorithm, based on a seed value and another other system component (such as the computer clock) to simulate a random number.
- Those who understand the workings of such a “random” number generator can predict particular values at particular times.

Format String Problems

- Computer languages often are equipped with built-in capabilities to reformat data while they're outputting it.
- The formatting instructions are usually written as a "format string." Unfortunately, some programmers may use data from untrusted sources as a format string.
- An attacker may embed characters that are meaningful as formatting directives (e.g., %x, %d, %p, etc.) into malicious input.
- If this input is then interpreted by the program as formatting directives (such as an argument to the C printf function), the attacker may be able to access information or overwrite very targeted portions of the program's stack with data of the attacker's choosing.

Neglecting Change Control

- Developers use a process known as change control to ensure that the working system delivered to users represents the intent of the developers.
- Early in the development process, change control ensures that developers do not work at cross purposes by altering the same programs or parts of programs at the same time.
- Once the system is in production, change control processes ensure that only authorized changes are introduced and that all changes are adequately tested before being released.

Improper File Access

- If an attacker changes the expected location of a file by intercepting and modifying a program code call, the attacker can force a program to use files other than the ones the program is supposed to use.
- This type of attack could be used to either substitute a bogus file for a legitimate file (as in password files), or trick the system into running a malware executable.
- The potential for damage or disclosure is great, so it is critical to protect not only the location of the files but also the method and communications channels by which these files are accessed.

Improper Use of SSL

- Programmers use Secure Sockets Layer (SSL) to transfer sensitive data, such as credit card numbers and other personal information, between a client and server.
- While most programmers assume that using SSL guarantees security, unfortunately they more often than not mishandle this technology.
- SSL and its successor, Transport Layer Security (TLS), both need certificate validation to be truly secure.
- Failure to use Hypertext Transfer Protocol Secure (HTTPS), to validate the certificate authority and then validate the certificate itself, or to validate the information against a certificate revocation list (CRL), can compromise the security of SSL traffic.

Information Leakage

- One of the most common methods of obtaining inside and classified information is directly or indirectly from an individual, usually an employee.
- The World War II military poster warned that “loose lips sink ships,” emphasizing the risk to naval deployments from enemy attack should the sailors, marines, or their families disclose the movements of these vessels.
- It was a widely-shared fear that the enemy had civilian operatives waiting in bars and shops at common Navy ports of call, just waiting for the troops to drop hints about where they were going and when.
- By warning employees against disclosing information, organizations can protect the secrecy of their operation.

Integer Bugs (Overflows/Underflows)

- Although paper and pencil can deal with arbitrary numbers of digits, the binary representations used by computers are of a particular fixed length.
- For example, adding 1 to 32,767 should produce 32,768, but in computer arithmetic with 16-bit signed integers, the result is –32,768.
- An underflow can occur when, for example, you subtract 5 from negative 32,767, which returns the incorrect result +32,764, because the largest negative integer that can be represented in 16 bits is negative 32,768.

Race Conditions

- A race condition is a failure of a program that occurs when an unexpected ordering of events in the execution of the program results in a conflict over access to the same system resource.
- This conflict does not need to involve streams of code inside the program, since current operating systems and processor technology automatically break a program into multiple threads that can be executed simultaneously.
- If the threads that result from this process share any resources, they may interfere with each other.
- A race condition occurs, when a program creates a temporary file, and an attacker is able to replace it between the time it is created and the time it is used.
- A race condition can also occur when information is stored in multiple memory threads if one thread stores information in the wrong memory location, by accident or intent.

SQL Injection

- SQL injection occurs when developers fail to properly validate user input before using it to query a relational database.
- For example, a fairly innocuous program fragment expects the user to input a user ID and then perform a SQL query against the USERS table to retrieve the associated name:

  Accept USER-ID from console;

  SELECT USERID, NAME FROM USERS WHERE USERID = USER-ID;

- This is very straightforward SQL syntax and, when used correctly, displays the userid and name.
- The problem is that the string accepted from the user is passed directly the SQL database server as part of the SQL command. What if an attacker enters the string “JOE OR 1=1”?
- This string includes some valid SQL syntax that will return all rows from the table where either the user id is “JOE” or “1=1.” Since one is always equal to one, the system returns all user ids and names.
- The possible effects of this “injection” of SQL code of the attacker’s choosing into the program are not limited to improper access to information.

Trusting Network Address Resolution

- The Domain Name System (DNS) is a function of the World Wide Web that converts a URL (Uniform Resource Locator) like www.course.com into the IP address of the Web server host.
- This distributed model is vulnerable to attack or “poisoning.”
- DNS cache poisoning involves compromising a DNS server and then changing the valid IP address associated with a domain name into one which the attacker chooses.
- usually a fake Web site designed to obtain personal information or one that accrues a benefit to the attacker, for example, redirecting shoppers from a competitor’s Web site.
- It is usually more sinister, for example, a simulated banking site used for a phishing attack that harvests online banking information.

Unauthenticated Key Exchange

- One of the biggest challenges in private key systems, which involve two users sharing the same key, is securely getting the key to the other party.
- Sometimes an “out of band” courier is used, but other times a public key system, which uses both a public and private key, is used to exchange the key.
- But what if the person who receives a key that was copied onto a USB device and shipped doesn’t really work for the company, but was simply expecting that particular delivery and intercepted it.
- The same scenario can occur on the Internet, where an attacker writes a variant of a public key system and places it out as “freeware,” or corrupts or intercepts the function of someone else’s public key encryption system, perhaps by posing as a public key repository.

Use of Magic URLs and Hidden Forms

- HTTP is a stateless protocol where the computer programs on either end of the communication channel cannot rely on a guaranteed delivery of any message.
- This makes it difficult for software developers to track a user's exchanges with a Web site over multiple interactions.
- Too often sensitive state information is simply included in a "magic" URL (for example, the authentication ID is passed as a parameter in the URL for the exchanges that will follow) or included in hidden form fields on the HTML page.
- If this information is stored as plain text, an attacker can harvest the information from a magic URL as it travels across the network, or use scripts on the client to modify information in hidden form fields.
- Depending on the structure of the application, the harvested or modified information can be used in spoofing or hijacking attacks, or to change the way the application operates

Use of Weak Password-Based Systems

- Failure to require sufficient password strength, and to control incorrect password entry, is a serious security issue.
- Password policy can specify the number and type of characters, the frequency of mandatory changes, and even the reusability of old passwords.
- Similarly, a system administrator can regulate the permitted number of incorrect password entries that are submitted and further improve the level of protection.
- Systems that do not validate passwords, or store passwords in easy-to-access locations, are ripe for attack.

References

Text Book(s): Michael E Whitman and Herbert J Mattord, —Principles of Information Security||, Cengage Learning, 2018. (Unit IV, V)

Reference Book(s):

Matt Bishop, —"Computer Security Art and Science", Pearson/PHI, 2018.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Enlightening Technical Minds Estd. 1998
An Autonomous Institution
(Since 2011)

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Affiliated to Anna University, Chennai; Approved by AICTE ; Accredited by NAAC with Grade 'A++'
Accredited by NBA - Tier1 (Mech, Auto, Civil, EEE, ECE, E&I and CSE)
Udumalai Road, Pollachi - 642 003. Tel: 04259-236030/40/50 Fax: 04259-236070 www.mcet.in

19ITOC1004 – Cyber Law and Information Security

Unit V -Security Investigation

CO5: Explain the secure application development using information security

LO1:To learn about laws and ethics in information security

SO2: Explain about laws and ethics in information security.

Prepared by

G. Keerthika

AP/IT

Unit V -Security Investigation

Need for Security - Business Needs - Threats - Secure Software Development – Law and Ethics in Information Security - International Laws and Laws Bodies - Ethics and Information Security

Law and Ethical in Information Security

- The rules the members of a society create to balance the individual rights to self-determination against the needs of the society as a whole are called *laws*.
- **Laws** are rules that mandate or prohibit certain behavior; they are drawn from ethics, which define socially acceptable behaviors.
- The key difference between laws and ethics is that laws carry the authority of a governing body, and ethics do not.
- Ethics in turn are based on **cultural mores**-the fixed moral attitudes or customs of a particular group.

Organizational Liability and the Need for Counsel

- Liability is the legal obligation of an entity that extends beyond criminal or contract law; it includes the legal obligation to make restitution, or to compensate for wrongs committed.
- An organization increases its liability if it refuses to take measures known as due care.
- **Due care** standards are met when an organization makes sure that every employee knows what is acceptable or unacceptable behavior, and knows the consequences of illegal or unethical actions.
- **Due diligence** requires that an organization make a valid effort to protect others and continually maintains this level of effort.

Policy versus Law

- Within an organization, information security professionals help maintain security via the establishment and enforcement of policies.
- These policies—guidelines that describe acceptable and unacceptable employee behaviors in the workplace—function as organizational laws, complete with penalties, judicial practices, and sanctions to require compliance.
- Because these policies function as laws, they must be crafted and implemented with the same care to ensure that they are complete, appropriate, and fairly applied to everyone in the workplace.

Five criteria:

Dissemination (distribution)—The organization must be able to demonstrate that the relevant policy has been made readily available for review by the employee.

Common dissemination techniques include hard copy and electronic distribution.

Review (reading)—The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non-English reading, and reading-impaired employees.

Common techniques include recordings of the policy in English and alternate languages.

Comprehension (understanding)—The organization must be able to demonstrate that the employee understood the requirements and content of the policy.

Common techniques include quizzes and other assessments.

Five criteria(contd...)

- **Compliance (agreement)—**The organization must be able to demonstrate that the employee agreed to comply with the policy through act or affirmation.
- Common techniques include logon banners, which require a specific action (mouse click or keystroke) to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.
- **Uniform enforcement—**The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

Types of Law

- **Civil law** comprises a wide variety of laws that govern a nation or state and deal with the relationships and conflicts between organizational entities and people.
- **Criminal law** addresses activities and conduct harmful to society, and is actively enforced by the state.
- Law can also be categorized as **private or public**.
- **Private law** encompasses family law, commercial law, and labor law, and regulates the relationship between individuals and organizations.
- **Public law** regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments.
- Public law includes criminal, administrative, and constitutional law.

References

Text Book(s): Michael E Whitman and Herbert J Mattord, —Principles of Information Security||, Cengage Learning, 2018. (Unit IV, V)

Reference Book(s):

Matt Bishop, —"Computer Security Art and Science", Pearson/PHI, 2018.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Enlightening Technical Minds Estd. 1998
An Autonomous Institution
(Since 2011)

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Affiliated to Anna University, Chennai; Approved by AICTE ; Accredited by NAAC with Grade 'A++'
Accredited by NBA - Tier1 (Mech, Auto, Civil, EEE, ECE, E&I and CSE)
Udumalai Road, Pollachi - 642 003. Tel: 04259-236030/40/50 Fax: 04259-236070 www.mcet.in

19ITOC1004 – Cyber Law and Information Security

Unit V -Security Investigation

CO5: Explain the secure application development using information security

LO1:To learn about laws and ethics in information security

SO2: Explain about laws and ethics in information security.

Prepared by

G. Keerthika

AP/IT

Unit V -Security Investigation

Need for Security - Business Needs - Threats - Secure Software Development – Law and Ethics in Information Security - International Laws and Laws Bodies - Ethics and Information Security

International Laws and Laws Bodies

- It is important for IT professionals and information security practitioners to realize that when their organizations do business on the Internet, they do business globally.
- As a result, these professionals must be sensitive to the laws and ethical values of many different cultures, societies, and countries.
- While it may be impossible to please all of the people all of the time, dealing with the laws of other states and nations is one area where it is certainly *not* easier to ask for forgiveness than for permission.
- The American Society of International Law is one example of an American institution that deals in international law

Council of Europe Convention on Cybercrime

- The Council of Europe adopted the **Convention on Cybercrime** in 2001.
- It created an international task force to oversee a range of security functions associated with Internet activities for standardized technology laws across international borders.
- It also attempts to improve the effectiveness of international investigations into breaches of technology law.
- This convention has been well received by advocates of intellectual property rights because it emphasizes prosecution for copyright infringement.
- However, many supporters of individual rights oppose the convention because they think it unduly infringes on freedom of speech and threatens the civil liberties of U.S. residents.

Council of Europe Convention on Cybercrime

- While thirty-four countries attended the signing in November 2001, only twenty-nine nations, including the United States, have ratified the Convention as of April 2010.
- The United States is technically not a “member state of the council of Europe” but does participate in the Convention.
- The overall goal of the convention is to simplify the acquisition of information for law enforcement agencies in certain types of international crimes. It also simplifies the extradition process.
- The convention has more than its share of skeptics, who see it as an overly simplistic attempt to control a complex problem.

Agreement on Trade-Related Aspects of Intellectual Property Rights

- The **Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)**, created by the World Trade Organization (WTO) and negotiated over the years 1986–1994, introduced intellectual property rules into the multilateral trade system.
- It is the first significant international effort to protect intellectual property rights. It outlines requirements for governmental oversight and legislation of WTO member countries to provide minimum levels of protection for intellectual property.
- The WTO TRIPS agreement covers five issues:
  - How basic principles of the trading system and other international intellectual property agreements should be appliedHow to give adequate protection to intellectual property rights
  - How countries should enforce those rights adequately in their own territories
  - How to settle disputes on intellectual property between members of the WTO
  - Special transitional arrangements during the period when the new system is being introduced.

The Digital Millennium Copyright Act (DMCA)

- **The Digital Millennium Copyright Act (DMCA)** is the American contribution to an international effort by the World Intellectual Properties Organization (WIPO) to reduce the impact of copyright, trademark, and privacy infringement, especially when accomplished via the removal of technological copyright protection measures.
- This law was created in response to the 1995 adoption of **Directive 95/46/EC** by the European Union, which added protection for individuals with regard to the processing of personal data and the use and movement of such data.
- The United Kingdom has implemented a version of this law called the **Database Right**, in order to comply with Directive 95/46/EC**.**

The Digital Millennium Copyright Act (DMCA)

The DMCA includes the following provisions:

- Prohibits the circumvention protections and countermeasures implemented by copyright owners to control access to protected content
- Prohibits the manufacture of devices to circumvent protections and countermeasures that control access to protected content
- Bans trafficking in devices manufactured to circumvent protections and countermeasures that control access to protected content
- Prohibits the altering of information attached or imbedded into copyrighted material
- Excludes Internet service providers from certain forms of contributory copyright infringement

References

Text Book(s): Michael E Whitman and Herbert J Mattord, —Principles of Information Security||, Cengage Learning, 2018. (Unit IV, V)

Reference Book(s):

Matt Bishop, —"Computer Security Art and Science", Pearson/PHI, 2018.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Enlightening Technical Minds Estd. 1998
An Autonomous Institution
(Since 2011)

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Affiliated to Anna University, Chennai; Approved by AICTE ; Accredited by NAAC with Grade 'A++'
Accredited by NBA - Tier1 (Mech, Auto, Civil, EEE, ECE, E&I and CSE)
Udumalai Road, Pollachi - 642 003. Tel: 04259-236030/40/50 Fax: 04259-236070 www.mcet.in

19ITOC1004 – Cyber Law and Information Security

Unit V -Security Investigation

CO5: Explain the secure application development using information security

LO1:To learn about laws and ethics in information security.

SO2:Explain about International Laws and Laws Bodies , Ethics in Information Security in information security.

Prepared by

G. Keerthika

AP/IT

Unit V -Security Investigation

Need for Security - Business Needs - Threats - Secure Software Development – Law and Ethical in Information Security - International Laws and Laws Bodies - Ethics and Information Security

Ethics and Information Security

- Many Professional groups have explicit rules governing ethical behavior in the workplace.
- For example, doctors and lawyers who commit egregious violations of their professions canons of conduct can be removed from practice.
- Unlike the medical and legal fields, however, the information technology field in general, and the information security field in particular, do not have a binding code of ethics.

Ethical Differences Across Cultures

- Cultural differences can make it difficult to determine what is and is not ethical—especially when it comes to the use of computers.
- Studies on ethics and computer use reveal that people of different nationalities have different perspectives; difficulties arise when one nationality's ethical behavior violates the ethics of another national group.
- For example, to Western cultures, many of the ways in which Asian cultures use computer technology is software piracy.
- This ethical conflict arises out of Asian traditions of collective ownership, which clash with the protection of intellectual property.
- Approximately 90 percent of all software is created in the United States. Some countries are more relaxed with intellectual property copy restrictions than others.

Software License Infringement

- software license infringement, or piracy, is routinely covered by the popular press.
- Among study participants, attitudes toward piracy were generally similar; however, participants from the United States and the Netherlands showed significant differences in attitudes from the overall group.
- Participants from the United States were significantly less tolerant of piracy, while those from the Netherlands were significantly more permissive.
- Although other studies have reported that the Pacific Rim countries of Singapore and Hong Kong are hotbeds of software piracy, this study found tolerance for copyright infringement in those countries to be moderate, as were attitudes in England, Wales, Australia, and Sweden.
- This could mean that the individuals surveyed understood what software license infringement was, but felt either that their use was not piracy, or that their society permitted this piracy in some way.

Software License Infringement(contd...)

- Peer pressure, the lack of legal disincentives, the lack of punitive measures, and number of other reasons could a explain why users in these alleged piracy centers disregarded intellectual property laws despite their professed attitudes toward them.
- Even though participants from the Netherlands displayed a more permissive attitude toward piracy, that country only ranked third in piracy rates of the nations surveyed in this study.

Illicit Use

- The study respondents unilaterally condemned viruses, hacking, and other forms of system abuse.
- There were, however, different degrees of tolerance for such activities among the groups.
- Students from Singapore and Hong Kong proved to be significantly more tolerant than those from the United States, Wales, England, and Australia.
- Students from Sweden and the Netherlands were also significantly more tolerant than those from Wales and Australia, but significantly less tolerant than those from Hong Kong.
- The low overall degree of tolerance for illicit system use may be a function of the easy correspondence between the common crimes of breaking and entering, trespassing, theft, and destruction of property and their computer-related counterparts

Misuse of Corporate Resources

- The scenarios used to examine the levels of tolerance for misuse of corporate resources each presented a different degree of non-company use of corporate assets without specifying the company's policy on personal use of company resources.
- In general, individuals displayed a rather lenient view of personal use of company equipment.
- Only students from Singapore and Hong Kong view personal use of company equipment as unethical. There were several substantial differences in this category, with students from the Netherlands revealing the most lenient views.
- With the exceptions of those from Singapore and Hong Kong, it is apparent that many people, regardless of cultural background, believe that unless an organization explicitly forbids personal use of its computing resources, such use is acceptable.
- It is interesting to note that only participants among the two Asian samples, Singapore and Hong Kong, reported generally intolerant attitudes toward personal use of organizational computing resources. The reasons behind this are unknown.

Ethics and Education

- Attitudes toward the ethics of computer use are affected by many factors other than nationality.Differences are found among individuals within the same country, within the same social class, and within the same company.
- Key studies reveal that the overriding factor in leveling the ethical perceptions within a small population is education.
- Employees must be trained and kept aware of a number of topics related to information security, not the least of which are the expected behaviors of an ethical employee.
- This is especially important in information security, as many employees may not have the formal technical training to understand that their behavior is unethical or even illegal.
- Proper ethical and legal training is vital to creating an informed, well prepared, and low-risk system user.

Deterring Unethical and Illegal Behavior

- There are three general causes of unethical and illegal behavior:

Ignorance—Ignorance of the law is no excuse; however, ignorance of policy and procedures is. The first method of deterrence is education.

This is accomplished by means of designing, publishing, and disseminating organization policies and relevant laws, and also obtaining agreement to comply with these policies and laws from all members of the organization.

Reminders, training, and awareness programs keep the policy information in front of the individual and thus better support retention and compliance.

Accident—Individuals with authorization and privileges to manage information within the organization are most likely to cause harm or damage by accident. Careful planning and control helps prevent accidental modification to systems and data.

Intent—Criminal or unethical intent goes to the state of mind of the person performing the act; it is often necessary to establish criminal intent to successfully prosecute offenders.

Protecting a system against those with intent to cause harm or damage is best accomplished by means of technical controls, and vigorous litigation or prosecution if these controls fail.

Deterring Unethical and Illegal Behavior(contd..)

Laws and policies and their associated penalties only deter if three conditions are present:

- **Fear of penalty—Potential** offenders must fear the penalty. Threats of informal reprimand or verbal warnings may not have the same impact as the threat of imprisonment or forfeiture of pay.
- **Probability of being caught—**Potential offenders must believe there is a strong possibility of being caught. Penalties will not deter illegal or unethical behavior unless there is reasonable fear of being caught.
- **Probability of penalty being administered—**Potential offenders must believe that the penalty will in fact be administered.

References

Text Book(s): Michael E Whitman and Herbert J Mattord, —Principles of Information Security||, Cengage Learning, 2018. (Unit IV, V)

Reference Book(s):

Matt Bishop, —"Computer Security Art and Science", Pearson/PHI, 2018.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You