Physical Security

If someone really wants to get at the information, it is not difficult if they can gain physical access to the computer or hard drive.

– Microsoft White Paper, July 1999

CSE 4471: Information Security
Instructor: Adam C. Champion, Ph.D.

Seven Major Sources of Physical Loss

- Temperature extremes
- Gases
- Liquids
- Living organisms
- Projectiles
- Movement
- Energy anomalies

Community Roles

- General management: responsible for security of buildings for organization
- IT mgmt. and professionals: responsible for environmental, access security
- Info. security mgmt. and pros: perform risk assessments, implementation reviews

Access Controls

- There are many physical access controls suitable to people's physical entry, exit to and from org.'s facilities, including
  - Biometrics
  - Smart cards
  - Wireless-enabled keycards

Facilities Management

- Secure facility: physical location with controls designed to minimize risk of physical attacks

Design Considerations:

- Natural terrain
- Traffic flow
- Urban development

Other Measures:

- Fences
- Gates
- Walls
- Guards
- Alarms

Controls for Protecting Secure Facilities

- Walls, fencing, gates
- Guards
- Dogs, ID cards, badges
- Locks, keys
- Mantraps
- Electronic monitoring (e.g., video cameras)
- Alarms, alarm systems
- Computer rooms
- Walls, doors

ID Cards and Badges

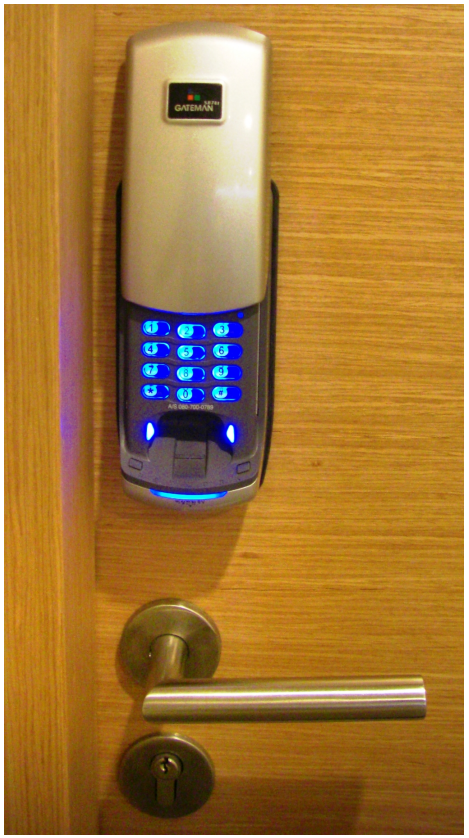
- Ties physical security to info. access with ID cards, name badges
  - ID cards: typically concealed
  - Name badges: visible
- Biometric devices (facial recognition)
- Should not be *only* control (easily duplicated, stolen, modified)
- Tailgating occurs when unauthorized people follow authorized ones through doors, barriers

Locks and Keys

- Two types of locks: mechanical, electro-mechanical
- Four categories of locks: manual, programmable, electronic, biometric
- Locks failure entails alternate access to facility
- Locks fail in one of two ways:
  - Fail-Safe: Upon lock failure, door unlocked
  - Fail-Secure: Upon lock failure, door locked

Examples: Locks

Biometric, Electronic Lock



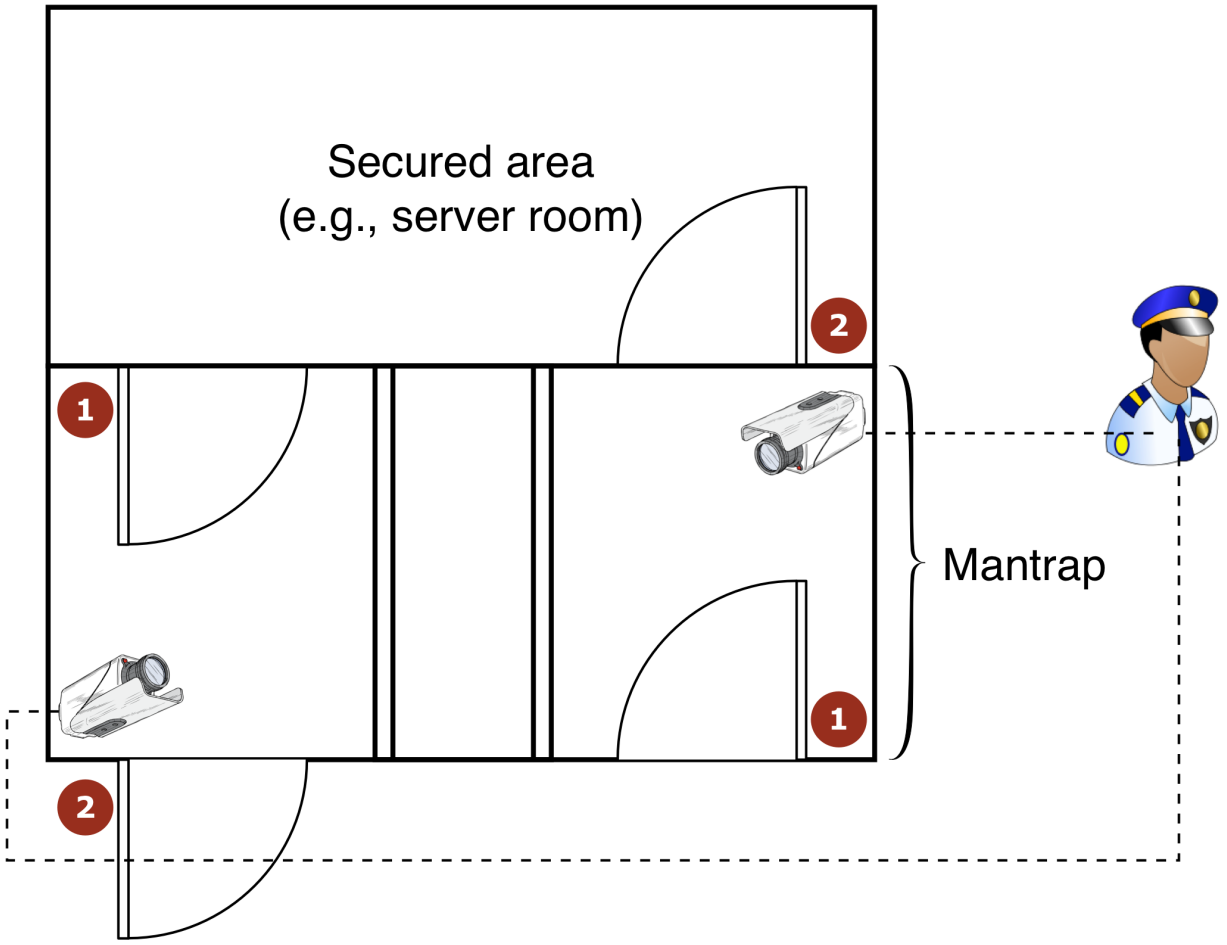
Mechanical Lock

Sources: Wikimedia Commons (Ronhjones, Sekuloff)

Mantraps

- Enclosures with different entry, exit points
- Person enters mantrap, requests access
  - If verified, allowed to exit mantrap into facility
  - Otherwise, denied entry: person can only exit when security official overrides mantrap locks

Example Mantrap



1. One person enters mantrap via unlocked door 1
2. Person's identity is verified
3. If authorized, person allowed to enter secure area via door 2 ; otherwise, person cannot leave mantrap unless released by security

Electronic Monitoring

- Records events where other types of physical controls are impractical
- May use cameras with video recorders
- Drawbacks:
  - Reactive; does not prevent access to facility (or property damage)
  - Recordings often not monitored in real time, must be reviewed to have any value
  - Video is data-intensive!

Alarms and Alarm Systems

- Alarm systems notify org. when “events” occur
- Use cases: fire alarms, environment disturbances, service interruption
- Systems rely on sensors for event detection:
  - Motion detectors
  - Smoke detectors
  - Thermal detectors
  - Glass breakage detectors
  - Weight/contact sensors

Computer Rooms and Wiring Closets

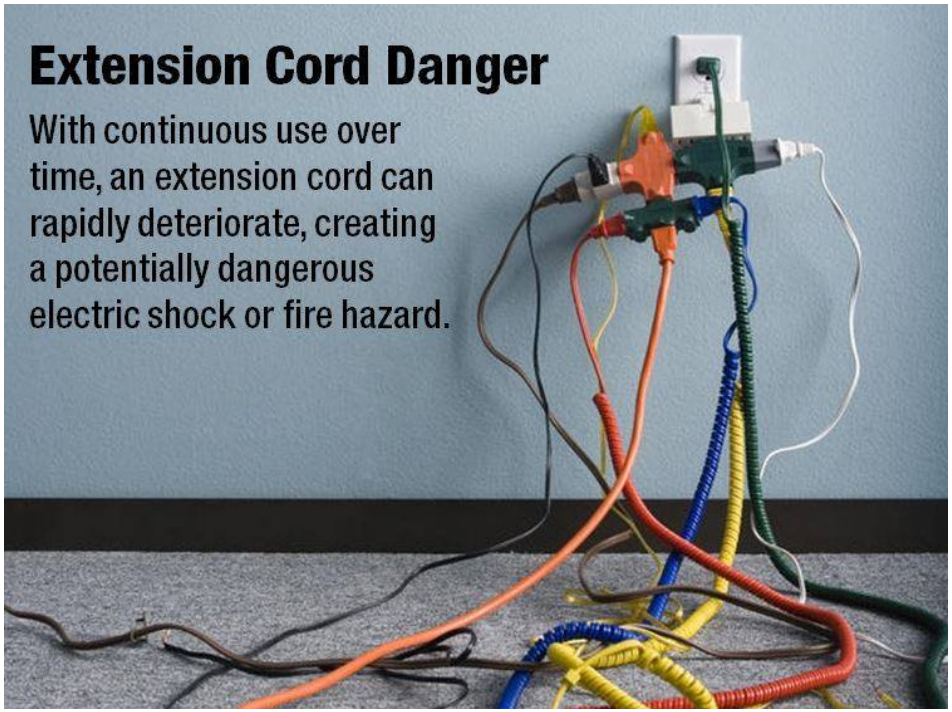
- Extra attention required for these areas
- Controls easily defeated if attacker gets physical access to computing equipment
- Custodial staff may be concern (security)
  - Low scrutiny, supervision
  - High degree of access to offices

Interior Walls and Doors

- Typical types of walls in facility:
  - Standard interior
  - Firewall
- High-security areas need physical firewalls to resist intruders, increases building resistance to fire
- Evaluate doors to secured rooms too
- Consider installing push/crash bars for computer rooms, wiring closets
  - Meets building codes
  - Provides higher levels of security than standard door handles

Fire Safety

- Fire: most serious threat to safety of people in org.
  - Cause more property damage, personal injury, and death than any other threat
  - Necessitates fire detection, response measures in physical security plans



How **NOT** to use extension cords

Source: https://twitter.com/Smart911/status/678641207006883840

Fire Detection and Response

- Fire suppression systems: devices that detect fire, respond accordingly
- Systems deprive fires of what they need to burn: heat, fuel, oxygen
  - Water (mist) systems: reduce temperature, saturate some fuels to prevent ignition
  - Carbon dioxide systems: deprive fire of oxygen
  - Soda acid systems block fire fuel, preventing spread
  - Gas-based systems: block combustion but leave enough oxygen for people to survive short time

Fire Detection

- Fire detection is precondition for fire suppression
- Fire detection systems have two categories: manual, automatic
- Fire safety entails people monitoring fire evacuation to prevent attacker entering offices
- Three main types of fire detection systems: thermal detection, smoke detection, and flame detection
  - Smoke detectors operate in one of three ways: photoelectric, ionization, and air-aspirating

Fire Suppression

- Can be portable, manual, or automatic
- Portable extinguishers are rated by type of fire:
  - Class A: fires of ordinary combustible fuels
  - Class B: fires fueled by combustible liquids, gases
  - Class C: fires with energized electrical equipment
  - Class D: fires fueled by combustible metals
- Installed systems spray liquid, gas for fire suppression
  - Sprinkler systems spray liquid (water)
  - Sprinkler system options: wet-pipe, dry-pipe, pre-action
  - Water mist sprinklers use fine mist to extinguish fires

Example: Fire Sprinkler System

57 °C
68 °C
79 °C
93 °C
141 °C
182 °C

Source: Wikimedia Commons (David40226543/Micha0001, Brandon Leon)

Gaseous Emission Systems

- Until recently there were only two types of systems: carbon dioxide, halon
  - Carbon dioxide deprives fire of oxygen
  - Halon: "clean agent" that depletes ozone layer; new installations prohibited
- Alternative clean agents include:
  - FM-200
  - Inergen
  - Carbon dioxide
  - FE-13 (trifluromethane)

Example: Gaseous Fire Suppression

Source: Flickr (Seeweb, CC-BY-SA 2.0)

Failure of Supporting Utilities and Structural Collapse

- Supporting utilities include heating, ventilation, and air conditioning (HVAC); electricity; water; sewage; garbage disposal
  - Utility failure obviously affects building safety
  - Interruption of services may lead to vulnerability injection in systems designed to protect info.

Heating, Ventilation, and Air Conditioning (HVAC)

- How can HVAC systems damage info. systems?
  - Extreme temperature
    - Most computers work between 70–75 °F (22–24 °C)
    - Comfortable temperatures for people too ☺
  - Filtration
  - Humidity
  - Static electricity
    - Damages sensitive circuitry, including computers
    - Person can generate up to 12,000 V walking on carpet!

Ventilation Shafts

- Security of the ventilation ductwork:
  - Ducts in commercial buildings could be large enough for person to climb through
  - Security can install wire mesh grids for large grids to split up the ducts

Power Management and Conditioning

- Concerns include electrical quantity (voltage, amperage); power quality (cleanliness, installation)
- Noise interfering with 60-Hz alternating current can yield inaccuracy in CPU clocks
- Electrical grounding:
  - Ensures that returning current is discharged to ground
  - Improper installation can damage equipment, injure people
- Overloading circuits can cause problems with circuit breakers and overload electrical cables
  - Risk of electrical fire

Uninterruptible Power Supplies (UPSs) (1)

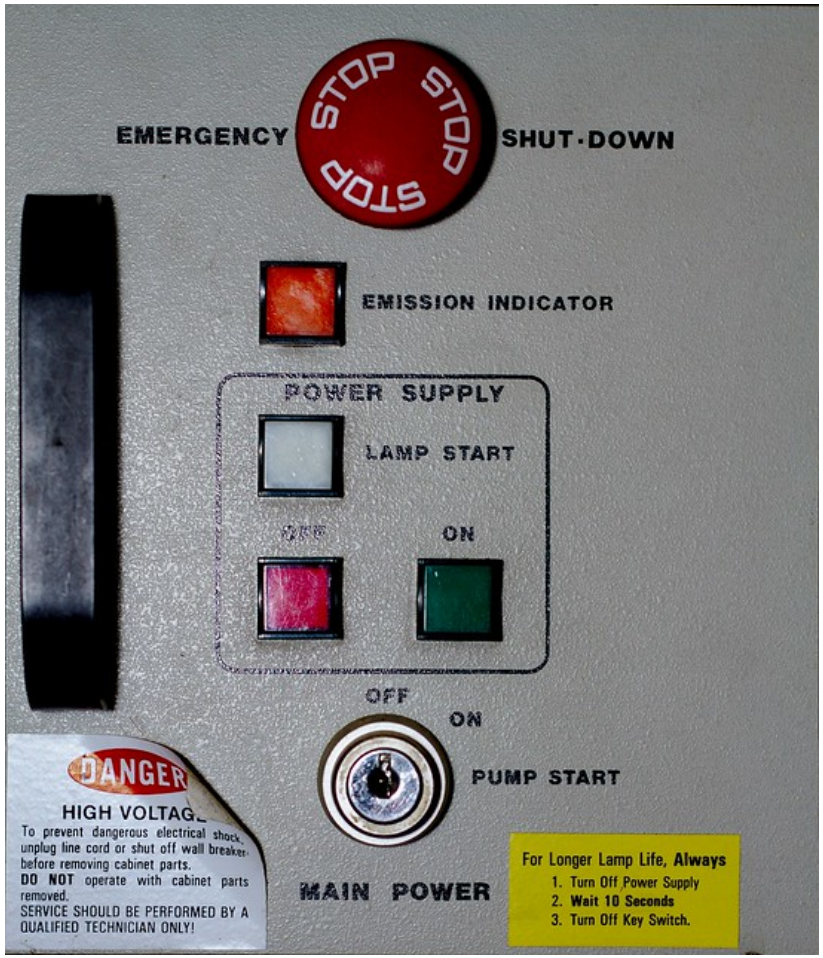
- In case of power outage, UPS provides backup power source for computer systems
- Four basic configurations of UPS:
  - Standby UPS
  - Ferroresonant standby UPS
  - Line-interactive UPS
  - True online UPS

Uninterruptible Power Supplies (UPSs) (2)

- Standby UPS: offline battery backup that detects power interruptions
- Ferroresonant standby UPS: offline UPS whose transformer reduces power problems
- Line-interactive UPS: always connected to output
  - Faster response time; conditions power, filters noise
- True online UPS: primary power source is battery
  - A/C-power from utility recharges batteries
  - Provides constant power to computers without power quality problems

Emergency Shutoff

- Key requirement: shut off power at once if current poses risk to machines, people
- Most computer rooms have emergency power shutoff ("big red button")



Source: Flickr (Dennis van Zuijlekom, CC-BY-SA 2.0)

Electrical Terms

Term	Definition
Fault	Momentary power interruption
Blackout	Prolonged power interruption
Sag	Momentary drop in power voltage levels
Brownout	Prolonged drop in power voltage levels
Spike	Momentary increase in power voltage levels
Surge	Prolonged increase in power voltage levels

Water Problems

- Lack of water poses problems to systems
  - Fire suppression systems
  - Water chillers for air conditioning
- Too much water (pressure): real threat
- Hence, we need to integrate water detection systems with alarms used to monitor buildings

Structural Collapse

- Structures housing an org. can fail due to environmental factors, forces of nature
- Structures designed with load limits
  - Overloading load limits results in structural failure, possibly injury or death
  - To prevent this, civil engineers should inspect buildings, identify dangers before failure

Testing Facility Systems

- Physical security of a facility must be constantly documented and tested
- Documentation of facility configuration, integrated into disaster recovery plans and operating procedures
- Testing provides necessary info. to improve facility security, find weak points

Interception of Data

- Three methods of data interception:
  - Direct observation
  - Data transmission
  - Eavesdropping on signals
    - All electronics emit electromagnetic signals; data on computer can be reconstructed
    - TEMPEST (NSA): technology control to prevent it
- Side-channel attacks: monitor keystroke acoustics, screen displays, etc.

Mobile and Portable Systems

- Mobile devices, laptops pose threat to information security
  - Devices may have (sensitive) org. info on them
  - Devices may be configured to access org.'s secure computing facilities
  - Not to mention ease of theft (mobile devices)

Stopping Laptop Losses

- Controls support security and retrieval of lost or stolen laptops
  - CompuTrace: installed on laptop hardware, reports to a central monitoring location
  - Burglar alarms (PC card with motion detector):
    - If laptop alarm is armed and laptop is moved beyond a certain distance, audible alarm triggers
    - The system shuts down the computer and includes an encryption option for info. on laptop
  - BitLocker (Windows Vista+), FileVault (OS X), home directory encryption (Linux)

Remote Computing Security

- Remote site computing: distant from org. facility
- Telecommuting: remote computing using networking technology
- Employees may need to access org. networks on business trips
- Remote workers need access from home systems or satellite offices
- External connections, systems need security to support these use cases (e.g., VPN)

Special Considerations for Physical Security Threats

- Develop physical security in-house or outsource?
  - Many qualified and professional agencies
  - Benefit of outsourcing: gain experience, knowledge of these agencies
  - Downsides: high expense, loss of control over the individual components, and level of trust placed in another company
- Social engineering: using people skills to obtain information from employees
  - For more info see Kevin Mitnick's *The Art of Deception*

Inventory Management

- Computing equipment should be inventoried, inspected on regular basis
- Classified information should also be inventoried and managed
  - Whenever classified document is copied, place stamp on it (with security level, document number)
  - Each classified copy sent to the receiver, who signs for the document
  - Electronic example: DocuSign, similar services

Summary

- Physical security complements info. security – it's just as important!
  - Controls include locks, keys, ID badges, etc.
  - Monitoring, intrusion detection via alarms, electronic systems
  - Utilities mgmt. (electrical, etc.), structural integrity
  - Fire detection/suppression are crucial
  - Data loss prevention and secure remote computing
  - Laptop/mobile device inventory, mgmt., security