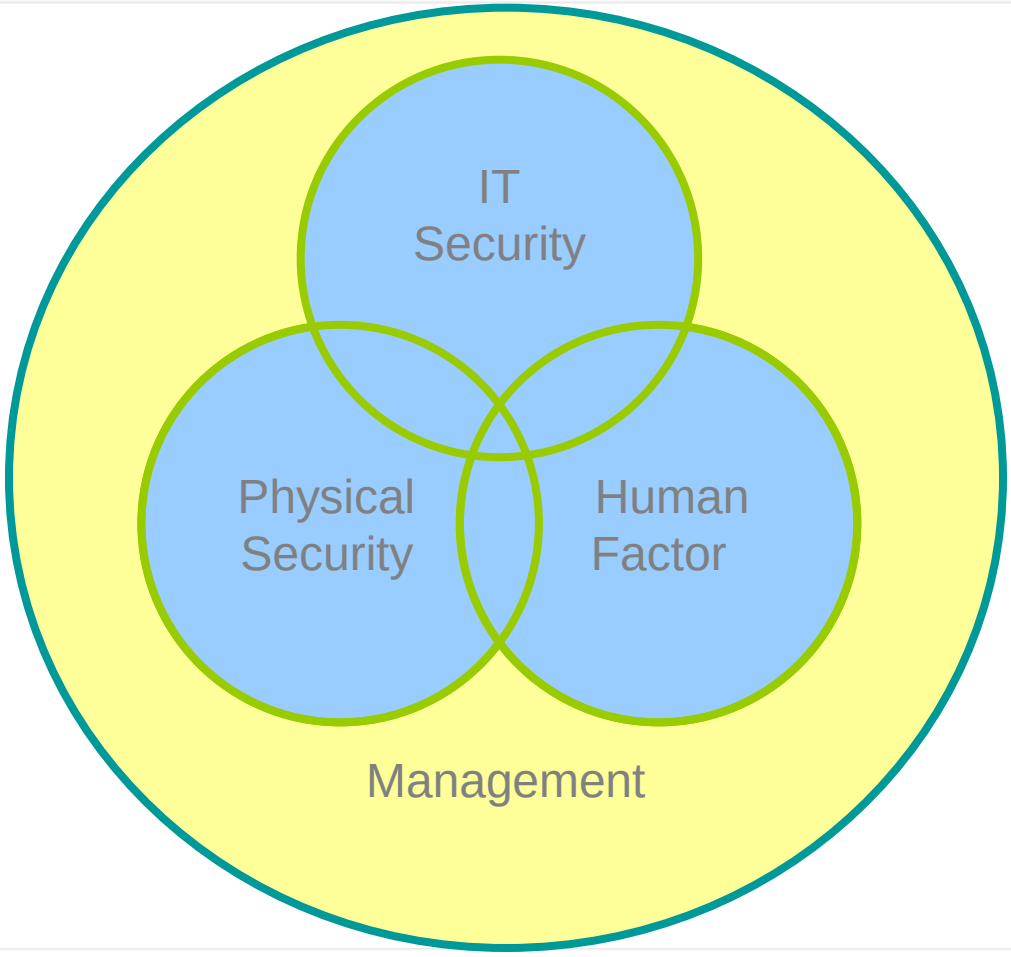
INF3510 Information Security
University of Oslo
Spring 2010

Lecture 9

Physical Security and the Human Factor

Audun Jøsang

Components of Security



PHYSICAL SECURITY

- **Natural Physical Security**
- **Physical Access Control**
- **Environmental Security**

Threats to Physical Security

- Inadvertent acts
  - acts of human error or failure,
  - deviations in quality of service,
- Deliberate acts
  - espionage or trespass,
  - information extortion
  - sabotage or vandalism,
  - theft and compromises to intellectual property
- Forces of nature
- Technical failures
  - technical hardware & equipment failures or errors
  - technical software failures or errors
- Management failures
  - technical obsolescence.

PHYSICAL SECURITY

- **Natural Physical Security**
- **Physical Access Control**
- **Environmental Security**

Natural Physical Security

Crime Prevention Through Environmental Design (CPTED)

- *CPTED is the proper design and effective use of the built environment which may lead to a reduction in the fear and incidence of crime, and an improvement of the quality of life." –*

  US National Crime Prevention Institute

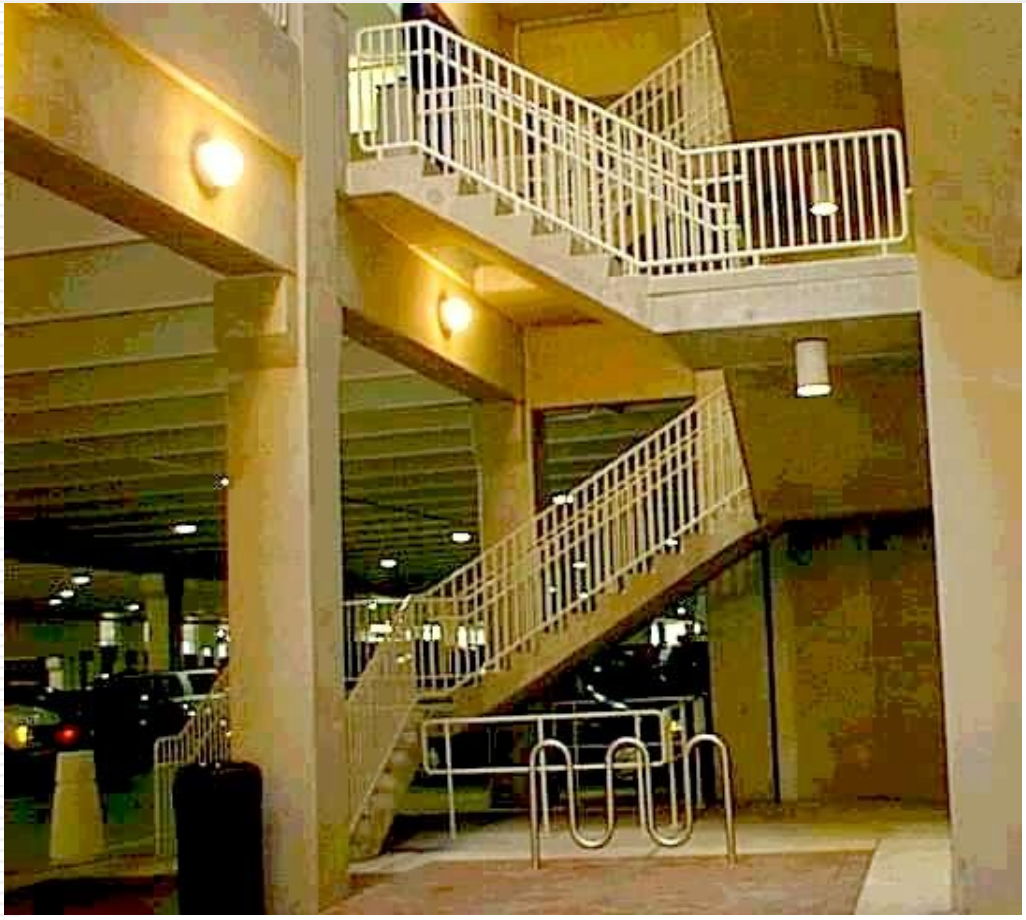
CPTED Strategies

- Natural Surveillance
- Natural Access Control
- Territorial Reinforcement
- Activity Support
- Target Hardening

CPTED Natural Surveillance

- A design concept directed primarily at keeping intruders easily observable. Promoted by features that maximize visibility of people, parking areas and building entrances: doors and windows that look out on to streets and parking areas; pedestrian-friendly sidewalks and streets; front porches; adequate night time lighting.

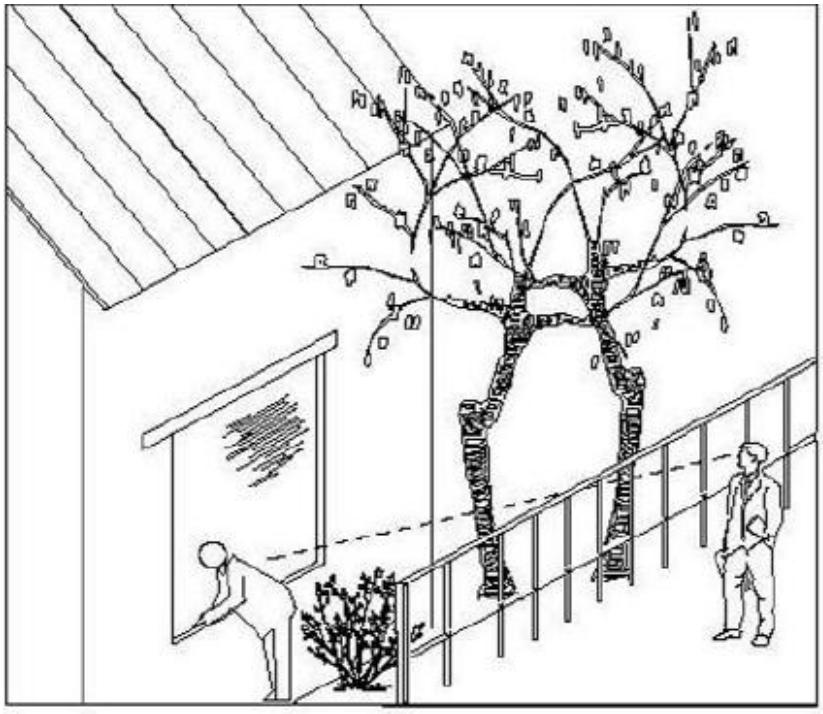
CPTED Natural Surveillance

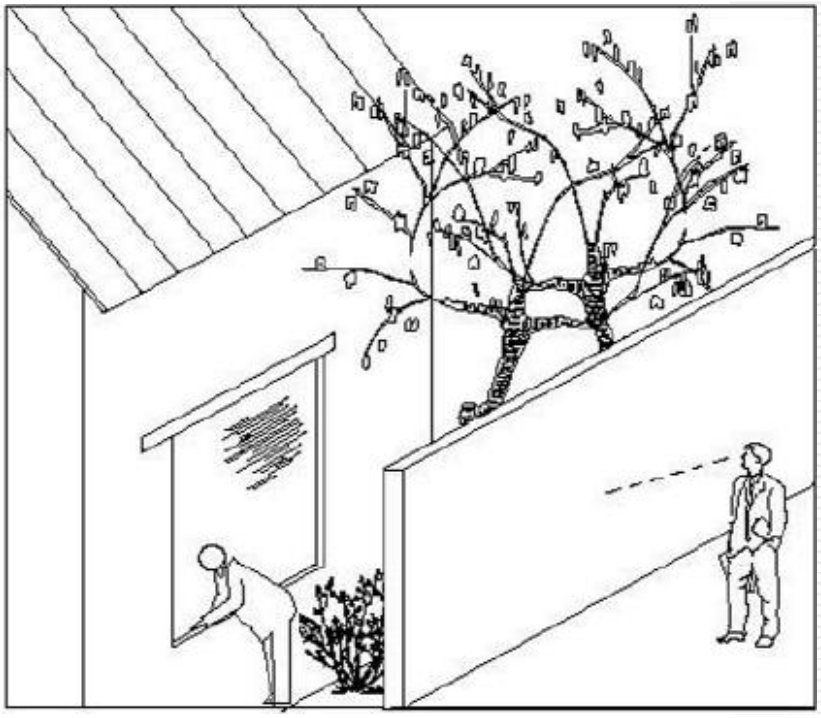


This stairwell design providing access to a parking garage creates opportunities for surveillance as well as creating the opportunity to be heard if assistance is needed.

CPTED Natural Surveillance

- **Permeable fencing allows surveillance**





CPTED Natural Access Control

- A design concept directed primarily at decreasing crime opportunity by denying access to crime targets and creating in offenders a perception of risk. Gained by designing streets, sidewalks, building entrances and neighbourhood gateways to clearly indicate public routes and discouraging access to private areas with structural elements.

CPTED Natural Access Control

The bollard lights placed at the entrance to this office building provide Natural Access Control because they guide you toward the building's entrance. There are no signs to indicate the building's entrance, but the combination of a walkway, landscaping, and bollard lights forces visitors to follow the path to the entrance.

CPTED Territorial Reinforcement

- Physical design can create or extend a sphere of influence. Users then develop a sense of territorial control while potential offenders, perceiving this control, are discouraged. Promoted by features that define property lines and distinguish private spaces from public spaces using landscape plantings, pavement designs, gateway treatments, and "CPTED" fences.

CPTED Territorial Reinforcement

Painting over graffiti immediately sends a message that the area is cared for and will be well maintained.

This shop front clearly defines the barrier from the public area to the office building.

CPTED Activity Support

- Planned activities for the areas that need to be protected. Designed to get people to work together to increase the overall awareness of acceptable and unacceptable activities in the area.
  - E.g.
    - Sport courts in parks attract healthy activity
    - Company BBQ parties on company grounds

CPTED Activity Support

This company BBQ gives staff and neighbours the perception that the area is being actively used and cared for, which discourages trespassing and littering.

CPTED Target Hardening

- Accomplished by features that prohibit and control entry or access: window locks, dead bolts for doors, interior door hinges, and security guards
- This is traditional physical access control
- Comes on top of previous CPTED strategies

Target hardening

Target hardening or mitigation is a process wherein a building is made into a more difficult or less attractive target. It does not necessarily mean the construction of an impenetrable bunker, although this would be the extreme case of target hardening.

PHYSICAL SECURITY

- **Natural Physical Security**
- **Physical Access Control**
- **Environmental Security**

Physical Access Controls

- Walls, Fencing, and Gates
- Guards
- Dogs, ID Cards, and Badges
- Locks and Keys
- Mantraps
- Electronic Monitoring
- Alarms and Alarm Systems
- Computer Rooms
- Walls and Doors

- *To ensure that no unauthorized person can get physical access to facilities and systems, or damage and steal equipment.*

Multilayered Physical AC

- Defence in depth
  - Requires that the organisation establish multiple layers of controls
  - Attackers will have to penetrate many protection layers in order to access sensitive information and systems
  - Slows down, and makes successful attacks much harder

Defence in Depth

- Physical perimeter security
  - Fences, hedges, bollards, gates, security guards, dogs, manned gate, CCTV
- Building entry security
  - Walls, doors, windows, locks, keys, guards, manned reception, alarms,CCTV, ID Cards, biometrics, etc.
- Interior security
  - Separate office areas and rooms, doors, locks, motion detectors , clean desks, lockable cabinets, alarms,CCTV, biometrics, etc.

Defence in Depth

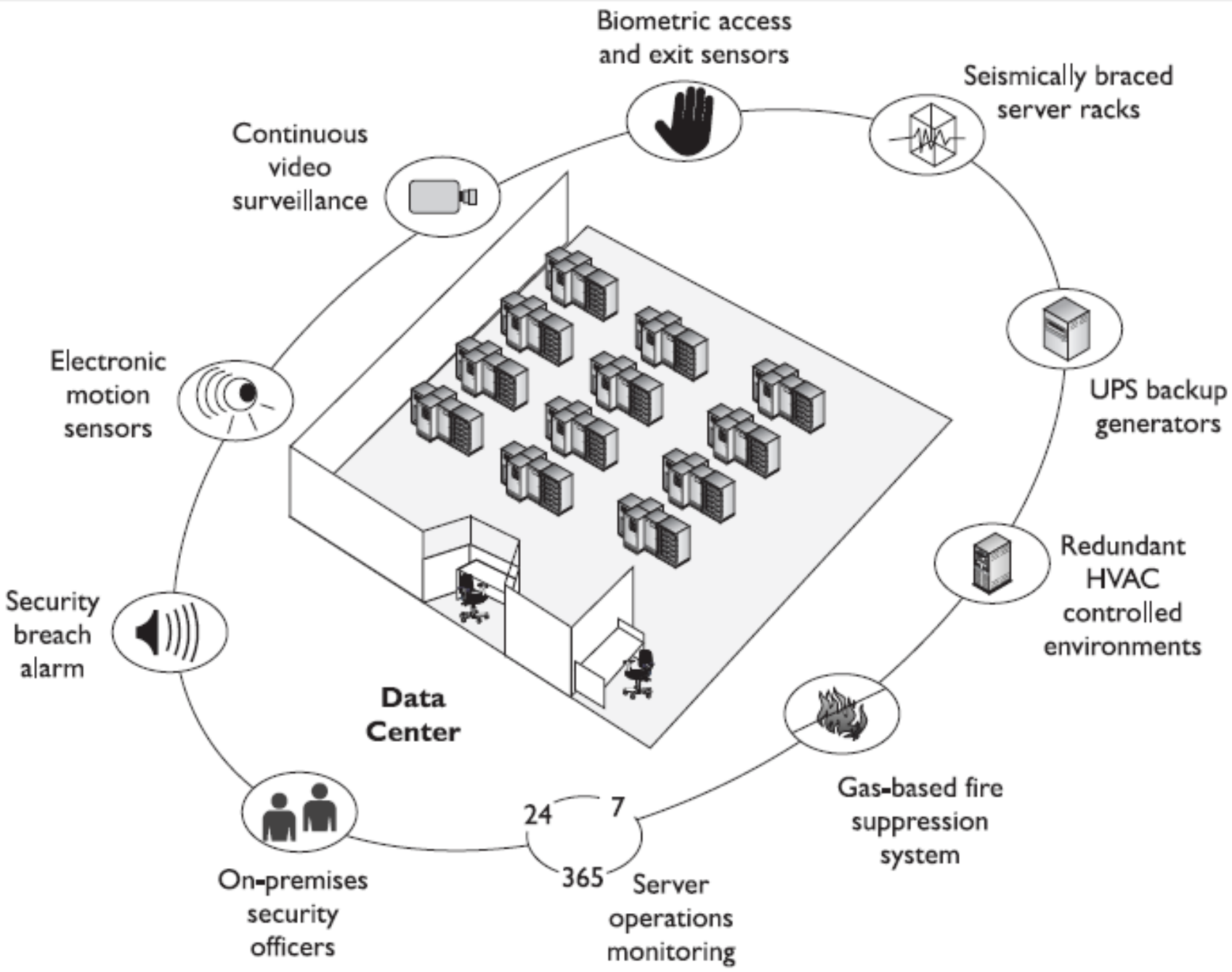


Figure 6-5 A data center should have many physical security controls.

Locks and Keys

- There are two types of locks
  - mechanical and electro-mechanical
- Locks can also be divided into four categories
  - manual, programmable, electronic, and biometric
- In case of lock failure, facilities need alternative procedures for access
- Locks fail in one of two ways:
  - when the lock of a door fails and the door becomes unlocked, that is a fail-safe lock
  - when the lock of a door fails and the door remains locked, this is a fail-secure lock

Mantraps

- An enclosure that has an entry point and a different exit point
- The individual enters the mantrap, requests access, and if verified, is allowed to exit the mantrap into the facility
- If the individual is denied entry, they are not allowed to exit until a security official overrides the automatic locks of the enclosure

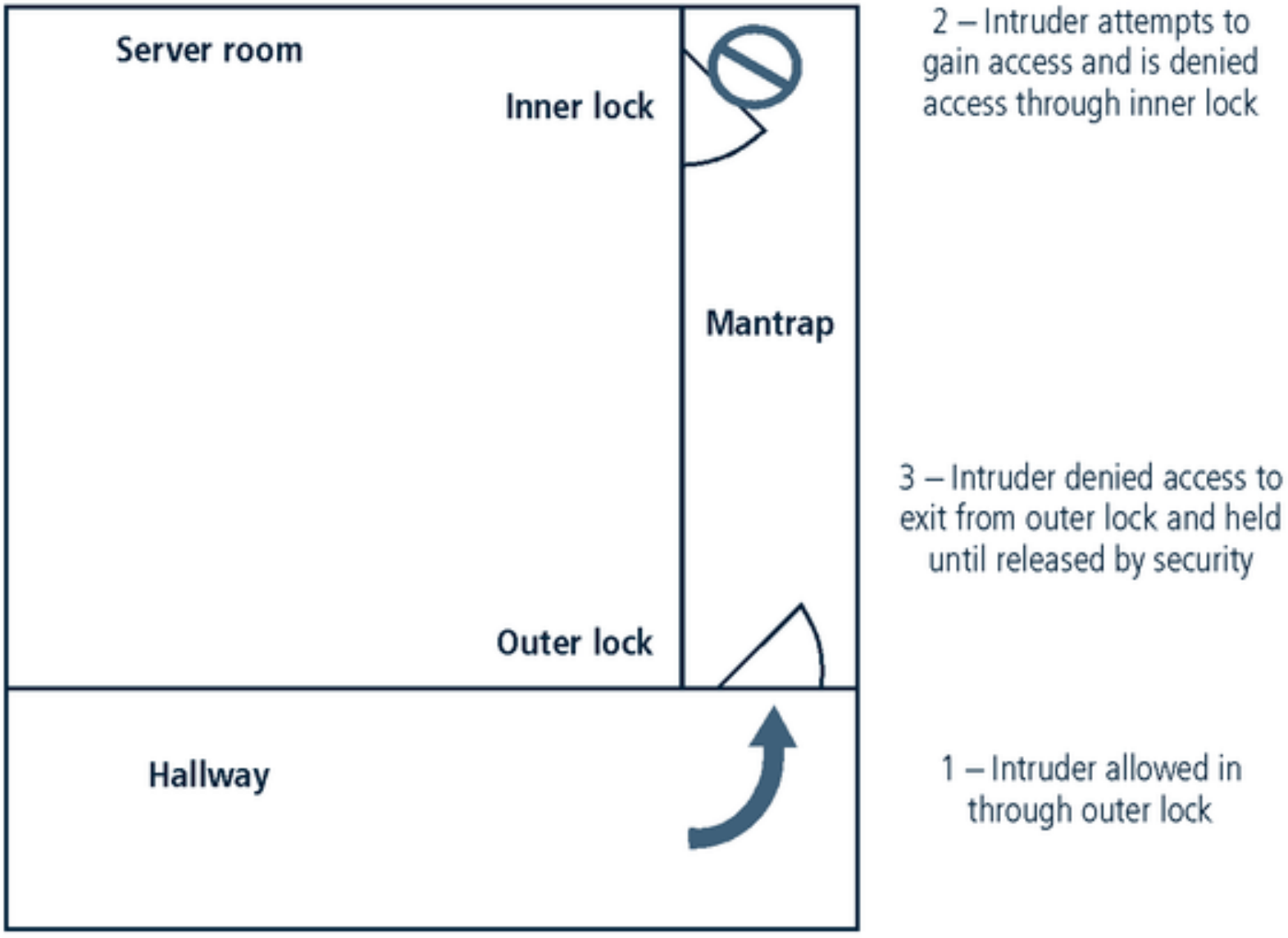


FIGURE 9-2 Mantraps

Interior Walls and Doors

- The walls in a facility are typically either:
  - standard interior
  - firewall
- All high-security areas must have firewall grade walls to provide physical security from potential intruders and improves the facility's resistance to fires
- Doors that allow access into secured rooms should also be evaluated
- Computer rooms and wiring closets can have push or crash bars installed.

Computer Rooms and Wiring Closets

- Computer rooms and wiring and communications closets require special attention
- Logical controls are easily defeated, if an attacker gains physical access to the computing equipment
- Custodial staff are often the least scrutinized of those who have access to offices and are given the greatest degree of unsupervised access

Alarms and Alarm Systems

- Alarm systems notify when an event occurs
- Used for fire, intrusion, environmental disturbance, or an interruption in services
- These systems rely on sensors that detect the event: motion detectors, smoke detectors, thermal detectors, glass breakage detectors, weight sensors, and contact sensors

ID Cards and Badges

- Ties physical security to information access with identification cards (ID) and/or name badges
  - ID card is typically concealed
  - Name badge is visible
- These devices are actually biometrics (facial recognition)
- Should not be the only control as they can be easily duplicated, stolen, and modified
- Tailgating occurs when unauthorized individuals follow authorized users through the control

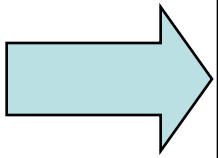
Electronic Monitoring

- Records events where other types of physical controls are not practical
- May use cameras with video recorders
- Drawbacks:
  - reactive and do not prevent access or prohibited activity
  - recordings often not monitored in real time and must be reviewed to have any value
  - Human security guards tire quickly and will no longer react to events recorded by video surveillance

Automated video surveillance

Suspicious events are rare

Attention from the guard is needed for very few occasions



Limited human participation

The guard is “replaced” by vision algorithms

Automated Video Surveillance

- Large scale video surveillance systems deployed on top of IP-network
- System of scattered low cost video sensors
- Existing surveillance systems VSAM,KNIGHT, SfinX, etc.
  - Focus on the design of computer vision algorithms
  - PC is attached to each video source
  - Stream full quality video or just images
- Alarms triggered by vision systems to get human attention to suspicious events.

Inventory Management

- Computing equipment should be inventoried and inspected on a regular basis
- Classified information should also be inventoried and managed
  - Whenever a classified document is reproduced, a stamp should be placed on the original before it is copied
  - This stamp states the document's classification level and document number for tracking
  - Each classified copy is issued to its receiver, who signs for the document

Mobile and Portable Systems

- With the increased threat to overall information security for laptops, handhelds, and PDAs, mobile computing requires even more security than the average in-house system
- Many of these mobile computing systems not only have corporate information stored within them, many are configured to facilitate the user's access into the organization's secure computing facilities

Stopping Laptop Theft

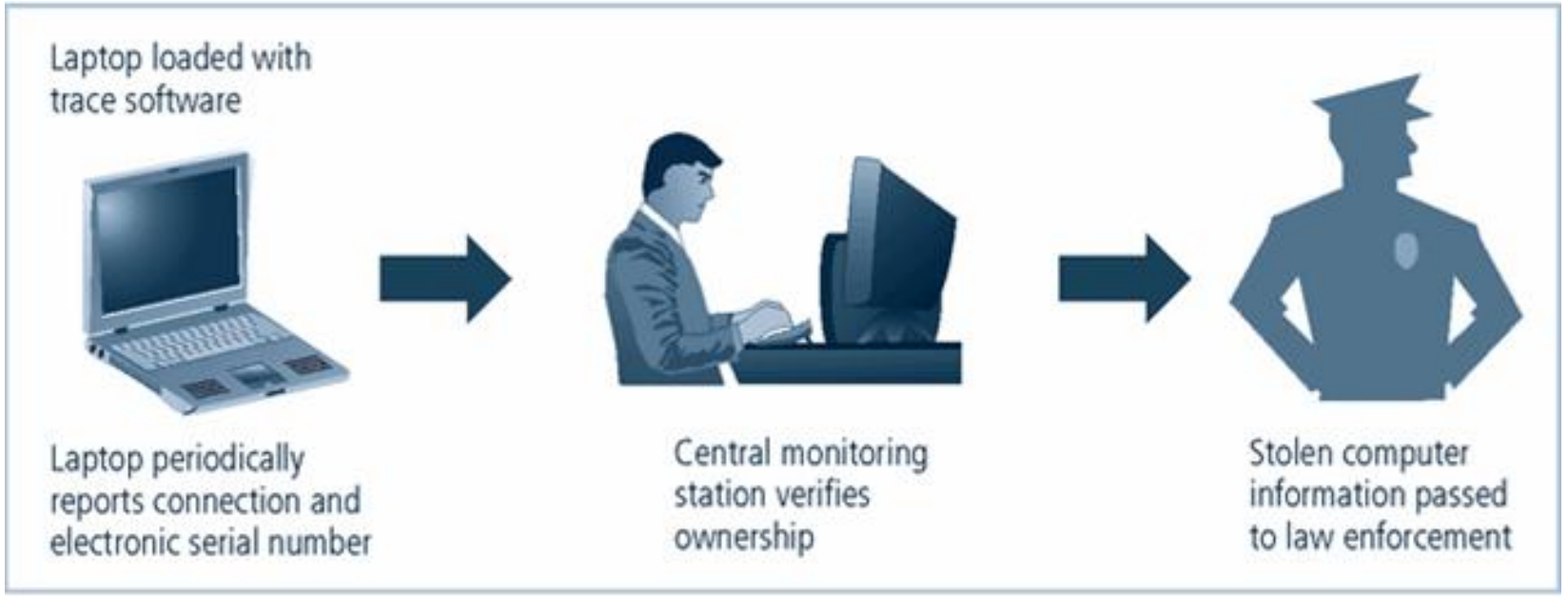
- Inventory all laptops, and register with vendor
- Harden the OS / Platform
- Password protect the BIOS
- Don’t check laptops in as luggage when flying
- Never leave a laptop unattended
- Carry laptop in a non-descriptive case or bag
- Engrave the laptop with identification signs
- Lock to stationary object with slot lock and cable
- Back up data from laptop
- Use special safe if left in vehicles
- Encrypt sensitive data
- Use laptop tracing service

Laptop Tracing Service (for the paranoid)

Support the security and retrieval of lost or stolen laptops

- CompuTrace is stored on a laptop's hardware and reports to a central monitoring center
- Burglar alarms made up of a PC card that contains a motion detector
  - If the alarm in the laptop is armed, and the laptop is moved beyond a configured distance, the alarm triggers an audible alarm
  - The system also shuts down the computer and includes an encryption option to completely render the information unusable

Laptop Tracing Service



- Laptop tracing can act as a strong theft deterrent

Remote Computing Security

- Remote site computing - distant from the organizational facility
- Telecommuting - computing using telecommunications including Internet, dial-up, or leased point-to-point links
- Employees may need to access networks on business trips
- Telecommuters need access from home systems or satellite offices
- To provide a secure extension of the organization's internal networks, all external connections and systems must be secured

PHYSICAL SECURITY

- **Natural Physical Security**
- **Physical Access Control**
- **Environmental Security**

Environmental Security

- Good physical security should protect resources against accidental damage and forces of nature,

  as well as deliberate acts, so include protection against
  - Fire & Smoke
  - Water damage
  - Power failure,
  - Structural collapse

Fire Safety

- The most serious threat to the safety of the people who work in the organization is the possibility of fire
- Fires account for more property damage, personal injury, and death than any other threat
- It is imperative that physical security plans examine and implement strong measures to detect and respond to fires and fire hazards

Supporting Utilities

- Supporting utilities, such as heating, ventilation and air conditioning, power, water, and other utilities, have a significant impact on the continued safe operation of a facility

- Extreme temperatures and humidity levels, electrical fluctuations and the interruption of water, sewage, and garbage services can create conditions that inject vulnerabilities in systems designed to protect information

Heating, Ventilation, and Air Conditioning

HVAC areas that can cause damage to IT systems:

- Temperature
  - Computer systems are subject to damage from extreme temperature
  - Optimal temperature for IT equipment (and people) is 20-24° Celsius
- Dust
- Humidity
  - Optimal humidity for IT equipment is 40%-55%
- Static
  - One of the leading causes of damage to sensitive circuitry is electrostatic discharge (ESD)
  - A person can generate up to 12,000 volts of static current by walking across a carpet
  - Often caused by low air humidity

Ventilation Shafts

- Security of the ventilation system air ductwork:
  - While in residential buildings the ductwork is quite small, in large commercial buildings it can be large enough for an individual to climb through
  - If the vents are large, security can install wire mesh grids at various points to compartmentalize the runs

Structural Collapse

- Unavoidable forces can cause failures of structures that house the organization
- Structures are designed and constructed with specific load limits, and overloading these design limits, intentionally or unintentionally, inevitably results in structural failure and potentially loss of life or injury
- Periodic inspections by qualified civil engineers assists in identifying potentially dangerous structural conditions well before they fail

Power Management and Conditioning

- Electrical quantity (voltage level and amperage rating) is a concern, as is the quality of the power (cleanliness and proper installation)
- Any noise that interferes with the normal 50 Hertz (or 60 Hertz) cycle can result in inaccurate time clocks or unreliable internal clocks inside the CPU
- Grounding
  - Grounding ensures that the returning flow of current is properly discharged
  - If not properly installed could cause damage to equipment and injury or death to the person
- Overloading a circuit not only causes problems with the circuit tripping but can also overload the power load on an electrical cable, creating the risk of fire

Electrical Terms

- Fault: momentary interruption in power
- Blackout: prolonged interruption in power
- 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

Emergency Shutoff

- One important aspect of power management in any environment is the need to be able to stop power immediately should the current represent a risk to human or machine safety
- Most computer rooms and wiring closets are equipped with an emergency power shutoff, which is usually a large red button, prominently placed to facilitate access, with an accident-proof cover to prevent unintentional use

Uninterruptible Power Supplies (UPSs)

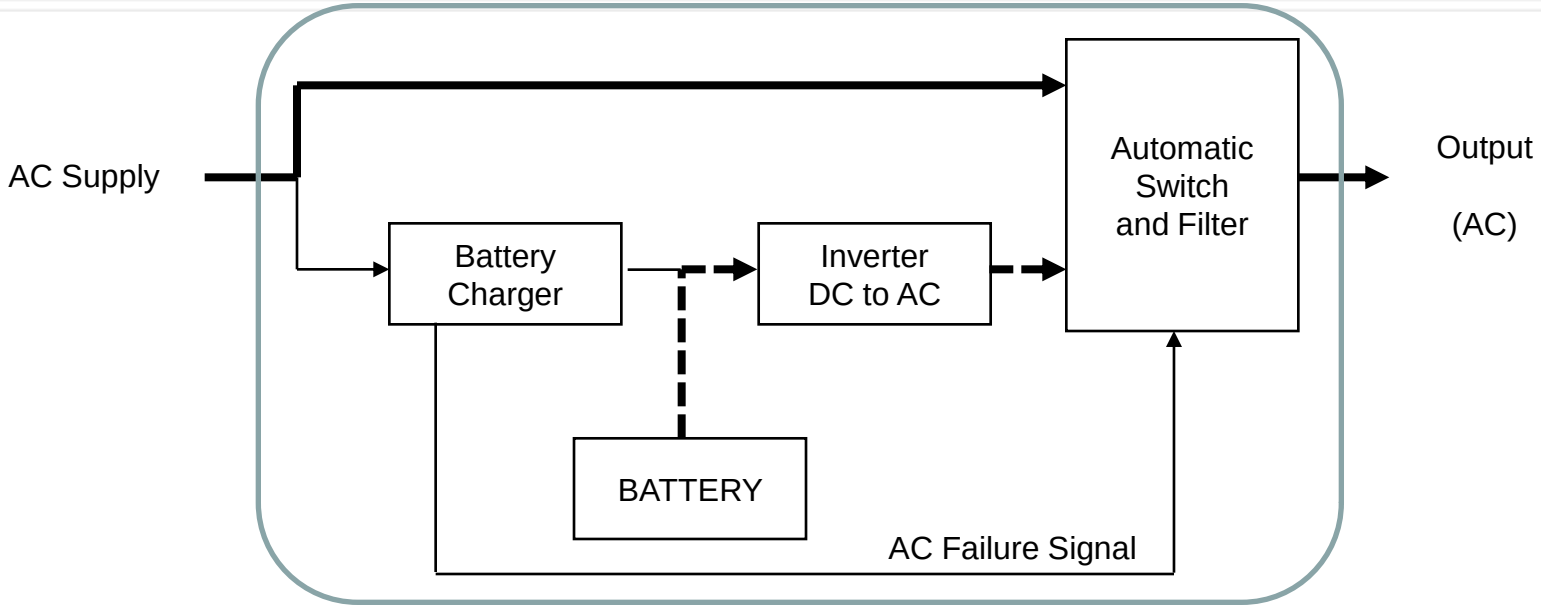
- In case of power outage, a UPS is a backup power source for major computer systems
- There are four basic configurations of UPS:
  - the standby
  - ferro-resonant standby
  - line-interactive
  - the true online

- AC: Alternate Current, provided by power company
  - 220V, 50Hz (Europe) or 110V, 60Hz (US)
- DC: Direct Current, provided by battery or power supply

Uninterruptible Power Supplies (UPSs)

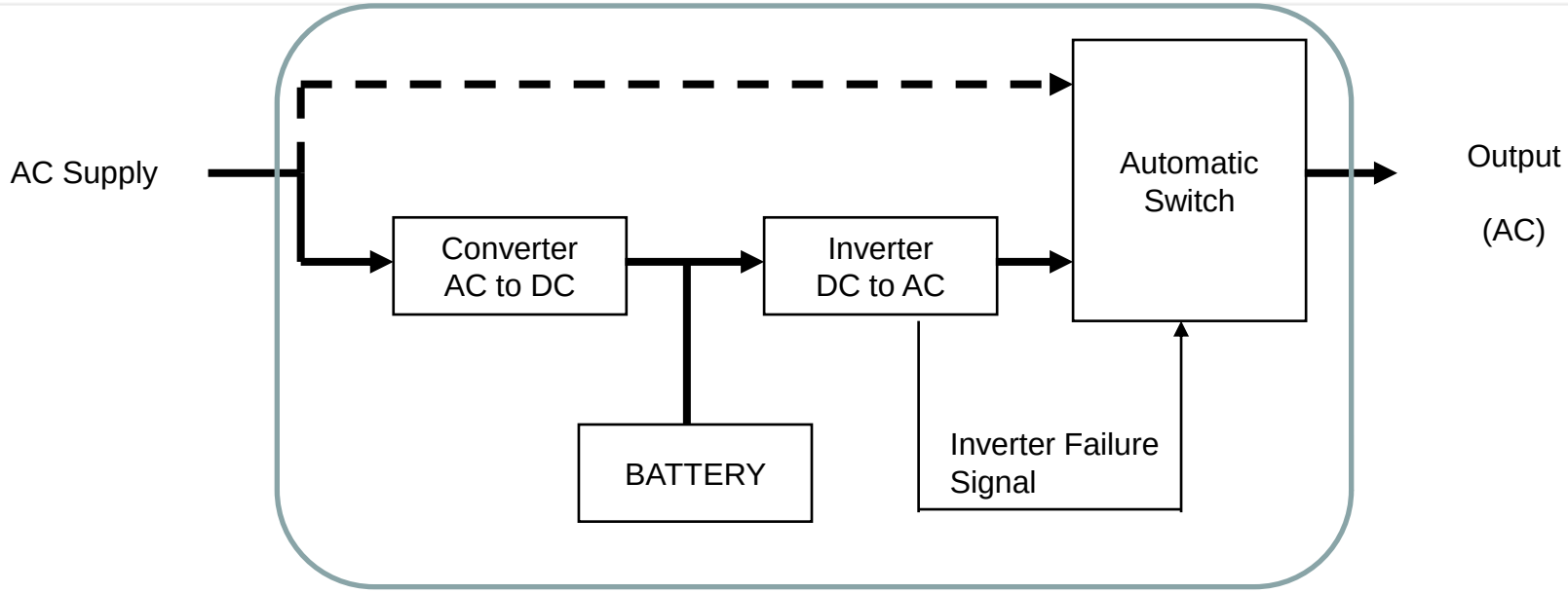
- A standby or offline UPS takes over in case of power supply failure from the power company.
  - Causes short interruption and irregularity during switchover
- A ferro-resonnant standby UPS is still an offline UPS
  - Reduces power irregularity problems
- The Line-Interactive UPS is always connected to the output
  - Fast response time and incorporates power conditioning and line filtering
- The True Online UPS works in the opposite fashion to a standby UPS since the primary power source is the battery, with the power feed from the utility constantly recharging the batteries
  - this model allows constant feed to the system, while completely eliminating power quality problems

Line-Interactive UPS



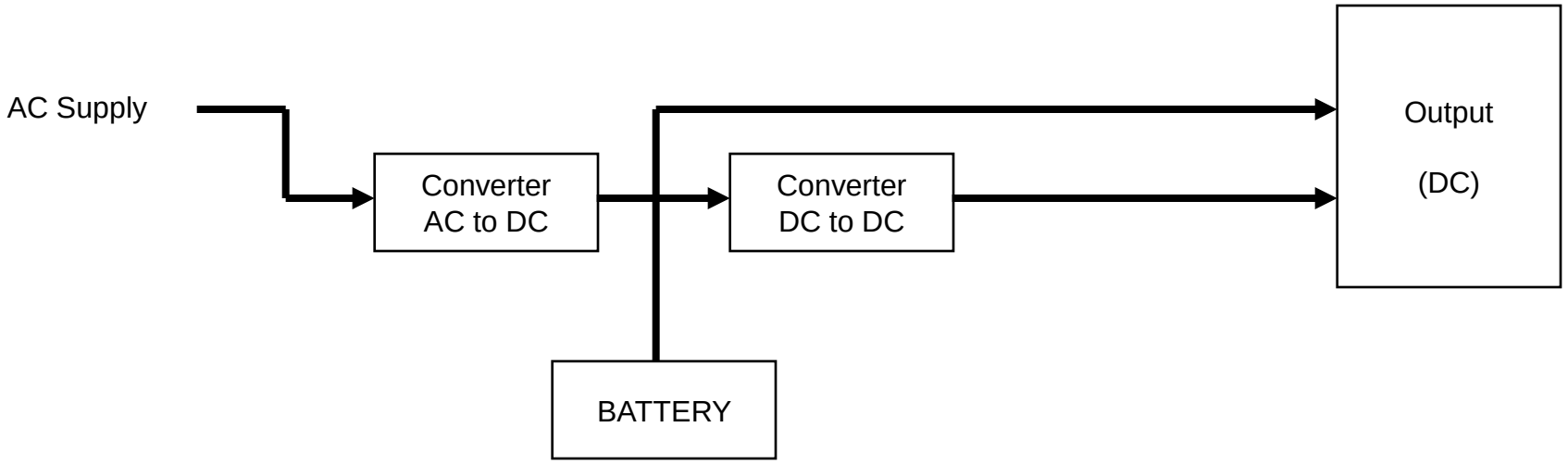
- AC power normally bypasses the battery and inverter
- Power is taken from battery in case AC supply fails

True On-line UPS



- Normal power supply always goes through converter, battery and inverter
- AC can bypass battery and inverter in case of failure

Laptop Computer Power Supply



- Power always goes through converter and battery
- DC leves other than that provided by the battery can be provided by DC-to-DC converter.

Water Problems

- Lack of water poses problems to systems, including the functionality of fire suppression systems, and the ability of water chillers to provide air-conditioning
- On the other hand, a surplus of water, or water pressure, poses a real threat
- It is therefore important to integrate water detection systems into the alarm systems that regulate overall facilities operations

Testing Facility Systems

- Physical security of the facility must be constantly documented, evaluated, and tested
- Documentation of the facility's configuration, operation, and function is integrated into disaster recovery plans and standing operating procedures
- Testing provides information necessary to improve the physical security in the facility and identifies weak points

The Human Factor

- Personnel integrity
  - Making sure personnel do not become attackers
- Personnel as defence
  - Making sure personnel do not fall victim to social engineering attacks
- Security Usability
  - Making sure people can operate security systems correctly

Personnel Integrity

Preventing employees from becoming attackers

- Consider:
  - Employees
  - Executives
  - Customers
  - Visitors
  - Contractors & Consultants
- All these groups obtain some form of access privileges
- How to make sure privileges are not abused?

Personnel crime statistics

- Organisations report that large proportion of computer crimes originate from inside
- US Statistics (CSI/FBI) 2005
  - http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf
  - 71% had inside (65% had external) computer crime attacks
- Australian Statistics (AusCERT) 2006
  - http://www.auscert.org.au/images/ACCSS2006.pdf
  - 30% had inside (82% had external) electronic attacks

Personnel Integrity

- A company's existence depends on the integrity of its employees.
- New employees may get access to extremely sensitive and confidential information.
- The new employee's ethical outlook is *a priori* unknown.
- Unauthorized release of sensitive information could destroy reputation or cause financial damage
- An employee, who has just accepted a position with a major competitor, may want to steal important trade secrets.

Hiring Practices

- Employers are often reluctant to release information about former staff.
- Former employees have successfully sued corporations and supervisors for making derogatory statements to prospective employers.
- Consider:
  - Informal phone calls
  - Ask for reference authorization and consider “hold-harmless agreement” for written requests

Hiring Practices

- Reference authorization and hold-harmless agreement
  - The applicant authorises the disclosure of past employment information and releases both the prospective employer and the former employer from all claims and liabilities arising from the release of such information.
  - Should have: signature of applicant, releases former & prospective employers, and clearly specifies the type of information that may be divulged.

Personnel Departure

- Different reasons for departure
  - Voluntary
  - Redundancy
  - Termination
- Different types of actions
  - Former employee may keep some privileges
  - Revoke all privileges
  - Escort to the exit.
- During exit interview, terms of original employment agreement reviewed (i.e. non-compete, wrongful disclosure, etc.

Personnel as Defence: Stopping Social Engineering Attacks

- Social Engineering Basics
  - "Management of human beings according to their place and function in society" (Websters Dictionary)
  - Everybody practices social engineering
    - Social interactions, negotiations, diplomacy
  - Social engineering can also be used as part of attacking information systems

Social Engineering Attacks

- According to Kevin Mitnick:
  - "The biggest threat to the security of a company is not a computer virus, an unpatched hole in a program, or a badly installed firewall. In fact the biggest threat could be you."
  - "What I found personally to be true was that it's easier to manipulate people rather than technology. Most of the time, organisations overlook that human element".

From "How to hack people", BBC NewsOnline, 14 Oct 2002

SE Tactics: Develop Trust

- People are naturally helpful and trusting
- Ask during seemingly innocent conversations
- Slowly ask for increasingly important information
- Learn company lingo, names of key personnel, names of servers and applications
- Cause a problem and subsequently offer your help to fix it (aka. reverse social engineering)
- Talk negatively about common enemy
- Talk positively about common hero

SE Tactics: Induce strong affect

- Heightened emotional state makes victim
  - Less alert
  - Less likely to analyse deceptive arguments
- Triggered by attacker by creating
  - Excitement (“you have won a price”)
  - Fear (“you will loose your job”)
  - Confusion (contradictory statements)

SE Tactics: Overload

- Reduced the target's ability to scrutinize arguments proposed by the attacker
- Triggered by
  - Providing large amounts of information to produce sensory overload
  - Providing arguments from an unexpected angle, which forces the victim to analyse the situation from new perspective, which requires additional mental processing

SE Tactics: Reciprocation

- Exploits our tendency to return a favour
  - Even if the first favour was not requested
  - Even if the return favour is more valuable
- Double disagreement
  - If the attacker creates a double disagreement, and gives in on one, the victim will have a tendency to give in on the other
- Expectation
  - If the victim is requested to give the first favour, he will believe that the attacker becomes a future ally

SE Tactics:
Diffusion of Responsibility and Moral Duty

- Make the target feel the he or she will not be held responsible for actions
- Make the target feel that satisfying attacker's request is a moral duty

SE Tactics: Authority

- People are conditioned to obey authority
  - Milgram and other experiments
  - Considered rude to even challenge the veracity of authority claim
- Triggered by
  - Faking credentials
  - Faking to be a director or superior
  - Skilful acting (con artist)

SE Tactics: Commitment Creep

- People have a tendency to follow commitments, even when recognising that it might be unwise.
- It's often a matter of showing personal consistency and integrity
- Triggered e.g. by creating a situation where one commitment naturally or logically follows another.
  - First request is harmless
  - Second request causes the damage

Multi-Level Defence against Social Engineering Attacks

Source: David Gragg: http://www.sans.org/rr/whitepapers/engineering/

SE Defence: Foundation

- Security policy to address SE attacks
  - The policy will always be the foundation of information security
  - Should address practices related to
    - Access controls
    - Account set-up
    - Password changes
    - Shredding
    - Visitor escorting
    - Authority obedience
  - Policy must not define practices that a SE attacker would use.

SE Defence: Awareness

- Security awareness training for all staff
  - Understanding SE tactics
  - Learn to recognise SE attacks
  - Know when to say “no”
  - Know what is sensitive
  - Understand their responsibility
  - Understand the danger of casual conversation
  - Friends are not always friends
  - Passwords are personal
  - Uniforms are cheap
- Awareness of policy shall make personnel feel that the only choice is to resist SE attempts

SE Defence: Fortress

- Resistance training for key personnel
  - Consider: Reception, Help desk, Sys.Admin., Customer service,
- Fortress training techniques
  - Inoculation
    - Expose to SE arguments, and learn counterarguments
  - Forewarming
    - of content and intent
  - Reality check:
    - Realising own vulnerability,

SE Defence: Persistence

- Ongoing reminders
  - SE resistance will quickly diminish after a training session
  - Repeated training
  - Reminding staff of SE dangers
    - Posters
    - Messages
    - Tests

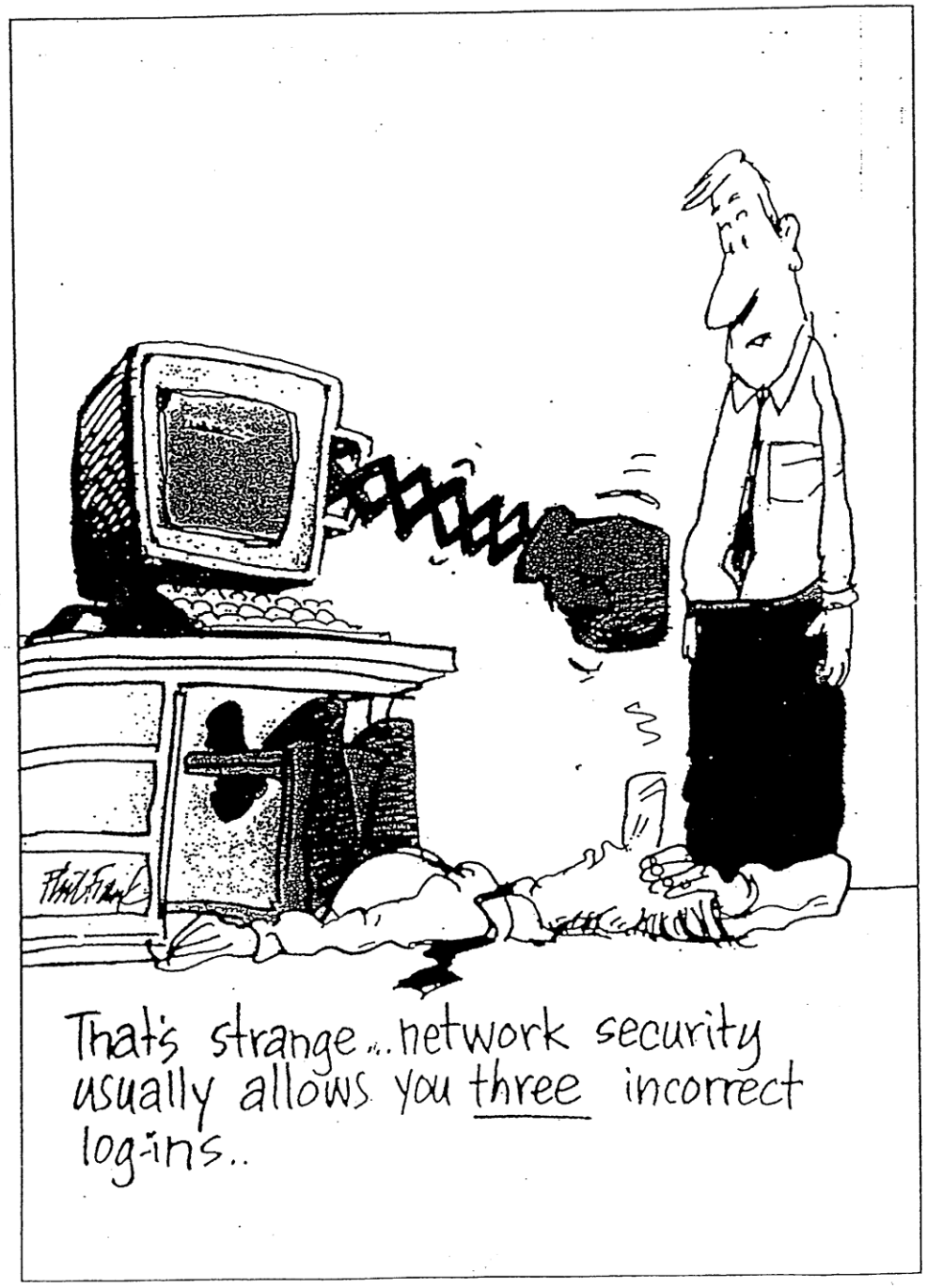
SE Defence: Gotcha

- Social Engineering Detectors
  - Filters and traps designed to expose SE attackers
- Consider:
  - The justified Know-it-all
    - Person who knows everybody
  - Centralised log of suspicious events
    - Can help discover SE patterns
  - Call backs mandatory by policy
  - Key questions, e.g. personal details
  - “Please hold” mandatory by policy
    - Time to think and log event
  - Deception
    - Bogus question
    - Login + password of “alarm account” on yellow sticker

SE Defence: Offensive

- Incident response
  - Well defined process for reporting and reacting to
    - Possible SE attack events,
    - Cases of successful SE attacks
- Reaction should be vigilant and aggressive
  - Go after SE attacker
  - Proactively warn other potential victims

Security Usability



Kerckhoffs 1883

- Auguste Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires,* IX(38):5-38 (January), and 161-191 (February), 1883.
- Famous principle; *"security by obscurity should be avoided"*
- Also defined security usability principles

Auguste Kerckhoffs

Kerckhoffs' security principles

1. The system must be substantially, if not mathematically, undecipherable;
2. The system must not require secrecy and can be stolen by the enemy without causing trouble;
3. It must be easy to communicate and remember the keys without requiring written notes, it must also be easy to change or modify the keys with different participants;
4. The system ought to be compatible with telegraph communication;
5. The system must be portable, and its use must not require more than one person;
6. Finally, regarding the circumstances in which such a system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.

Saltzer and Schroeder 1975

- Jerome H. Saltzer and Michael D. Schroeder. The Protection of Information in Computer Systems". *Communications of the ACM 17, 7 (July 1974).* 1975

- *It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.*
- *To the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized.*
- *If the user must translate his image of his protection needs into a radically different specification language, he will make errors.*

Jerome Saltzer

Michael Schroeder

Whitten & Tygar 1999

- Alma Whitten and J.D. Tygar. *Why Johnny Can't Encrypt: A Usability Evaluation of PGP5.0.*

  In *Proceedings of the 8th USENIX Security Symposium,* Washington, D.C. 1999.

Alma Whitten

Doug Tygar

Why Johnny Can't Encrypt. A Usability Evaluation of PGP 5.0

- PGP 5.0 had good usability from a traditional CHI (Computer-Human Interface) perspective.
- Still, 8 out of 12 participants were unable to encrypt and sign a message within 90min.
- Usability problems identified:
  - Misunderstood metaphors
  - No direct utility by security
  - Policy abstraction
  - Lack of feedback
  - The open barn door
  - Finding the weakest link

Security usability vulnerabilities

Security vulnerabilities are caused by:

- *Users who don't know or understand what conclusion is required for making an informed security decision.*
- *System that do not provide the user with sufficient information for deriving a security conclusion.*
- *Intolerable mental or manual load of deriving a security conclusion.*
- *Intolerable mental or manual load of deriving security conclusions for any practical number of instances.*

Implications of Current Landscape

- Security systems must be viewed as socio-technical systems that depend on the social context in which they are embedded to function correctly.
- There is a very real difference between the degree by which systems can be considered theoretically secure (assuming they are correctly operated) and actually secure (acknowledging that often they will be operated incorrectly).
- Consequence of poor security usability
  - Poor usability in an IT system prevents people from using it
  - Poor security usability still allows people to use the system, but in an insecure way.

Security / Usability Trade-off

- In many cases, there appears to be a trade-off between usability and theoretical security.
- It may be meaningful to reduce the level of theoretical security to improve the overall level of actual security.
- E.g.
  - User-friendly passwords
  - Remote villages and ATMs
- Policy should state the acceptable reduction in security for a specific security aspect
  - Implicitly in order to improve the overall security

Security Learning

- Good metaphors are important for learning
- Many security concepts do not have intuitive metaphors
- Better avoid metaphors than use bad ones
- Define new security concepts
  - and give them semantic content
- Security learning design
  - Design systems to facilitate good security learning
  - Largely unexplored field

End of Lecture

This lecture has focused on:

- Physical Security
  - Natural physical security
  - Physical Access Control
  - Environmental Security
- The Human Factor
  - Personnel security
  - Security Awareness
  - Security Usability