

3.2.4 Physical Network Protection Facts

This lesson covers the following topics:

- Secured areas
- Physical security attacks against smart cards and USB devices
- Isolated networks

Secured Areas

Physical security can protect a network from misuses of equipment by untrained employees or contractors. It can protect the network from hackers, competitors, and terrorists who might enter the premises and try to change equipment configurations. Physical security can also protect resources from natural disasters, such as floods, fires, storms, and earthquakes.

Depending on your particular network design, physical security should be installed to protect core routers, demarcation points, cabling, modems, servers, hosts, backup storage, and so on. Because physical security is such an obvious requirement, it is easy to forget to plan for it. However, it should never be overlooked or considered less important than other security mechanisms.

Security Measure	Description
Locked network closet	Regardless of the size of your organization, networking components should always be inside of a locked room that only specific individuals have access to. Make sure the lock to this room has some sort of access logging. For example, many key card locking mechanisms track the time, date, and individual who opens the door. This can be helpful when identifying the source of an attack.
Vault	Another way you can secure networking devices is to keep them in a locked cage, or a vault. You can do this in addition to a locked room or you can place the vault inside a locked room. Obviously, combining the two physical security measures is best, but make sure to have at least one.
Faraday cage	Faraday cages are designed to block all electromagnetic emissions. Faraday cages are used to protect against attackers who collect electronic emissions from electronic devices. The technique of collecting electronic emissions is known as Van Eck phreaking. It is a form of eavesdropping.
Protected cable distribution	A metal cabinet that locks away all the networking cables and prevents any type of emissions. PDSs also keep attackers from physically removing cables or plugging in additional cables. PDSs are most commonly used by utility companies.

Physical Security Attacks Against Smart Cards and USB Devices

Organizations should be aware of physical security attacks against smart cards and USB devices.

Attack Type	Description
Malicious universal	It is common now to find USB charging stations in public places, such as airports, hotels, and

serial bus (USB) cable	restaurants. It is possible that these could be used to copy data from a users device. Users can protect themselves by using USB data blockers. These are used to prevent data transfers to USB drives. This device is connected between the USB charging port and your charging cable and helps to protect access to your data.
Malicious flash drive	<p>Plugging an infected USB flash drive to a host system or network can be a major risk. These USB drives can be infected with malware which later can be used to disrupt the operation of a business.</p> <p>A malicious USB drive can install malware such as backdoors, trojans, and ransomware. These drives could also install browser hijackers that will redirect a victim to a website of choice for the hacker.</p> <p>One of the first incident was thought to have happened in 2010 when the Stuxnet worm was distributed via USB sticks to launch attacks on the networks of an Iranian facility.</p>
Card cloning	Card cloning is the process of making copies of smart cards. Lost, misplaced, or stolen cards can be copied, if there is not cryptographic protection on them.
Skimming	Card skimming is when there is a card reader placed in order to copy the credentials of a users smart card. Once the cards details are copied, it can be used to create counterfeit cards. Proximity cards can also be copied. These transmit the credentials and can be captured with portable RFID reader.

Isolated networks

If your organization allows internet access to email servers or web servers, you've allowed untrusted networks access to your network. An attacker could use this opening to access other devices on your organization's private network.

Here are a few security measures that can be taken to ensure that your private network and devices are isolated from the public network.

Security Measure	Description
Demilitarized zone (DMZ) or Screened Subnet	A demilitarized zone, also called a screened subnet, provides enhanced security by isolating your publicly accessible network from your privately accessible network. Basically, you're using a firewall to creating two separate networks.
Air gap	An air gap is a security method in which a computer, a server, or a small network of computers is physically isolated from the internet or other unsecured networks. This means that only individuals authorized to access that computer or network can access it. It can be accessed only in person, not over the internet, not even from another internetwork within the organization.