SENG 460

Practice of Information Security and Privacy

Physical (Environmental) Security

Physical Security Overview

- Physical security encompasses a specific set of threats, vulnerabilities, and risks.

- Physical security includes site design and layout, environmental components, emergency response readiness, training, access control, intrusion detection, and power and fire protection etc.

- Physical security mechanisms protect people, data, equipment, systems, facilities, and a long list of company assets.

Samples of Improper Physical Security Implementations and Maintenance

- A convenience store hangs too many advertising signs and posters on the exterior windows.
- Bollards are not implemented in high foot traffic areas outside of a retail store.
- Bushes are growing too close to an ATM.
- A gas station’s outside restroom has a broken lock.
- A financial organization doesn’t have secure recycling bin.

Physical Threats Categories

- **Natural environmental threats:** Floods, earthquakes, storms and tornadoes, fires, extreme temperature conditions, and so forth
- **Supply system threats:** Power distribution outages, communications, interruptions, and interruption of other resources such as water, gas, air filtration, and so on
- **Manmade threats** Unauthorized access (both internal and external), explosions, employee errors and accidents, vandalism, fraud, theft, ***Collusion*** and others
- **Politically motivated threats** Strikes, riots, civil disobedience, terrorist attacks, bombings, and so forth

Physical Security Design Goals

- **Deter Criminal Activity: L**ayout and supporting policies should deter criminal activity.
- **Delay Intruders:** Add impediments to entry, such as locks, fences, and barriers and implement procedures that slow and monitor the entry of people.
- **Detect Intruders:** Systems and procedures should be in place that allow for criminal activity to be detected.
- **Assess Situation:** Identify specific personnel and actions to be taken when an event occurs.
- **Respond to Intrusions and Disruptions:** Anticipate and develop appropriate responses to intruders and to common disruptions.

A General Model in Physical Security Design

- Layered Defense Model

In such a model, reliance should not be based on any single physical security concept but on the use of **multiple approaches** that support one another.

Practical Approaches in Physical Security Development

- Target Hardening Approach

- Focuses on denying access through physical and artificial barriers (alarms, locks, fences, and so on).

- Traditional target hardening can lead to restrictions on the use, enjoyment, and aesthetics of an environment.

Practical Approaches in Physical Security Development

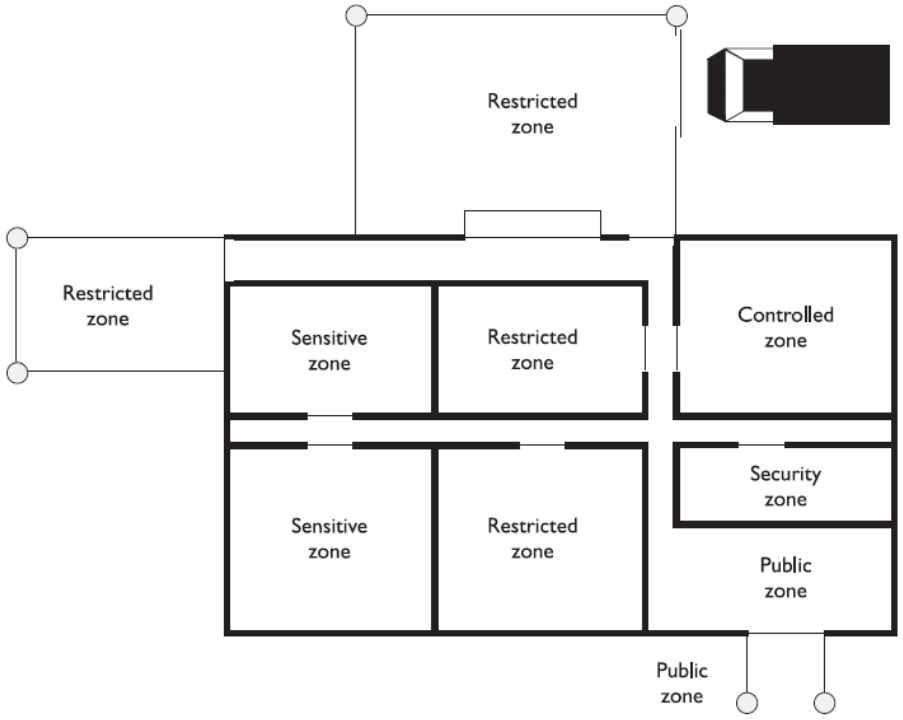
- CPTED Approach

- **Crime Prevention Through Environmental Design (CPTED):**

  - A discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior.
  - It provides guidance in loss and crime prevention through proper facility construction and environmental components and procedures.
  - CPTED concepts were developed in the 1960s. They have been expanded upon and have matured as our environments and crime types have evolved.
  - CPTED provides three main strategies to bring together the physical environment and social behavior to increase overall protection:
    - natural access control,
    - natural surveillance,
    - natural territorial reinforcement.

CPTED - Natural Access Control

The guidance of people entering and leaving a space, which encompasses placement of the doors, lights, fences, and landscaping to satisfy security goals in the least obtrusive and aesthetically appealing manner.



Security Zones with different classifications can use different access controls

CPTED - Natural Surveillance

Promotes visibility of all areas to discourage crime in those areas.

- Organized means (security guards),
- Mechanical means (CCTV),
- Natural strategies (Large window, Open Benches).

CPTED - Natural Territorials Reinforcement

Promotes a feeling of community in the area and attempts to extend the sense of ownership to the employees.

- Walls, fences, landscaping, light fixtures, flags, clearly marked addresses, and decorative sidewalks.
- basketball courts, soccer fields, or baseball fields in open area for supporting activities such as neighborhood watch groups, company barbeques, block parties, or civic meetings.

Physical Security Assessment

- Construction materials of walls and ceilings
- Power distribution systems
- Communication paths and types (copper, telephone, fiber)
- Surrounding hazardous materials
- Regulations and Legal issues
- Exterior components:
  - Topography
  - Proximity to airports, highways, railroads
  - Potential electromagnetic interference from surrounding devices
  - Climate
  - Existing fences, detection sensors, cameras, barriers
  - Operational activities that depend upon physical resources
  - Vehicle activity
  - Neighbors

Facility Selection Security Concerns

- Visibility : Amount of visibility desired depends on the organization and the processes being carried out at the facility.
- Surrounding Area and External Entities: Consider the nature of the operations of the surrounding businesses.
- Accessibility: Ease with which employees and officers can access the facility is a consideration.
- Natural disaster
  - Likelihood of floods, tornadoes, earthquakes, or hurricanes
  - Hazardous terrain (mudslides, falling rock from mountains, or excessive snow or rain)

Construction Security Concerns

- **Walls**
  - Combustibility of material (wood, steel, concrete)
  - Fire rating
  - Reinforcements for secured areas
- **Doors**
  - Combustibility of material (wood, pressed board, aluminum)
  - Fire rating
- **Ceilings**
  - Combustibility of material (wood, steel, concrete)
  - Fire rating
- **Windows**
  - Translucent or opaque requirements
  - Alarms

Flooring

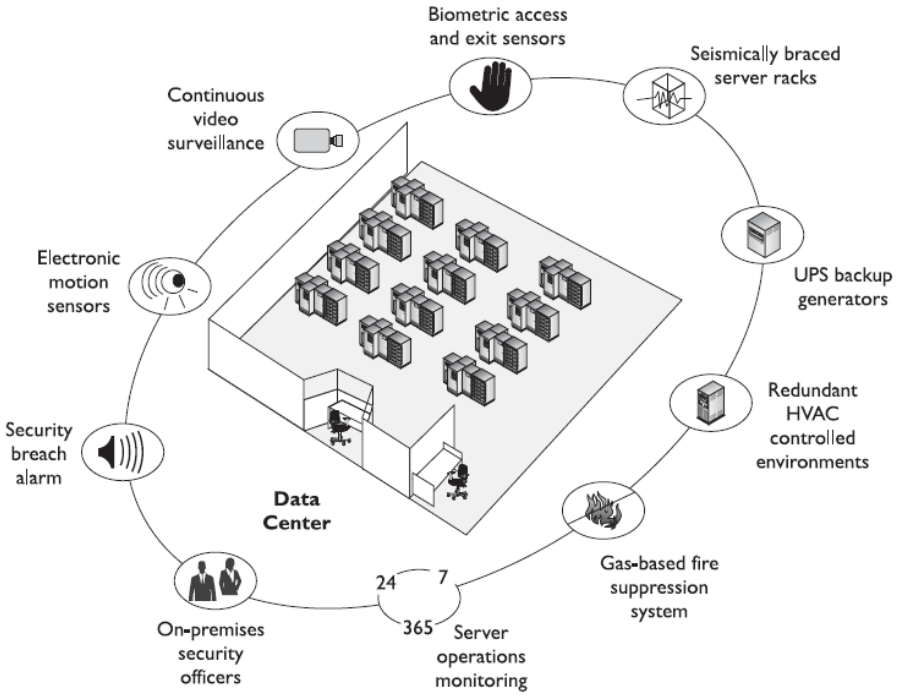
Weight-bearing rating
Combustibility of material (wood, steel, concrete)

- **Heating, ventilation, and air conditioning**
  - Positive air pressure
  - Protected intake vents
  - Dedicated power lines
  - Emergency shutoff valves and switches
- **Electric power supplies**
  - Backup and alternate power supplies
- **Water and gas lines**
  - Shutoff valves—labeled and brightly painted for visibility
  - Placement—properly located and labeled
- **Fire detection and suppression**
  - Placement of sensors and detectors
  - Placement of suppression systems

Computer and Equipment Rooms Security

- Should have a single access door or point of entry and Should be locked at all times.
- Should be in the center of the building, when possible.
- Avoid the top floors or basement of buildings for computer and equipment rooms.
- Install and frequently test fire detection and suppression systems.
- Install separate power supplies for computer and equipment rooms when possible.
- Use only solid doors.

Entry Points of a room is not just the access door)



Safety Controls vs Security Controls

A physical security program should comprise safety and security controls.

- Safety controls deals with the protection of life and assets against fire, natural disasters, and devastating accidents.

- Security controls addresses vandalism, theft, and attacks by individuals.

(Many times an overlap occurs between the two, sometimes safety control conflicts with security control, e.g. **Fail-Safe** vs **Fail-secure**)

Perimeter Security Controls - Fences/Walls and Gates

Fences (first line of defense)

- Three to four feet tall fences deter only casual intruders.
- Six to seven feet tall fences are too tall to climb easily.
- Eight feet and taller fences deter more determined intruders, especially when augmented with razor wire.
- Perimeter Intrusion Detection and Assessment System (PIDAS) Fencing

- **Gates (**classifications developed by Underwriters Laboratory (UL), a non-profit organization that tests, inspects, and classifies electronic devices, fire protection equipment, and specific construction materials)
  - Class 1: Residential use
  - Class 2: Commercial usage
  - Class 3: Industrial usage
  - Class 4: Restricted area

Perimeter Security Controls - Barriers (Bollards)

- Used as protection from Vehicles
- Can be built with aesthetic appearance

Perimeter Security Controls - Lighting Systems

- **Types of Systems**
  - **Continuous lighting:** An array of lights that provide an even amount of illumination across an area.
  - **Standby lighting:** A type of system that illuminates only at certain times or on a schedule.
  - **Movable lighting:** Lighting that can be repositioned as needed.
  - **Emergency lighting:** Lighting systems with their own power source to use when power is out.
- **Types of Lighting**
  - **Fluorescent:** Low pressure mercury-vapor gas-discharge lamp that uses fluorescence to produce visible light.
  - **Mercury vapor:** Gas-discharge lamp that uses an electric arc through vaporized mercury to produce light.
  - **Sodium vapor:** Gas-discharge lamp that uses sodium in an excited state to produce light.
  - **Quartz lamps:** A lamp consisting of an ultraviolet light source, such as mercury vapor, contained in a fused-silica bulb that transmits ultraviolet light with little absorption.

Perimeter Security Controls
- Perimeter Intrusion Detection Systems

Infrared Sensors: Identifies changes in heat waves.

Electromechanical systems: Operate by detecting a break in an electrical circuit.

Photometric or photoelectric systems: Operate by detecting changes in the light and thus are used in windowless areas.

Acoustical systems: Use strategically placed microphones to detect any sound made during a forced entry.

Wave Motion: Generate a wave pattern in the area and detect any motion that disturbs the wave pattern.

Capacitance Detector: Emit a magnetic field and monitor that field.

Closed-circuit television system (CCTV): Uses sets of cameras that can either be monitored in real time or can record days of activity that can be viewed as needed at a later time.

.

Perimeter Security Controls - Additional Perimeter Measures

Patrol Force

One of the main benefits of this approach is that guards can use discriminating judgment based on the situation, which automated systems cannot do.

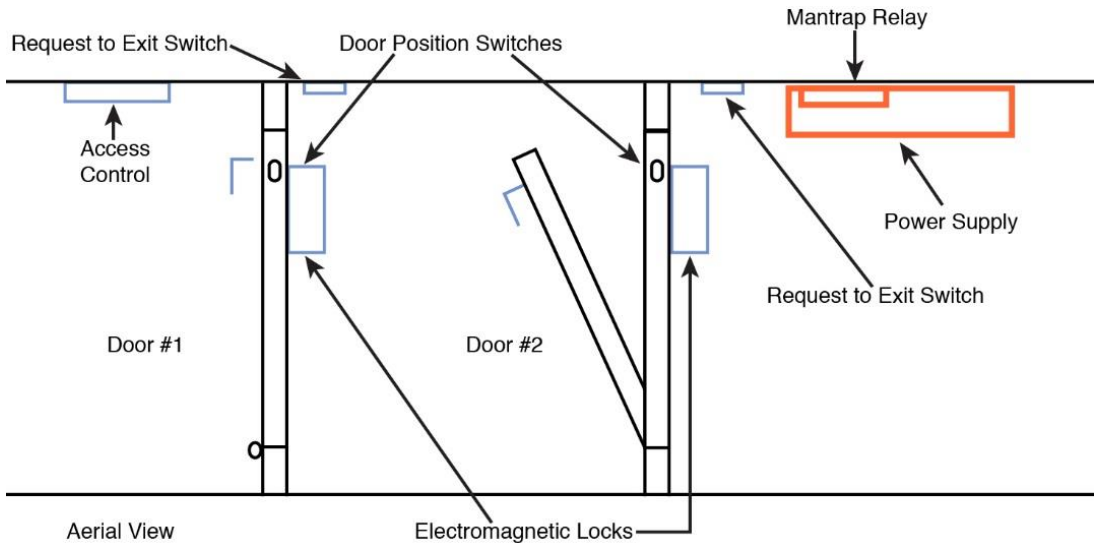
Access Control

Every successful and unsuccessful attempt to enter the facility should record

- Date and time
- Specific entry point
- User ID employed during the attempt

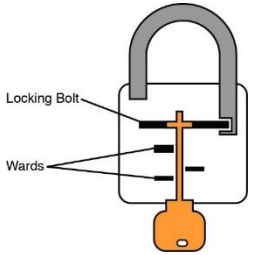
Building and Internal Security Controls -Doors

- **Door Types**
  - **Vault doors:** Leading into walk-in safes or security rooms
  - **Personnel doors:** Used by humans to enter the facility
  - **Industrial doors:** Large doors that allow access to larger vehicles
  - **Vehicle access doors:** Doors to parking building or lots
  - **Bullet-resistant doors:** Doors designed to withstand firearms
  - **Turnstile:** Doors usually designed to avoid ***piggybacking***
  - **Mantraps:** Doors designed to trap unauthorized individuals.

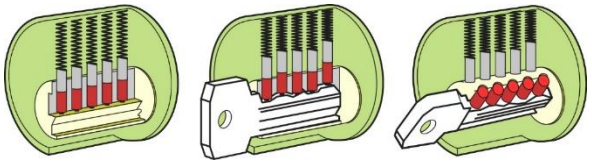


Building and Internal Security Controls -Locks

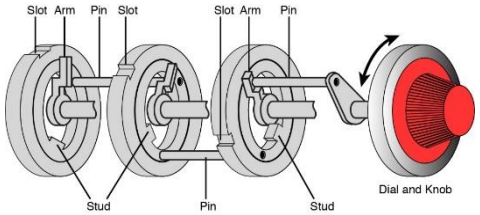
- **Warded locks:**



- **Tumbler locks:**



- **Combination locks:**



- **Electric locks or cipher locks:** use a key pad that require the correct code to open the lock.

- **Proximity authentication devices:** uses a programmable card to deliver an access code to the device either by swiping the card or in some cases just being in the vicinity of the reader.

- **Biometric authentication devices:** is able to read human characteristics for authentication.

Building and Internal Security Controls - Glass Entries

- **Standard:** Used in residential area and is easily broken
- **Tempered:** Created by heating the glass, which gives it extra strength
- **Acrylic:** Made of polycarbonate acrylic; is much stronger than regular glass but produces toxic fumes when burned
- **Laminated:** Two sheets of glass with a plastic film between, which makes breaking it more difficult

Building and Internal Security Controls - Additional Interior Considerations

- **Visitor control:** Ways to accompany a contractor or visitor to their destination.

- **Equipment rooms:** Lock and keep a strict inventory of all equipment so theft can be discovered.

- **Work areas:** Prohibiting some employees from certain areas might be beneficial.

Environmental Security Controls - Fire Detection

- **Smoke-activated:** Operates using a photoelectric device to detect variations in light caused by smoke particles.
- **Heat-activated (also called heat-sensing):** Operates by detecting temperature changes. These can either alert when a predefined temperature is met or alert when the rate of rise is a certain value.
- **Flame-actuated:** Optical devices that “look at” the protected area. They generally react faster to a fire than non-optical devices do.

Environmental Security Controls - Fire Suppression

- **Wet pipe**
  - •Use water contained in pipes to extinguish the fire. In some areas, the water might freeze and burst the pipes, causing damage, so this system is not recommended for rooms where equipment will be damaged by the water.
- **Dry pipe**
  - •The water is not held in the pipes but in a holding tank. The pipes hold pressurized air.
- **Preaction**
  - Operates like a dry pipe system except that the sprinkler head holds a thermal-fusible link that must be melted before the water is released. This is currently the recommended system for a computer room.
- **Deluge**
  - Allows large amounts of water to be released into the room, which obviously makes this not a good choice where computing equipment will be located.
- **Halon gas**
  - Works well for fire suppression, but can be toxic to humans by affecting the central nervous system and other bodily functions, also damage Earth's atmospheric ozone layer.

Environmental Security Controls - Power Outages

- Types of Power Outages
  - **Surge:** A prolonged high voltage
  - **Brownout:** A prolonged drop in power that is below normal voltage
  - **Fault:** A momentary power outage
  - **Blackout:** A prolonged power outage
  - **Sags:** A momentary reduction in the level of power
- To protect Against Static Electricity
  - Use antistatic sprays.
  - Maintain proper humidity levels.
  - Use antistatic mats and wrist bands
- To Protect Against Dirty Power
  - Power conditioners (sags, faults, surges)
  - Uninterruptible power supplies (UPS) (blackout)

Environmental Security Controls - HVAC Issues and Guidelines

Heating and Air Conditioning System Issues:

- **Heat:** Excessive heat causes reboots and crashes.
- **High humidity:** Causes corrosion problems with connections.
- **Low humidity:** Dry conditions encourage static electricity, which can damage equipment.

Some Guidelines:

- At 100 degrees, damage starts occurring to magnetic media; in fact, floppy diskettes are the most susceptible to this.
- At 175 degrees, damage starts occurring to computers and peripherals.
- At 350 degrees, damage starts occurring to paper products.

Equipment Security Control

Corporate procedures should address the following issues:

- Tamper Protection
- Encryption
- Inventory
- Physical Protection of Security Devices
- Tracking Devices
- Portable Media Procedures

Personnel Privacy and Safety

- **Human Resources are the most important assets!**
  - An Occupant Emergency Plan (OEP) provides coordinated procedures for minimizing loss of life or injury.
- Organizations is responsible for protecting the privacy of each individual's information. (More details about Privacy controls will be introduced in later chapters)