

CompTIA Security+

Lecture 06

SY0-701

Physical Security

By
Dr. Khaled ELMenshawy

Lecture

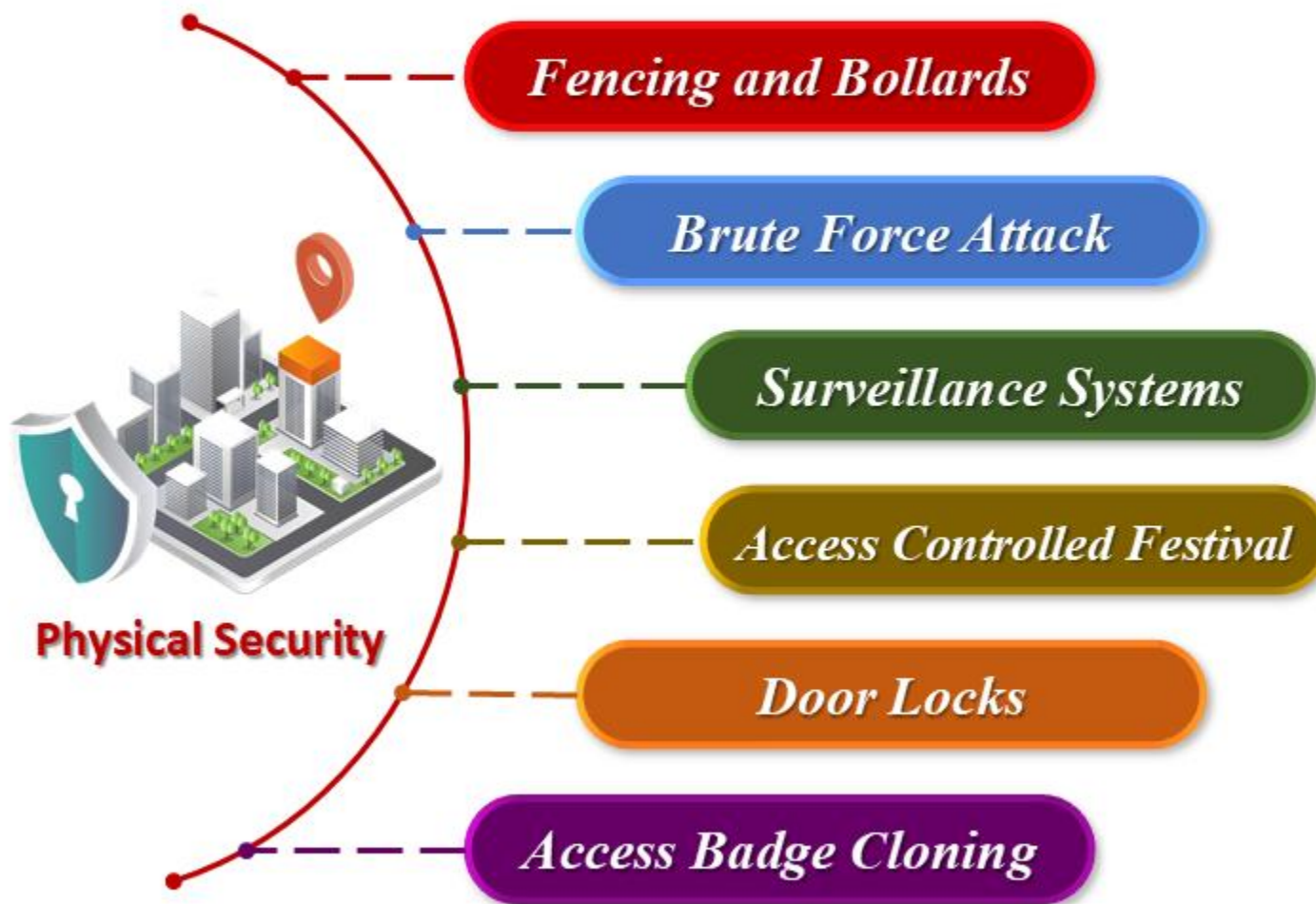
06

LEARNING OUTCOMES

- Understanding the meaning of Physical Security.
- Understanding Fencing and Bollards.
- Recognize the types of Brute Force Attack.
- Understanding Surveillance Systems.
- Understanding Access Control Vestibules.
- Recognize different types of Door Locks
- Understanding Access Badge Cloning.

What is Physical Security?

Physical Security; refers to measures taken to *protect tangible assets* like buildings, equipment, and people *from any kind of harm or unauthorized access*.



What is Fencing?

Fence; designed to *delay and deny, unauthorized access and threats to a site*. It helps form *secure perimeters*, acting as the *first line in defense* to protect assets and premises from intruders.

Fence structures can be crafted from a wide range of materials from wood to metal to wire mesh to concrete and more.



In terms of physical security, fences are going to serve several different purposes:

- **First**; fences are a great way to *provide a visual deterrent* by defining a boundary that should not be violated by unauthorized personnel.
- **Second**; fences can be used to *establish a physical barrier* against unauthorized entry.
- **Third**; fences can be used to effectively *delay intruders* which can help provide the security personnel a longer time to react to an intrusion.

In terms of physical security, fences are going to serve several different purposes:

- **First**; fences are a great way to *provide a visual deterrent* by defining a boundary that should not be violated by unauthorized personnel.
- **Second**; fences can be used to *establish a physical barrier* against unauthorized entry.
- **Third**; fences can be used to effectively *delay intruders* which can help provide the security personnel a longer time to react to an intrusion.

What is Bollards?

Bollards; are short vertical posts made from steel or concrete that designed to manage or redirect vehicular traffic and *prevent unauthorized access to specific areas.*

Bollards need to be designed to be *able to accept a large amount of force* without failing.



Fences

Prevent People



Bollards

Prevent Vehicles



What is Brute Force ?

Brute Force ; is a type of attack where access to a system is gained by *trying all the possibilities* until you break through.

In term of physical security, brute force attack could be one of the following:

- **Forcible entry;** is the act of *getting unauthorized access* to a space *by physically breaking or bypassing its barriers*, such as a window, a door, or a fence.
- **Tampering with security devices;** is *manipulating security devices* to create new vulnerabilities that could be exploited.

- **Confronting security personnel;** is a *direct confrontation or attack of the organization's security personnel* who is a special agent that manage and minimize the risk of attackers exploiting legitimate access to an organization's assets or premises for unauthorized purposes. Attackers will employ *distraction techniques*, *physically assault* the security guards, or *using weapons* to overpower the organization's security guards.
- **Ramming barriers with vehicles** is brute force attack that's going to use any type of motorized vehicle to *ram into the organization's physical security barriers*.

Mitigation of brute force attack:

- **Reenforcing** fences by using electric or barbed wire, using laminated windows, and armored doors with metal frame and deadbolt locks.
- **Redundancy** is a system design in which a component is duplicated so if it fails there will be a backup. So, having multiple backups of the security devices, ensure that if one line of defense is compromised by an attacker, their still other defenses lines remain operational and online.

Deadbolt Door Lock Types

Brute Force Attack

- *Security personnel training* in both conflict resolution, self-defense, and best communication methods to call backups.
- *Using Bollards or reinforce barriers* to prevent vehicles from being able to drive into the organization perimeter.



What is Surveillance Systems?

Surveillance Systems; could be *video surveillance, security guards, lighting and sensors* designed to keep an eye out for suspicious or harmful activities inside the organization.



- **Video surveillance** not only a *closed-circuit television system* (wired or wireless / indoor or outdoor) used to maintain close observation of a person, group, or place inside the organization, but also it includes *motion detection, night vision, facial recognition and remote access* through your smartphone or computer. Also, it provides the ability to *real-time visual feedback*, the capability for *recording the events* so they could be reviewed later, and the ability to *Pan-Tilt-Zoom (PTZ)*.



- **Security guards** can detect unusual or suspicious behavior, and they can also respond immediately to situations.
- **Lighting** is important for conducting effective surveillance using both video and security guards reducing shadows and hiding spots and enhancing the quality of the video recordings.
- **Sensors** are devices that detect and respond to external changes in the environment and then converts that information into a readable signal or data that can be sent over the network. *There are four categories of sensors:*
 - **Infrared sensors** are used to detect changes in infrared radiation that's often emitted by warm bodies like humans or animals (used in low light or dark area).

- *Pressure sensors* are activated whenever a specified amount of weight is detected on the sensor that's embedded into the floor or into a mat.
- *Microwave sensors* are going to be used to detect movement in an area by emitting microwave pulses and measuring the reflection of moving objects back to them.
- *Ultrasonic sensors* are going to be used to measure the reflection of ultrasonic waves off moving objects and used in automated systems such as automated doors or to detect movement within an indoor environment.

How might an attacker bypass your surveillance systems?

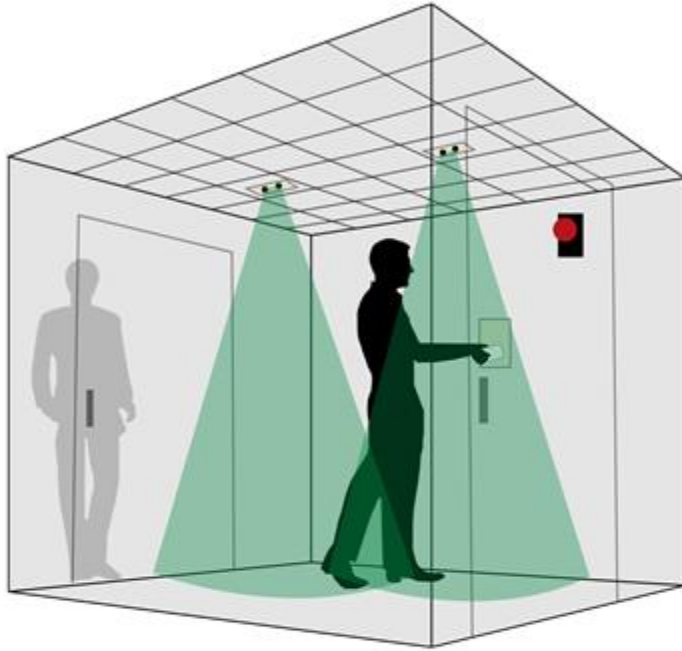
- **Visual obstruction;** is *blocking the camera's line of sight* by using paint, foaming, or umbrellas on camera).
- **Blinding sensors and cameras;** is *overwhelming the sensor or the camera with a sudden burst of light* to render it ineffective for a limited period of time.
- **Acoustics Interference;** occurs when sound waves from different sources interact with each other, so the attacker may *play a loud sound or use jamming devices* to emit frequencies to disrupt the microphone functionality and to be able to bypass one of these sound-based systems.

- ***Electromagnetics Interference;*** *is jamming the signals* that surveillance systems rely on to monitor the environment.
- ***Physical environment attacks;*** are going to *exploit the environment around the surveillance equipment* to compromise their functionality such as increasing the temperature to overcome IR sensors and cameras or shut down the main power supply.

Mitigation of Surveillance Systems attack:

- **Tamper alarm** is notifying security personnel if somebody attempts to physically tamper with surveillance cameras.
- **Backup power supplies** is a backup power generator that operates once the main power supply is offline such as UPS.
- **Encrypted frequency** is hopping signals (*the repeated switching of the carrier frequency during radio transmission to reduce interference and avoid interception*) to guard against jamming attacks that an attacker might try to do.

Access Control Vestibules



What is Access Control Vestibules?

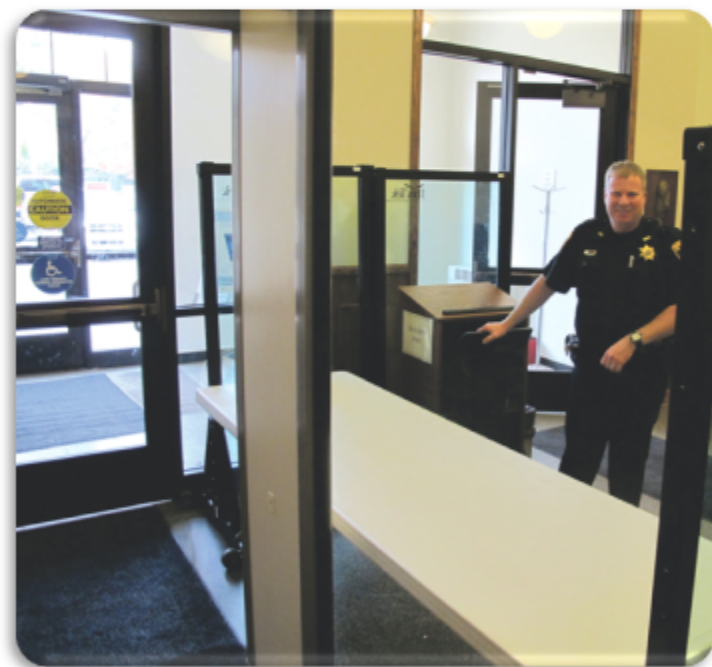
Access Control Vestibules; is a part of a physical access control system designed with two-doors that are electronically controlled with a space between them to ensure that only one door can be opened at a given time.

Access badges; are designed to act as an *individual's key to unlock doors*, systems, or access control vestibules to gain access to a protected or secured space. These access badges are equipped with embedded technologies such as:

- **Radio Frequency Identification (RFID);** is a device that reads information contained in a wireless device from a distance without making any physical contact or requiring a line of sight.
- **Near-Field Communication (NFC);** a set of short-range wireless technologies, requiring a distance of 4 cm or less to initiate a connection. NFC shares a small payloads of data with an Android-powered device, or between two Android-powered devices.

- ***Magnetic strips;*** is a magnetic area on the back of a plastic card that contains information in electronic form, especially information about who the owner of the card is.

Most access control vestibules are *set up at the entrance of the building*, and they'll also have *security guards stationed there at access control points* to provide us with a *visual deterrent, verification, assistance*, and an *immediate response* capability, if required, at those access control vestibules.



What is Access Door Locks?

Door Locks; are physical security controls that are designed to secure entryways by *restricting and regulating access to a particular space or property* and act as a *primary barrier against unauthorized intrusions* to ensure that only individuals with the appropriate key, code, or access method can open the lock and gain entry.



Traditional padlocks:

These are not automated locks and need to be manually engaged for the lock to be in action.

When inserting a key, the uneven edge pushes the pins upward to fit the key's height in that location within the lock body.

Traditional padlocks can *easily be defeated in about 60 seconds or less.*



Electronic door locks:

They are a locking device which operates by means of electric current and rely on identification numbers.



The complexity of the code depends on the number of digits that make up the code according to (10^{length}), so if the code consists of eight digits there's a 1 in 100 million chance that somebody could randomly guess my identification number. Also, some users tend to use their common numbers such as birthdays which the attacker can be predict them using social engineering.

Wireless door locks:

They are a locking device which using NFC, RFID, or Bluetooth signals to open the door by using mobile phones or smart cards.

Wireless door locks could be hacked using MIM or DoS attack.



Biometric door locks:

They are a type of keyless lock that uses a unique part of a user's body as a credential such as fingerprint, facial recognition, or retina scanning. When it comes to biometric locks, there are two factors should be considered. The first is called False Acceptance Rate (FAR) and the other is False Rejection Rate (FRR).



What is False Acceptance Rate (FAR) :

It measures the likelihood of an authentication *system incorrectly granting access to unauthorized individuals*.

To prevent unauthorized people from entering the building or using our systems, we want to ideally get that False Acceptance Rate down to zero by *increasing the sensitivity of the scanners*.

What is False Rejection Rate (FRR) :

It occurs when an authorized person is rejected by the biometric system as unauthorized.

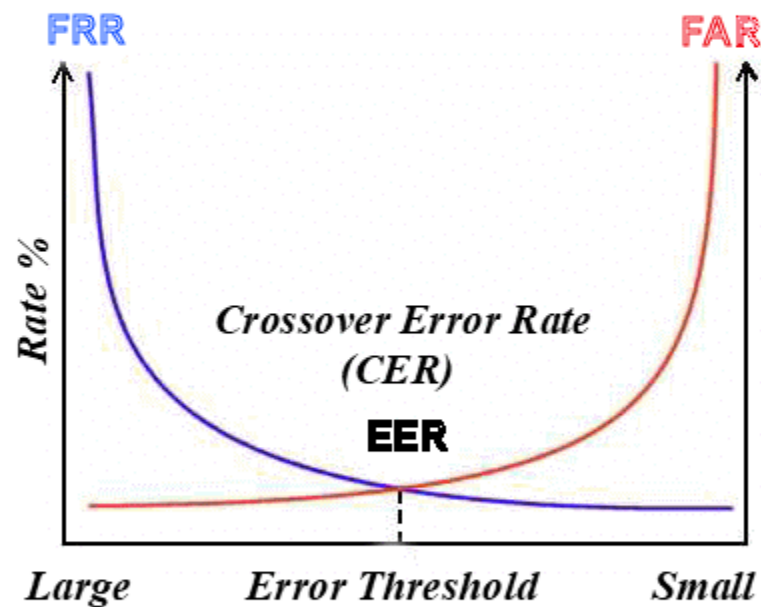
This may happen when increasing the sensitivity of the scanners.

How can I perfectly tune the system to eliminate the false acceptance and the false rejections?

What is Equal Error Rate (ERR) :

It is the point at which the false acceptance rate (FAR) and false rejection rate (FRR) are equal.

The lower the Crossover Error Rate the better that lock is going to be.



Cipher door locks:

A cipher lock provides excellent protection using a mechanical locking mechanism with push buttons that are numbered and require a person to enter the correct combination in order to open that door.



Combining multiple authentication factors to give you additional security to be able to protect that area.

For Example, secure the data center room with 8 digits pass code and a fingerprint biometric pass. This is known as a *multi-factor authentication system*.

Access badges; are designed to act as an *individual's key to unlock doors*, systems, or access control vestibules to gain access to a protected or secured space. These access badges use **RFID** or **NFC** technology.

Access badges cloning; are copying the data from an RFID or NFC card or badge onto another card or device. The clone card or device then *behaves as if it was the original access badge* which can be used to trick the system integrating access or completing a transaction for the attacker.

How the attacker clone the access badge?

There's four basic steps: scanning, data extraction, writing to a new card or device, and using a cloned access badge.

- ***Scanning;*** An attacker can use a handheld RFID or NFC reader to capture the data from a victim's card and store it for further processing and occurs without the access badge owner's knowledge.
- ***Data extraction;*** Once the data is captured, the attacker extracts the relevant authentication credentials from the card, such as a unique identifier or a set of encrypted data. This process can be done at any time.

- ***Writing to a new card or device;*** Using specialized writing tools, the attacker will then transfer the extracted data onto a blank RFID or NFC card or another compatible device.
- ***Using the cloned access badge;*** the attacker has cloned that access badge, and he have a duplicate of it. He can now gain unauthorized access to your building, computer systems or even make payments using a cloned NFC enabled credit card.
- ***Access badge cloning*** is a security concern for us because of the *ease of its execution*, *its ability to be stealthy when conducting the attack*, and *compromising physical security*.

Mitigation of Access Badge Cloning:

- ***Implement advanced encryption;*** Many basic RFID or NFC systems use simple identifiers without any form of robust encryption, it becomes much more difficult for an attacker to clone your organization's access badges if organization's access badges is encrypted using advanced algorithms.
- ***Implement multifactor authentication;*** Instead of solely relying on an RFID or NFC badge for access, you should combine them with a second form of authentication like a pin, a password, or some kind of biometric input.

- ***Regularly update your security protocols;*** By periodically updating the encryption keys and authentication mechanisms being used, your organization can prevent cloned access badges from being usable for extended periods of time.
- ***Provide security awareness to the users;*** It is important to inform the users about the risk of badge cloning and to encourage them to be cautious and report any suspicious activities or unauthorized access attempts that are being levied against their badge.

- ***Shielded wallets or sleeves;*** users should implement the use of shielded wallets or sleeves with your RFID access badges. RFID shielding wallets or sleeves can prevent scanners from being able to read the card.
- ***Audit the access logs;*** By regularly reviewing access logs, this help to identify any unauthorized or suspicious access attempts. If a cloned access badge is going to be used, you may be able to identify patterns that indicate the access badge is a cloned badge and not actually the original.

