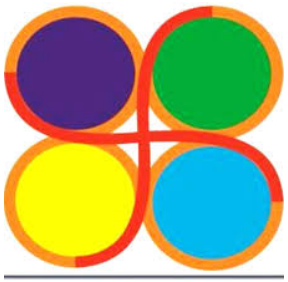


Government Polytechnic Ahmedabad
Program: Diploma in Computer Engg
Computer and Network Security (3350704-C304)

UNIT_2
Organizational security

Unit-2

- Password selection
- People as a security tool
- Physical security
- Password management

Password selection

- The front line of defense against intruders is the password system.
- Virtually all multiuser systems require that a user provide not only a name or identifier (ID) but also a password.
- The password serves to authenticate the ID of the individual logging on to the system.
- Passwords are usually stored encrypted rather than in the clear (which would make them more vulnerable to theft).
- More recent O/S's use a cryptographic hash function.

Poor password

- Your first name, last name, or login name, in any form
- Consecutive or repetitive numbers or letters such as 12345678 or AAAAAAAA
- Adjacent keyboard letters such as qwerty or asdfghjk
- Common and obvious letter-number replacements (e.g. replace the letter O with number 0)
- Easily guessed personal information such as names and dates of yourself, family members, pets and close acquaintances

Poor password

- Dictionary words, in any language, forward and backward
- Popular book titles, movie titles, or phrases
- Short passwords
- Easily obtained information, such as:
  - Address
  - License plate numbers
  - Telephone numbers
  - Credit card or ATM numbers
  - Social security or Social insurance numbers
  - Email addresses

Piggybacking

- People are often in a hurry and will frequently not follow good physical security practices and procedures.
- Attackers know this and may try to exploit this characteristic in human behaviour.
- Tailgating or piggybacking is the simple tactic of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building.
- An attacker can thus gain access to the facility without having to know the access code or having to acquire an access card.
- It is similar to shoulder surfing in that it relies on the attacker taking advantage of an authorized user not following security procedures.

Piggybacking

- Frequently the attacker may even start a conversation with the target before reaching the door so that the user may be more comfortable with allowing the individual in without challenging them.
- In this sense piggybacking is related to social engineering attacks. Both the piggybacking and shoulder surfing attack techniques can be easily countered by using simple procedures to ensure nobody follows you too closely or is in a position to observe your actions. Both of these rely on the poor security practices of an authorized user in order to be successful.
- A more sophisticated countermeasure to piggybacking is a “man trap,” which utilizes two doors to gain access to the facility. The second door does not open until the first one is closed and is spaced close enough to the first that an enclosure is formed that only allows one individual through at a time.

Shoulder Surfing

- Shoulder surfing does not necessarily involve direct contact with the target, but instead involves the attacker directly observing the individual entering sensitive information on a form, keypad, or keyboard.
- The attacker may simply look over the shoulder of the user at work, for example, or may set up a camera or use binoculars to view the user entering sensitive data.
- The attacker can attempt to obtain information such as a personal identification number (PIN) at an automated teller machine (ATM), an access control entry code at a secure gate or door, or a calling card or credit card number.

Shoulder Surfing

- Many locations now use a small shield to surround a keypad so that it is difficult to observe somebody entering information. More sophisticated systems can actually scramble the location of the numbers so that the top row at one time includes the numbers 1, 2, and 3 and the next time 4, 8, and 0.

- While this makes it a bit slower for the user to enter information, it thwarts an attacker's attempt to observe what numbers are pressed and enter the same buttons/pattern, since the location of the numbers constantly changes.

- Although methods such as adding shields to block the view or having the pad "scramble" the numbers can help make shoulder surfing more difficult, the best defense is for users to be aware of their surroundings and to not allow individuals to get into a position from which they can observe what the user is entering.

- The attacker may attempt to increase the chance of successfully observing the target entering the data by starting a conversation with the target.
- This provides an excuse for the attacker to be physically closer to the target. Otherwise, the target may be suspicious if the attacker is standing too close. In this sense, shoulder surfing can be considered a social engineering attack.

Dumpster Diving

- As mentioned earlier, attackers need a certain amount of information before launching their attack.
- One common place to find this information, if the attacker is in the vicinity of the target, is the target's trash.
- The attacker might find little bits of information that could be useful for an attack.
- This process of going through a target's trash in hopes of finding valuable information that might be used in a penetration attempt is known in the computer community as dumpster diving.
- The tactic is not, however, unique to the computer community; it has been used for many years by others, such as identity thieves, private investigators, and law enforcement personnel, to obtain information about an individual or organization.

Dumpster Diving

- If the attackers are very lucky, and the target's security procedures are very poor, they may actually find user IDs and passwords.
- users sometimes write their password down. If, when the password is changed, they discard the paper the old password was written on without shredding it, the lucky dumpster diver can gain a valuable clue.
- Even if the attacker isn't lucky enough to obtain a password directly, he undoubtedly will find employee names, from which it's not hard to determine user IDs.

Dumpster Diving

- Manuals from hardware or software that have been purchased may also provide clues as to what vulnerabilities exist on the target's computer systems and networks.
- Finally, the attacker may gather a variety of information that can be useful in a social engineering attack.
- In most locations, trash is no longer considered private property after it has been discarded (and even where dumpster diving is illegal, little enforcement occurs).
- An organization should have policies about discarding materials. Sensitive information should be shredded and the organization should consider securing the trash receptacle so that individuals can't forage through it.

Installing Unauthorized Hardware and Software

- Organizations should have a policy that restricts the ability of normal users to install software and new hardware on their systems.
- A common example is a user installing unauthorized communication software and a modem to allow them to connect to their machine at work via a modem from their home.
- Another common example is a user installing a wireless access point so that they can access the organization's network from many different areas.
- In these examples, the user has set up a backdoor into the network, circumventing all the other security mechanisms in place. The term "rogue modem" or "rogue access point" may be used to describe these two cases.

Installing Unauthorized Hardware and Software

- A backdoor is an avenue that can be used to access a system while circumventing normal security mechanisms and can often be used to install additional executable files that can lead to more ways to access the compromised system.
- Security professionals can use widely available tools to scan their own systems periodically for either of these rouge devices to ensure that users haven’t created a backdoor.

Cont…

- Another common example of unauthorized software that users install on their systems is games. Unfortunately, not all games come in shrink wrapped packages. Numerous small games can be downloaded from the Internet.
- The problem with this is that users don't always know where the software originally came from and what may be hidden inside it. Many individuals have unwittingly installed what seemed to be an innocuous game, only to have downloaded a piece of malicious code capable of many things, including opening a backdoor that allows attackers to connect to, and control, the system from across the Internet.

- Because of these potential hazards, many organizations do not allow their users to load software or install new hardware without the knowledge and assistance of administrators.

Access by non employee

- As has been mentioned, if an attacker can gain physical access to a facility, chances are very good that the attacker can obtain enough information to penetrate computer systems and networks.
- Many organizations require employees to wear identification badges when at work. This is an easy method to quickly spot who has permission to have physical access to the organization and who does not.
- While this method is easy to implement and can be a significant deterrent to unauthorized individuals, it also requires that employees actively challenge individuals who are not wearing the required identification badge.

Access by non employee

- This is one area where organizations fail. Combine an attacker who slips in by piggybacking off of an authorized individual and an environment where employees have not been encouraged to challenge individuals without appropriate credentials and you have a situation where you might as well not have any badges in the first place.
- Organizations also frequently become complacent when faced with what appears to be a legitimate reason to access the facility, such as when an individual shows up with a warm pizza claiming it was ordered by an employee.
- It has often been stated by security consultants that it is amazing what you can obtain access to with a pizza box or a vase of flowers. If the organization doesn't enforce good password policies, a casual stroll through an office may yield passwords or other important information.

Access by non employee

- Another aspect that must be considered is personnel who have legitimate access to a facility but also have intent to steal intellectual property or otherwise exploit the organization.
- Physical access provides an easy opportunity for individuals to look for the occasional piece of critical information carelessly left out.
- With the proliferation of devices such as cell phones with built-in cameras, an individual could easily photograph information without it being obvious to employees.

Access by non employee

- Contractors, consultants, and partners frequently not only have physical access to the facility but may also have network access.
- Other individuals who typically have unrestricted access to the facility when no one is around are nighttime custodial crewmembers and security guards. Such positions are often contracted out.
- As a result, hackers have been known to take temporary custodial jobs simply to gain access to facilities.

People as a Security Tool

- Security Awareness
- Individual User Responsibilities

Security Awareness

- Probably the single most effective method to counter potential social engineering attacks, after establishment of the organization's security goals and policies, is an active security awareness program.

- The extent of the training will vary depending on the organization's environment and the level of threat, but initial employee training on social engineering at the time a person is hired is important, as well as periodic refresher training.

- Many government organizations have created security awareness posters to constantly remind individuals of this possible avenue of attack.
- Security news letters, often in the form of e-mail, have also been used to remind employees of their security responsibilities.

Security Awareness

- An important element that should be stressed in training about social engineering is the type of information that the organization considers sensitive and which may be the target of a social engineering attack.

- There are undoubtedly signs that the organization could point to as indicative of an attacker attempting to gain access to sensitive corporate information.
- All employees should be aware of these indicators. The scope of information that an attacker may ask for is very large, and many questions attackers pose might also be legitimate in another context (asking for the phone number for somebody, for example).

- Employees should be taught to be cautious about revealing personal information and should especially be alert for questions regarding account information, personally identifiable information, or passwords.

Individual User Responsibilities

- Individual user responsibilities vary between organizations and the type of business the organization is involved in, but there are certain very basic responsibilities that all users should be instructed to adopt:

Individual User Responsibilities

- Lock the door to your office or workspace.
- Do not leave sensitive information inside your car unprotected.
- Secure storage media containing sensitive information in a secure storage device.
- Shred paper containing organizational information before discarding it.
- Do not divulge sensitive information to individuals (including other employees) who do not have an authorized need to know it.

Individual User Responsibilities

- Do not discuss sensitive information with family members. (The most common violation of this rule occurs in regard to HR information, as employees, especially supervisors, may complain to their spouse about other employees or problems that are occurring at work.)
- Protect laptops that contain sensitive or important organization information wherever the laptop may be stored or left. (It's a good idea to ensure that sensitive information is encrypted on the laptop so that, should the equipment be lost or stolen, the information remains safe.)
- Be aware of who is around you when discussing sensitive corporate information. Does everybody within earshot have the need to hear this information?

Individual User Responsibilities

- Enforce corporate access control procedures. Be alert to, and do not allow, piggybacking, shoulder surfing, or access without the proper credentials.
- Be aware of the correct procedures to report suspected or actual violations of security policies.
- Follow procedures established to enforce good password security practices. Passwords are such a critical element that they are frequently the ultimate target of a social engineering attack. Though such password procedures may seem too oppressive or strict, they are often the best line of defense.

Individual User Responsibilities

- As a final note on user responsibilities, corporate security officers must cultivate an environment of trust in their office, as well as an understanding of the importance of security.
- If users feel that security personnel are only there to make their life difficult or dredge up information that will result in an employee's termination, the atmosphere will quickly turn adversarial and be transformed into an "us versus them" situation.
- Security personnel need the help of all users and should strive to cultivate a team environment in which users, when faced with a questionable situation, will not hesitate to call the security office.
- In situations like this, security offices should remember the old adage of "don't shoot the messenger."

Physical Security

- Physical security consists of all mechanisms used to ensure that physical access to the computer systems and networks is restricted to only authorized users.
- Additional physical security mechanisms may be used to provide increased security for especially sensitive systems such as servers and devices such as routers, firewalls, and intrusion detection systems.
- When considering physical security, access from all six sides should be considered—not only should the security of obvious points of entry be examined, such as doors and windows, but the walls themselves as well as the floor and ceiling should also be considered.

Physical Security

Questions such as the following should be addressed:

- Is there a false ceiling with tiles that can be easily removed?
- Do the walls extend to the actual ceiling or only to a false ceiling?
- Is there a raised floor?
- Do the walls extend to the actual floor, or do they stop at a raised floor?
- How are important systems situated?
- Do the monitors face away from windows, or could the activity of somebody at a system be monitored?
- Who has access to the facility?
- What type of access control is there, and are there any guards?
- Who is allowed unsupervised access to the facility?
- Is there an alarm system or security camera that covers the area?
- What procedures govern the monitoring of the alarm system or security camera and the response should unauthorized activity be detected? These are just some of the numerous questions that need to be asked when examining the physical security surrounding a system.

Access Controls

- The purpose of physical access controls is the same as that of computer and network access controls—you want to restrict access to only those who are authorized to have it.

- Physical access is restricted by requiring the individual to somehow authenticate that they have the right or authority to have the desired access.

- As in computer authentication, access in the physical world can be based on something the individual has, something they know, or something they are. Frequently, when dealing with the physical world, the terms “authentication” and “access control” are used interchangeably.

Access Controls

- The most common physical access control device is a lock. Combination locks represent an access control device that depends on something the individual knows (the combination).
- Locks with keys depend on something the individual has (the key). Each of these has certain advantages and disadvantages. Combinations don’t require any extra hardware, but they must be remembered and are hard to control.
- Anybody who knows the combination may provide it to somebody else. Key locks are simple and easy to use, but the key may be lost, which means another key has to be made or the lock has to be rekeyed.

Access Controls

- For example, if one employee enters the combination to a door and then opens it, another individual might follow quickly behind before the door closes to avoid having to enter the combination.
- A security guard checking each individual's identification would eliminate this problem.

Access control

- Access control is security technique that regulates who can view or use resources or information in a computing environment.
- Access control systems performs identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans.
- The goal of access control is to minimize the risk of unauthorized access to physical and logical systems.
- AC is a process that is integrated into an organization's IT environment.
- AC systems are complex and can be challenging to manage in dynamic IT environments

AC

- Two categories of AC:
  - Physical AC:
    - Limits access to campuses, building,rooms and physical IT assets.
  - Logical AC:
    - Limits connections to computer networks, system files and data.

Cont..

- Types of AC:
  - Mandatory AC(MAC)
  - Discretionary AC(DAC)
  - Role based AC(Non DAC)
  - Rule based AC

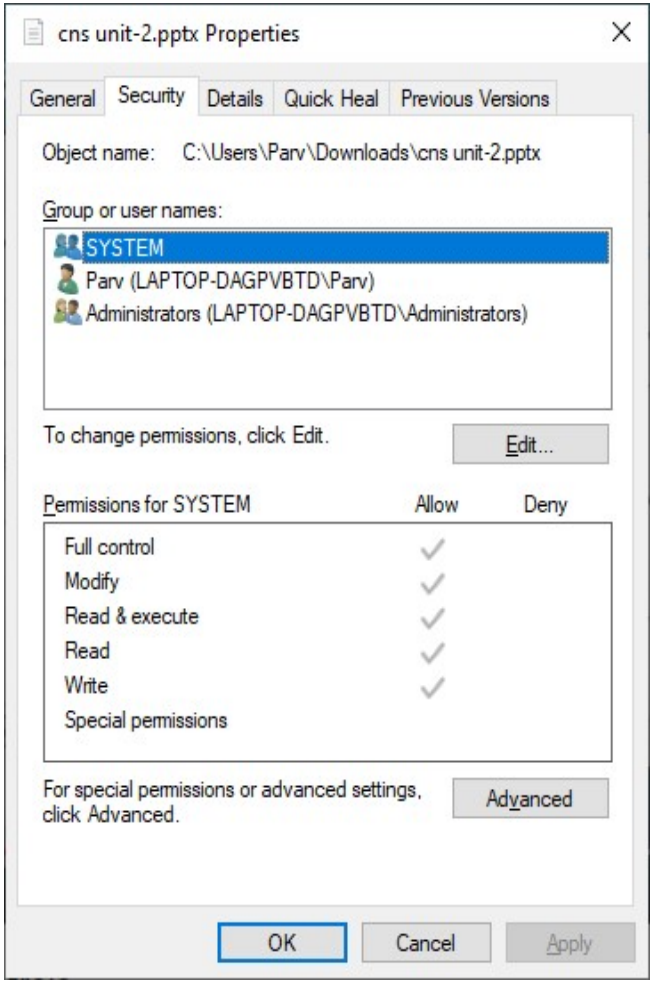
MAC

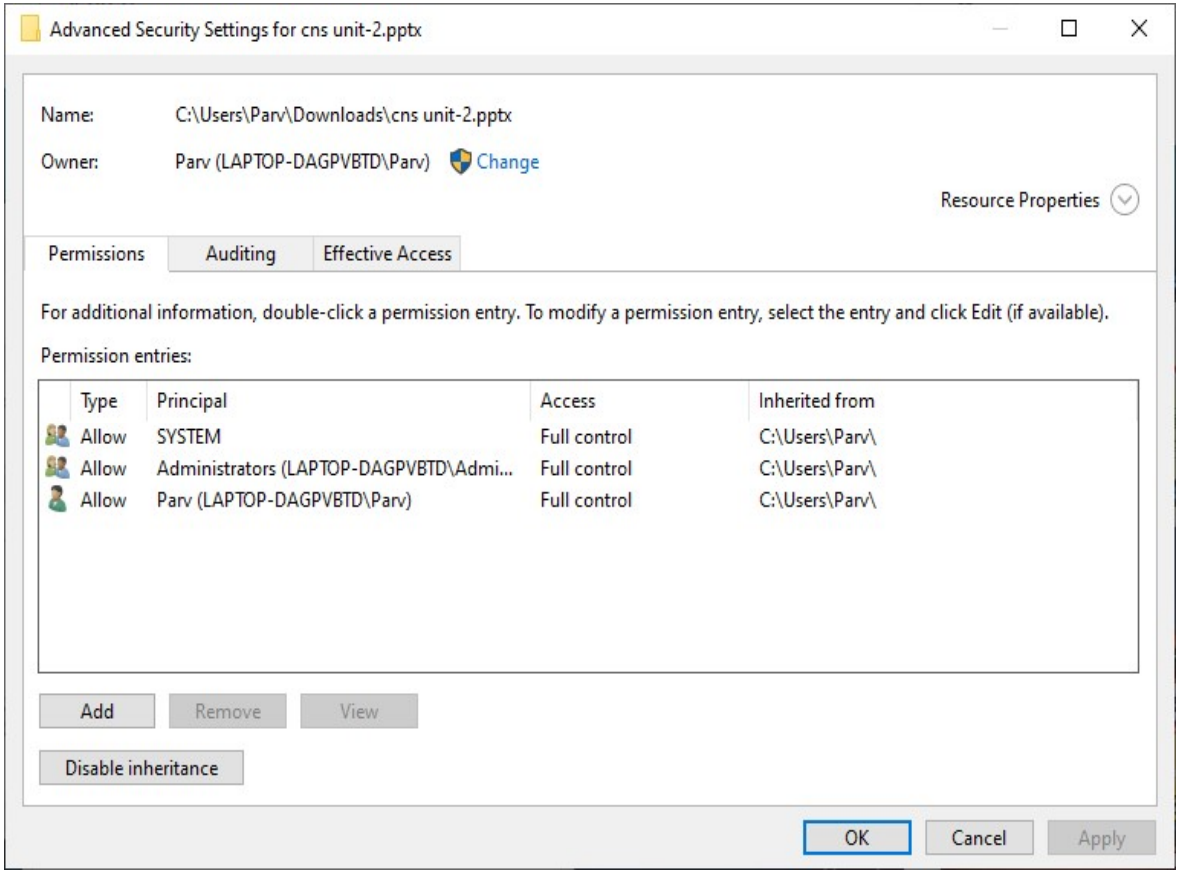
- Strictest form of AC mechanism using by organizing
- Use hierarchical approach to controlling access to resources.
- Used in government and military environments.
- Access to all resource objects is controlled by setting defined by system administrator (OS based)
- Resource object and user accounts are assigned security labels (classification and category)
- When user attempts to access a resource, the system checks with user's security label and compare to the properties of object's security labels.
- MAC requires high amount of planning before implementation, and also imposes a high system management overhead.

Discretionary AC(DAC)

- Allow each user to control access to their own data.
- Default access control mechanism for most desktop OS.
- Instead of security label in case of MAC, DAC has an AC list (ACL) associated with each resource objects.
- An ACL contains list of users or groups to which the owner user has permitted access to resource object with level of access(read, write, full control).
- User A provides read-only access on one of his file to User B, and read and write access on same file to user C.
- More flexible environment than mandatory AC.

DAC


cns unit-2.pptx Properties
General
Security
Details
Quick Heal
Previous Versions
Object name: C:\Users\Parv\Downloads\cns unit-2.pptx
Group or user names:
SYSTEM
Parv (LAPTOP-DAGPVBTD\Parv)
Administrators (LAPTOP-DAGPVBTD\Administrators)
To change permissions, click Edit.
Edit...
Permissions for SYSTEM
Allow
Deny
Full control
Modify
Read & execute
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply


Advanced Security Settings for cns unit-2.pptx
Name: C:\Users\Parv\Downloads\cns unit-2.pptx
Owner: Parv (LAPTOP-DAGPVBTD\Parv)
Change
Resource Properties
Permissions
Auditing
Effective Access
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).
Permission entries:
Type
Principal
Access
Inherited from
Allow SYSTEM Full control C:\Users\Parv\
Allow Administrators (LAPTOP-DAGPVBTD\Admi... Full control C:\Users\Parv\
Allow Parv (LAPTOP-DAGPVBTD\Parv) Full control C:\Users\Parv\
Add
Remove
View
Disable inheritance
OK
Cancel
Apply

Role based AC

- Also known as Non discretionary access control.
- Based on user's job function (role) within the organization.
- RBAC assigns permission to access resource object to particular roles in organization.
- Users are then assigned to that particular roles.
- An accountant in a company will be assigned to the *Accountant_Role,* permits access to all the resources permitted for all accountants.
- Similarly a software engineer might be assigned to the Developer_Role.
- Users may have multiple roles also.

RULE BASED AC

- Access is allowed or denied to resource object based on set of rules defined by system administrator.
- Access properties are stored in access control list (ACL) associated with each resource object.
- When user attempts to access a resource, operating system checks the rules contained in the ACL.
- These rules are based on conditions, such as days of the week, time of day or location.
- It is common scenario that most of the organization uses Role based and Rule based AC mechanism to enforce access policies and procedures.

Biometrics

- Access controls that utilize something you know (for example, combinations) or something you have (such as keys) are not the only methods to limit facility access to authorized individuals.
- A third approach is to utilize something unique about the individual—their fingerprints, for example—to identify them. Unlike the other two methods, the something-you-are method, known as biometrics, does not rely on the individual to either remember something or to have something in their possession.
- Biometrics is a more sophisticated access control approach and is also more expensive. Other methods to accomplish biometrics include handwriting analysis, retinal scans, iris scans, voiceprints, hand geometry, and facial geometry.

Biometrics

- Biometrics can be used both to control access to computer systems and networks and to control physical access to restricted areas, but when used for physical access control, methods can be used that are not generally used in biometric access control for computer systems and networks.
- Hand geometry, for example, requires a fairly large device. This can easily be placed outside of a door to control access to the room but would not be as convenient to control access to a computer system, since a reader would need to be placed with each computer or at least with groups of computers.
- In a mobile environment where laptops are being used, a device such as a hand geometry reader would be unrealistic.

Biometrics

- To add an additional layer of security, biometric devices are normally used in conjunction with another access control method.
- An individual might, for example, be required to also provide a personal access code (something they know) or to pass a card through a reader (something they have).
- While it may seem at first that nothing else should be needed besides a biometric access control, the biometric devices currently in use are not 100 percent accurate and have been known to allow access to individuals who were not authorized.
- This is the reason for the additional something-you-know or something-you-have method to supplement the biometric device.

Biometrics

- All forms of authentication have weaknesses that can be exploited. It is for this reason that “strong authentication” or “two-factor authentication” is often used.
- These methods use two of the three different types of authentication (something you have, know, or are) to provide two levels of security, as in the previous example of a biometric device and a swipe card.
- Which two are used in combination depends on a number of factors, including user acceptance, budget, and the exact level of security the organization is trying to obtain.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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**

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.

PHYSICAL BARRIERS

- 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.

PHYSICAL BARRIERS

- 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.

PHYSICAL BARRIERS

- 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.

PHYSICAL BARRIERS

- 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.

PHYSICAL BARRIERS

- 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.

PHYSICAL BARRIERS

- 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.

Password management

- Common method for authentication of users
- First line defense against unauthorized access
- Password hacking-easiest & common way to obtain unauthorized access
- Password must be strong
- Password cracking software

Password vulnerabilities

- One big problem with relying solely on passwords for information security is that more than one person can know them. Sometimes, this is intentional; often, it's not. The tough part is that there's no way of knowing who, besides the password's owner, knows a password.
- Remember that knowing a password doesn't make someone an authorized user.
- Here are the two general classifications of password vulnerabilities:
- **Organizational or user vulnerabilities:** This includes lack of password policies that are enforced within the organization and lack of security awareness on the part of users.
- **Technical vulnerabilities:** This includes weak encryption methods and unsecure storage of passwords on computer systems.

Organizational password vulnerabilities

- It’s human nature to want convenience, especially when it comes to remembering five, ten, and often dozens of passwords for work and daily life. This desire for convenience makes passwords one of the easiest barriers for an attacker to overcome.
- Almost 3 trillion eight-character password combinations are possible by using the 26 letters of the alphabet and the numerals 0 through 9.
- The keys to strong passwords are: 1) easy to remember and 2) difficult to crack.
- However, most people just focus on the easy-to-remember part. Users like to use such passwords as *password,* their login name, *abc123*, or no password at all!

Organizational password vulnerabilities

- Unless users are educated and reminded about using strong passwords, their passwords usually are-
  - **Easy to guess.**
  - **Rarely changed**
  - **Reused for many security points.** When bad guys crack one password, they can often access other systems with that same password and username.
  - **Written down in unsecure places.** The more complex a password is, the more difficult it is to crack. However, when users create complex passwords, they're more likely to write them down. External attackers and malicious insiders can find these passwords and use them against you and your business.

Technical password vulnerabilities

- You can often find these serious technical vulnerabilities after exploiting organizational password vulnerabilities:
  - **Weak password encryption schemes.** Many vendors and developers believe that passwords are safe as long as they don't publish the source code for their encryption algorithms. *Wrong!* A persistent, patient attacker can usually crack this *security by obscurity* fairly quickly. After the code is cracked, it is distributed across the Internet and becomes public knowledge.
  - Password-cracking utilities take advantage of weak password encryption. These utilities do the grunt work and can crack any password, given enough time and computing power.

Technical password vulnerabilities

- Programs that store their passwords in memory, unsecured files, and easily accessed databases.
- Unencrypted databases that provide direct access to sensitive information to anyone with database access, regardless of whether they have a business need to know.
- User applications that display passwords on the screen while the user is typing.

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.

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, favourite 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.

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.

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.

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^.")

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.

CONTINUE…

- **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.

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.