INFO 6027: Fall 2022
Week 13

Physical Security and Internal Investigations

FANSHAWE

Housekeeping

- Final Exam is on **Wednesday December 14th at 10:00 am EST R1019**
- Please reach out to me today to finalize alternate dates – this applies only to part-timers and those students who have reached out prior due to other issues ☺.

Our Agenda for This week…

- Distinguish the three elements of Information systems security:
  - **Logical**, **Physical** and **Premises** security.
- Understanding Internal Investigations
- Final Exam Review Exercises

Physical and Infrastructure Security

Logical security

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

Physical security

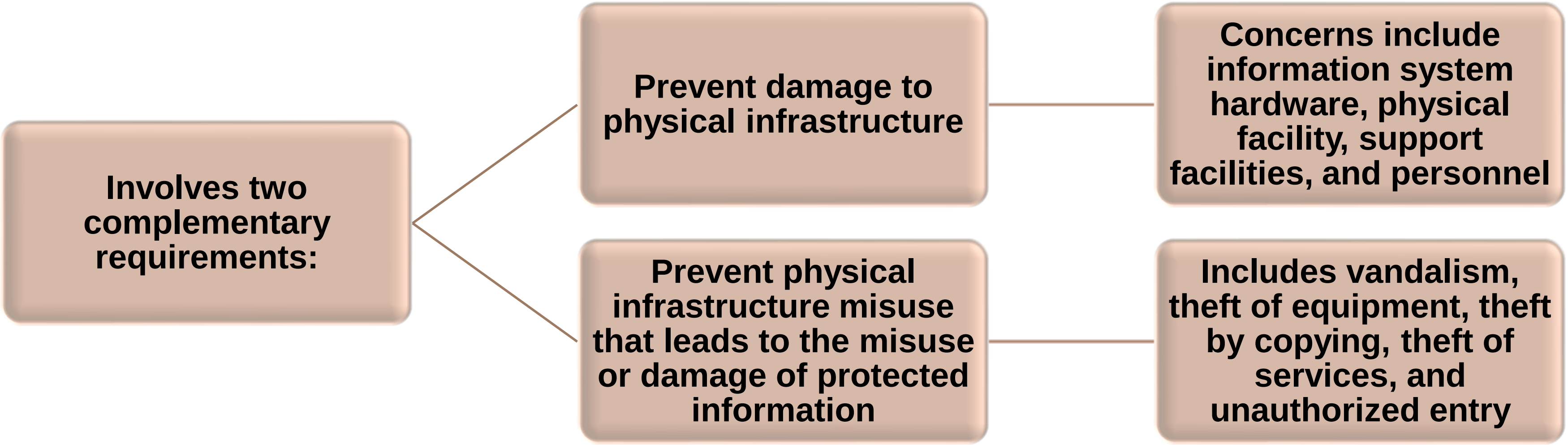
- Also called infrastructure security
- Protects the information systems that contain data and the people who use, operate, and maintain the systems

Premises security

- Also known as corporate or facilities security
- 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



Involves two complementary requirements:
Prevent damage to physical infrastructure
Concerns include information system hardware, physical facility, support facilities, and personnel
Prevent physical infrastructure misuse that leads to the misuse or damage of protected information
Includes vandalism, theft of equipment, theft by copying, theft of services, and unauthorized entry

Physical Security Threats

Physical situations/occurrences that threaten information systems are:

- Environmental threats
- Technical threats
- Human-caused threats

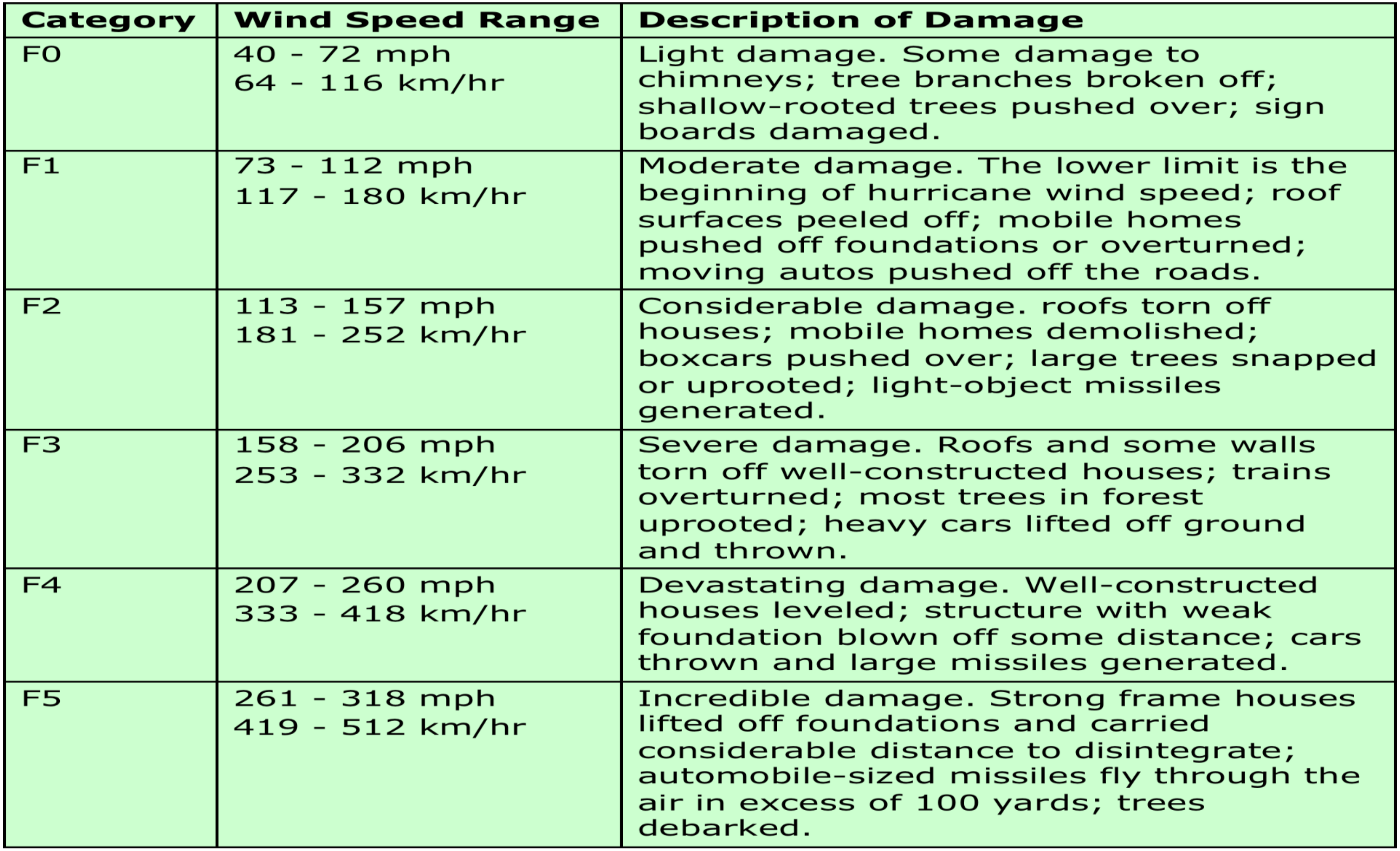
Physical Security Issue #1

Environmental Threats

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

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.

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

Temperature Thresholds for Damage to Computing Resources

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

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

FANSHAWE

Physical Security Issue #2

Technical Threats

FANSHAWE

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

Physical Security Issue #3

Human-Caused Threats

FANSHAWE

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 Issues

Prevention, Mitigation, and Recovery

FANSHAWE

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

- Uninterruptible power supply (UPS) for each piece of critical equipment.
- Critical equipment should be connected to an emergency power source (like a generator).
- To deal with electromagnetic interference (EMI) a combination of filters and shielding can be used

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*”

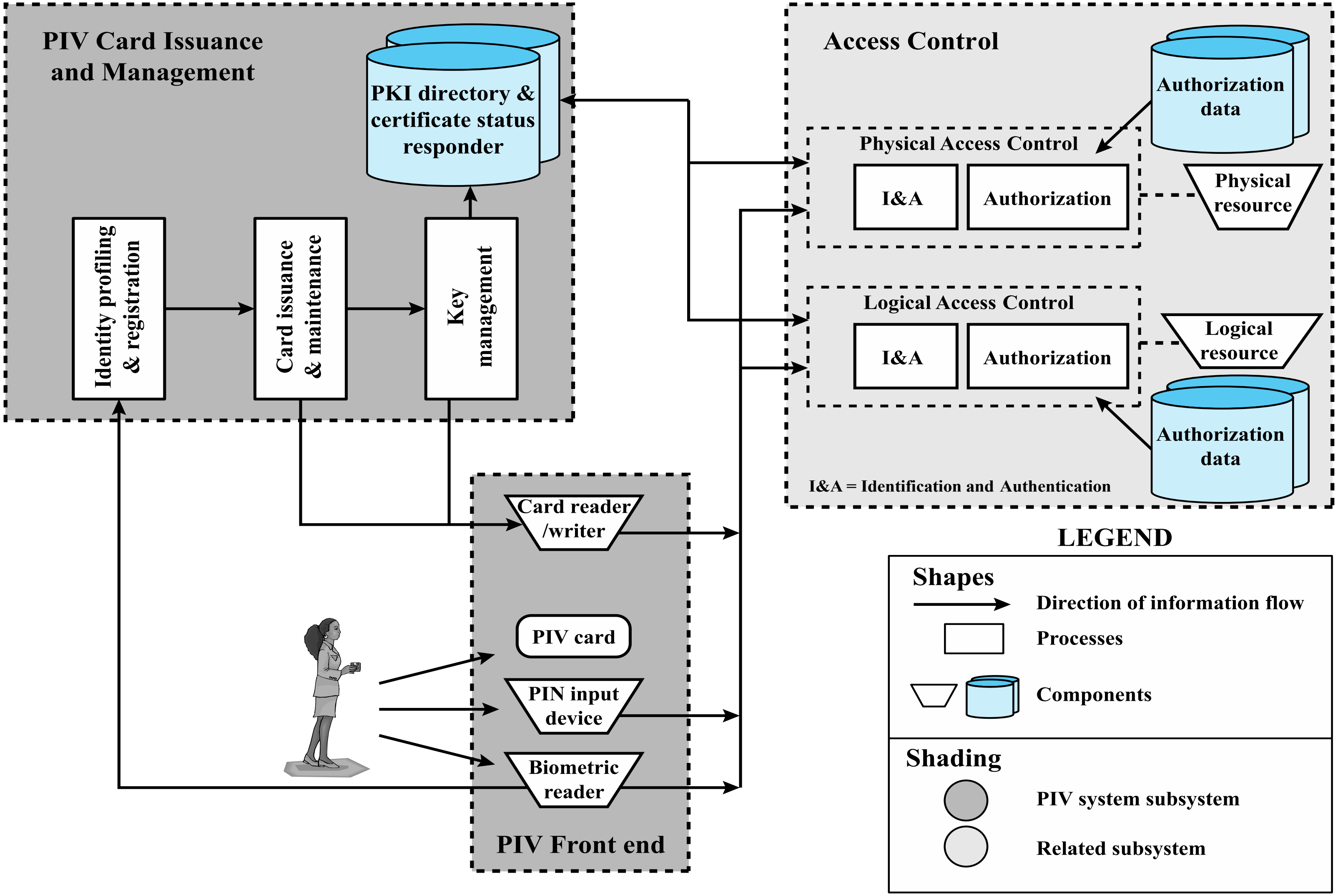


Figure 16.2 FIPS 201 PIV System Model

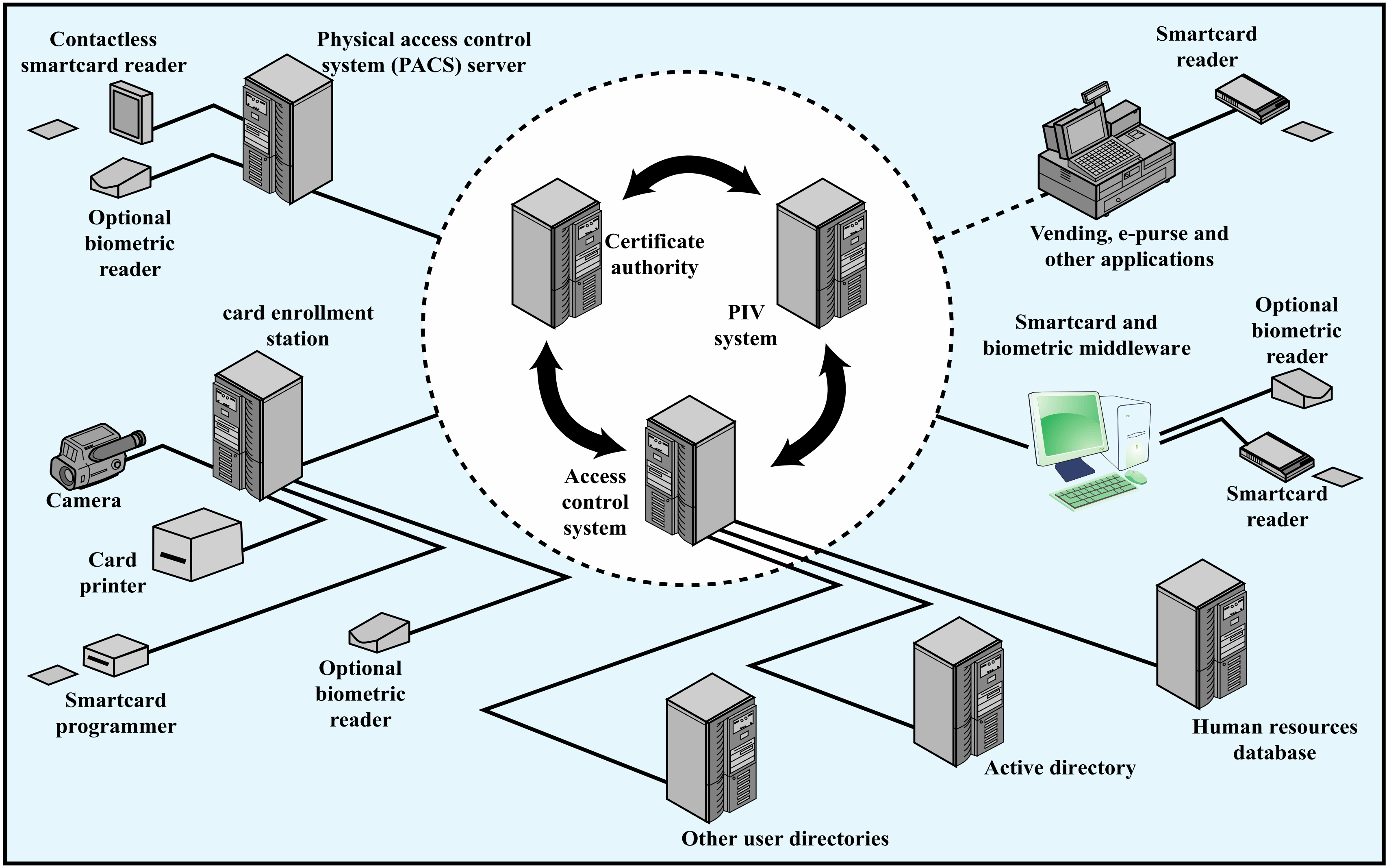

Contactless smartcard reader
Physical access control system (PACS) server
Optional biometric reader
Smartcard reader
Vending, e-purse and other applications
Certificate authority
PIV system
card enrollment station
Smartcard and biometric middleware
Optional biometric reader
Camera
Access control system
Smartcard reader
Card printer
Smartcard programmer
Optional biometric reader
Human resources database
Active directory
Other user directories

Figure 16.3 Convergence Example

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.

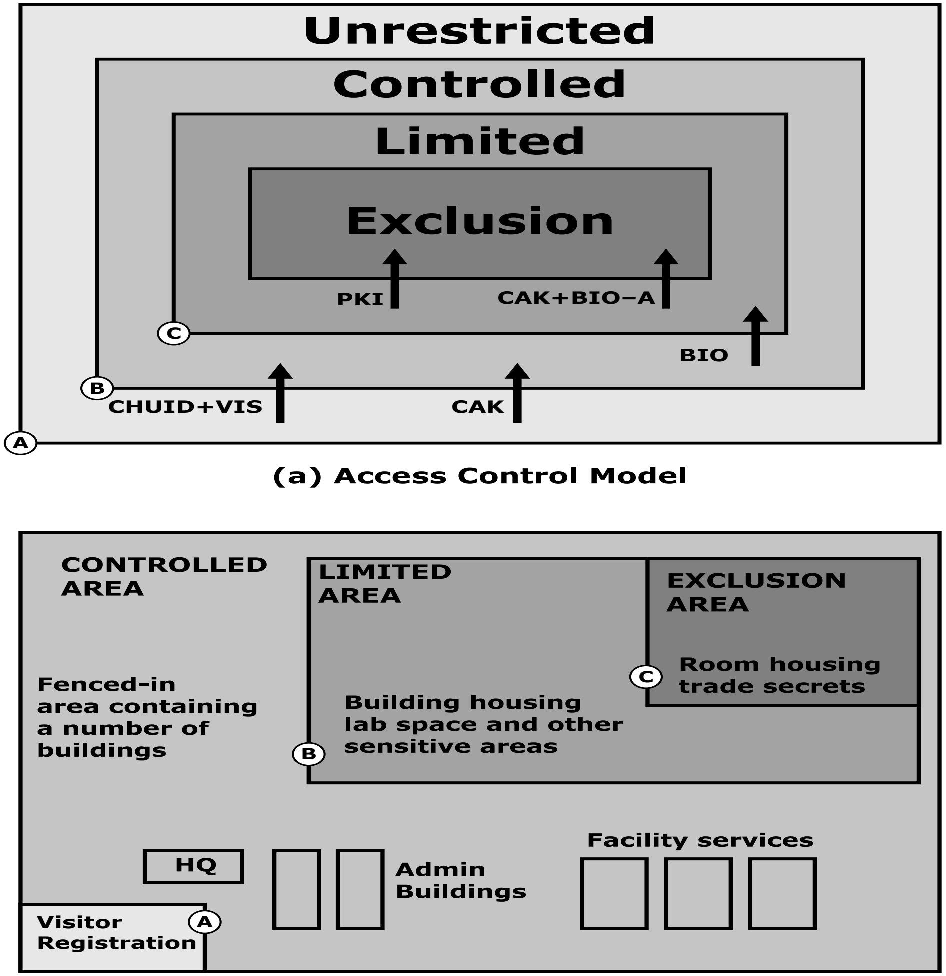


Figure 16.4 Use of Authentication Mechanisms for Physical Access Control

Internal Investigations

FANSHAWE

Managing Investigations in the Organization

- When (not if) an organization finds itself dealing with a suspected policy or law violation
  - **Must appoint an individual to investigate it**
  - How the internal investigation proceeds
    - Dictates whether or not the organization has the ability to take action against the perpetrator if in fact evidence is found that substantiates the charge

- In order to protect the organization, and to possibly assist law enforcement in the conduct of an investigation
  - The investigator (CISO, InfoSec Manager or other appointed individual) must document what happened and how

Managing Investigations in the Organization

- Forensics
  - –The coherent application of methodical investigatory techniques to present evidence of crimes in a court or court-like setting
- Digital forensics
  - –The investigation of what happened and how
  - –Involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis
  - –Like traditional forensics, it follows clear, well-defined methodologies, but still tends to be as much art as science

Managing Investigations in the Organization

- Digital forensics can be used for two key purposes:
  - Investigate allegations of digital malfeasance
    - A crime against or using digital media, computer technology or related components
  - Perform root cause analysis
    - If an incident occurs and the organization suspects an attack was successful, digital forensics can be used to examine the path and methodology used to gain unauthorized access, as well as to determine how pervasive and successful the attack was

Managing Investigations in the Organization

- Digital forensics approaches
  - Protect and forget (a.k.a. patch and proceed)
    - Focuses on the defense of the data and the systems that house, use, and transmit it
  - Apprehend and prosecute (a.k.a. pursue and prosecute)
    - Focuses on the identification and apprehension of responsible individuals, with additional attention on the collection and preservation of potential EM that might support administrative or criminal prosecution

Managing Investigations in the Organization

- Evidentiary material (EM)
  - –Also called item of potential evidentiary value
  - –Any information that could potentially support the organization’s legal-based or policy-based case against a suspect
  - –An item does not become evidence until it is formally admitted to evidence by a judge or other ruling official

Affidavits and Search Warrants

- Investigations begin with an allegation or an indication of an incident
- Forensics team requests permission to examine digital media for potential Evidentiary Material (EM)
- An “affidavit” is a sworn testimony
  - That the investigating officer has certain facts they feel warrant the examination of specific items located at a specific place

Affidavits and Search Warrants

- Search warrant
  - Judicial permission to search for EM at the specified location and/or to seize items to return to the investigator’s lab for examination
  - Created when an approving authority signs the affidavit or creates a synopsis form based on it

Evidentiary Procedures

- Organizations should develop specific procedures and guidance for their use (cont'd.)
  - What methodology should be followed
  - What methods are required for chain of custody or chain of evidence
  - What format the final report should take, and to whom it should it be given

Summary

- **Physical security <u>threats</u>**
  - Natural disasters
  - Environmental threats
  - Technical threats
  - Human-caused physical threats
- **Physical security <u>prevention</u> and <u>mitigation</u> measures**
- **<u>Recovery</u> from physical security breaches**
- **Integration of physical and logical security**
  - Personal identity verification
  - Use of PIV credentials in physical access control systems
- **Managing investigations in the organization**

Review for the Final Exam

FANSHAWE

Tips and Strategies for Tests

- Go through the test at least once. Identify the questions that will require more time to answer.
- Estimate the time you have/need for each question
- Use the clock to help you manage time
- Read each question CAREFULLY and identify *what is being asked*.
- Note how many marks are assigned to each answer and use this as a tool for your answer and for your time management
    - 1 mark = 1 minute (on average)
- When faced with multiple "right" answers, choose the best one.
- Don't dwell on a question you don't know the answer to.

Resources

- Computer Security Principles and Practice. 4th Ed. (Stallings & Brown, 2018)
- Management of information Security. 4th Ed. (Whitman & Mattord, 2012)

Good luck on the Final Test!!!

Thank You