UNIT II SECURITY INVESTIGATION

Need for Security, Business Needs, Threats, Attacks, Legal, Ethical and Professional Issues.

Business Needs First

Information security performs four important functions for an organization:

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

1. Protecting the functionality of an organization

- Decision makers in organizations must set policy and operate their organizations in compliance with the complex, shifting legislation that controls the use of technology.

2. Enabling the safe operation of applications

- Organizations are under immense pressure to acquire and operate integrated, efficient, and capable applications
- The modern organization needs to create an environment that safeguards applications using the organization’s IT systems, particularly those applications that serve as important elements of the infrastructure of the organization.

3. Protecting data that organizations collect & use

- Protecting data in motion
- Protecting data at rest
- Both are critical aspects of information security.
- The value of data motivates attackers to seal, sabotage, or corrupt it.
- It is essential for the protection of integrity and value of the organization’s data

4. Safeguarding Technology assets in organizations

- Must add secure infrastructure services based on the size and scope of the enterprise.
- Organizational growth could lead to the need for **public key infrastructure,** PKI, an integrated system of software, encryption methodologies.

Threats

To protect an organization’s information, you must

1. Know yourself

(i.e) be familiar wit the information to be protected, and the systems that store, transport and process it.

2. Know the threats you face

To make sound decisions about information security, management must be informed about the various threats facing the organization, its application, data and information systems.

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

Threats to Information Security

Categories of threat	Examples
Acts of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and/or/data collection
Deliberate acts of information extortion	Blackmail or information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial-of-service
Forces of nature	Fire, flood, earthquake, lightning
Deviations in quality of service	ISP, power ,or WAN service providers
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Threats

1. Acts of Human Error or Failure:

- Acts performed without intent or malicious purpose by an authorized user.
- because of in experience ,improper training,
- Making of incorrect assumptions.

One of the greatest threats to an organization's information security is the organization's own employees.

- Entry of erroneous data
- accidental deletion or modification of data
- storage of data in unprotected areas.
- Failure to protect information

can be prevented with
- Training
- Ongoing awareness activities
-Verification by a second party
- Many military applications have robust, dual- approval controls built in .

2. Compromises to Intellectual Property

- is defined as the ownership of ideas and control over the tangible or virtual representation of those ideas.
- Intellectual property includes trade secrets, copyrights, trademarks, and patents.
- Once intellectual property has been defined and properly identified, breaches to IP constitute a threat to the security of this information.
- Organization purchases or leases the IP of other organizations.
- Most Common IP breach is the unlawful use or duplication of software based intellectual property more commonly known as **software Piracy**.
- Software Piracy affects the world economy.

- U.S provides approximately 80% of world's software.

In addition to the laws surrounding software piracy, two watch dog organizations investigate allegations of software abuse.

1. Software and Information Industry Association (SIIA) (i.e)Software Publishers Association
2. Business Software Alliance (BSA)
    - Another effort to combat (take action against) piracy is the online registration process.

3. Deliberate Acts of Espionage or Trespass

- Electronic and human activities that can breach the confidentiality of information.
- When an unauthorized individual's gain access to the information an organization is trying to protect is categorized as act of espionage or trespass.
- Attackers can use many different methods to access the information stored in an information system.

1. Competitive Intelligence[use web browser to get information from market research]
2. Industrial espionage(spying)
3. Shoulder Surfing(ATM)

Trespass

- Can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.
- Sound principles of authentication & authorization can help organizations protect valuable information and systems.
- **Hackers->** "People who use and create computer software to gain access to information illegally"
- There are generally two skill levels among hackers.
- **Expert Hackers**-> Masters of several programming languages, networking protocols, and operating systems .
- **Unskilled Hackers**

4. Deliberate Acts of information Extortion (obtain by force or threat)

- Possibility of an attacker or trusted insider stealing information from a computer system and demanding compensation for its return or for an agreement not to disclose the information.

5. Deliberate Acts of sabotage or Vandalism

- Destroy an asset or
- Damage the image of organization
- Cyber terrorism-Cyber terrorists hack systems to conduct terrorist activities through network or internet pathways.

6. Deliberate Acts of Theft

- Illegal taking of another's property-- is a constant problem.
- Within an organization, property can be physical, electronic, or intellectual.
- Physical theft can be controlled by installation of alarm systems.
- Trained security professionals.
- Electronic theft control is under research.

7. Deliberate Software Attacks

- Because of **malicious code** or **malicious software** or sometimes **malware.**

- These software components are designed to damage, destroy or deny service to the target system.
- More common instances are
  Virus, Worms, Trojan horses, Logic bombs, Backdoors.
- "The British Internet Service Provider Cloudnine" be the first business "hacked out of existence"

Virus

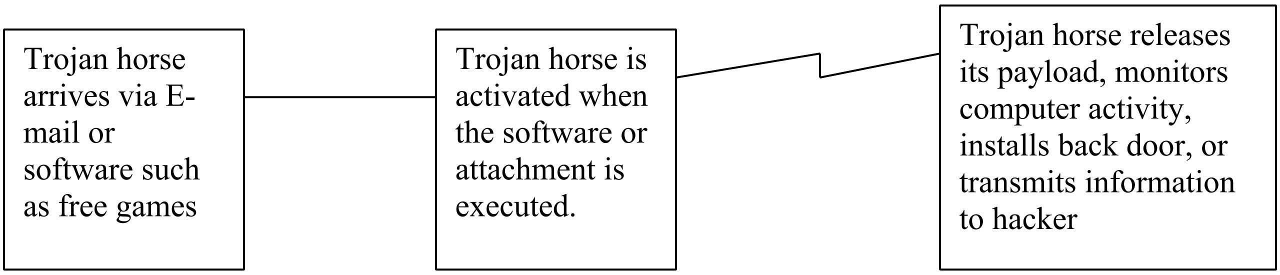
- Segments of code that performs malicious actions.
- Virus transmission is at the opening of Email attachment files.
- **Macro virus**-> Embedded in automatically executing macrocode common in word processors, spreadsheets and database applications.
- **Boot Virus**-> infects the key operating files located in the computer's boot sector.

Worms

- A worm is a malicious program that replicates itself constantly, without requiring another program to provide a safe environment for replication.
- Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.
- Eg: MS-Blaster, MyDoom, Netsky, are multifaceted attack worms.
- 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 systems can reach, so that users who subsequently visit those sites become infected.

Trojan Horses

- Are software programs that hide their true nature and reveal their designed behavior only when activated.



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

Trojan horse Attack

Back Door or Trap Door

- A Virus or Worm has a payload that installs a backdoor or trapdoor component in a system, which allows the attacker to access the system at will with special privileges.

Eg: Back Orifice

Polymorphism

- A **Polymorphic threat** is one that changes its apparent shape over time, making it undetectable by techniques that look for preconfigured signatures.
- These viruses and Worms actually evolve, changing their size, and appearance to elude detection by antivirus software programs.

Virus & Worm Hoaxes

Types of Trojans

- Data Sending Trojans
- Proxy Trojans
- FTP Trojans
- Security software disabler Trojans
- Denial of service attack Trojans(DOS)

Virus

A program or piece of code that be loaded on to your computer, without your knowledge and run against your wishes.

Worm

A program or algorithm that replicates itself over a computer network and usually performs malicious actions.

Trojan Horse

A destructive program that masquerade on beginning application, unlike viruses, Trojan horse do not replicate themselves.

Blended threat

Blended threats combine the characteristics of virus, worm, Trojan horses & malicious code with server and Internet Vulnerabilities.

Antivirus Program

A Utility that searches a hard disk for viruses and removes any that found.

Forces of Nature

Fire: Structural fire that damages the building. Also encompasses smoke damage from a fire or water damage from sprinkles systems.

Flood: Can sometimes be mitigated with flood insurance and/or business interruption Insurance.

Earthquake: Can sometimes be mitigated with specific causality insurance and/or business interruption insurance, but is usually a separate policy.

Lightning: An Abrupt, discontinuous natural electric discharge in the atmosphere.

Landslide/Mudslide: The downward sliding of a mass of earth & rocks directly damaging all parts of the information systems.

Tornado/Severe Windstorm:

Huricane/typhoon:
Tsunami:
Electrostatic Discharge (ESD):
Dust Contamination:

Since it is not possible to avoid force of nature threats, organizations must implement controls to limit damage.

- They must also prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans, to limit losses in the face of these threats.

Deviations in Quality of Service

- A product or service is not delivered to the organization as expected.
- The Organization's information system depends on the successful operation of many interdependent support systems.
- It includes power grids, telecom networks, parts suppliers, service vendors, and even the janitorial staff & garbage haulers.
- This degradation of service is a form of **availability disruption.**

Internet Service Issues

- Internet service Provider(ISP) failures can considerably undermine the availability of information.
- 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 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 & Other Service Provider Issues

- Other utility services can affect the organizations are telephone, water, waste water, 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.
- For an example, if the waste water system fails, an organization might be prevented from allowing employees into the building.
- This would stop normal business operations.

Power Irregularities

- Fluctuations due to power excesses.
- Power shortages &
- Power losses

This can pose problems for organizations that provide inadequately conditioned power for their information systems equipment.

- When voltage levels **spike** (experience a momentary increase),or **surge** (experience prolonged increase), the extra voltage can severely damage or destroy equipment.
- The more expensive uninterruptible power supply (UPS) can protect against spikes and surges.

Technical Hardware Failures or Errors

- Resulting in unreliable service or lack of availability
- Some errors are terminal, in that they result in unrecoverable loss of equipment.
- Some errors are intermittent, in that they resulting in faults that are not easily repeated.

Technical software failures or errors

- This category involves threats that come from purchasing software with unknown, hidden faults.
- Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved.
- These failures range from bugs to untested failure conditions.

Technological obsolescence

- 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.

Man-in-the –Middle

- Otherwise called as **TCP hijacking attack**.
- An attacker monitors packets from the network, modifies them, and inserts them back into the network.
- This type of attack uses IP spoofing.
- It allows the attacker to change, delete, reroute, add, forge or divert data.
- TCP hijacking session, the spoofing involves the interception of an encryption key exchange.

SPAM

- Spam is unsolicited commercial E-mail.
- It has been used to make malicious code attacks more effective.
- Spam is considered as a trivial nuisance rather than an attack.
- It is the waste of both computer and human resources it causes by the flow of unwanted E-mail.

Mail Bombing

- Another form of E-mail attack that is also a DOS called a **mail bomb**.
- Attacker routes large quantities of e-mail to the target.
- The target of the attack receives unmanageably large volumes of unsolicited e-mail.
- By sending large e-mails, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker.
- The target e-mail address is buried under thousands or even millions of unwanted e-mails.

Sniffers

- A **sniffer** is a program or device that can monitor data traveling over a network.
- Unauthorized sniffers can be extremely dangerous to a network's security, because they are virtually impossible to detect and can be inserted almost anywhere.
- Sniffer often works on TCP/IP networks, where they are sometimes called **"packet Sniffers".**

Social Engineering

- It is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.
- An attacker gets more information by calling others in the company and asserting his/her authority by mentioning chief's name.

Buffer Overflow

- A buffer overflow is an application error that occurs when more data is sent to a buffer than it can handle.

- Attacker can make the target system execute instructions.

Timing Attack

- Works by exploring the contents of a web browser’s cache.
- These attacks allow a Web designer to create a malicious form of cookie, that is stored on the client’s system.
- The cookie could allow the designer to collect information on how to access password- protected sites.

Attacks

- An attack is an act of or action that takes advantage of a vulnerability to compromise a controlled system.
- It is accomplished by a **threat agent** that damages or steals an organization’s information or physical asset.
- **Vulnerability** is an identified weakness in a controlled system, where controls are not present or are no longer effective.
- Attacks exist when a specific act or action comes into play and may cause a potential loss.

Malicious code

- The malicious code attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.
- The state –of-the-art malicious code attack is the polymorphic or multivector, worm.
- These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.

Attack Replication Vectors

1. IP scan & attack
2. Web browsing
3. Virus
4. Unprotected shares
5. Mass mail
6. Simple Network Management Protocol(SNMP)

1. IP scan & attack

The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers.

2. Web browsing

If the infected system has write access to any Web pages, it makes all Web content files (.html,.asp,.cgi & others) infectious, so that users who browse to those pages become infected.

3. Virus

Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection.

4. Unprotected shares

Using vulnerabilities in file systems and the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.

5. Mass Mail

By sending E-mail infections to addresses found in the address book, the infected machine infects many users, whose mail -reading programs also automatically run the program & infect other systems.

6. Simple Network Management Protocol (SNMP)

- By using the widely known and common passwords that were employed in early versions of this protocol, the attacking program can gain control of the device. Most vendors have closed these vulnerabilities with software upgrades.

Hoaxes

- A more devious approach to attacking the computer systems is the transmission of a virus hoax with a real virus attached.
- Even though these users are trying to avoid infection, they end up sending the attack on to their co-workers.

Backdoors

- Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door.
- Sometimes these entries are left behind by system designers or maintenance staff, and thus referred to as trap doors.
- A trap door is hard to detect, because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system.

Password Crack

- Attempting to reverse calculate a password is often called **cracking.**
- A password can be hashed using the same algorithm and compared to the hashed results, If they are same, the password has been cracked.
- The (SAM) Security Account Manager file contains the hashed representation of the user’s password.

Brute Force

- The application of computing & network resources to try every possible combination of options of a password is called a **Brute force attack.**
- This is often an attempt to repeatedly guess passwords to commonly used accounts, it is sometimes called a **password attack.**

Dictionary

- This is another form of the brute force attack noted above for guessing passwords.
- The **dictionary attack** narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords instead of random combinations.

Denial –of- Services(DOS) & Distributed Denial –of- Service(DDOS)

- The attacker sends a large number of connection or information requests to a target.
- This may result in the system crashing, or simply becoming unable to perform ordinary functions.
- DDOS is an attack in which a coordinated stream of requests is launched dagainst a target from many locations at the same.

Spoofing

- It is a technique used to gain unauthorized access to computers, where in the intruder sends messages to a computer that has an IP address that indicates that the messages are coming from a trusted host.

Data: Payload	IP source: 192.168.0.25	IP destination: 100.0.0.75

Original IP

packet

From

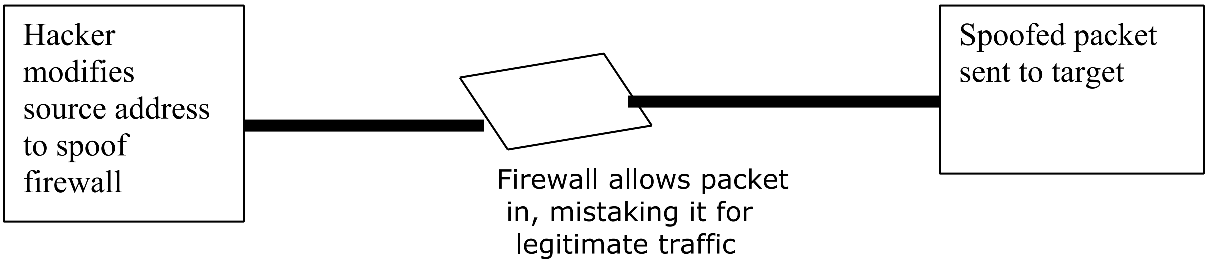
hacker's system

Data: Payload	IP source: 100.0.0.80	IP destination: 100.0.0.75

Spoofed

(modified)

IP packet


Hacker modifies source address to spoof firewall
Firewall allows packet in, mistaking it for legitimate traffic
Spoofed packet sent to target

IP spoofing

Legal, Ethical, and Professional Issues in Information Security

Law and Ethics in Information Security

Laws are rules that mandate or prohibit certain behavior in society; they are drawn from **ethics**, which define socially acceptable behaviors. The key difference between laws and ethics is that laws carry the sanctions of a governing authority and ethics do not. Ethics in turn are based on **Cultural mores.**

Key U.S Laws of Interest to Information Security Professionals

ACT	SUBJECT	DATE	DESCRIPTION
Communications Act of 1934,updated by Telecommunications Deregulation & Competition Act	Telecommunications	1934	Regulates interstate and foreign Telecommunications.
Computer Fraud & Abuse Act	Threats to computers	1986	Defines and formalizes laws to counter threats from computer related acts and offenses.
Computer Security Act of 1987	Federal Agency Information Security	1987	Requires all federal computer systems that contain classified information to have

			surety plans in place, and requires periodic security training for all individuals who operate, design, or manage such systems.
Economic Espionage Act of 1996	Trade secrets.	1996	Designed to prevent abuse of information gained by an individual working in one company and employed by another.
Electronic Communications Privacy Act of 1986	Cryptography	1986	Also referred to as the Federal Wiretapping Act; regulates interception and disclosure of electronic information.
Federal Privacy Act of 1974	Privacy	1974	Governs federal agency use of personal information.
Gramm-Leach-Bliley Act of 1999	Banking	1999	Focuses on facilitating affiliation among banks, insurance and securities firms; it has significant impact on the privacy of personal information used by these industries.
Health Insurance Portability and Accountability Act	Health care privacy	1996	Regulates collection, storage, and transmission of sensitive personal health care information.
National Information Infrastructure protection Act of 1996	Criminal intent	1996	Categorized crimes based on defendant's authority to access computer and criminal intent.
Sarbanes-Oxley Act of 2002	Financial Reporting	2002	Affects how public organizations and accounting firms deal with corporate governance, financial disclosure, and the practice of public accounting.
Security and Freedom through Encryption Act of 1999	Use and sale of software that uses or enables encryption.	1999	Clarifies use of encryption for people in the United states and permits all persons in the U.S. to buy or sell any encryption product and states that the government cannot require the use of any kind of key escrow system for encryption products.
U.S.A. Patriot Act of 2001	Terrorism	2001	Defines stiffer penalties for prosecution of terrorist crimes.

Review Questions

PART A

1. Why is information security a management problem? What can management do that technology cannot?
2. How does a threat to information security differ from an attack? How can the two overlap?
3. What are the steps to be taken by Security Personnel in case of Technical Hardware failure or error?
4. What is the difference between a skilled hacker and an unskilled hacker? How does the protection against each differ?
5. What are the various types of malware? How do worms differ from viruses? Do Trojan Horses carry viruses or worms?
6. Why does polymorphism cause greater concern than traditional malware? How does it affect detection?
7. Explain DOS and DDOS.
8. What is the most common form of violation of intellectual property? How does an organization protect against it? What agencies fight it?
9. How does technological obsolescence constitute a threat to information security? How can an organization protect against it?
10. What is the difference between exploit and Vulnerability?
11. What are the types of password attacks? What can a systems administrator do to protect against them?
12. What is a buffer overflow, and how is it used against a Web server?
13. Explain how a culture affects the ethic of an organization.
14. How will Sarbanes- Oxley Act of 2002 affect Information Security managers?
15. What is the difference between Criminal law and civil law?
16. Write any four commandments of Computer Ethics.
17. What is Digital Millennium Copyright Act (DMCA)?
18. What are the primary examples of public law?
19. Which law amended the computer Fraud and Abuse Act of 1986, and what did it change?
20. Which law from 1997 provides guidance on the use of encryption?
21. What is intellectual property (IP)? Is it afforded the same protection in every country of the world? What laws currently protect it in the United States and Europe?
22. What is a policy? How does it differ from a Law?
23. What are the three general categories of unethical and illegal behavior?
24. What is the best method for preventing an illegal or unethical activity?

PART B

1. Explain in detail the different types of cryptanalytic attacks.
2. Discuss in detail the Legal, Ethical and Professionalism issues during security investigation.
3. What is the difference between a denial-of-service attack and a distributed denial-of-service attack? Which is potentially more dangerous and devastating? Why?
4. For a sniffer attack to succeed, what must the attacker do? How can an attacker gain access to a network to use the sniffer system?
5. What are some ways a social engineering hacker can attempt to gain information about a user’s login and password? How would this type of attack differ if it were targeted towards an administrator’s assistant versus a data-entry clerk?