BAIT1093 Introduction to Computer Security

Chapter 3: Physical and Infrastructure Security

Topics

3.1 Three Elements of IS Security
3.2 Physical Security Overview
3.3 Physical Security Threats
3.4 Physical Security Prevention and Mitigation Measures
3.5 Recovery from Physical Security Breaches
3.6 Integration of Physical and Logical Security

3.1 Three Elements of Information System (IS) Security [1]

logical security - protect computer data

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

physical security - protect systems & access

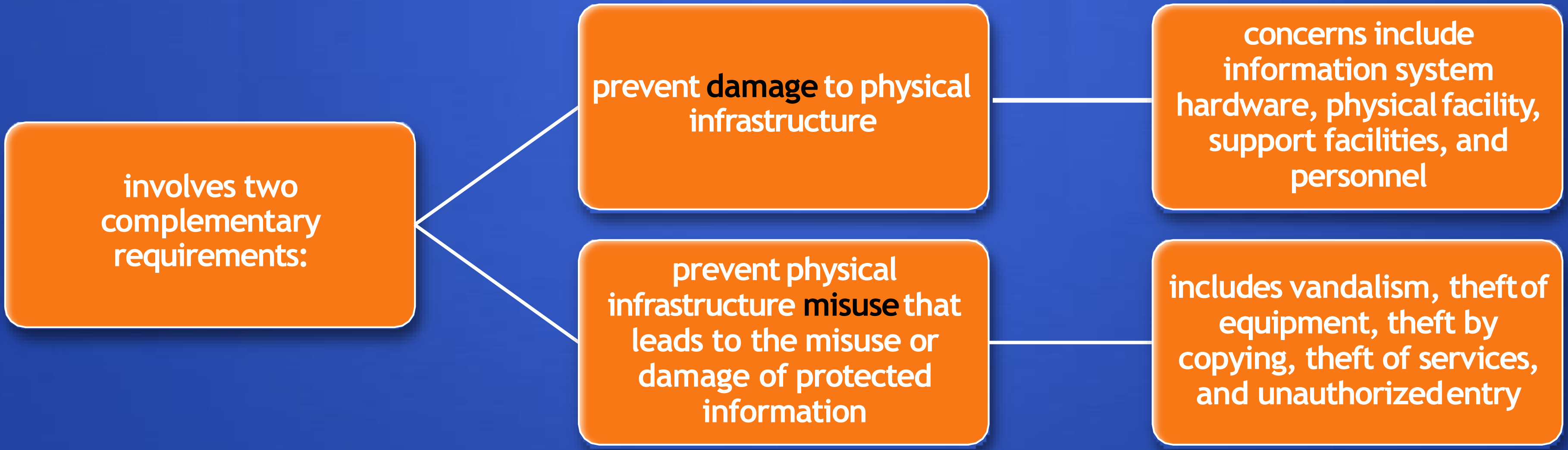
- also called infrastructure security
- protects the information systems that contain data and the people who use, operate, and maintain the systems
- must prevent any type of physical access or intrusion that can compromise logical security

premises security - protect people & property

- 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

3.2 Physical Security Overview [1]

- 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

3.2 Physical Security Overview [1]

- **Information system hardware:** Includes data processing and storage equipment, transmission and networking facilities, and offline storage media. We can include in this category supporting documentation.

- **Physical facility:** The buildings and other structures housing the system andnetwork components.

- **Supporting facilities:** These facilities underpin the operation of the information system. This category includes electrical power, communication services, and environmental controls (heat, humidity, etc.).

- **Personnel:** Humans involved in the control, maintenance, and use of the information systems.

3.3 Physical Security Threats [2]

- A physical security threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.
- No matter how sophisticated the security features of hardware/software deployed, if it is left unattended in an unlocked rooms, it is not secure at all.
- There are cases where servers, routers and switches are located in a janitorial closets where cleaning staff has access to the equipment besides security personnel and network administrators.

Source: https://www.guru99.com/potential-security-threats-to-your-computer-systems.html

3.3 Physical Security Threats

- The following list classifies the physical security threats into three (3) main categories;
  - **Internal**: The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc.
  - **External:** These threats include lightning, floods, earthquakes, etc.
  - **Human**: These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.

Source: https://www.guru99.com/potential-security-threats-to-your-computer-systems.html

3.4 Physical Security Prevention and Mitigation Measures [2]

- The following list shows some of the possible measures that can be taken:
  - **Internal:**
    - Fire threats could be prevented by the use of **automatic fire detectors and extinguishers** that do not use water to put out a fire.
    - Backup tapes should be stored in a **fireproof safe**.
    - The unstable power supply can be prevented by the use of **voltage controllers**.
    - An **air conditioner** can be used to control the humidity in the computer room.

Source: https://www.guru99.com/potential-security-threats-to-your-computer-systems.html

3.4 Physical Security Prevention and Mitigation Measures

- The following list shows some of the possible measures that can be taken:
  - **External:**
    - **Lightning protection systems** can be used to protect computer systems against such attacks. Lightning protection systems are not 100% perfect, but to a certain extent, they reduce the chances of lightning causing damage.
    - Housing computer systems in **high lands** are one of the possible ways of protecting systems against floods.

Source: https://www.guru99.com/potential-security-threats-to-your-computer-systems.html

3.4 Physical Security Prevention and Mitigation Measures [2]

- The following list shows some of the possible measures that can be taken:
  - **Humans**:
    - Servers, routers, switches, hubs, and so forth must be in a locked and secure room with as few people to access the server room as possible.
    - Security policies/procedures related to server rooms, company mobile devices for example, must be in place to:
      - Ensure protection against accidental physical damage by inexperienced personnel or intentional damage
      - Enforce access restrictions to reduce the risk of unauthorized access from intruders
      - Ensure the controls for physical access are current and effective to protect company's assets

Source: https://www.guru99.com/potential-security-threats-to-your-computer-systems.html

3.4 Physical Security Prevention and Mitigation Measures [2]

- The following list shows some of the possible measures that can be taken:
  - **Humans**:
    - Documents and old backup tapes **should be destroyed** before disposal (for example, by melting tapes, magnetizing hard disks, breaking CDs).

Source: https://www.guru99.com/potential-security-threats-to-your-computer-systems.html

3.4 Physical Security Prevention and Mitigation Measures [2]

- Some basic rules company should follow regarding physical security specific for server rooms/data centers:
  - **Server Rooms/Data Centers**
    - Design server rooms that is fully compliant with the leading industry standards. Eg ISO 27001, National Institute of Standards and Technology (NIST) SPs , Department of Defense (DoD) Information Assurance Technical Framework
    - the room should be fire-resistant, have a strong door with a **strong lock** such as a deadbolt.
    - Must have a **good HVAC (**Heating, Ventilation, and Air Conditioning) system.

Source: https://www.bmc.com/blogs/secure-server-room/

-

3.4 Physical Security Prevention and Mitigation Measures [2]

- Some basic rules company should follow regarding physical security specific for server rooms/data centers:
  - **Server Rooms/Data Centers**
    - **Only those personnel** who actually have a need to go in the room should have a **key**. It is better to enforce **multi-layer authentication** (eg passwords, RFID tags and biometrics can be combined)
    - Should have a **server room log** wherein each person logs in when the person enters or exits the room. The logs can also be captured automatically if there is any electronic locks or biometric locks.
-

3.4 Physical Security Prevention and Mitigation Measures [2]

- Some basic rules company should follow regarding physical security specific for server rooms/data centers:
  - **Server Rooms/Data Centers**
    - Data stored in the servers/data centers should be **encrypted**, so that even though the physical security is breached, data will still remain secure.
    - Server systems should be designed **for redundancy**. If one device is no longer operational or is compromised, the stored data should be accessible through alternative and redundant storage devices.

Source: https://www.bmc.com/blogs/secure-server-room/

3.4 Physical Security Prevention and Mitigation Measures [2]

- Some basic rules company should follow regarding physical security specific for server rooms/data centers:
  - **Server Rooms/Data Centers**
    - In event of a security breach or emergency incident, access to **emergency services**—police, healthcare, and firefighting services—**should be automated** and **highly available**. Deploy automated technology systems to inform the appropriate emergency services in event of an incident and engage with private security services to enhance building security.

Source: https://www.bmc.com/blogs/secure-server-room/

3.4 Physical Security Prevention and Mitigation Measures [2]

- Some basic rules company should follow regarding physical security specific for workstations/laptops:
  - **Workstations/Laptops**
    - Every workstation should have an **engraved identifying mark.**
    - Must routinely **inventory them**.
    - Attach the workstations/laptops to the desks with **cables,** which is effective and affordable.

3.5 Recovery from Physical Security Breaches [1]

- most essential element of recovery is **redundancy**
  - provides for recovery from loss of data, although it does not undo any breaches of confidentiality, such as theft of data or documents.
  - ideally all important data should be available off-site and updated as often as possible
  - can use batch encrypted remote backup, since broadband connections now almost universally available.
  - for critical situations a remote hot-site that is ready to take over operation instantly can be created with near-real-time copy of operational data.

3.5 Recovery from Physical Security Breaches [1]

- physical equipment damage recovery
  - depends on nature of damage and nature of the residue. Water, smoke, and fire damage may leave behind hazardous materials that must be meticulously removed from the site before normal operations
  - may need disaster recovery specialists from outside the organization to do the cleanup

3.6 Integration of Physical and Logical Security [1]

- Physical security involves numerous **detection devices**, such as **sensors and alarms,** and numerous **prevention devices**, such as **locks and physical barriers.**

- Physical security is more effective if there is a **central destination** for all alerts and alarms and if there is a **central control** of all automated access control mechanisms (eg smart card entry sites)

- Integrating automated physical security functions as central destination and central control is needed to save cost as well as to be effective.

3.6 Integration of Physical and Logical Security [1]

- In addition, integration also extended to both automated physical and logical security functions, especially in the area of access control.
- Examples of ways to integrate physical and logical access control include the following:
    - Use of a single ID card (eg simple magnetic-strip card or a smart card)for physical and logical access.
    - Single-step user/card enrollment and termination across all identity and access control databases.
    - A central ID-management system instead of multiple disparate user directories and databases.
    - Unified event monitoring and correlation.

3.6 Integration of Physical and Logical Security [1]

- Example of a use case of the integration of physical and logical security, supposedly there is an alert to show Bob access to the company’s wireless network (an event generated by the logical access control system), but he did not enter to the building (an event generated from the physical access control system) → possible hijacking Bob’s wireless account.

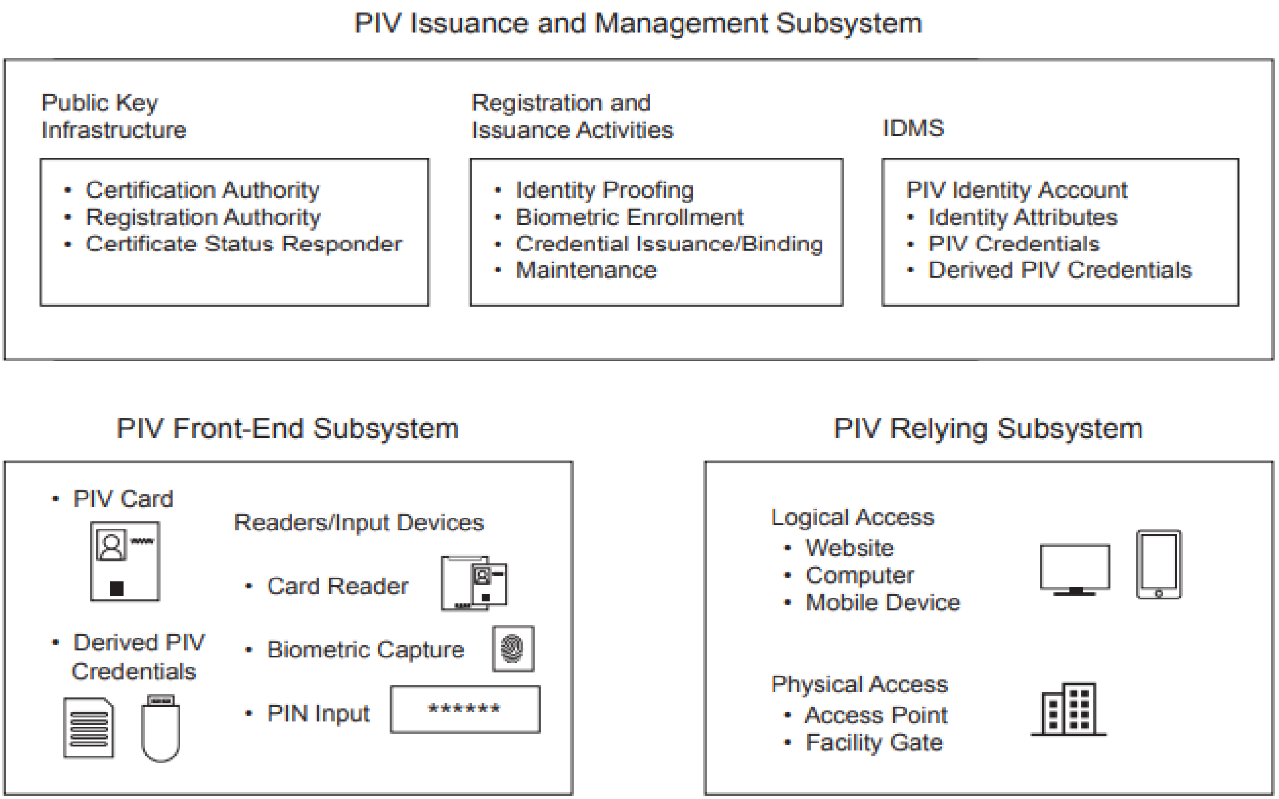
3.6 Integration of Physical and Logical Security [1]

Personal Identity Verification

- need standards for the integration of physical and logical access
- Example of a standard is Federal Information Processing Standards (FIPS) 201-3 [*Personal Identity Verification (PIV) of Federal Employees and Contractors*] issued by NIST in 2022. It is based on secure and reliable forms of identity credentials issued by the Federal Government to its employees and contractors. These credentials are used by mechanisms that authenticate individuals who require access to federally controlled facilities, information systems, and applications.

Source: https://csrc.nist.gov/publications/detail/fips/201/3/final

3.6 Integration of Physical and Logical Security [1]



PIV Issuance and Management Subsystem

Public Key Infrastructure

- Certification Authority
- Registration Authority
- Certificate Status Responder

Registration and Issuance Activities

- Identity Proofing
- Biometric Enrollment
- Credential Issuance/Binding
- Maintenance

IDMS

PIV Identity Account

- Identity Attributes
- PIV Credentials
- Derived PIV Credentials

PIV Front-End Subsystem

- PIV Card
- Derived PIV Credentials

Readers/Input Devices

- Card Reader
- Biometric Capture
- PIN Input

******

PIV Relying Subsystem

Logical Access

- Website
- Computer
- Mobile Device

Physical Access

- Access Point
- Facility Gate

Figure 3-1. PIV System Overview

Source: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf

3.6 Integration of Physical and Logical Security [1]

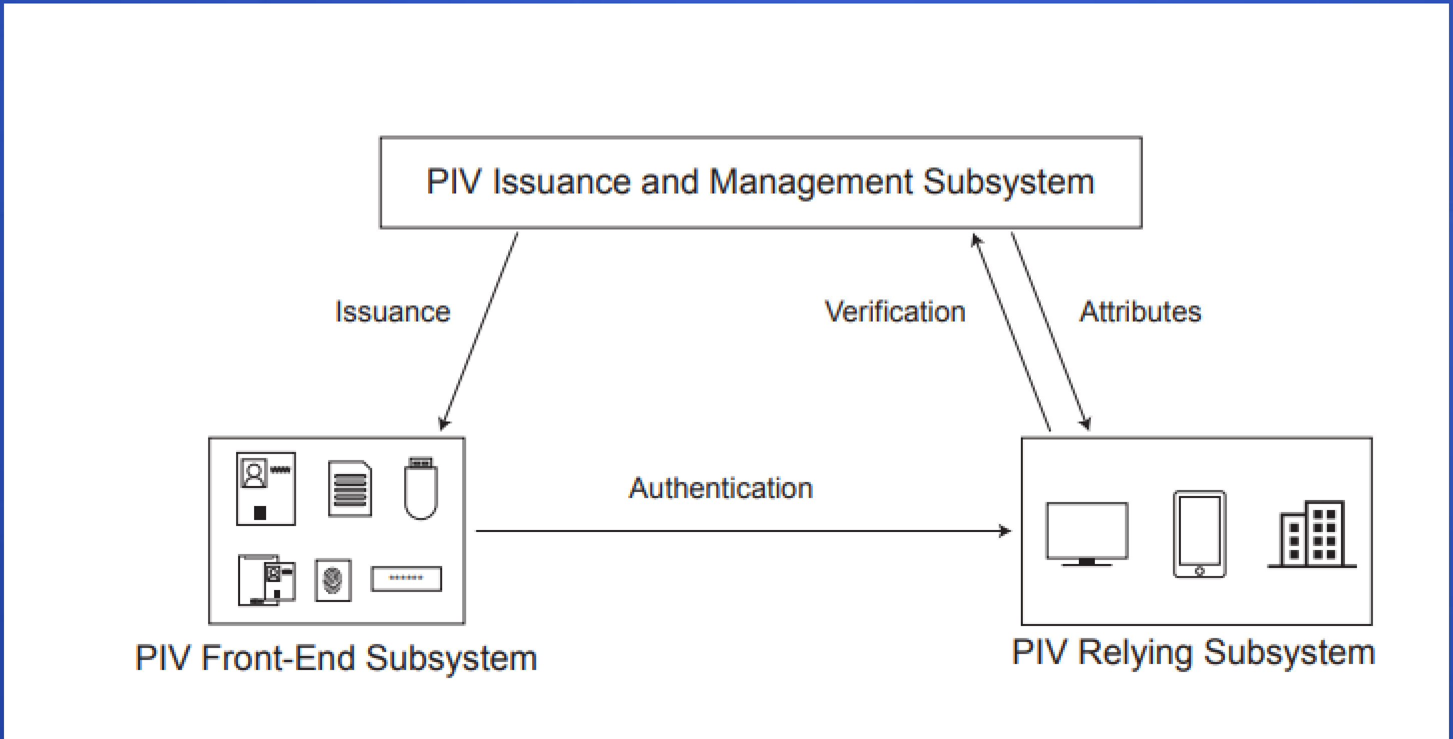
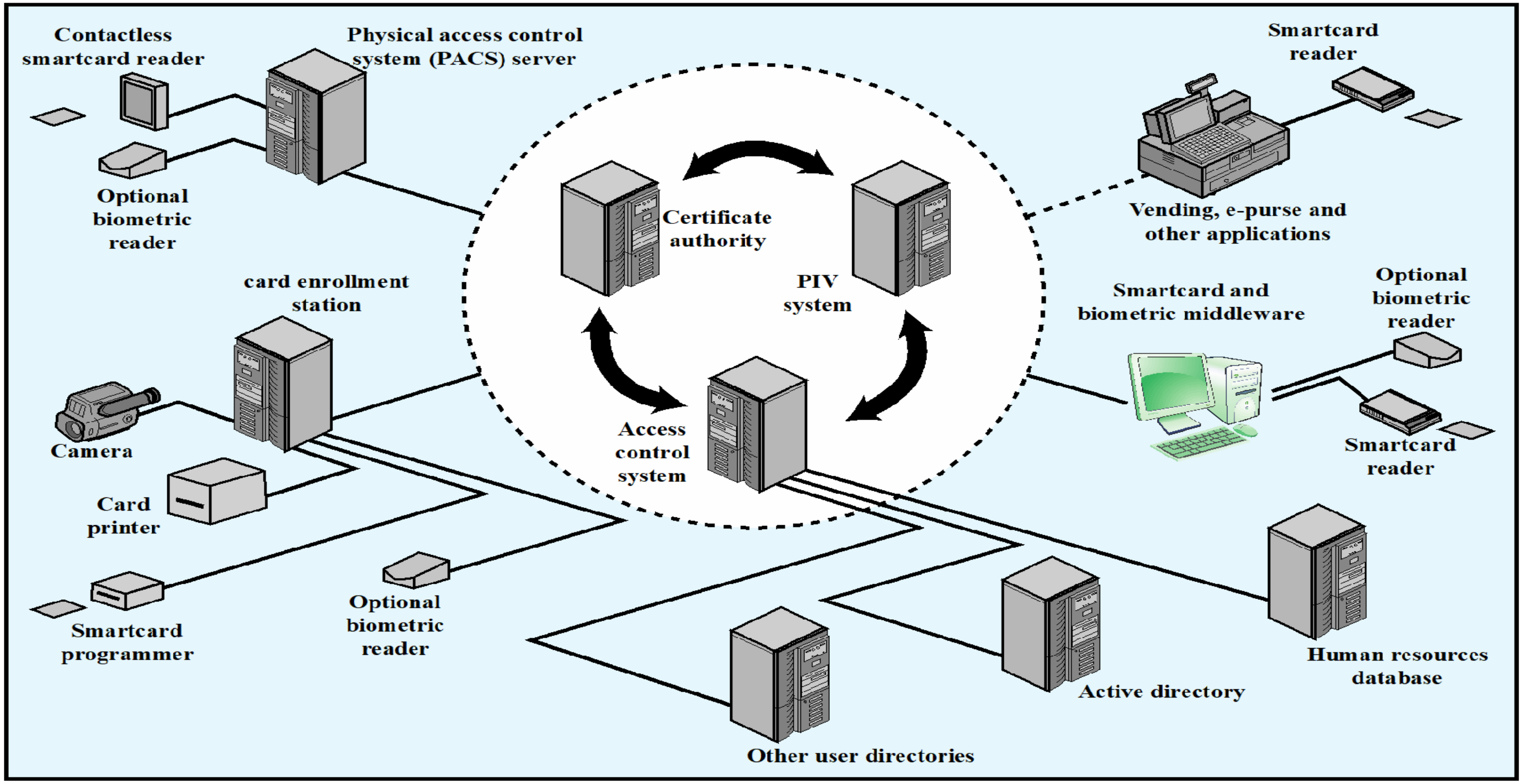


Figure 3-3. PIV System Connections

Source: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf

3.6 Integration of Physical and Logical Security [1]



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

Figure 16.3 Convergence Example

3.6 Integration of Physical and Logical Security [1]

Personal Identity Verification

- Benefits of the integration of physical and logical access control:
  - Employees gain a single, unified access control authentication device; this cuts down on misplaced tokens, reduces training and overhead, and allows seamless access.
  - A single logical location for employee ID management reduces duplicate data
  - entry operations and allows for immediate and real-time authorization revocation of all enterprise resources.
  - Auditing and forensic groups have a central repository for access control investigations.

3.6 Integration of Physical and Logical Security [1]

Personal Identity Verification

- Benefits of the integration of physical and logical access control:
  - Hardware unification can reduce the number of vendor purchase-and-support contracts.
  - Certificate-based access control systems can leverage user ID certificates for other security applications, such as document e-signing and data encryption.

3.6 Integration of Physical and Logical Security [1]

Use of PIV in Physical Access Control Systems

- NIST issued SP 800-116 Rev. 1 (2018) which is a recommendation that provides a technical guideline to use Personal Identity Verification (PIV) Cards in facility access or Physical Access Control Systems (PACS); enabling federal agencies to operate as government-wide interoperable enterprises. These guidelines cover the risk-based strategy to select appropriate PIV authentication mechanisms as expressed within Federal Information Processing Standard (FIPS) 201.

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-116r1.pdf

3.6 Integration of Physical and Logical Security [1]

Use of PIV in Physical Access Control Systems

- SP 800-116 makes use of the following authentication mechanisms:
  - **Visual (VIS)**: Visual identity verification of a PIV card is done by a human guard. The human guard checks to see that the PIV card looks genuine, compares the cardholder's facial features with the picture on the card, checks the expiration date printed on the card, verifies the correctness of other data elements printed on the card, and visually verifies the security feature(s) on the card.

3.6 Integration of Physical and Logical Security [1]

Use of PIV in Physical Access Control Systems

- SP 800-116 makes use of the following authentication mechanisms:
  - **Cardholder unique identifier (CHUID)**: The CHUID is a PIV card data object. Authentication is implemented by transmission of the CHUID from the PIV card to PACS.
  - **Biometric (BIO)**: Authentication is implemented by using a fingerprint or iris data object sent from the PIV card to the PACS.

3.6 Integration of Physical and Logical Security [1]

Use of PIV in Physical Access Control Systems

- SP 800-116 makes use of the following authentication mechanisms:
  - **Attended biometric (BIO-A):** This authentication mechanism is the same as BIO authentication but an attendant supervises the use of the PIV card and the submission of the PIN and the sample biometric by the cardholder.
  - **PIV authentication key (PKI):** PACS may be designed to perform public key cryptography-based authentication using the PIV authentication key. Use of the PKI provides two-factor authentication, since the cardholder must enter a PIN to unlock the card in order to successfully authenticate

3.6 Integration of Physical and Logical Security [1]

Use of PIV in Physical Access Control Systems

- SP 800-116 makes use of the following authentication mechanisms:
  - **Card authentication key (CAK):** The CAK is an optional key that may be present on any PIV card. The purpose of the CAK authentication mechanism is to authenticate the card and therefore its possessor. The CAK is unique among the PIV keys in several respects: The CAK may be used on the contactless or contact interface in a challenge/response protocol; and the use of the CAK does not require PIN entry.

3.6 Integration of Physical and Logical Security [1]

Use of PIV in Physical Access Control Systems

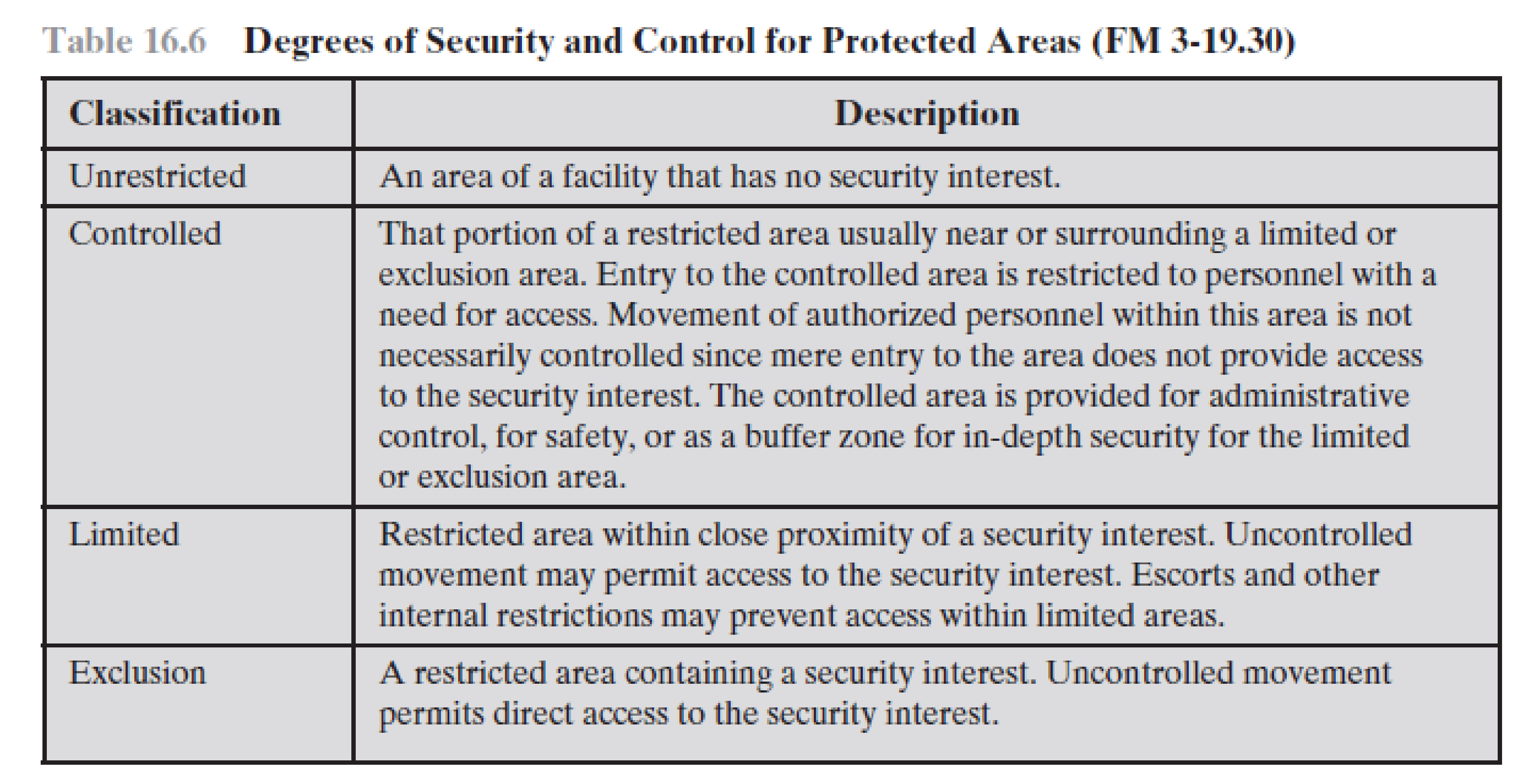


Table 16.6 **Degrees of Security and Control for Protected Areas (FM 3-19.30)**

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.

3.6 Integration of Physical and Logical Security [1]

Use of PIV in Physical Access Control Systems

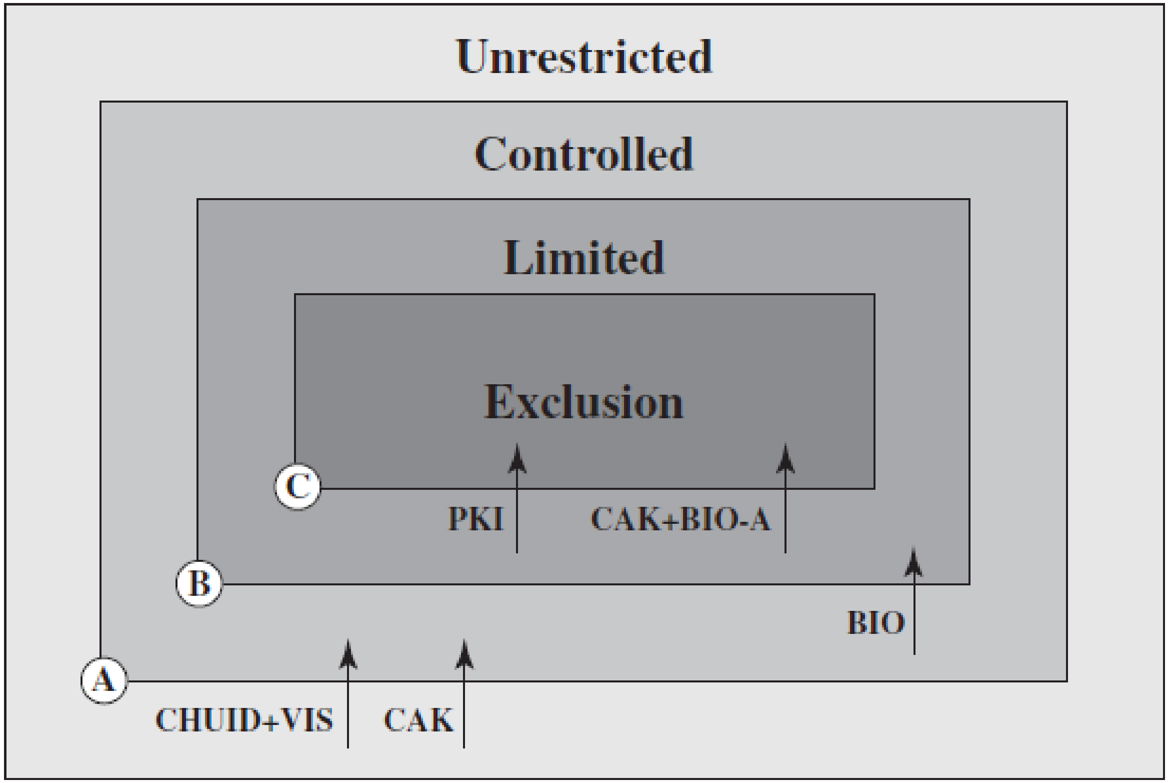
Examples:

- Unrestricted Area: outside the fence or walls of the facility
- Controlled Area: inside the fence or front door
- Limited Area: past a security checkpoint for employees in a facility
- Exclusion Area: secure areas granted to individuals for specific needs

Source: https://www.nist.gov/news-events/news/2008/04/new-nist-publication-recommends-best-fits-between-federal-locks-and-keys

3.6 Integration of Physical and Logical Security [1]

Use of PIV in Physical Access Control Systems



(a) Access control model

3.6 Integration of Physical and Logical Security [1]

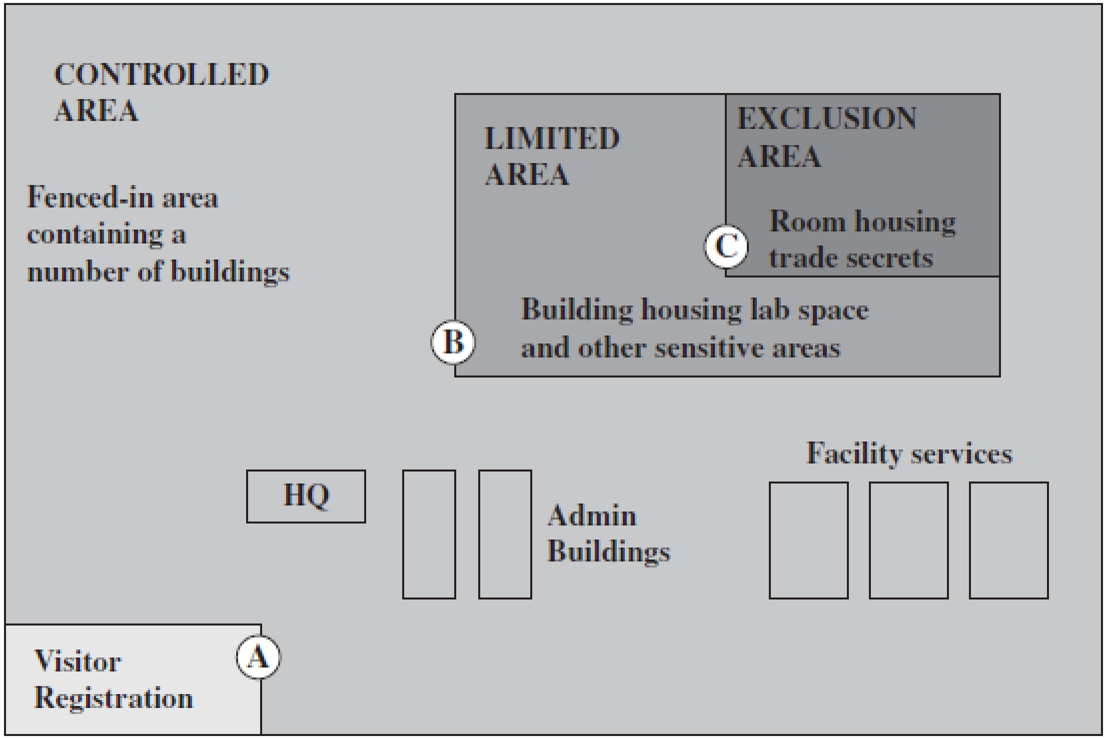
Use of PIV in Physical Access Control Systems

- The model indicates alternative authentication mechanisms that may be used for access to specific areas.

- The model is designed such that at least one authentication factor is required to enter a controlled area, two authentication factors for a limited area, and three authentication factors for an exclusion area.

3.6 Integration of Physical and Logical Security [1]

Use of PIV in Physical Access Control Systems


CONTROLLED AREA
Fenced-in area containing a number of buildings
LIMITED AREA
EXCLUSION AREA
Room housing trade secrets
C
Building housing lab space and other sensitive areas
B
Facility services
HQ
Admin Buildings
Visitor Registration
A

(b) Example use

Figure 16.4 Use of Authentication Mechanisms for Physical Access Control

3.6 Integration of Physical and Logical Security [1]

Use of PIV in Physical Access Control Systems

- The nested arrangement may not be suitable for all facilities. In some facilities, direct access from outside to a limited area or an
- exclusion area may be necessary. In that case, all of the required authentication factors must be employed at the access point. Thus a direct access point to an exclusion area may employ, in combination, CHUID+VIS, BIO or BIO-A, and PKI.

Additional Source: https://www.govinfo.gov/content/pkg/GOVPUB-C13-23b75a7cb52b8bf3d6f439c091ba83a4/pdf/GOVPUB-C13-23b75a7cb52b8bf3d6f439c091ba83a4.pdf

Main References

[1] William Stallings and Lawrie Brown. 2018. Computer Security: Principles and Practice. Pearson.

[2] Easttom, Chuck. 2020. Computer Security Fundamentals. 4th ed. Pearson