CompTIA Security+ SY0-601

21- Explaining Physical Security

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

21.1- Explain the Importance of Physical Site Security Controls

21.2- Explain the Importance of Physical Host Security Controls

21.1- Explain the Importance of Physical Site Security Controls

21.2- Explain the Importance of Physical Host Security Controls

PHYSICAL SECURITY CONTROLS

- Physical access controls are security measures that restrict and monitor access to specific physical areas or assets.
- They can control access to a building, to equipment, or to specific areas, such as server rooms, finance or legal areas, data centers, network cable runs, or any other area that has hardware or information that is considered to have important value and sensitivity.
- Determining where to use physical access controls requires a cost–benefit analysis and must consider any regulations or other compliance requirements for the specific types of data that are being safeguarded.

PHYSICAL SECURITY CONTROLS (cont.)

- Physical access controls depend on the same access control fundamentals as network or operating system security:

  - ✓ Authentication—create access lists and identification mechanisms to allow approved persons through the barriers.
  - ✓ Authorization—create barriers around a resource so that access can be controlled through defined entry and exit points.
  - ✓ Accounting—keep a record of when entry/exit points are used and detect security breaches.

SITE LAYOUT, FENCING, AND LIGHTING

1. Barricades and Entry/Exit Points
    - A barricade is something that prevents access.
    - As with any security system, no barricade is completely effective; a wall may be climbed or a lock may be picked, for instance.
    - The purpose of barricades is to channel people through defined entry and exit points.
    - Each entry point should have an authentication mechanism so that only authorized persons are allowed through.
    - Effective surveillance mechanisms ensure that attempts to penetrate a barricade by other means are detected.

SITE LAYOUT, FENCING, AND LIGHTING (cont.)

2. Fencing
   - The exterior of a building may be protected by fencing.
   - Security fencing needs to be transparent (so that guards can see any attempt to penetrate it), robust (so that it is difficult to cut), and secure against climbing (which is generally achieved by making it tall and possibly by using razor wire).
   - Fencing is generally effective, but the drawback is that it gives a building an intimidating appearance.

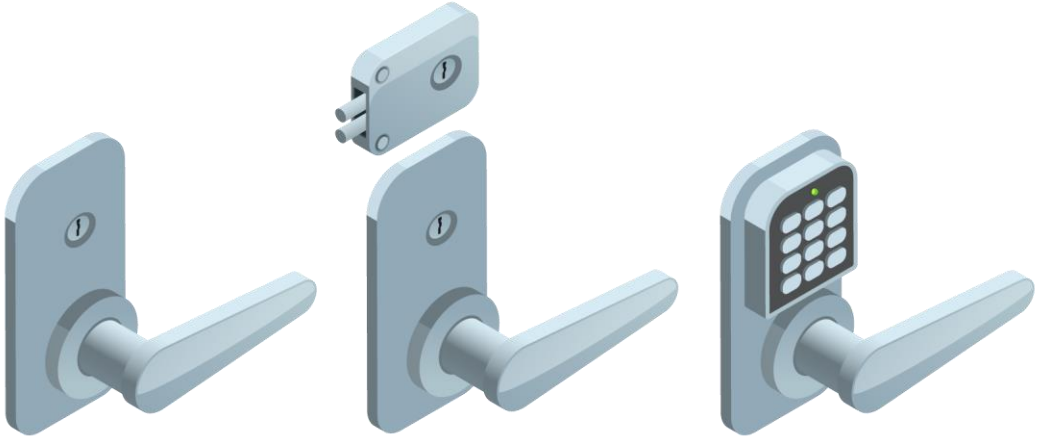
SITE LAYOUT, FENCING, AND LIGHTING (cont.)

3. Lighting
   - Security lighting is important in contributing to the perception that a building is safe and secure at night.
   - Well-designed lighting helps to make people feel safe, especially in public areas or enclosed spaces, such as parking garages.
   - Security lighting also acts as a deterrent by making intrusion more difficult and surveillance (whether by camera or guard) easier.
   - The lighting design needs to account for overall light levels, the lighting of surfaces or areas (allowing cameras to perform facial recognition, for instance), and avoiding areas of shadow and glare.

GATEWAYS AND LOCKS

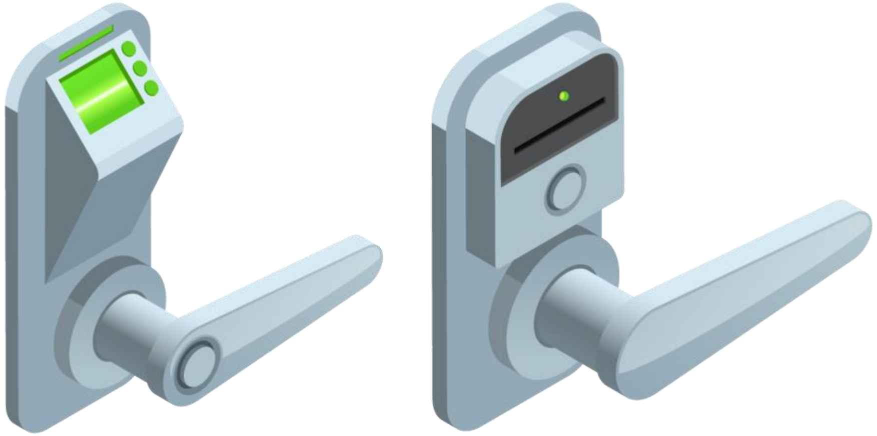
- In order to secure a gateway, it must be fitted with a lock.
- A secure gateway will normally be self-closing and self-locking, rather than depending on the user to close and lock it.
- Lock types can be categorized as follows:
  - ✓ Physical—a conventional lock prevents the door handle from being operated without the use of a key, More expensive types offer greater resistance against lock picking.
  - ✓ Electronic—rather than a key, the lock is operated by entering a PIN on an electronic keypad, This type of lock is also referred to as cipher, combination, or keyless. A smart lock may be opened using a magnetic swipe card or feature a proximity reader to detect the presence of a physical token, such as a wireless key fob or smart card.

GATEWAYS AND LOCKS (cont.)



From left to right, a standard key lock, a deadbolt lock, and an electronic keypad lock

GATEWAYS AND LOCKS (cont.)



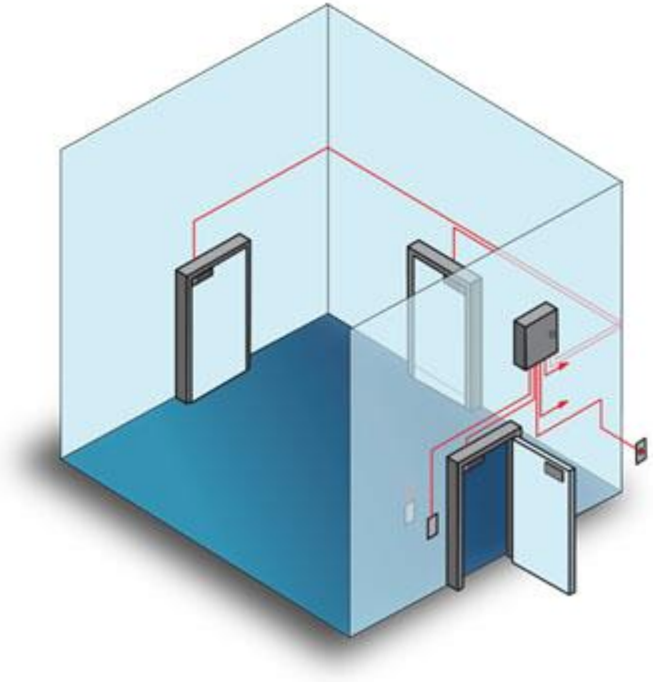
Biometric thumbprint scanner lock and a token-based key card lock

GATEWAYS AND LOCKS (cont.)

- Mantraps
  - ✓ Apart from being vulnerable to lock picking, the main problem with a simple door or gate as an entry mechanism is that it cannot accurately record who has entered or left an area.
  - ✓ Multiple people may pass through the gateway at the same time; a user may hold a door open for the next person; an unauthorized user may "tailgate" behind an authorized user.
  - ✓ This risk may be mitigated by installing a **turnstile** (a type of gateway that only allows one person through at a time).
  - ✓ The other option is to add some sort of surveillance on the gateway or mantrap.
  - ✓ A **mantrap** is where one gateway leads to an enclosed space protected by another barrier.

GATEWAYS AND LOCKS (cont.)

- Mantraps (cont.)



ALARM SYSTEMS

- When designing premises security, you must consider the security of entry points that could be misused, such as emergency exits, windows, hatches, grilles, and so on.
- These may be fitted with bars, locks, or alarms to prevent intrusion.
  - ✓ Circuit alarm—a circuit-based alarm sounds when the circuit is opened or closed.
  - ✓ Motion detection alarm—a motion-based alarm is linked to a detector triggered by any movement within an area.
  - ✓ Noise detection alarm—an alarm triggered by sounds picked up by a microphone.

SECURITY GUARDS AND CAMERAS

- **Human security guards**, armed or unarmed, can be placed in front of and around a location to protect it.
- They can monitor critical checkpoints and verify identification, allow or disallow access, and log physical entry events.
- They also provide a visual deterrent and can apply their own knowledge and intuition to potential security breaches.
- The visible presence of guards is a very effective intrusion detection and deterrence mechanism but is correspondingly **expensive**.

SECURITY GUARDS AND CAMERAS (cont.)

- **CCTV (closed circuit television)** is a cheaper means of providing surveillance than maintaining separate guards at each gateway or zone.
- The advantage is that movement and access can be recorded.
- The main drawback compared to the presence of security guards is that response times are longer, and security may be compromised if not enough staff are in place to monitor the camera feeds.

21.1- Explain the Importance of Physical Site Security Controls

21.2- Explain the Importance of Physical Host Security Controls

SECURE AREAS

- A secure area is designed to store critical assets with a higher level of access protection than general office areas.
- An **air gapped host** is one that is not physically connected to any network.
- An air gap within a secure area serves the same function as a demilitarized zone.
- It is an empty area surrounding a high-value asset that is closely monitored for intrusions.
- Portable devices and media (backup tapes or USB media storing encryption keys, for instance) may be stored in a **safe**.
- A **vault** is a room that is hardened against unauthorized entry by physical means, such as drilling or explosives.

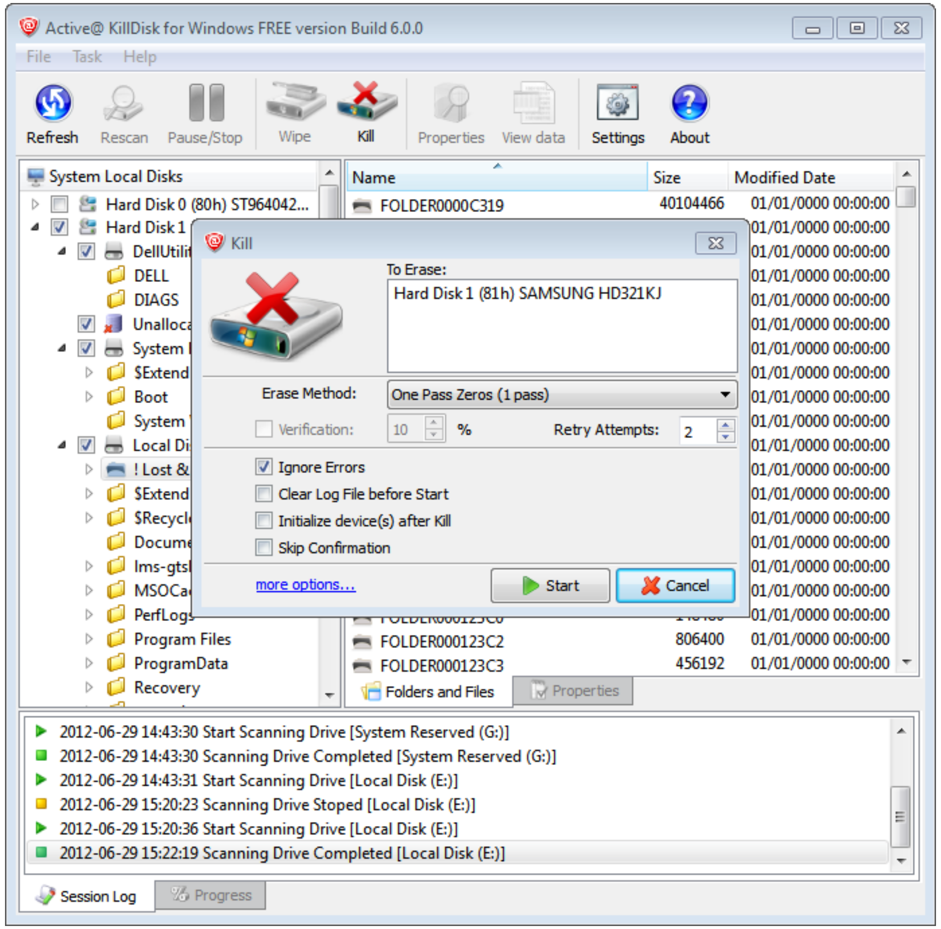
SECURE DATA DESTRUCTION

- Physical security controls also need to take account of the disposal phase of the data life cycle.
- Media sanitization and remnant removal refer to erasing data from hard drives, flash drives/SSDs, tape media, CD and DVD ROMs before they are disposed of or put to a different use.
- Paper documents must also be disposed of securely.

DATA SANITIZATION TOOLS

- Files deleted from a magnetic-type hard disk are not erased.
- Rather, the sectors are marked as available for writing and the data they contain will only be removed as new files are added.
- Similarly, using the standard Windows format tool will only remove references to files and mark all sectors as usable.
- The standard method of sanitizing an HDD is called **overwriting**.
- This can be performed using the drive's firmware tools or a utility program.
- The most basic type of overwriting is called zero filling, which just sets each bit to zero. Single pass zero filling can leave patterns that can be read with specialist tools.
- A more secure method is to overwrite the content with one pass of all zeros, then a pass of all ones, and then a third pass in a pseudorandom pattern.

DATA SANITIZATION TOOLS (cont.)



Name	Size	Modified Date
FOLDER0000C319	40104466	01/01/0000 00:00:00
FOLDER000123C2	806400	01/01/0000 00:00:00
FOLDER000123C3	456192	01/01/0000 00:00:00

Kill

To Erase:
Hard Disk 1 (81h) SAMSUNG HD321KJ

Erase Method: One Pass Zeros (1 pass)

□ Verification: 10 % Retry Attempts: 2

☑ Ignore Errors
□ Clear Log File before Start
□ Initialize device(s) after Kill
□ Skip Confirmation

more options...

Start Cancel

```
2012-06-29 14:43:30 Start Scanning Drive [System Reserved (G:)]
2012-06-29 14:43:30 Scanning Drive Completed [System Reserved (G:)]
2012-06-29 14:43:31 Start Scanning Drive [Local Disk (E:)]
2012-06-29 15:20:23 Scanning Drive Stoped [Local Disk (E:)]
2012-06-29 15:20:36 Start Scanning Drive [Local Disk (E:)]
2012-06-29 15:22:19 Scanning Drive Completed [Local Disk (E:)]
```