Computer Security: Principles and Practice

Fourth Edition, Global Edition

By: William Stallings and Lawrie Brown

Chapter 16

Physical and Infrastructure Security

Physical and Infrastructure Security

Logical security

- Protects computer-based data from software-based and communication-based threats

Physical security

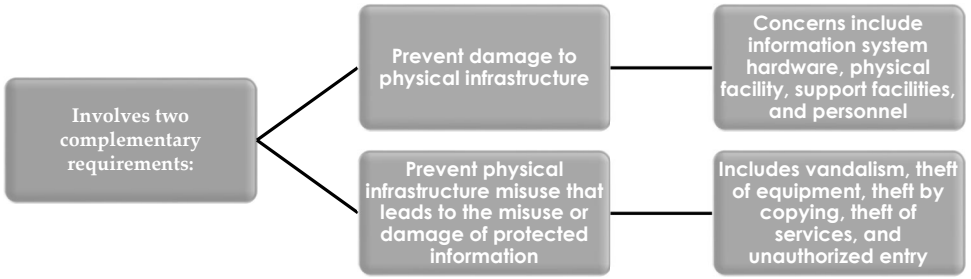
- Also called infrastructure security
- Protects the information systems that contain data and the people who use, operate, and maintain the systems
- Must prevent any type of physical access or intrusion that can compromise logical security

Premises security

- Also known as corporate or facilities security
- Protects the people and property within an entire area, facility, or building(s), and is usually required by laws, regulations, and fiduciary obligations
- Provides perimeter security, access control, smoke and fire detection, fire suppression, some environmental protection, and usually surveillance systems, alarms, and guards

Physical Security Overview

- Protect physical assets that support the storage and processing of information



Physical Security Threats

Physical situations and occurrences that threaten information systems:

- Environmental threats
- Technical threats
- Human-caused threats

Table 16.1
Characteristics of Natural Disasters

	Warning	Evacuation	Duration
Tornado	Advance warning of potential; not site specific	Remain at site	Brief but intense
Hurricane	Significant advance warning	May require evacuation	Hours to a few days
Earthquake	No warning	May be unable to evacuate	Brief duration; threat of continued aftershocks
Ice storm/ blizzard	Several days warning generally expected	May be unable to evacuate	May last several days
Lightning	Sensors may provide minutes of warning	May require evacuation	Brief but may recur
Flood	Several days warning generally expected	May be unable to evacuate	Site may be isolated for extended period

Source: ComputerSite Engineering, Inc.

Table 16.2

Fujita Tornado Intensity Scale

Category	Wind Speed Range	Description of Damage
F0	40 - 72 mph 64 - 116 km/hr	Light damage. Some damage to chimneys; tree branches broken off; shallow-rooted trees pushed over; sign boards damaged.
F1	73 - 112 mph 117 - 180 km/hr	Moderate damage. The lower limit is the beginning of hurricane wind speed; roof surfaces peeled off; mobile homes pushed off foundations or overturned; moving autos pushed off the roads.
F2	113 - 157 mph 181 - 252 km/hr	Considerable damage. roofs torn off houses; mobile homes demolished; boxcars pushed over; large trees snapped or uprooted; light-object missiles generated.
F3	158 - 206 mph 253 - 332 km/hr	Severe damage. Roofs and some walls torn off well-constructed houses; trains overturned; most trees in forest uprooted; heavy cars lifted off ground and thrown.
F4	207 - 260 mph 333 - 418 km/hr	Devastating damage. Well-constructed houses leveled; structure with weak foundation blown off some distance; cars thrown and large missiles generated.
F5	261 - 318 mph 419 - 512 km/hr	Incredible damage. Strong frame houses lifted off foundations and carried considerable distance to disintegrate; automobile-sized missiles fly through the air in excess of 100 yards; trees debarked.

(Table is on page 510 in the textbook)

Table 16.3
Saffir/Simpson Hurricane Scale

Category	Wind Speed Range	Storm Surge	Potential Damage
1	74 - 95 mph 119 - 153 km/hr	4 - 5 ft 1 - 2 m	Minimal
2	96 - 110 mph 154 - 177 km/hr	6 - 8 ft 2 - 3 m	Moderate
3	111 - 130 mph 178 - 209 km/hr	9 - 12 ft 3 - 4 m	Extensive
4	131 - 155 mph 210 - 249 km/hr	13 - 18 ft 4 - 5 m	Extreme
5	> 155 mph > 249 km/hr	>18 ft > 5 m	Catastrophic

(Table is on page 511 in the textbook)

Table 16.4
Temperature Thresholds for Damage to Computing Resources

Component or Medium	Sustained Ambient Temperature at which Damage May Begin
Flexible disks, magnetic tapes, etc.	38 ºC (100 ºF)
Optical media	49 ºC (120 ºF)
Hard disk media	66 ºC (150 ºF)
Computer equipment	79 ºC (175 ºF)
Thermoplastic insulation on wires carrying hazardous voltage	125 ºC (257 ºF)
Paper products	177 ºC (350 ºF)

Source: Data taken from National Fire Protection Association.

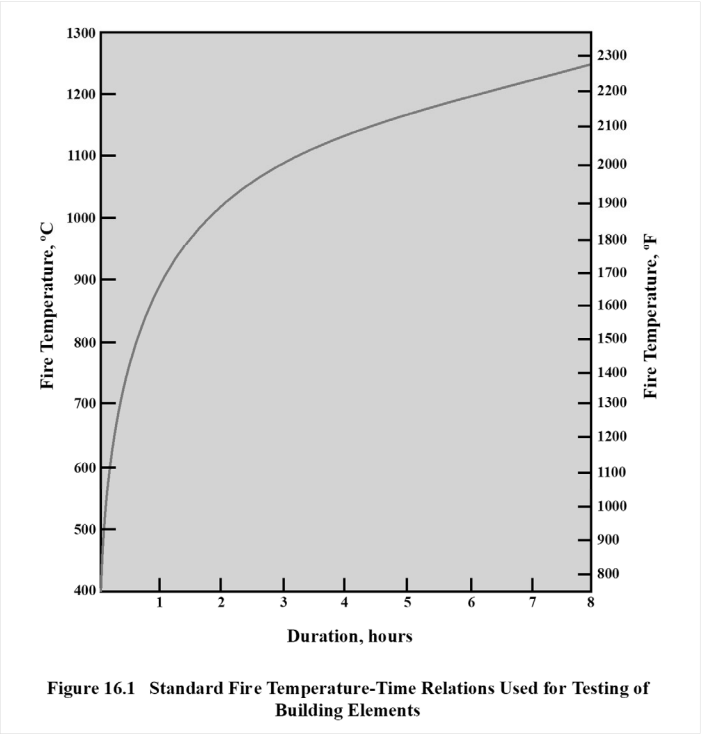


Figure 16.1 Standard Fire Temperature-Time Relations Used for Testing of Building Elements

Temperature	Effect
260 Cº/ 500 ºF	Wood ignites
326 Cº/ 618 ºF	Lead melts
415 Cº/ 770 ºF	Zinc melts
480 Cº/ 896 ºF	An uninsulated steel file tends to buckle and expose its contents

Table 16.5

Temperature Effects

Temperature	Effect
625 Cº/ 1157 ºF	Aluminum melts
1220 Cº/ 2228 ºF	Cast iron melts
1410 Cº/ 2570 ºF	Hard steel melts

Water Damage

Primary danger is an electrical short

A pipe may burst from a fault in the line or from freezing

Sprinkler systems set off accidentally

Floodwater leaving a muddy residue and suspended material in the water

Due diligence should be performed to ensure that water from as far as two floors above will not create a hazard

Chemical, Radiological, and Biological Hazards

- Pose a threat from intentional attack and from accidental discharge
- Discharges can be introduced through the ventilation system or open windows, and in the case of radiation, through perimeter walls
- Flooding can also introduce biological or chemical contaminants

Dust and Infestation

Dust

- Often overlooked
- Rotating storage media and computer fans are the most vulnerable to damage
- Can also block ventilation
- Influxes can result from a number of things:
  - Controlled explosion of a nearby building
  - Windstorm carrying debris
  - Construction or maintenance work in the building

Infestation

- Covers a broad range of living organisms:
  - High-humidity conditions can cause mold and mildew
  - Insects, particularly those that attack wood and paper

Technical Threats

- Electrical power is essential to run equipment
  - Power utility problems:
    - Under-voltage - dips/brownouts/outages, interrupts service
    - Over-voltage - surges/faults/lightening, can destroy chips
    - Noise - on power lines, may interfere with device operation

Electromagnetic interference (EMI)
• Noise along a power supply line, motors, fans, heavy equipment, other computers, cell phones, microwave relay antennas, nearby radio stations • Noise can be transmitted through space as well as through power lines • Can cause intermittent problems with computers

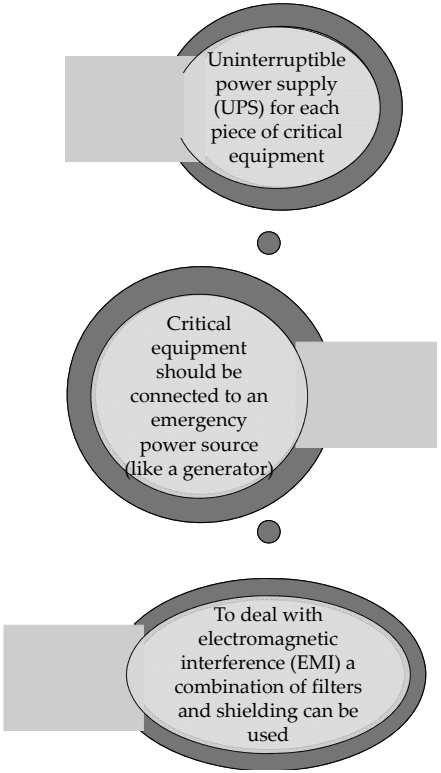
Human-Caused Threats

- Less predictable, designed to overcome prevention measures, harder to deal with
- Include:
  - Unauthorized physical access
    - Information assets are generally located in restricted areas
    - Can lead to other threats such as theft, vandalism or misuse
  - Theft of equipment/data
    - Eavesdropping and wiretapping fall into this category
    - Insider or an outsider who has gained unauthorized access
  - Vandalism of equipment/data
  - Misuse of resources

Physical Security Prevention and Mitigation Measures

- One prevention measure is the use of cloud computing
- Inappropriate temperature and humidity
  - Environmental control equipment, power supply
- Fire and smoke
  - Alarms, preventative measures, fire mitigation
  - Smoke detectors, no smoking
- Water
  - Manage lines, equipment location, cutoff sensors
- Other threats
  - Appropriate technical counter-measures, limit dust entry, pest control

Mitigation Measures



Technical Threats

Mitigation Measures Human-Caused Physical Threats

Physical access control

- **Restrict building access**
- **Controlled areas patrolled or guarded**
- **Locks or screening measures at entry points**
- **Equip movable resources with a tracking device**
- **Power switch controlled by a security device**
- **Intruder sensors and alarms**
- **Surveillance systems that provide recording and real-time remote viewing**

Recovery from Physical Security Breaches

Most essential element of recovery is redundancy

- Provides for recovery from loss of data
- Ideally all important data should be available off-site and updated as often as feasible
- Can use batch encrypted remote backup
- For critical situations a remote hot-site that is ready to take over operation instantly can be created

Physical equipment damage recovery

- Depends on nature of damage and cleanup
- May need disaster recovery specialists

Physical and Logical Security Integration

- Numerous detection and prevention devices
- More effective if there is a central control
- Integrate automated physical and logical security functions
  - Use a single ID card
  - Single-step card enrollment and termination
  - Central ID-management system
  - Unified event monitoring and correlation
- Need standards in this area
  - FIPS 201-1 "*Personal Identity Verification (PIV) of Federal Employees and Contractors*"

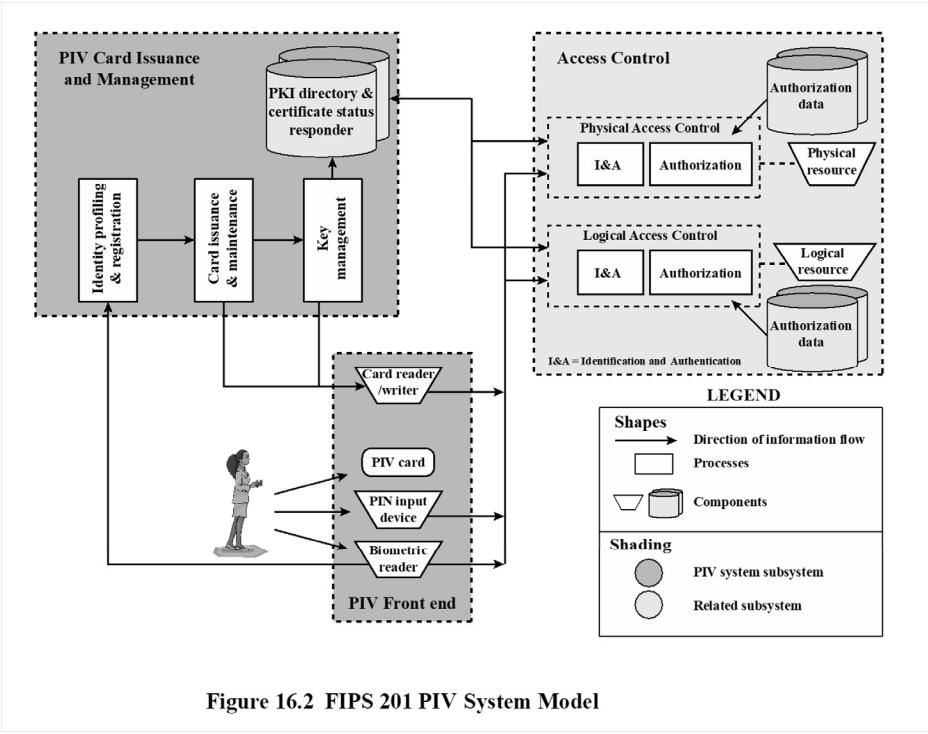


Figure 16.2 FIPS 201 PIV System Model

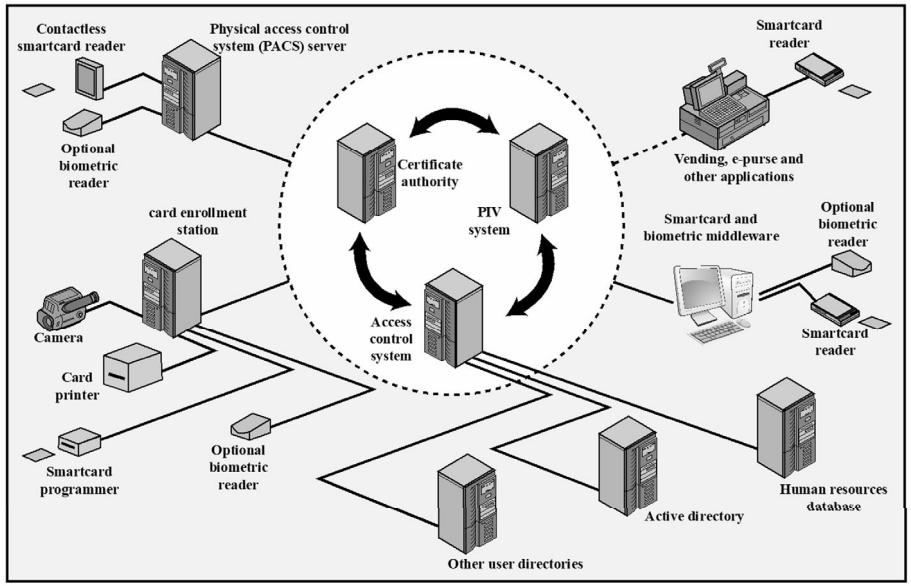
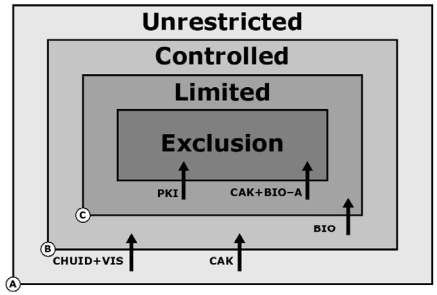


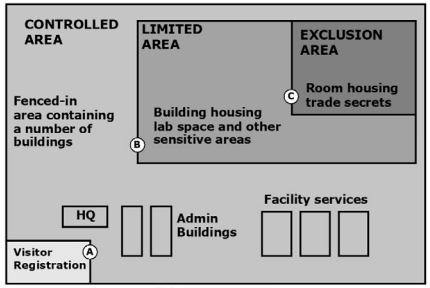
Figure 16.3 Convergence Example

Table 16.6
Degrees of Security and Control for Protected Areas (FM 3-19.30)

Classification	Description
Unrestricted	An area of a facility that has no security interest.
Controlled	That portion of a restricted area usually near or surrounding a limited or exclusion area. Entry to the controlled area is restricted to personnel with a need for access. Movement of authorized personnel within this area is not necessarily controlled since mere entry to the area does not provide access to the security interest. The controlled area is provided for administrative control, for safety, or as a buffer zone for in-depth security for the limited or exclusion area.
Limited	Restricted area within close proximity of a security interest. Uncontrolled movement may permit access to the security interest. Escorts and other internal restrictions may prevent access within limited areas.
Exclusion	A restricted area containing a security interest. Uncontrolled movement permits direct access to the security interest.



(a) Access Control Model



(b) Example Use

Figure 16.4 Use of Authentication Mechanisms for Physical Access Control

Summary

- Overview
- Physical security threats
  - Natural disasters
  - Environmental threats
  - Technical threats
  - Human-caused physical threats
- Recovery from physical security breaches
- Physical security prevention and mitigation measures
  - Environmental threats
  - Technical threats
  - Human-caused physical threats
- Integration of physical and logical security
  - Personal identity verification
  - Use of PIV credentials in physical access control systems