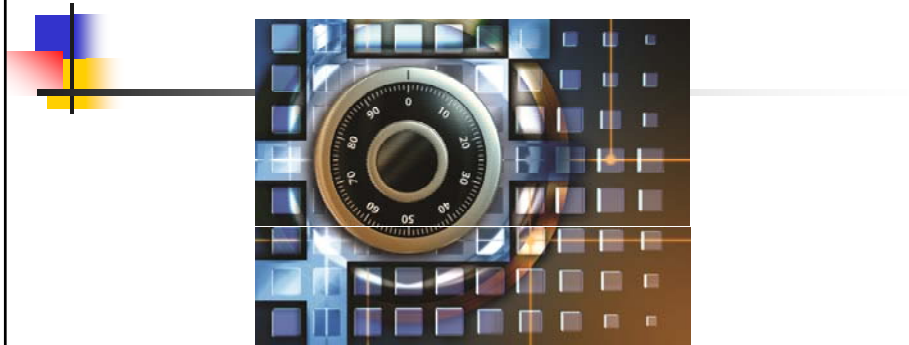# Physical Security

Chapter 8
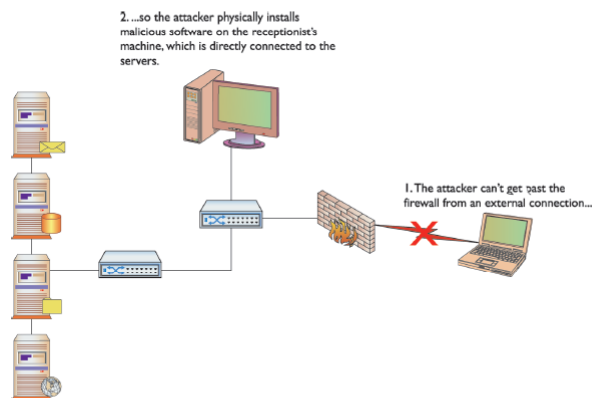

Background

- Businesses have the responsibility of attempting to secure their profitability.
- They need to secure:
    - Employees
    - Product inventory
    - Trade secrets
    - Strategy information

- All these assets affect the profitability of a company and its future survival.
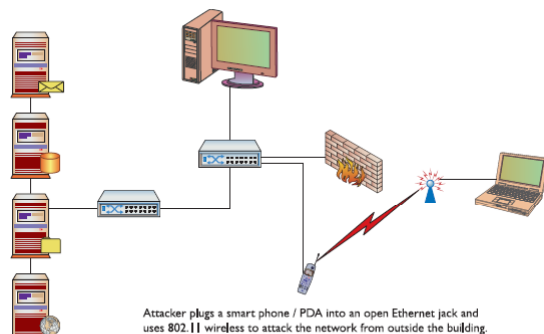
The Security Problem

- The problem that faces professionals charged with securing a company's network can be stated rather simply:
    - **Physical access negates all other security measures.**

- No matter how impenetrable the firewall and intrusion detection system (IDS), if an attacker can find a way to walk up to and touch a server, he can break into it.

- Physically securing information assets doesn't mean just the servers;
- It means protecting physical access to all the organization's computers and its entire network infrastructure.

The Security Problem Illustrated

2. ...so the attacker physically installs malicious software on the receptionist's machine, which is directly connected to the servers.

1. The attacker can't get past the firewall from an external connection...

- Figure 8.1   Using a lower-privilege machine to get at sensitive information

Using a Lower Privilege Machine to Get Sensitive Information

Attacker plugs a smart phone / PDA into an open Ethernet jack and uses 802.11 wireless to attack the network from outside the building.

• Figure 8.2   A wireless bridge can allow remote access

Personal digital assistants (PDAs) acting as a *wireless bridge*

Bootdisks

- Bootdisk:
  - Any media used to boot a computer into an operating system that is not the native OS on its hard drive
  - These can be in the form of a floppy disk, CD, DVD, or a USB flash drive.

- Boot floppy disks can be used to attack machines with floppy drives.
- Utilities can be installed on the disk to allow for the stealing of password files and other information.

Access to Boot Disk

- A simple attack that can be used with physical access is by using a boot disk.
- Once an attacker is able to read the drive, the password file can be copied off the machine for offline password-cracking attacks.
  - If write access to the drive is obtained, the attacker could alter the password file.
  - The attacker can place a remote control program to be automatically executed upon the next boot.
  - This guarantees continued access to the machine.

Access to Boot Disk

- Bootable CD-ROMs are a threat.
  - May contain a bootable version of an entire operating system complete with drivers for most devices

  - Gives an attacker a greater array of tools than could be loaded onto a floppy disk.

  - Also allows for making an image of the hard drive since some form of bootable media is often used to load the imaging software.
    - The process of taking the entire contents of a hard drive and copying them to a single file on a different media is **called drive imaging.**

LiveCDs

- LiveCD
  - Contains a bootable version of an entire operating system.
  - This is typically a variant of Linux, complete with drivers for most devices.
  - LiveCDs give an attacker a greater array of tools than could be loaded onto a floppy disk.
  - These tools include scanners, sniffers, vulnerability exploits, forensic tools, drive imagers, password crackers, and more.

Drive Imaging

- Drive imaging is the process of copying the entire contents of a hard drive to a single file on a different media.
- This process is often used by people who perform forensic investigations of computers.
  - A bootable media is used to start the computer and load the drive imaging software.
  - It makes a bit-by-bit copy of the hard drive or other attached media.
  - There will be no record of the copy being made.
- The information obtained from drive imaging contains every bit of data that is on the computer: any locally stored documents, locally stored e-mails, and every other piece of information that the hard drive contains.
- This data could be very valuable if the machine holds sensitive information about the company.
- **Protection**
  - Encrypting files or the drive provides protection.
  - Storing files on a files server can also help.

Computer Theft

- Outright theft of computers.
    - A simpler version of the drive imaging attack

- The theft of computers is mostly performed for the financial value of the computers.
- However, stealing computers also allows an attacker to obtain the data contained on them.

Perhaps Better than DoS

- Computer theft can be used to perform a Denial-of-Service (DoS) attack.
    - If the computers (servers) are not on network / not working – it causes denial of service to the concerned user

- The theft of computers, using a boot disk to erase all data on the drives, or unplugging computers is effective for DoS attacks.

Physical Security Safeguards

- Walls and guards
- Policies and procedures
- Access control and monitoring
- Environmental controls
- Fire suppression

Physical Security Safeguards

- While it is difficult to be completely secure, several steps can be taken to mitigate the risk to information systems from a physical threat.
  - Policies & Procedures
  - Access Controls

- Policies and procedures affect two distinct areas that affect:
  - Computers.
  - Users.

- To mitigate the physical security risk to computers physical security should be extended to the computers themselves.

Physical Access

- Physical access negates all other security measures.
- Physical access allows an attacker to plug into an open Ethernet jack.
  - Hand-held devices that run operating systems with full networking support make this attack feasible.
  - Originally, the attacker would have to be in a secluded area with dedicated access to the Ethernet.
    - An attacker can sit with a laptop and run a variety of tools against the network.
    - Being internally based puts them behind the firewall and intrusion detection system.

Boot from Other Devices

- To combat the threat of boot disks:
  - Remove or disable floppy drives on all desktops that do not require them.
  - Disable auto run feature
  - Set the BIOS Password
    - Delays / prevent attacker from resetting the boot sequence to boot from a device other than the hard drive

USB and Security USB Boot

- USB ports
  - expand the ability for users to connect devices
  - have them auto-recognize and work, usually without needing additional drivers or software.

- Remedies:
  - Disallow the USB devices if OS permits
  - Unload / disable the entire USB driver if running an OS that does not support disabling of the device.
  - If these USB devices are allowed, aggressive virus scanning should be implemented.

Theft of Systems

- The final physical access attack that can be performed is outright theft of machines.
  - Frequently the most effective countermeasure is to lock machines with sensitive data.
  - Special access to server rooms should be considered.
  - There should be minimal distribution of sensitive data.

User Responsibility

- Users are the weakest link in the security chain.
- They need to be aware of security issues and also need to be involved in security enforcement.
- Users should know whom to contact when they suspect a security violation.
- They can perform one of the simple security tasks – Locking a workstation immediately when stepping away from it.
- Security guards are not always users. However, they need to be educated about proper network security as well as physical security involving users.

Walls and Guards

- The primary defense against a majority of physical attacks are the barriers between the assets and a potential attacker—walls, fences, gates, and doors.
- Some employ private security staff to attempt to protect their assets.

- The most valuable assets should be contained on company servers.
- To protect the physical servers, you must look in all directions:
  - Doors and windows should be safeguarded and a minimum number of each should be used in a server room.
  - Is there a drop ceiling?
  - Is there a raised floor?

Guards

- Guards are a visible presence with direct responsibility for security, so they provide an excellent security measure.
- Guards can monitor entrances and exits and can maintain access logs of who has entered and departed the building.
- Everyone who passes through security as a visitor should sign the log. It can be useful in tracing who was at what location and why.

Policies and Procedures

- Physical security policies and procedures relate to two distinct areas:
  - Those that affect the computers themselves
  - Those that affect users

Computer Policies

- Remove/disable the floppy disk system.
- Remove/disable the optical drive system.
  - If that is not possible, remove the device from the boot menu and set a BIOS password.
- Disallow USB drive keys, either with active directory or registry settings.
  - If that is not possible, implement aggressive anti-malware scanning.
- Lock up equipment that contains sensitive data.
- Train all employees:
  - To challenge strangers
  - To follow procedures
  - To lock workstations before leaving them

Environmental Controls

- Sophisticated environmental controls are needed for current data centers.
- Fire suppression is also an important consideration when dealing with information systems.
- Heating ventilating and air conditioning (HVAC) systems are critical for keeping data centers cool.
  - Properly securing these systems is important in helping prevent an attacker from performing a physical DoS attack on your servers.

Fire Suppression

- The ability to respond to a fire quickly and effectively is critical to the long-term success of any organization.
- The goal—never to have a fire—however, in the event that one does occur, mechanisms are in place to limit the damage the fire can cause.

- Fire suppression system
  - Water-based
  - Halon-based
  - Clean-agent
  - Handheld fire extinguishers

Fire Detection Devices

- An essential complement to fire suppression systems and devices are fire detection devices (fire detectors).
- Detectors may be able to detect a fire in its very early stages.
- There are several different types of fire detectors.
  - Smoke activated
    - Ionization – Detects ionized particles caused by fire
    - Photoelectric – Detects degradation of light from smoke
  - Heat activated
    - Fixed-temperature – Alerts if temperature exceeds a pre-defined level
    - Rate-of-rise temperature – Detects sudden increases in temperature
  - Flame activated
    - Relies on the flames from the fire to provide a change in the infrared energy that can be detected

Access Controls and Monitoring

- Access control means having control of doors and entry points.
  - Locks
  - Layered access systems
  - Electronic door control systems
  - Closed circuit television (CCTV)

Layered Access

- Physical barriers help safeguard the information infrastructure.

- Layered Access
  - Assets should be protected with several perimeters.
  - Servers should be placed in a separate secure area with a separate authentication mechanism.
  - Access to the server room should be limited to staff with legitimate need.
  - To layer the protection, the area surrounding the server room should also be limited to just the people who work in that area.

Electronic Access Control

- Electronic access control systems manage opening and closing doors.
    - A centralized system can instantly grant or refuse access.
    - The system works with a software package running on a computer.
    - It should not be on a network.

Closed Circuit Television (CCTV)

- Closed circuit television (CCTV) cameras are similar to the door control systems—they can be very effective, but how they are implemented is an important consideration.
- Carefully consider camera placement and the type of cameras used.
- Different iris types, focal lengths, and color or infrared capabilities are all options that make one camera superior over another in a specific location.

Authentication

- Authentication is the process by which a user proves that she is who she says she is.
- Authentication is performed to allow or deny a person access to a physical space.
- The heart of any access control system is to allow access to authorized users and to make sure access is denied to unauthorized people.
- Access controls, network or physical, do not work without some form of authentication.
- During authentication, users prove they are who they claim to be.
- Authentication is done to allow or deny access to a physical space.

Access Tokens (Keys)

- Access tokens are the traditional form of physical access authentication.
- Defined as "something you have."
- An access token is a physical object that identifies specific access rights. Your house key, for example, is a basic physical access token that allows you access into your home.
- The primary drawback of token-based authentication - Only the token is being authenticated.
  - The theft of the token could grant anyone who possessed the token access to what the system protects.
- Keys have worked as token authentication for over a hundred years, but they have several limitations
- Some of the limitations of tokens are:
  - Keys are paired exclusively with a lock or a set of locks, and they are not easily changed
  - They are easy to copy.
  - They are difficult to invalidate.

Radio Frequency Cards

- When contactless radio frequency cards and readers are passed near a card reader, the card sends out a code via radio.
- The reader picks up this code and transmits it to the control panel.
- The control panel checks the code against the reader it is being read from and the type of access the card has in its database.
- Advantages of Radio Frequency Cards
    - Any card can be deleted from the system.
    - All doors can be segmented to create multiple access areas.

Biometrics

- Biometrics
    - Uses the measurements of certain biological factors to distinguish one specific person from others.
    - These factors are based on parts of the human body that are unique.
    - The most well known of these unique biological factors is the fingerprint.

- Biometric Concerns
    - False positives and false negatives are two issues with biometric scanners.
    - There is a chance of attackers stealing the uniqueness factor the machine scans and reproducing it to fool the scanner.
        - Stolen Factors (Fingerprint from glass).
    - Changes over time can affect the accuracy.

- **A False Positive**
  - When a biometric is scanned and allows access to someone who is not authorized
  - for example, two people who have very similar fingerprints might be recognized as the same person by the computer, which grants access to the wrong person.

- **A False Negative**
  - When the system denies access to someone who is actually authorized
  - for example, a user at the hand geometry scanner forgot to wear a ring he usually wears and the computer doesn't recognize his hand and denies him access.

Multiple-factor Authentication

- Authentication can be separated into three broad categories:
  - What you are (for example, biometrics)
  - What you have (for example, tokens)
  - What you know (for example, passwords)

- Multiple factor authentication is simply the combination of two or more types of authentication.
  - Two-factor authentication combines two factors before granting access.
  - Three-factor authentication combines all the three types.

- Multiple factor authentication makes it very difficult for an attacker to have the correct materials for authentication.
  - This method of authentication reduces risk of stolen tokens.
  - It also enhances biometric security.