Physical and Infrastructure Security

"*Computer Security: Principles and Practice*" 4th ed.
W. Stallings and L. Brown

Francesco Mucci

Corso di Laurea Magistrale in Informatica

SECURITY ENGINEERING

2018-2019

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Overview

1. Physical Security Overview

2. Physical Security Threats & Prevention and Mitigation Measures
   - Natural Disasters
   - Environmental Threats
   - Technical Threats
   - Human-Caused Physical Threats

3. Recovery from Physical Security Breaches

4. Integration of Physical and Logical Security
   - FIPS 201-2: Personal Identity Verification
   - NIST SP 800-116: Use of PIV Credentials in PACS

Elements of Information System Security

Logical Security:

- **protects computer-based data**;
- from SW-based and communication-based threats.

Physical Security (Infrastructure Security):

- **protects information systems and the people who use/operate/maintain them**;
- prevent any type of physical access or intrusion that can compromise logical security.

Elements of Information System Security

Premises Security (Corporate or Facilities Security):

- **protects people/property within an area/facility/building(s)**;
- usually required by laws/regulations;
- provides perimeter security, access control, smoke/fire detection, fire suppression, some environmental protection, and usually surveillance systems, alarms, and guards.

We deal with physical security and with some overlapping areas of premises security.

Physical Security Role

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

Requirement 1

Prevent damage to the physical infrastructure that sustains the Information System.

- IS hardware: data processing/storage equipment, transmission/networking facilities, offline storage media, supporting documentation.
- Physical facility: buildings/structures housing the system and network components.
- Supporting facilities: electrical power, communication services, environmental controls (heat, humidity, etc.).
- Personnel: humans that control/maintain/use the ISs.

Physical Security Role

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

Requirement 2

Prevent misuse (accidental or malicious) **of the physical infrastructure** that leads to the misuse or damage of the protected information.

- Vandalism.
- Theft (of equipment, by copying, of services).
- Unauthorized entry.

Overview

1. Physical Security Overview
2. Physical Security Threats & Prevention and Mitigation Measures
   - Natural Disasters
   - Environmental Threats
   - Technical Threats
   - Human-Caused Physical Threats
3. Recovery from Physical Security Breaches
4. Integration of Physical and Logical Security
   - FIPS 201-2: Personal Identity Verification
   - NIST SP 800-116: Use of PIV Credentials in PACS

Physical Security Threats

- Enviromental threats: conditions in the environment that can damage or interrupt the service of information systems and the data they contain.
- Technical threats: threats related to electrical power and electromagnetic emission.
- Human-caused threats: unauthorized physical access, theft, vandalism, misuse.

Physical Security Prevention and Mitigation Measures

Standard that include lists of related controls:

- **ISO 27002** *Code of practice for information securit management*, 2013
- **NIST SP 800-53** *Recommended Security Controls for Federal Information Systems*, 2015

Cloud Computing as a General Preventive Measures

- Reduced need for information system assets on site.
- Portion of data assets are not subject to on-site physical threats.

Overview

1 Physical Security Overview

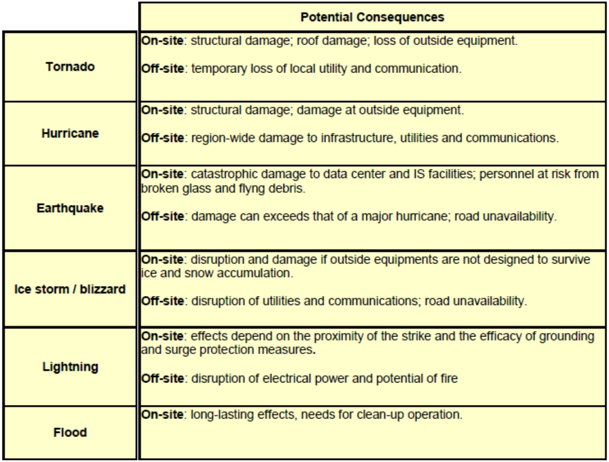
2 Physical Security Threats & Prevention and Mitigation Measures
- Natural Disasters
- Environmental Threats
- Technical Threats
- Human-Caused Physical Threats

3 Recovery from Physical Security Breaches

4 Integration of Physical and Logical Security
- FIPS 201-2: Personal Identity Verification
- NIST SP 800-116: Use of PIV Credentials in PACS

Characteristic of Natural Disasters

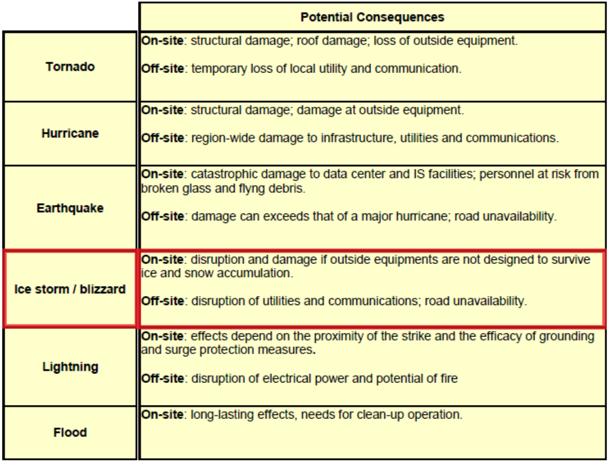
Prime, but not the only, **source of environmental threats.**
Assess the risk and take suitable precautions to prevent catastrophic loss.



	Potential Consequences
Tornado	**On-site**: structural damage; roof damage; loss of outside equipment. **Off-site**: temporary loss of local utility and communication.
Hurricane	**On-site**: structural damage; damage at outside equipment. **Off-site**: region-wide damage to infrastructure, utilities and communications.
Earthquake	**On-site**: catastrophic damage to data center and IS facilities; personnel at risk from broken glass and flyng debris. **Off-site**: damage can exceeds that of a major hurricane; road unavailability.
Ice storm / blizzard	**On-site**: disruption and damage if outside equipments are not designed to survive ice and snow accumulation. **Off-site**: disruption of utilities and communications; road unavailability.
Lightning	**On-site**: effects depend on the proximity of the strike and the efficacy of grounding and surge protection measures. **Off-site**: disruption of electrical power and potential of fire
Flood	**On-site**: long-lasting effects, needs for clean-up operation.

Characteristic of Natural Disasters

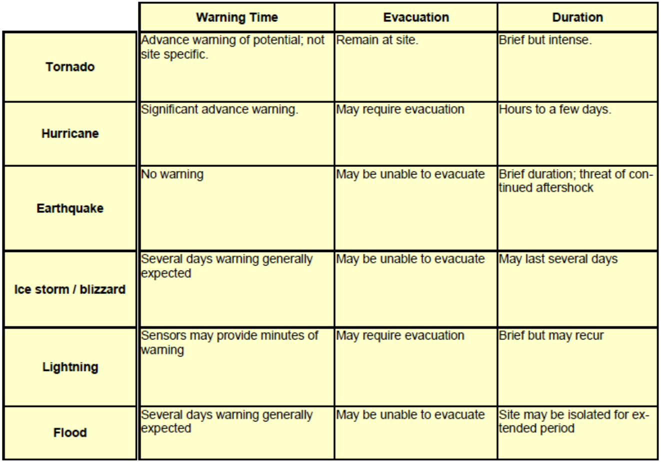
Prime, but not the only, **source of environmental threats**.
Assess the risk and take suitable precautions to prevent catastrophic loss.



	Potential Consequences
Tornado	**On-site**: structural damage; roof damage; loss of outside equipment. **Off-site**: temporary loss of local utility and communication.
Hurricane	**On-site**: structural damage; damage at outside equipment. **Off-site**: region-wide damage to infrastructure, utilities and communications.
Earthquake	**On-site**: catastrophic damage to data center and IS facilities; personnel at risk from broken glass and flyng debris. **Off-site**: damage can exceeds that of a major hurricane; road unavailability.
Ice storm / blizzard	**On-site**: disruption and damage if outside equipments are not designed to survive ice and snow accumulation. **Off-site**: disruption of utilities and communications; road unavailability.
Lightning	**On-site**: effects depend on the proximity of the strike and the efficacy of grounding and surge protection measures. **Off-site**: disruption of electrical power and potential of fire
Flood	**On-site**: long-lasting effects, needs for clean-up operation.

Characteristic of Natural Disasters

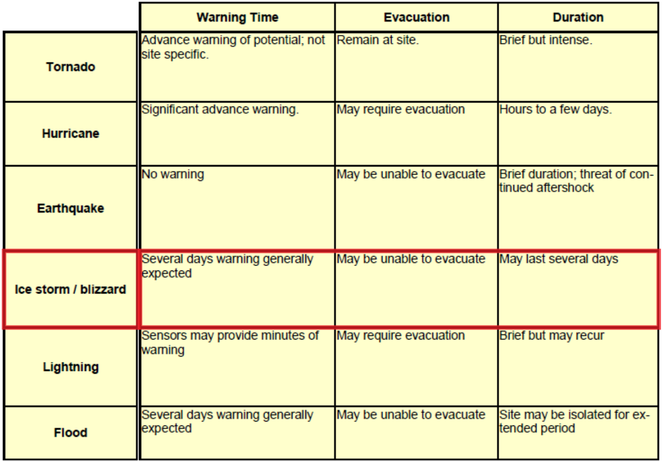
Prime, but not the only, **source of environmental threats**.
Assess the risk and take suitable precautions to prevent catastrophic loss.



	Warning Time	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 aftershock
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

Characteristic of Natural Disasters

Prime, but not the only, **source of environmental threats**.
Assess the risk and take suitable precautions to prevent catastrophic loss.



	Warning Time	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 aftershock
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

Overview

1 Physical Security Overview

2 Physical Security Threats & Prevention and Mitigation Measures
- Natural Disasters
- Environmental Threats
- Technical Threats
- Human-Caused Physical Threats

3 Recovery from Physical Security Breaches

4 Integration of Physical and Logical Security
- FIPS 201-2: Personal Identity Verification
- NIST SP 800-116: Use of PIV Credentials in PACS

Environmental Threats: Humidity and Temperature

Humidity should be maintained **between 40% and 60%**.

High Humidity

Threat to electrical and electronic equipment:

- corrosion (if long-term exposure);
- condensation ⇒ short circuit;
- electroplating (metal from one connector slowly migrates to the mating connector, bonding the two together).

Low Humidity

- some materials may change shape (if long-term exposure);
- static electricity ⇒ an electric discharge can damage electronic equipment.

Environmental Threats: Humidity and Temperature

Computer systems should be kept **between** **10°C** **and** **32°C**.

- Outside of this range continue to operate, but undesiderable results.
- If cannot adequately cool itself ⇒ internal components damaged.
- If thermal shock, due to cold, on start-up ⇒ integrated circuit crack.

Temperature dissipation and cooling mechanisms of computer can be affected by:

- excessive ambient temperature; interruption of supply of power; interruption of HVAC (heating, ventilation, and air-conditioning) services; vent blockage.

Prevention and Mitigation Measures

Environmental-control equipment, maintenance of a power supply.

Environmental Threats: Fire and Smoke

Fire is a **threat to human life and property**:

- direct flame, heat, release of toxic fumes, water damage from fire suppression, smoke damage.

Smoke Damage

- Smoke is an abrasive.
- It collects on the heads of unsealed magnetic/optical disks.
- Electrical fires can produce an acrid smoke that may damage other equipment and may be poisonous or carcinogenic.

Prevention and Mitigation Measures

Fire/smoke detectors, alarms, emergency procedures, hand-operated/automatic fire extinguishers, power-off switch, records stored in fireproof cabinets, smoking should not be permitted.

Environmental Threats: Water Damage

Primary danger is an **electrical short**.

Possible Causes

- a pipe may burst from a fault in the line or from freezing;
- sprinkler systems may be set off by a faulty temperature sensor;
- overflowing toilet and similar hazards;
- floodwater.

Floodwater leaves a **muddy residue** that is extraordinarily **difficult to clean up**.

Prevention and Mitigation Measures

Locate equipment sensibly (knowing water supply lines layout), water sensors to cut off power automatically in the event of a flood, manage water supply lines.

Environmental Threats: Chemical, Radiological, and Biological Hazards

Primary **risk** of these hazards is **to personnel**. Radiation and chemical agents can cause **damage to electronic equipment**.

How these hazardous agents can be present in an IS environment?

- Accidental or intentional intrusion (attack).
- Nearby 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.

Prevention and Mitigation Measures

Specific technical approaches: infrastructure design, sensor design and placement, mitigation procedures, personnel training.

Environmental Threats: Dust

Equipment with moving parts (e.g. rotating storage media, computer fans) are the **most vulnerable** to damage from dust. Dust can also **block ventilation**.

Dust can result from:

- controlled explosion of a nearby building;
- windstorm carrying debris from a wildfire;
- within the building due to construction or maintenance work.

Prevention and Mitigation Measures

Proper filter maintenance and regular IS room maintenance.

Environmental Threats: Infestation

- **Mold** can be harmful to both personnel and equipment: high-humidity conditions can lead to the growth of it.
- **Insects** are a common threat, particularly those that attack wood and paper.
- **Rodents** can chew wires.

Prevention and Mitigation Measures

Regular pest control, maintain a clean enviroment.

Overview

1. Physical Security Overview
2. Physical Security Threats & Prevention and Mitigation Measures
   - Natural Disasters
   - Environmental Threats
   - Technical Threats
   - Human-Caused Physical Threats
3. Recovery from Physical Security Breaches
4. Integration of Physical and Logical Security
   - FIPS 201-2: Personal Identity Verification
   - NIST SP 800-116: Use of PIV Credentials in PACS

Technical Threats: Electrical Power

Electrical power (sometimes uninterrupted) is essential.

Undervoltage ⇒ Service Interruption

- Categories: temporary dips, prolonged undervoltage, power outages.
- Consequences: systems shutdown (if prolonged undervoltage more than 20% or blackouts lasting more than few *ms*).

Overvoltage ⇒ Components Destruction

- Caused by: utility supply anomaly, internal wiring fault, lightning.
- Consequences: can destroy silicon-based components.

Noise along power supply line ⇒ Logical Errors

- Caused by: spurious signals passing the filtering circuitry.
- Consequences: interference with signals inside electronic devices.

Technical Threats: Electromagnitic Interference (EMI)

Electrical noise that can cause **intermittent problems with computers**. Can be transmitted through space as well as through nearby power lines.

Sources of EMI

- noise along a power supply line;
- motors, fans, heavy equipment, other computer;
- high-intensity emissions from nearby radio stations and microwave relay antennas;
- low-intensity emissions from cell phones.

Technical Threats: Prevention and Mitigation Measures

To deal with:

- Brief Power Interruptions: uninterruptible power supply (a battery backup unit) for critical equipment.
- Prolonged Undervoltage and Blackouts: critical equipment connected to an emergency power source (generator).
- Electromagnatic Interference: combination of filters and shielding.

Overview

1 Physical Security Overview

2 Physical Security Threats & Prevention and Mitigation Measures
- Natural Disasters
- Environmental Threats
- Technical Threats
- Human-Caused Physical Threats

3 Recovery from Physical Security Breaches

4 Integration of Physical and Logical Security
- FIPS 201-2: Personal Identity Verification
- NIST SP 800-116: Use of PIV Credentials in PACS

Human-Caused Physical Threats

- Unauthorized physical access
  - Information assets (servers, mainframe computers, network equipment, and storage networks) are generally located in restricted areas.
  - Can lead to other threats, such as theft, vandalism, or misuse.
- Theft
  - of equipment and/or data by copying/eavesdropping/wiretapping;
  - by outsider who has gained unauthorized access or by an insider.
- Vandalism of equipment/data
- Misuse of resources (by authorized or unauthorized)

More difficult to deal with.

- Less predictable.
- Specifically designed to overcome prevention measures.
- Seek the most vulnerable point of attack.

Human-Caused Physical Threats: Prevention and Mitigation Measures

General approach: **Physical Access Control**.

Methods to restrict equipment access

1. Isolate the equipments:
   - restrict access to the building that house the resource;
   - put the resource in a locked cabinet/safe/room.
2. Secure accessible machine to an object difficult to move.
3. Power switch controlled by security device.
4. Movable/portable resorces/objects equipped with tracking device.

Human-Caused Physical Threats: Prevention and Mitigation Measures

General approach: **Physical Access Control**.

Techniques used for physical access control

- controlled areas patrolled/guarded, barriers that isolate each area, entry points in the barrier, and locks or screening measures at each entry point;
- sensors and alarms to detect intruders and unauthorized access/movement of equipment;
- video surveillance systems.

Overview

1. Physical Security Overview

2. Physical Security Threats & Prevention and Mitigation Measures
   - Natural Disasters
   - Environmental Threats
   - Technical Threats
   - Human-Caused Physical Threats

3. Recovery from Physical Security Breaches

4. Integration of Physical and Logical Security
   - FIPS 201-2: Personal Identity Verification
   - NIST SP 800-116: Use of PIV Credentials in PACS

Recovery from Physical Security Breaches

Redundancy to **recovery from loss of data**:

- ideally, important data (real time updated) available off site;
- batch encrypted backups over private networks or the Internet;
- in critical situations, a hot site can be created off site that is ready to take over operation instantly.

Recovery from physical damage to the equipment or the site depends on the nature of the damage and the residue: may requires disaster recovery specialists to do the clean up.

Overview

1 Physical Security Overview

2 Physical Security Threats & Prevention and Mitigation Measures
- Natural Disasters
- Environmental Threats
- Technical Threats
- Human-Caused Physical Threats

3 Recovery from Physical Security Breaches

4 **Integration of Physical and Logical Security**
- FIPS 201-2: Personal Identity Verification
- NIST SP 800-116: Use of PIV Credentials in PACS

Integration of Physical and Logical Security

Automated physical security functions:

- detection devices (sensors/alarms);
- prevention devices (lock/barriers);

Integrating automated physical security functions:

- central destination for alerts/alarms;
- central control of all automated access control mechanisms.

Integration of Physical and Logical Security

Integrating automated physical and logical security functions:
integrate physical and logical access control:

- single ID card (magnetic strip or smart card);
- single-step user/card enrollment and termination;
- central ID-management system;
- unified event monitoring and correlation.

Example of the utility of this integration

- Logical access control system alert indicates that Bob has logged on to the company's wireless network.
- Physical access control system say that Bod did not enter the building.
- ⇒ **Someone is hijacking Bob's wireless account**.

Overview

1. Physical Security Overview

2. Physical Security Threats & Prevention and Mitigation Measures
   - Natural Disasters
   - Environmental Threats
   - Technical Threats
   - Human-Caused Physical Threats

3. Recovery from Physical Security Breaches

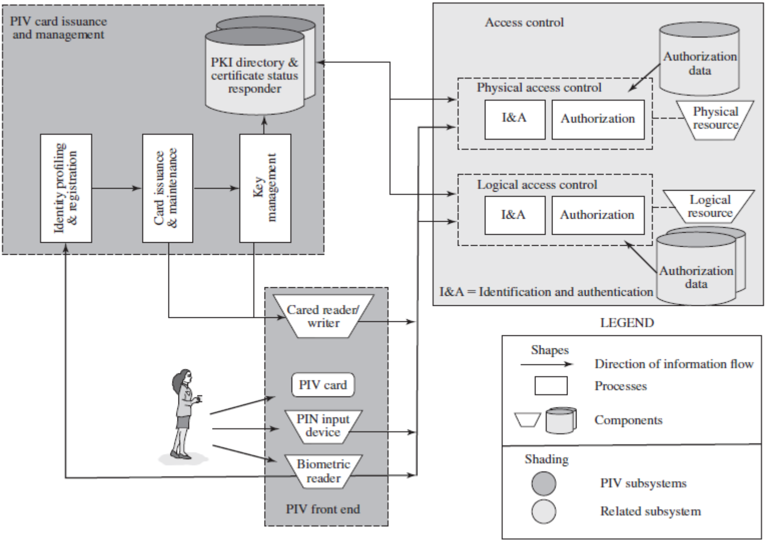
4. Integration of Physical and Logical Security
   - FIPS 201-2: Personal Identity Verification
   - NIST SP 800-116: Use of PIV Credentials in PACS

Standard for the Integration of Physical and Logical Acces Control

Federal Information Processing Standard (FIPS) 201-2
"*Personal Identity Verification (PIV) of Federal Employees and Contractors*", 2013:

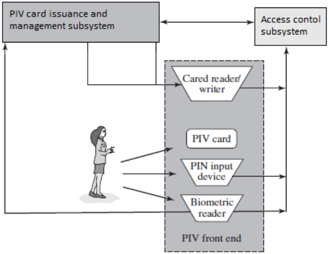
- **define a reliable PIV system** for use in applications such as access to federally controlled facilities and information systems;
- **identifies** Federal **requirements for security levels** that are dependent on risks to the facility or information being protected.

FIPS 201-2 PIV system model



PIV front end

Defines the physical user interface for physical/logical access.

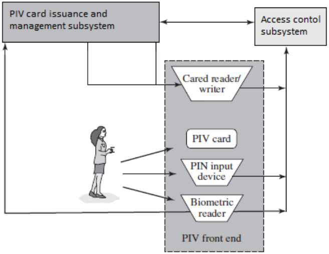


Uses **three-factor authentication**:

1. PIV card, a dual-interface contact and contactless smart card. Holds photograph, X.509 certificates, crypto keys, biometric data, and a cardholder unique identifier (CHUID).
2. PIN used for access to read-protected cardholder information.
3. Biometric reader: fingerprint reader or iris scanner.

PIV front end

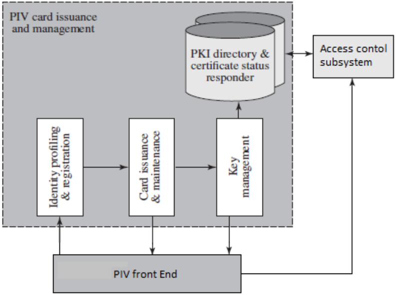
Defines the physical user interface for physical/logical access.



The number of factors used depends on the **level of security required**:

- Low: card reader and PIN;
- High: add biometric comparison (bio-data encoded on the card and theese scanned at the physical access point are compared);
- Very High: add control point attended by an official observer.

PIV Card Issuance and Management Subsystem

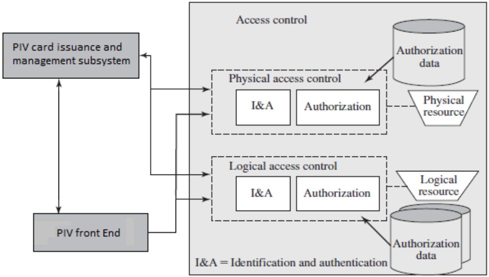

PIV card issuance and management
PKI directory & certificate status responder
Access contol subsystem
Identity profiling & registration
Card issuance & maintenance
Key management
PIV front End

Includes the components responsible for:

- identity proofing and registration;
- card and key issuance and management;
- repositories and services required as part of the verification infrastructure: e.g., public key infrastructure directory, certificate status servers.

Access Control Subsystem

Includes components responsible for determining access to a physical/logical resource.



FIPS 201-2 standardizes data formats and protocols for interaction between the PIV system and the access control system.

FIPS 201-2 Cardholder Unique Identifier (CHUID)

CHUID, data-object of the PIV card, has

- an expiration date (required): independent from the one associated with cardholder privileges;
- a digital signature (optional): ensure that the CHUID was signed by a trusted source and that the CHUID data have not been altered since the signing.

CHUID **authenticates the card data**, not the cardholder.

PIN and biometric factors provide identity verification of the individual.

Benefits of Extended Logical/Physical Access Control

If the integration extends beyond a unified front end to an integration of system elements, we have the following **benefits**:

1. single access control authentication device ⇒ cuts down on misplaced tokens, reduces training and overhead, and allows seamless access;
2. single logical location for employee ID management ⇒ reduces duplicate data entry and allows for immediate authorization/revocation of all resources;
3. central repository for access control investigations done by Auditing/Forensic group;
4. use user ID certificates for other security applications (document e-signing and data encryption).

Overview

1 Physical Security Overview

2 Physical Security Threats & Prevention and Mitigation Measures
- Natural Disasters
- Environmental Threats
- Technical Threats
- Human-Caused Physical Threats

3 Recovery from Physical Security Breaches

4 Integration of Physical and Logical Security
- FIPS 201-2: Personal Identity Verification
- NIST SP 800-116: Use of PIV Credentials in PACS

Use of PIV Credentials in Physical Access Control Systems

NIST SP 800-116 "*A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*", 2008 (revised during 2017):

- provide specific guidance for applying PIV-standard in an environment in which different physical access points within a facility do not all have the same security requirements.

NIST SP 800-116 Authentication Mechanisms

- Visual (VIS): **visual identity verification of a PIV card** done by a human guard.
- Cardholder unique identifier (CHUID): 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**.

NIST SP 800-116 Authentication Mechanisms

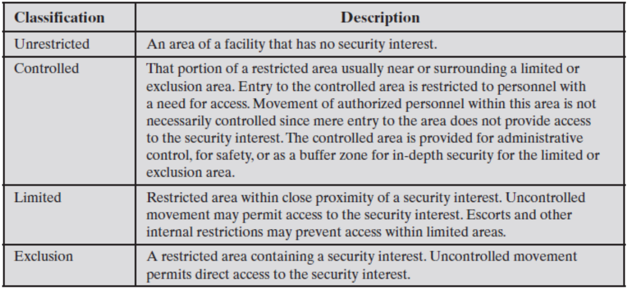
- Attended biometric (BIO-A): the **same as BIO**, **but an attendant supervises** the use of the PIV card and the submission of the PIN and the sample biometric by the cardholder.

- PIV authentication key (PKI): PACS perform **public key cryptography-based authentication using the PKI** (two-factor authentication since the cardholder must enter a PIN to unlock the card).

- Card authentication key (CAK): **optional key** present on PIV card used to authenticate the card and its possessor; **does not require PIN entry** ⇒ used on contactless/contact interface and in challenge/response protocol;

NIST SP 800-116 "Controlled, Limited, Exclusion" Area

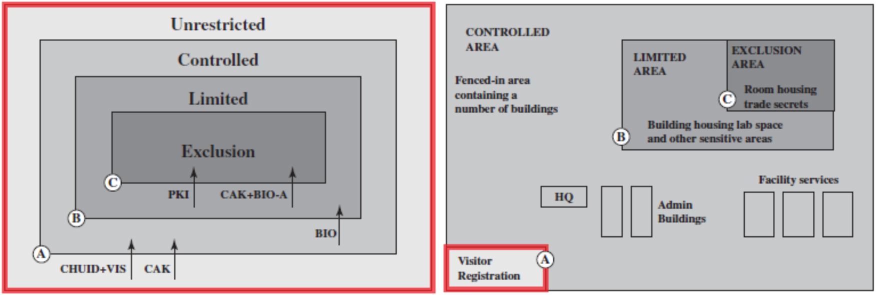
Authentication mechanism should be **selected to conform to the security requirements of the different protected areas** around assets:



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.

- Controlled: proof of affiliation is sufficient.
- Limited: limited to functional subgroup or role.
- Exclusion: access gained by individual authorization only.

General Model and Example of use of NIST SP 800-116

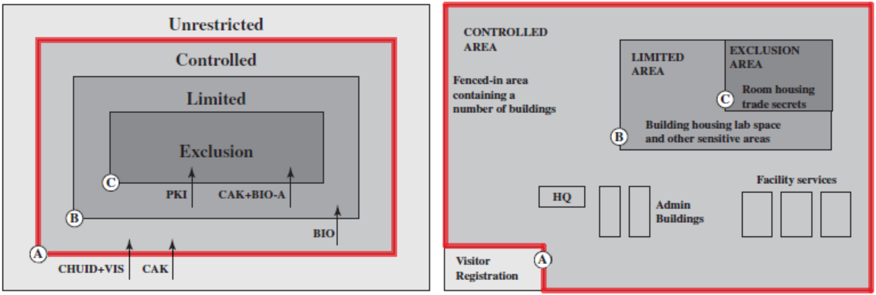


(a) Access control model

(b) Example use

At least one authentication factor is required to enter a controlled area, two factors for a limited area, and three factors for an exclusion area.

General Model and Example of use of NIST SP 800-116

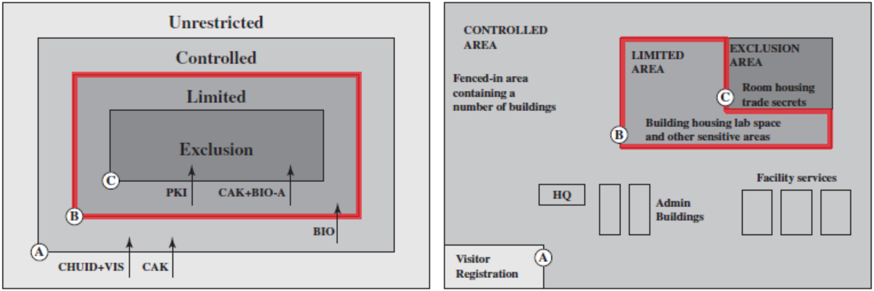


(a) Access control model

(b) Example use

At least one authentication factor is required to enter a controlled area, two factors for a limited area, and three factors for an exclusion area.

General Model and Example of use of NIST SP 800-116

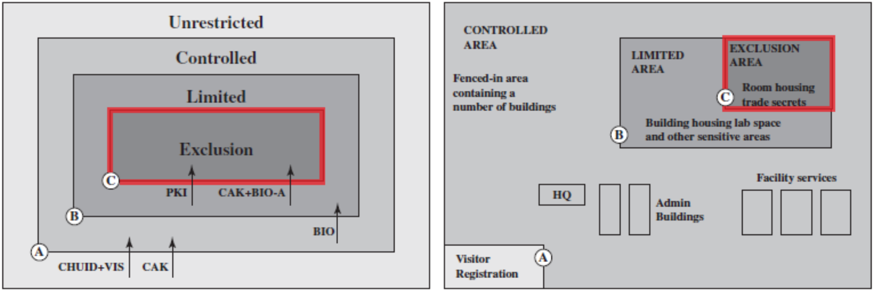


(a) Access control model

(b) Example use

At least one authentication factor is required to enter a controlled area, two factors for a limited area, and three factors for an exclusion area.

General Model and Example of use of NIST SP 800-116



(a) Access control model

(b) Example use

At least one authentication factor is required to enter a controlled area, two factors for a limited area, and three factors for an exclusion area.

Recap

1. Physical Security Overview
2. Physical Security Threats & Prevention and Mitigation Measures
   - Natural Disasters
   - Environmental Threats
   - Technical Threats
   - Human-Caused Physical Threats
3. Recovery from Physical Security Breaches
4. Integration of Physical and Logical Security
   - FIPS 201-2: Personal Identity Verification
   - NIST SP 800-116: Use of PIV Credentials in PACS

Conclusion

Physical security is not always the first thought when it comes to security. Anyway, all the network intrusion detection systems and firewalls are completely useless if someone can get to the equipment and steal data.

To prevent catastrophic loss due to **enviromental**, **technical** or **human-caused threats**, an organization need to implement a physical security program:

- conduct a **risk assessment** to determine the amount of resources to devote to physical security and the allocation of those resources against the various threats.

Thanks for the attention.

THAT CONCLUDES MY TWO-HOUR PRESENTATION. ANY QUESTIONS?
scottadams@aol.com
www.dilbert.com
DID YOU INTEND THE PRESENTATION TO BE INCOMPREHENDIBLE, OR DO YOU HAVE SOME SORT OF RARE "POWERPOINT" DISABILITY?
© 2003 United Feature Syndicate, Inc.
8/4/03
ARE THERE ANY QUESTIONS ABOUT THE CONTENT?
THERE WAS CONTENT?
© 2003 United Feature Syndicate, Inc.