UNIT – II

The Role of People in Security

- Absolute protection of computer systems and networks is not possible
- Technology alone will not solve the security problem.
    I. No matter how advanced the technology is, it will ultimately be deployed in an environment where humans exist.
    II. The human element is the biggest problem to security.
- Humans:
    I. Deliberately or accidentally cause security problems
    II. Circumvent security mechanisms.
    III. Some people will not do what they are supposed to, and will create vulnerability in an organization's security posture

Unit-II Organizational Security

2.1 Introduction

2.2 List & de ne various human security threats.

- Password selection,
- Piggybacking,
- Shoulder surfing,
- Dumpster diving,
- Installing unauthorized software /hardware,
- Access by non employees.

2.3 Determine ways in which users can aid security.

- People as Security Tool: Security awareness, and Individual user responsibilities.

2.4 Describe physical security components that can protect any computer and network.

- Physical security: Access controls
- Biometrics: finger prints, hand prints, Retina, Patterns, voice patterns, signature and writing patterns, keystrokes, Physical barriers

2.5 List poten al threats on password and explain characteris cs of a strong password.

- Password Management,
- vulnerability of password,
- password protection,
- password selection strategies,
- Components of a good password.

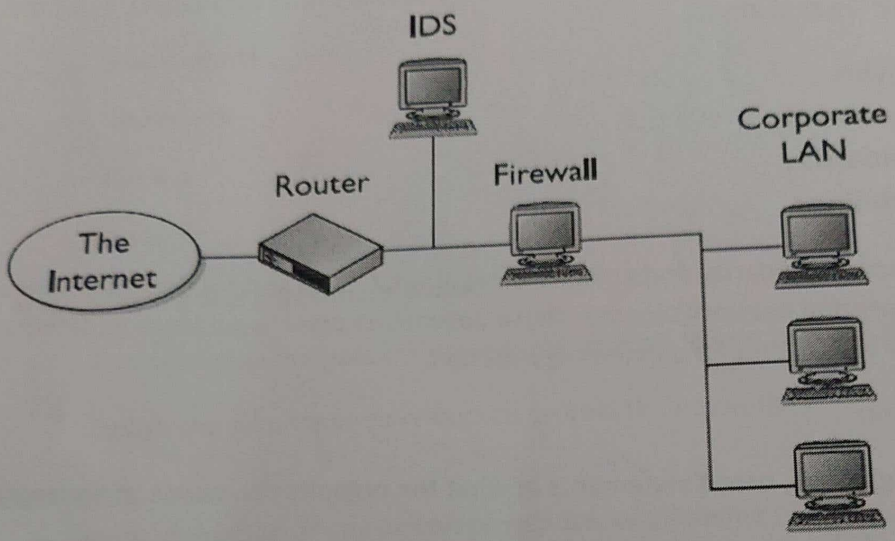
Unit-II Organizational Security

2.1 Introduction

2.1.1 Background:

- Prevention technologies prevent unauthorized individuals from gaining access to systems or data.
  - In an operational environment, prevention is difficult.
  - Relying on prevention technologies alone is not sufficient.
- Prevention technologies are static.
- They are put in place and generally left alone.
- Detection and response technologies are dynamic.
- They acknowledge that security is an ongoing process.
- The first presentation introduced the operational model of computer security.
- The model described the various components in computer security and network security.
- The operational model of computer security stated that:
  - Protection = Prevention + (Detection + Response).
- This presentation addresses the issues surrounding computer security and network security.

2.1.2 General Block Diagram Of Organization Network.



- This diagram includes the major components typically found in a network.
- There is some connection to the Internet.
- This connection will generally have some sort of protection attached to it such as a firewall.
- An intrusion detection system will also often be part of the security perimeter for the organization. This may be on the inside of the firewall, or the outside, or it may in fact be on both sides, the specific location depending on the company and what they are more concerned with preventing (i.e., the insider threat or external threats).
- Beyond this security perimeter is the corporate network. This is obviously a very simple depiction—an actual network may have numerous subnets and extranets—but the basic components are present.
- Unfortunately, if this were the diagram provided by the administrator to show the organization's basic network structure, the administrator would have missed a very important component.

2.1.3 Security Operations:

- **Policies**
- **Procedures**
- **Standards**
- **Guidelines**

Policies, procedures, standards, and guidelines detail what users and administrators should do to maintain system and network security. These documents provide guidance to determine how security will be implemented in the organization.

- Policies are:
  - High-level, broad statements of what the organization wants to accomplish.
  - Made by the management when laying out the organization's position on some issues.
- Standards are:
  - Mandatory elements regarding the implementation of a policy.
  - Accepted specifications of specific details on how a policy is to be implemented or enforced.
- Guidelines are:
  - Recommendations relating to a policy.
  - Not mandatory.
- Procedures are step-by-step instructions on how to implement policies in an organization.
  - Step-by-step instructions that describe exactly how employees are expected to act in a given situation or to accomplish a specific task.
- As the network constantly changes, the policies, procedures, and guidelines should be periodically evaluated and changed if necessary.
- The constant monitoring of the network and the periodic review of the relevant documents are part of the operational model.
- When applied to policies, this process results in the policy life cycle.

2.1.4 Policy Life Cycle

1. The four steps of the policy life cycle are:
   - Plan (Adjust)
   - Implement
   - Monitor
   - Evaluate

- **In the planning and adjustment phase:**
  - Users develop the policies, procedures, and guidelines that will be implemented.
  - Design the security components to protect the network.
- **Implementa on:**
  - Implementation of any policy, procedure, or guideline requires an instruction period to about its contents.
- **Monitoring**
  - Constant monitoring ensures that hardware and software, policies, procedures, and guidelines are effective in securing the systems.
- **Evalua on:**
  - Evaluating the effectiveness of security includes a vulnerability assessment and penetration test of the system to ensure that security meets expectations.
  - After evaluating the organization's stand on security, the process restarts at step one, this time adjusting the security mechanisms that are in place.
  - Evaluation is a continuous process.

2.2 List & de ne various human security threats.

2.2.1 Password Selection:

"Password is defined as a secret word or phrase that must be used to gain admission to a place or to access a particular system."

- The use of passwords is known to be ancient.
- Sentries would challenge those wishing to enter an area or approaching it to supply a password or watchword, and would only allow a person or group to pass if they knew the password.
- In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc.
- A typical computer user has passwords for many purposes: logging into accounts, retrieving e-mail, accessing applications, databases, networks, web sites, and even reading the morning newspaper online.

Password Problem:

- Computer intruders rely on poor passwords to gain unauthorized access to a system or network.
- Users choose passwords that are easy to remember and often choose the same sequence of characters as they have for their userIDs.
- Users also frequently select names of family members, their pets, or their favorite sports team for their passwords.

Improving Password:

- To complicate the attacker's job:
  - Mix uppercase and lowercase characters.
  - Include numbers and special characters in passwords.

2.2.2 Human Attack

- Piggybacking and shoulder sur ng
- Dumpster diving
- Installing unauthorized hardware and so ware
- Access by non-employees
- Social engineering

Piggybacking

- In security, piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint.
- The act may be legal or illegal, authorized or unauthorized, depending on the circumstances. However, the term more often has the connotation of being an illegal or unauthorized act.
- To describe the act of an unauthorized person who follows someone to a restricted area without the consent of the authorized person, the term tailgating is also used. "Tailgating" implies without consent (similar to a car tailgating another vehicle on the freeway), while "piggybacking" usually implies consent of the authorized person.
- Piggybacking is the tactic of closely following a person who has just used an access card or PIN to gain physical access to a room or building.

Shoulder Surfing

- In computer security, shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, PINs, security codes, and similar data.
- Shoulder surfing is particularly effective in crowded places because it is relatively easy to observe someone as they:
    - fill out a form
    - enter their PIN at an automated teller machine or a POS terminal
    - use a telephone card at a public payphone
    - enter a password at a cybercafe, public and university libraries, or airport kiosks
    - enter a code for a rented locker in a public place such as a swimming pool or airport
    - public transport is a particular area of concern

Dumpster Diving:

- Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.)
- In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network.
- Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes.
- Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network.
- To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash.

Installing unauthorized hardware and so ware

- Organizations should have a policy to restrict normal users from installing software and hardware on their systems.
- Communication software and a modem may allow individuals to connect to their machines at work using a modem from home.
- This creates a backdoor into the network and can circumvent all the other security mechanisms.
- There are numerous small programs that can be downloaded from the Internet.
- Users cannot always be sure where the software originally came from and what may be hidden inside.

Access by non-employees:

- If an attacker gains access to a facility, there are chances of obtaining enough information to penetrate computer systems and networks.
- Many organizations require employees to wear identification badges at work.
- This method is easy to implement and may be a deterrent to unauthorized individuals.
- It also requires that employees challenge individuals not wearing identification badges.
- One should examine who has legitimate access to a facility.
- Non-employees may not have the same regard for the intellectual property rights of the organization that employees have.
- Contractors, consultants, and partners may frequently not only have physical access to the facility but also have network access.

- Nighttime custodial crewmembers and security guards have unrestricted access to the facility when no one is around.

Social engineering:

- Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information.
- A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.
- Using social engineering, the attacker deceives to:
  - Obtain privileged information.
  - Convince the target to do something that they normally would not.
- Social engineering is successful because of two reasons.
  - The first is the basic human nature to be helpful.
  - The second reason is that individuals normally seek to avoid confrontation and trouble.
- The first reason that social engineering works can be further broken into one of the three categories:
  - The attacker may simply ask a question hoping to obtain the desired information immediately.
  - The attacker may first attempt to engage the target in conversation. He may then try to evoke sympathy so the target feels sorry for the individual and may release the information willingly.
  - The attacker may also try another approach, appealing to the individual's ego.
- A variation on social engineering uses means other than direct contact between the target and the attacker.
- Insiders may also attempt to gain unauthorized information.
- The insider may be more successful.
- They have a level of information regarding the organization.
- They can better spin a story that may be believable to other employees.

- Social Engineering Technique:
  - Pretexting
  - Diversion theft
  - Phishing
  - IVR or phone phishing
  - Baiting
  - Quid Pro Quo
  - Tailgating

2.3 Determine ways in which users can aid security.

2.3.1 People as Security Tool & General Awareness

- A paradox of social engineering attacks is that people are not only the biggest problem and security risk, but also the best tool to defend against these attacks.
- Organizations must fight social engineering attacks by establishing policies and procedures that define roles and responsibilities for all users and not just security personnel.
- Organizations can counter potential social engineering attacks by conducting an active security awareness program for the organization's security goals and policies.
- The training will vary depending on the organization's environment and the level of threat.
- An important element that should be stressed in the training on social engineering is th type of information that the organization considers sensitive and that may be the target of a social engineering attack.

Individual User Responsibilities in terms of Organizational Security

1. Locking the door to the office or workspace.
2. Not leaving sensitive information unprotected inside the car.
3. Securing storage media containing sensitive information.
4. Shredding paper containing organizational information before discarding it.
5. Not divulging sensitive information to unauthorized individuals.
6. Not discussing sensitive information with family members.
7. Protecting laptops that contain sensitive or important organization information.
8. Being aware of who is around when discussing sensitive corporate information.
9. Enforcing corporate access control procedures.
10. Being aware of the procedures to report suspected or actual violations of security policies.
11. Enforcing good password security practices, which all employees should follow.
12. Cultivating an environment of trust in the office and an understanding of the importance of security.

2.4 Describe physical security components that can protect any computer and network.

2.4.1 Physical Security

"Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks)."

Physical security involves the use of multiple layers of interdependent systems which include CCTV surveillance, security guards, protective barriers, locks, access control protocols, and many other techniques.

Access control

Access control methods are used to monitor and control traffic through specific access points and areas of the secure facility. This is done using a variety of systems including CCTV surveillance, identification cards, security guards, and electronic/mechanical control systems such as locks, doors, and gates.

2.4.2 Bio Metric:

- Biometrics refers to metrics related to human characteristics and traits.
- Biometric identification (or biometric authentication)is used in computer science as a form of identification and access control.
- It is also used to identify individuals in groups that are under surveillance.
- Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals.
- Biometric identifiers are often categorized as physiological versus behavioral characteristics.
- Physiological characteristics are related to the shape of the body.
- Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent.
- Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.

Finger Print

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity.

Retina Biometric

A retinal scan, commonly confused with the more appropriately named "iris scanner", is a biometric technique that uses the unique patterns on a person's retina to identify them. It is

not to be confused with another ocular-based technology, iris recognition. The biometric use of this scan is used to examine the pattern of blood vessels at the back of the eye.

Voice Recognition

- In computer science and electrical engineering, speech recognition (SR) is the translation of spoken words into text. It is also known as "automatic speech recognition" (ASR), "computer speech recognition", or just "speech to text" (STT).
- Application of voice recognition
  - in a car system
  - Health care system
  - High performance fighter aircraft
  - Helicopters
  - Training air traffic controller
  - Telephony and other domains
  - Usage in education and daily life

Writing pattern recognition

- Keystroke dynamics, keystroke biometrics or typing dynamics, is the detailed timing information that describes exactly when each key was pressed and when it was released as a person is typing at a computer keyboard.
- Data needed to analyze keystroke dynamics is obtained by keystroke logging. Normally all that is retained when logging a typing session is the sequence of characte corresponding to the order in which keys were pressed and timing information discarded. When reading email, the receiver cannot tell from reading the phrase "I sa 3 zebras!" whether:
- That was typed rapidly or slowly
- the sender used the left shift key, the right shift key, or the caps-lock key to make the turn into a capitalized letter "I"
- the letters were all typed at the same pace, or if there was a long pause before letter "z" or the numeral "3" while you were looking for that letter
- the sender typed any letters wrong initially and then went back and corrected ther if they got them right the first time.
- Application: in commercial products

2.5 List potential threats on password and explain characteristics of a strong password.

- Password Management,
- vulnerability of password,
- password protection,
- password selection strategies,
- Components of a good password.

Password Management, protection and vulnerability of password:

- A sequence of symbols that only you know and the system that authenticates you can verify
- Password related threats
- **Guessing**
  - Exhaustive Search (Brute Force)
  - try all possible combinations
  - may work if the symbol space and password length are small
  - Intelligent Search
  - search possible passwords in a restricted space
  - related to the user: girlfriend/boyfriend name, car brand, phone number, birth date, ...
  - generic: meaningful words or phrases, dictionary attack

- **Spoofing**

- **Are you really talking to the server that you want to talk?**
  - fake login prompts
    - when you try to login a shared station
    - previous user may leave a fake login screen
  - how to avoid/detect
    - reboot
    - remote login is even worse,
    - telnet sends passwords in clear
    - use SSH (Secure Shell)
  -

password selection strategies,

1. Many users choose a password that is too short or too easy to guess. At the other extreme, if users are assigned passwords consisting of eight randomly selected printable characters, password cracking is effectively impossible. But it would be almost as impossible for most users to remember their passwords

2. Fortunately, even if we limit the password universe to strings of characters that are reasonably memorable, the size of the universe is still too large to permit practical cracking. Our goal, then, is to eliminate guessable passwords while allowing the user to select a password that is memorable. Four basic techniques are in use.

a. **Computer-generated passwords**
b. **Reactive password checking**
c. **Proactive password checking**

a. Computer-generated passwords

i) **Computer-generated passwords** also have problems. If the passwords are quite random in nature, users will not be able to remember them.

ii) Even if the password is pronounceable, the user may have difficulty remembering it and so be tempted to write it down.

iii) In general computer-generated password schemes have a history of poor acceptance by users

b. Reactive password checking

i) A **reactive password checking** strategy is one in which the system periodically runs its own password cracker to find guessable passwords. The system cancels any passwords that are guessed and notifies the user.

ii) This tactic has a number of drawbacks. First, it is resource intensive if the job is done right

Because a determined opponent who is able to steal a password file can devote full CPU time to the task for hours or even days, an effective reactive password checker is at a distinct disadvantage.

iii) Furthermore, any existing passwords remain vulnerable until the reactive password checker finds them.

c. **Proactive password checking**

i) The most promising approach to improved password security is a proactive password checker. In this scheme, a user is allowed to select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and, if not, rejects it.

ii) Such checkers are based on the philosophy that, with sufficient guidance from the system users can select memorable passwords from a fairly large password space that are not likely t be guessed in a dictionary attack.

iii) The trick with a proactive password checker is to strike a balance between user acceptability and strength.

Components of a good password.

- Use more than 8 characters (More Characters = Stronger Passwords)
- Include random characters within the password (#, @, %, $, etc.)
- Use both upper and lower case characters (i.e. – AbCdeF)
- Avoid using "dictionary" words or stereotypical passwords such as "dog", "red", o "password"
- Avoid using important dates or other meaningful information in your password
- Try using a passphrase instead of a password ."I8burger4d!NER" (I ate burger fo dinner).