UNIT:2

Organizational Security

Organizational Security Syllabus:

- 2.1 Password selection, Piggybacking, Shoulder surfing, Dumpster diving, Installing unauthorized software /hardware, Access by non-employees.
- 2.2 People as Security Tool: Security awareness, and Individual user responsibilities.
- 2.3 Physical security: Access controls

  Biometrics: finger prints, hand prints, Retina, Patterns, voice patterns, signature and writing patterns, keystrokes, Physical barriers
- 2.4 Password Management, vulnerability of password, password protection, password selection strategies, components of a good password.

VPMP POLYTECHNIC

2.1 Password Selection

- Guidelines on to how-to make a hard-to-crack password.
- **Steps:**
- Use appropriate length.
- Form a "random" sequence of words and/or letters.
- Add numbers to the base-word to make it more secure.
- Use punctuation and symbols to "complicate" it further.
- Create complexity with upper and lowercase letters.
- Generate similar but altered passwords.

VPMP POLYTECHNIC

CONTINUE…

- Change your passwords periodically or whenever it may have become compromised.
- Don't re-use an expired password.
- If you have trouble remembering all the passwords you need, try using a **password manager**, they can store all your passwords securely using a single master password.
- Try to memorize the password, and avoid writing it down.
- Do not use the same password for everything.
- Do not tell anybody your password.

VPMP POLYTECHNIC

PIGGYBACKING

- Piggybacking on Internet access is the practice of establishing a wireless Internet connection by using another subscriber's wireless Internet access service without the subscriber's explicit permission or knowledge.
- Piggybacking, in a wireless communications context, is the **unauthorized access of a wireless LAN.**
- Piggybacking is sometimes referred to as **"Wi-Fi squatting."**
- The usual **purpose** of piggybacking is simply **to gain free network access** rather than any malicious intent, but it can slow down data transfer for legal users of the network.

VPMP POLYTECHNIC

CONTINUE…

- Furthermore, a network that is vulnerable to piggybacking for network access is equally vulnerable when the purpose is data theft, dissemination of viruses etc.
- It's quite simple to access an unsecured wireless network: All you have to do is get into the range of a Wi-Fi hotspot's signal and select your chosen network from the options presented.
- However, unauthorized network access, even to free Wi-Fi, may be illegal. People have been fined for accessing hot spots from outside businesses, such as coffee shops, that provide free Wi-Fi for customers' use.

VPMP POLYTECHNIC

Continue…

- **To protect** your network from piggybacking, ensure that **encryption is enabled** for your router.
- Use Wireless Encryption Protocol (**WEP**), if possible use Wireless Protected Access (**WPA**) or WPA2.
- Use a strong password for your encryption key, consisting of at least 14 characters and mixing letters and numbers.
- Piggybacking can be defeated by logging out before walking away from a workstation or terminal or by initiating a screensaver that requires re-authentication when resuming

VPMP POLYTECHNIC

SHOULDER SURFING

- A term used to describe a **person that looks over another person's shoulder as they enter data into a computer or other device.**
- For example, someone might shoulder surf when you are entering your computer password, ATM pin, or credit card number.
- Criminals often use used this technique to gain access to your personal accounts or read personal information, such as e-mails.

VPMP POLYTECHNIC

Dumpster Diving

- In IT, dumpster diving refers to using various methods to get information about a technology user.
- In general, dumpster diving involves **searching through trash or garbage looking** for something useful. This is often done to uncover useful information that may help an individual get access to a particular network.
- In many cases, dumpster diving involves getting data about a user in order to impersonate that user and gain access to his or her user profiles or other restricted areas of the Internet or a local network.

VPMP POLYTECHNIC

INSTALLING UNAUTHORIZED SOFTWARE /HARDWARE

- One of the nightmares that many administrators face is users installing unauthorized software on their notebook computers. Such installations can have very bad consequences, but tracking them can be difficult. Here are a couple of approaches you can take to counteract this user behavior.
- Organizations may want to limit the installation of applications on notebook computers that they assign to employees.
- One way to do this is to make sure that all users are members of the users group, and NOT a member of the administrators group. This will prevent the user from installing applications that can alter the configuration.

VPMP POLYTECHNIC

Continue…

- Another approach is to modify a sub key in the registry, which can be done by performing the following:
- Start regedit
  Go to
  HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion PoliciesExplorer
  Double-click the PromptRunasInstallNetpath value (If this is not present you can create a new string value)
  Set this value to 1
  Click OK
- The above procedure can lock the system down thereby preventing the user from installing any new software.

VPMP POLYTECHNIC

ACCESS CONTROL BY NON-EMPLOYEES

- **Access controls:**
- Physical access control:
- Physical security is primarily concerned with restricting physical access by unauthorized people (commonly interpreted as intruders) .

VPMP POLYTECHNIC

2.2 People as Security Tool

- **Security awareness , and Individual user responsibilities:**
- **Security awareness:**
- **Security awareness** is the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization.
- Being security aware means you understand that there is the potential for some people to deliberately or accidentally steal, damage, or misuse the data that is stored within a company's computer systems and throughout its organization.

VPMP POLYTECHNIC

Continue…

- Be polite and use appropriate language:
- You are a representative of your organization.
- You should not submit threatening materials or messages either public or private.
- **Privacy:**
- Do not reveal any personal information about yourself(like Home address, phone no., photographs)
- **E-mail:**
- Include your signature at the bottom of email message.
- Send email only to individuals and groups you know.
- **Accountability**:
- User should not provide their password to any person.

VPMP POLYTECHNIC

2.3 Physical security: Access Control

- The meaning of access control has changed over the last several years.
- Originally, access control usually refereed to restricting physical access to a facility, building or room to authorized persons. This used to be enforced mainly through a physical security guard.
- Then, with the advent of electronic devices, access control has evolved into the use of physical card access systems of a wide variety including biometric activated devices.

VPMP POLYTECHNIC

Continue…

- Initially "access control lists" evolved specifying the user identities and the privileges granted to them in order to access a network operating system or an application.
- Access control authentication devices evolved to include id and password, digital certificates, security tokens, smart cards and biometrics.
- Access control authorization means role based access control (RBAC).
- Mandatory access control is access control policies that are determined by the system and not the application or information owner. RBAC is commonly found in government, military and other enterprises where the role definitions are well defined.

VPMP POLYTECHNIC

PHYSICAL ACCESS CONTROL

- Physical security is primarily concerned with restricting physical access by unauthorized people (commonly interpreted as intruders) .

VPMP POLYTECHNIC

Continue…

- For instance, physical access controls for protected facilities are generally intended to:
- deter potential intruders (e.g. warning signs and perimeter markings);
- distinguish authorized from unauthorized people (e.g. using keycards/access badges)
- delay, frustrate and ideally prevent intrusion attempts (e.g. strong walls, door locks and safes);
- detect intrusions and monitor/record intruders (e.g. intruder alarms and CCTV systems); and
- trigger appropriate incident responses (e.g. by security guards and police).

VPMP POLYTECHNIC

LOGICAL ACCESS CONTROLS

- logical access controls are tools used for identification, authentication, authorization, and accountability in computer information systems.
- Logical access controls enforce access control measures for systems, programs, processes, and information.
- The controls can be embedded within operating systems, applications, add-on security packages, or database and telecommunication management systems.

VPMP POLYTECHNIC

CONTINUE…

- The line between Logical access and physical access can be blurred when physical access is controlled by software.
- For example, entry to a room may be controlled by a chip and PIN card and an electronic lock controlled by software.
- Only those in possession of an appropriate card, with an appropriate security level and with knowledge of the PIN are permitted entry to the room.

VPMP POLYTECHNIC

Continue…

- On swiping the card into a card reader and entering the correct PIN, the user's security level is checked against a security database and compared to the security level required to enter the room.
- If the user meets the security requirements, entry is permitted.
- Having logical access controlled centrally in software allows a user's physical access permissions to be rapidly amended or revoked.

VPMP POLYTECHNIC

Continue…

- Logical Controls, also called logical access controls and technical controls, protect data and the systems, networks, and environments that protect them.
- In order to authenticate, authorize, or maintain accountability a variety of methodologies are used such as password protocols, devices coupled with protocols and software, encryption, firewalls, or other systems that can detect intruders and maintain security, reduce vulnerabilities and protect the data and systems from threats.

VPMP POLYTECHNIC

Biometric

Why we use Biometric Security System?

- Each person has a set of unique characteristics that can be used for authentication.
- Biometrics uses these unique characteristics for authentication.
- Today’s Biometric systems examine retina patterns, iris patterns, fingerprints, handprints, voice patterns, keystroke patterns etc for authentication.
- But most of the biometric devices which are available on the market, only retina pattern, iris patterns, fingerprint and handprint systems are properly classified as biometric systems. Others are more classified as behavioral systems.

VPMP POLYTECHNIC

CONTINUE…

- Biometric identification systems normally work by obtaining unique characteristics from you, like a handprint, a retina pattern etc. The biometric system then compares that to the specimen data stored in the system.
- Biometrics authentication is much better when compared with other types of authentication methods. But the users are reluctant in using biometric authentication.
- **For example**, many users feel that retina scanner biometric authentication system may cause loss of their vision. False positives and false negatives are a serious problem with Biometric authentication.

VPMP POLYTECHNIC

FINGER PRINT

- Fingerprints are used in forensic and identification for long time. Fingerprints of each individual are unique.
- Fingerprint Biometric Systems **examine the unique characteristics of your fingerprints** and use that information to determine whether or not you should be allowed access.
- Some smart phones like the Apple iPhone 5S even have sensors to capture our fingerprints and thus guarantee that we are the only people who can unlock our phones.
- The user's finger is placed on the scanner surface. Light flashes inside the machine, and the reflection is captured by a scanner, and it is used for analysis and then verified against the original specimen stored in the system.
- Implementation costs are low and the technology has good user acceptance.

VPMP POLYTECHNIC

Voice Pattern

- Voice biometric authentication is the use of the voice pattern to verify the identity of the individual. It is fast becoming a widely deployed form of biometric authentication.
- Voice biometrics works by digitizing a profile of a person's speech to produce a stored model voice print, or template.
- Biometric technology reduces each spoken word to segments composed of several dominant frequencies called formants. Each segment has several tones that can be captured in a digital format. The tones collectively identify the speaker's unique voice print. Voice prints are stored in databases in a manner similar to the storing of fingerprints or other biometric data.

VPMP POLYTECHNIC

CONTINUE…

- A person's speech is subject to change depending on health and emotional state. Matching a voice print requires that the person speak in the normal voice that was used when the template was created at enrollment.
- If the person suffers from a physical ailment, such as a cold, or is unusually excited or depressed, the voice sample submitted may be different from the template and will not match.
- Other factors also affect voice recognition results. Background noise and the quality of the input device (the microphone) can create additional challenges for voice recognition systems.

VPMP POLYTECHNIC

CONTINUE…

- If authentication is being attempted remotely over the telephone, the use of a cell phone instead of a landline can affect the accuracy of the results.
- Voice recognition systems may be vulnerable to replay attacks: if someone records the authorized user's phrase and replays it, that person may acquire the user's privileges.

VPMP POLYTECHNIC

Retina Pattern Biometric Systems

- Everybody has a unique retinal vascular pattern. Retina Pattern Biometric system uses an infrared beam to scan your retina.
- Retina pattern biometric systems examine the unique characteristics of user's retina and compare that information with stored pattern to determine whether user should be allowed access.
- Retina Pattern Biometric Systems are highly reliable. Users are often worried in using retina scanners because they fear that retina scanners will blind or injure their eyes.

VPMP POLYTECHNIC

HANDPRINTS BIOMETRIC SYSTEMS

- As in the case of finger print, everybody has unique handprints.
- A handprint Biometric Systems scans hand and finger ,the data is compared with the specimen stored for you in the system.
- The user is allowed or denied based on the result of this verification.

VPMP POLYTECHNIC

KEYSTROKE BIOMETRIC SYSTEM

- A keystroke biometric system for long-text input was developed and evaluated for identification and authentication applications.
- TypeSense is a software-only authentication solution based on the science of typeprint recognition that uses keystroke dynamics to accurately identify a user by the way they type characters across a keyboard.

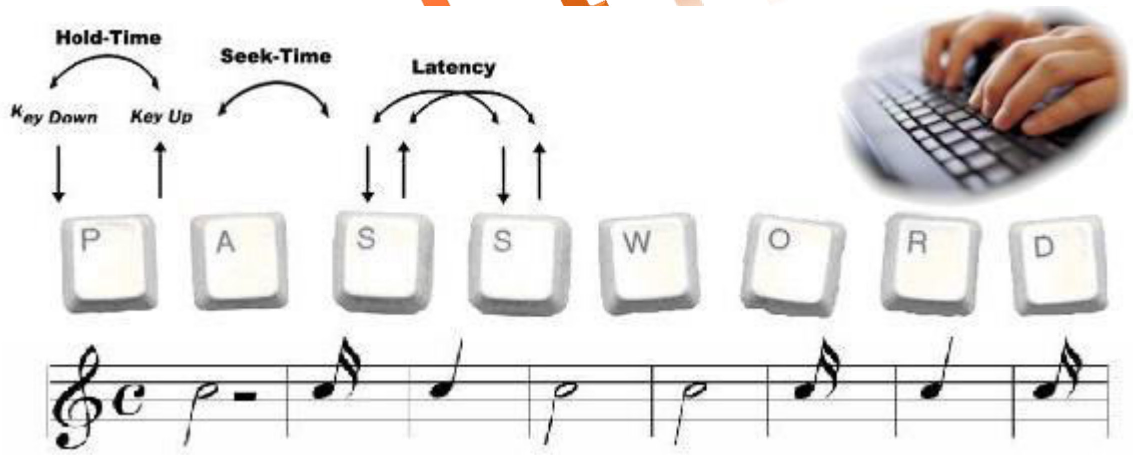
VPMP POLYTECHNIC

How it works

- Keystroke Dynamics technology extracts the distinctive characteristics found in typed sequences of characters, and creates a statistically unique signature from the typing patterns of a person.
- These distinctive features include the duration for which keys are held and the elapsed time between successive keystrokes.

VPMP POLYTECHNIC

Continue…



VPM
LYTECHNIC

KEY FEATURES

- **No Hardware Required**

  Unlike fingerprint and other biometric solutions that require a special hardware reader or scanner, TypeSense does not need to install any new hardware – it works with the standard computer keyboard.

- **No Software Installed**

  Type Sense does not require any software to be pre-installed on the user's PC for web-based applications.

VPMP POLYTECHNIC

Continue…

- **Nothing to Carry, Lose, or Forget**

  Across all types of authentication technologies, TypeSense is the only solution that does not require users to carry any device.

- **Nothing Extra to Type at Logon**

  With TypeSense, you will be asked to type what you always enter at logon: your username and password. TypeSense is completely transparent to the users.

- **Flexible Enrolment**

VPMP POLYTECHNIC

PHYSICAL BARRIERS

- Barriers are used in physical security to define boundaries, delay or prevent access, restrict movement to a particular area, obscure visual observation into or from an area, and prevent technical penetration of an area.
- When barriers are selected and installed properly, they can represent not only a physical impediment but also a psychological deterrent to an attacker.

VPMP POLYTECHNIC

CONTINUE…

- Manmade structural barriers and natural barriers are two general types of barriers. Often, both types are used to secure Forest Service facilities. Other types of barriers (human barriers, such as guards; animal barriers, such as dogs) are beyond the scope of this Web site.
- Manmade structural barriers include fences and walls, doors, gates, turnstiles, vehicular barriers, glazing (usually glass), and nearly all building materials.

VPMP POLYTECHNIC

CONTINUE…

- Natural barriers include berms, rocks, trees and other foliage, water features, sand and gravel, and other natural terrain features that are difficult to traverse or that expose an attacker.
- Barriers, whether natural or manmade, must be tested regularly and maintained.
- Barring any unusual occurrences, an inspection every week or two generally is adequate.

VPMP POLYTECHNIC

CONTINUE…

- To the greatest extent possible without sacrificing security, barriers should be esthetically compatible with your facility.
- This is more than a "look nice" issue.
- Physical security measures should not attract undue attention to your facility.
- Putting an eight-foot chain link fence with.

VPMP POLYTECHNIC

CONTINUE…

- The barriers you select and install to keep attackers out also may keep rescuers out. Work closely with public safety first responders to ensure they know the barriers you have used and where they have been deployed.
- Barriers also can work against you psychologically. The more imposing the barrier and the more impenetrable it looks, the more likely employees are to presume that anyone inside the barrier (inside the "secure" area) belongs there. An effective barrier does not immediately guarantee everyone inside is supposed to be there.

VPMP POLYTECHNIC

CONTINUE…

- Physical barriers such as fences, walls, and vehicle barriers act as the outermost layer of security.
- They serve to prevent, or at least delay, attacks, and also act as a psychological deterrent by defining the perimeter of the facility and making intrusions seem more difficult.
- Tall fencing, topped with barbed wire, razor wire or metal spikes are often emplaced on the perimeter of a property, generally with some type of signage that warns people not to attempt to enter.

VPMP POLYTECHNIC

CONTINUE…

- However, in some facilities imposing perimeter walls/fencing will not be possible (e.g. an urban office building that is directly adjacent to public sidewalks) or it may be aesthetically unacceptable (e.g. surrounding a shopping center with tall fences topped with razor wire); in this case, the outer security perimeter will be defined as the walls/windows/doors of the structure itself.

VPMP POLYTECHNIC

2.4 Password Protection: How to Create Strong Passwords

- **Use Different Passwords Everywhere** Why would you do this when it's so easy to just type "fido" at every password prompt?
- Here's why: If "fido" gets cracked once, it means the person with that info now has access to all of your online accounts.

VPMP POLYTECHNIC

CONTINUE…

- **Avoid Common Passwords** If the word you use can be found in the dictionary, it's not a strong password.
- If you use numbers or letters in the order they appear on the keyboard ("1234" or "qwerty"), it's not a strong password.
- If it's the name of your relatives, your kids, or your pet, favorite team, or city of your birth, guess what—it's not a strong password.
- If it's your birthday, anniversary, date of graduation, even your car license plate number, it's not a strong password.

VPMP POLYTECHNIC

Continue…

- It doesn't matter if you follow this with another number.
- These are all things hackers would try first. They write programs to check these kinds of passwords first, in fact.

VPMP POLYTECHNIC

STRONG PASSWORD SOLUTIONS

- **How to Build Strength** To create a strong password, you should use a string of text that mixes numbers, letters that are both lowercase and uppercase, and special characters.
- It should be eight characters, preferably many more. A lot more. The characters should be random, and not follow from words, alphabetically, or from your keyboard layout.

VPMP POLYTECHNIC

CONTINUE…

- So how do you make such a password?
- **1)** Spell a word backwards. (Example: Turn "New York" into "kroywen.")
  2) Use l33t speak: Substitute numbers for certain letters. (Example: Turn "kroywen" into "kr0yw3n.")
  3) Randomly throw in some capital letters. (Example: Turn "kr0yw3n" into "Kr0yw3n.")
  4) Don't forget the special character. (Example: Turn "Kr0yw3n" into "Kr0yw3^.")

VPMP POLYTECHNIC

PASSWORD SELECTION STRATEGIES

- **User Education:**
  - User can be told the importance of using hard to guess password and can be provided with guidelines for selecting strong passwords.
- **Computer generated password:**
  - Computer generated password also have problems.
  - If the passwords are quite random in nature, user will not be able to remember it, and write it down.

VPMP POLYTECHNIC

CONT…

- **Reactive password checking:**
  - The system periodically runs its own password cracker to find guessable passwords.
  - The system cancels passwords that are guessed and notifies user.
  - Consumes resources.
  - Hackers can use this on their own machine with a copy of the password file. Can they get the password file?
- **Proactive password checking:**
  - The system checks at the time of selection if the password is allowable.
  - With guidance from the system, users can select memorable passwords that are difficult to guess.

VPMP POLYTECHNIC

Components of a Good Password

- Common guidelines to make the password more difficult to guess or obtain are as follows:
- It should be at least eight characters long.
- It should include uppercase and lowercase letters, numbers, special characters or punctuation marks.
- It should not contain dictionary words.
- It should not contain the user's personal information such as their name, family member's name, birth date, pet name, phone number or any other detail that can easily be identified.
- It should not be the same as the user's login name.
- It should not be the default passwords as supplied by the system vendor such as password, guest, admin and so on.

VPMP POLYTECHNIC