Network Security – Organizational Security

Password Selection

- Poor password selection is one of the most common of poor security practices, and one
- of the most dangerous.
- Numerous studies that have been conducted on password selection have found that,
  - while overall more users are learning to select good passwords, a significant percentage of users still make poor choices.
- a poor password choice can enable an attacker to compromise a computer system or network more easily.
- Even when users have good passwords, they often resort to another poor security practice
  - writing the password down in an easily located place, which can also lead to system compromise if an attacker gains physical access to the area.

Password Selection

- For many years, computer intruders have relied on users selecting poor passwords to help them gain unauthorized access to a system or network.
- If attackers could obtain a list of the users' names, chances were good they could eventually access the system.
- Users tend to pick passwords that are easy for them to remember, and what easier password could there be than the same sequence of characters that they use for their user ID?
- If a system has an account with the username *jdoe*,
  - an attacker's reasonable first guess of the account's password would be *jdoe*.
  - If this doesn't work, the attacker would try variations on the same, such as *doej*, *johndoe*, *johnd*, and *eodj*, all of which would be reasonable possibilities.

Password Selection

- If the attacker's attempt to use variations on the username does not yield the correct password, they might simply need more information.
- Users also frequently pick names of family members, pets, or favorite sports team.
- then the attacker might next try hobbies of the user, the name of their favorite model of car, or similar pieces of information.
- The key is that the user often picks something easy for them to remember,
  - which means that the more you know about the user, the better your chance of discovering their password.

Password Selection

- In an attempt to complicate the attacker's job, organizations have encouraged their users to mix upper- and lowercase characters and to include numbers and special characters in their password.
- Organizations may also require users to frequently change their password.

Password Selection

- Another policy or rule governing password selection often adopted by organizations is that passwords must not be written down.
- This, of course, is difficult to enforce, and thus users will frequently write them down, often as a result of what we refer to as the “password dilemma.”
- The more difficult we make it for attackers to guess our passwords, and the more frequently we force password changes, the more difficult the passwords are for authorized users to remember and the more likely they are to write them down.

Password Selection

- Writing them down and putting them in a secure place is one thing, but all too often users will write them on a slip of paper and keep them in their calendar, wallet, or purse.
- Most security consultants generally agree that if they are given physical access to an office, they will be able to find a password somewhere—the top drawer of a desk, inside of a desk calendar, attached to the underside of the keyboard, or even simply on a yellow “sticky note” attached to the monitor

Password Selection

- Good Passwords –
- have eight or more characters in your password,
- include a combination of upper- and lowercase letters,
- Include at least one number and
- one special character,
- do not use a common word, phrase, or name,
- choose a password that you can remember so that you do not need to write it down.

Piggybacking

- In security, piggybacking is similar to tailgating, refers to when a person tags along with another person who is authorized to gain into a restricted area.
- The act may be legal or illegal, authorized or unauthorized, depending on the circumstances.
- People are often in a hurry and will frequently not follow good physical security practices and procedures.
- Attackers know this and may attempt to exploit this characteristic in human behavior.

Piggybacking

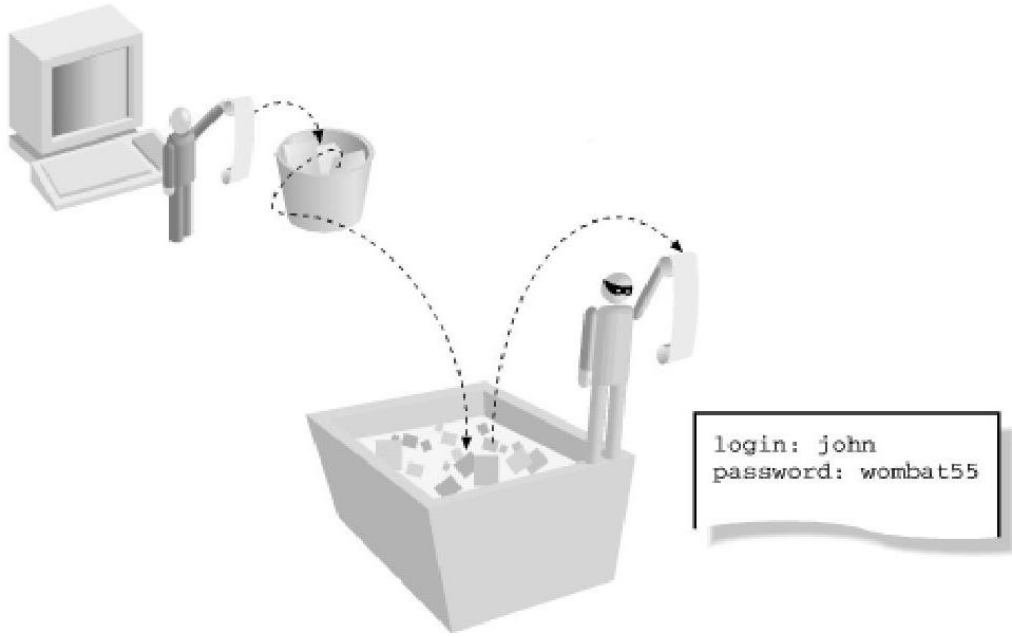
- **Piggybacking** is the simple tactic of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building.
- An attacker can thus gain access to the facility without having to know the access code or having to acquire an access card.
- It is similar to shoulder surfing in that it relies on the attacker taking advantage of an authorized user not following security procedures.
- 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.

Piggybacking

- 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.
- 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.

Dumpster Diving

- The amount of useful information that users throw away in unsecured trash receptacles often amazes security professionals.
- Hackers know that they can often find manuals, network diagrams, and even user IDs and passwords by rummaging through dumpsters



Dumpster Diving

- 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**.
- Thieves can go through your trash looking for bills, credit card numbers, mobile number, and other information.
- 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.

Dumpster Diving

- 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.
- People should also consider shredding personal or sensitive information that they wish to discard in their own trash.
- A reasonable quality shredder is inexpensive and well worth the price when compared with the potential loss that could occur as a result of identity theft.

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.

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.

Installing Unauthorized Hardware and Software

- Another common example of unauthorized software that users install on their systems is games.
- 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.

Installing Unauthorized Hardware and Software

- Many organizations do not allow their users to load software or install new hardware without the knowledge and assistance of administrators.
- Many organizations also screen, and occasionally intercept, e-mail messages with links or attachments that are sent to users.
- This helps prevent users from, say, unwittingly executing a hostile program that was sent as part of a worm or virus.
- Consequently, many organizations have their mail servers strip off executable attachments to e-mail so that users can't accidentally cause a security problem.

Physical Access by Non-Employees

- 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.

Physical Access by Non-Employees

- it also requires that employees actively challenge individuals who are not wearing the required identification badge.
- 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.

Physical Access by Non-Employees

- 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.

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

- These are just some of the numerous questions that need to be asked when examining the physical security surrounding a system.
  - 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?

Physical Security

- 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?

Physical Security – Access Control

- In addition to locks on doors, other common physical security devices include video surveillance and even simple access control logs (sign-in logs).
- another common access control mechanism is a human security guard.

Physical Security – Access Control

- **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.

Physical Security – Access Control

- 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.

Physical Security – Access Control

- 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 in use may 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 (two-factor-authentication).