Network Physical Security

by Sophia

WHAT'S COVERED

In this lesson, you will learn about the physical security of network devices.

Specifically, this lesson will cover the following:

1. Physical Security

Throughout this entire challenge, you have learned about some of the myriad devices we use to secure traffic coming into our networks and devices and the things we depend on to detect and prevent attacks on them. It is an important subject and one that you must solidly understand in order to be effective in networking. Knowing how to implement an effective security program requires working knowledge of these devices, but it does not end there because there's always more you can know.

There are a few more really significant and valuable concepts you should have a good grasp of when setting up and managing the security on your network. In this lesson, and the next, we will cover key issues you need to be aware of, including physical security and corresponding logical security structures, and restricting access.

Many system administrators seem really eager to talk all about the information security systems they have in place, including firewalls, IDS/IPS and directory policies. But interestingly, one of the things few administrators seem to get excited about is physical security, which they may treat as an afterthought. Maybe the server room has a locked door, maybe it does not. Maybe the badges that open that door are owned by the right people, or maybe they are not. Perhaps on a subconscious level, humans tend to inherently trust the people working within their organization, and focus their fears, suspicions, and attention on unknown outside forces that might break in, steal data, or totally incapacitate our networks. Some of the sharpest, most talented, and savvy system administrators have a tendency to neglect inside security and fail to reasonably monitor things going on within the building.

And there are some vital resources to secure on the inside. For instance, does it really matter if your network has a secured subnet for the servers, with its own dedicated internal firewall, if the servers are sitting in racks in a hallway right across from the lunch room? Or, if the door to the server room is propped open because otherwise it gets too hot in there? Imagine backup media clearly marked and sitting there on a shelf open to anyone who walks by. The bottom line is that if your systems are not physically secured, you are basically sending out an open invitation to a lot of potential problems.

☆ BIG IDEA

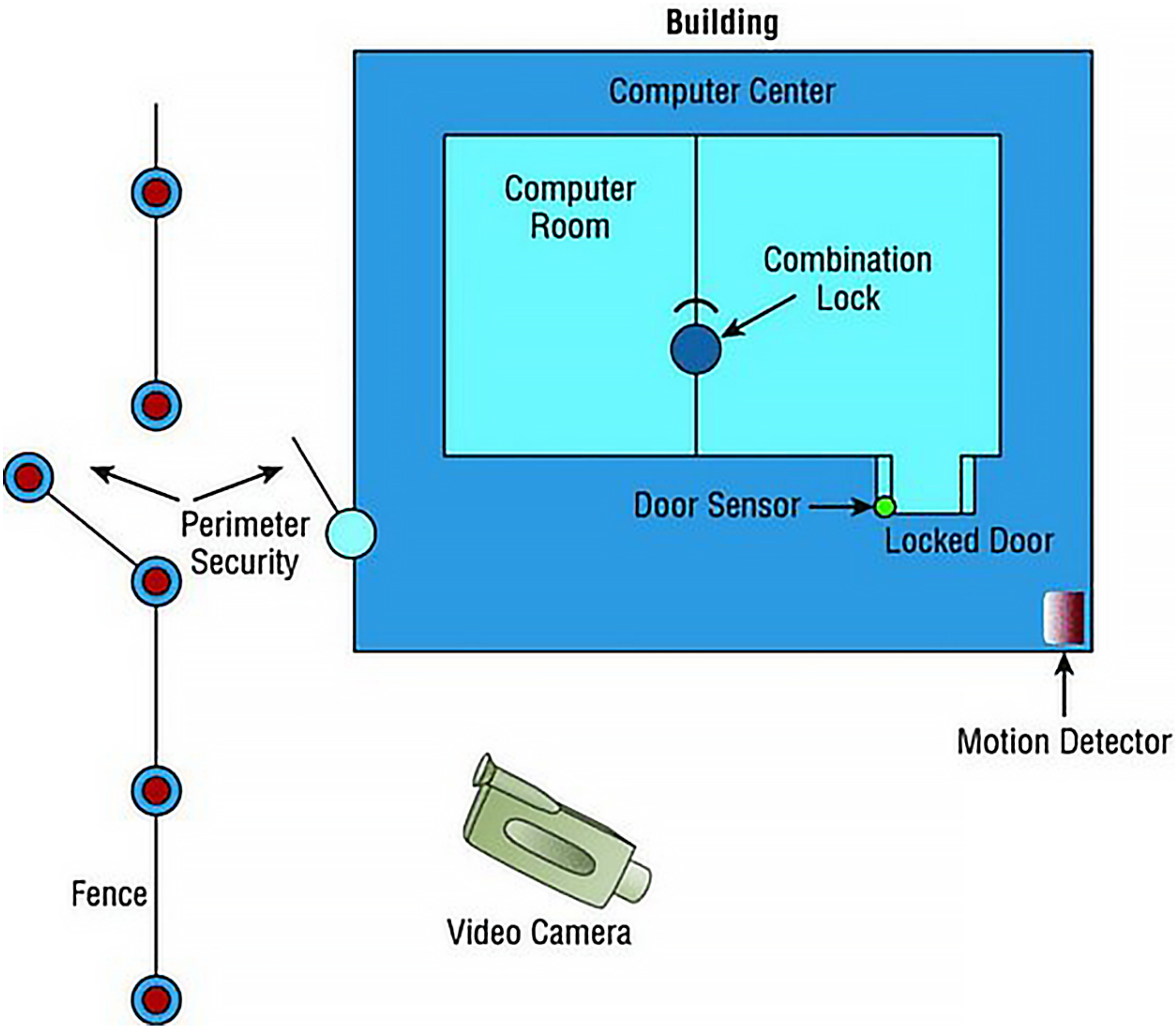
If an attacker can physically touch a network device, they can often easily create administrative privileges for themselves, and essentially take over command and control of the device.

1a. Physical Barriers

Your first objective is to keep people from physically getting to your equipment. Clearly, end users need to be able to get to their workstations, but only authorized personnel should be anywhere near your servers. The best way to do this is to have a dedicated, two-stage, air-conditioned server room with really secure doors and locks. Even better, your data center should have more than one form of physical security—and preferably three. We call that a **multiple barrier system**.

EXAMPLE You could have a perimeter security system controlling access to the building as your first line of defense. The second would be a secured door to the computer room, and the third would be another security door to the server room itself.

This is illustrated in the diagram below.



TERM TO KNOW

Multiple Barrier System

A security system designed with multiple points of access control.

1b. Security Zones

Your network probably has different **security zones**. Let us say your servers are in one zone and the clients are in another. Maybe your engineering department has its own zone. So why not have the same zones for physical access to the computers? Many companies today use RFID badges to control where employees are allowed to go inside the building. You may need a safety clearance and/or certification before you can go in the room where the pilot production machine lives. People should be cleared and certified before they are allowed in the server room as well.

TERM TO KNOW

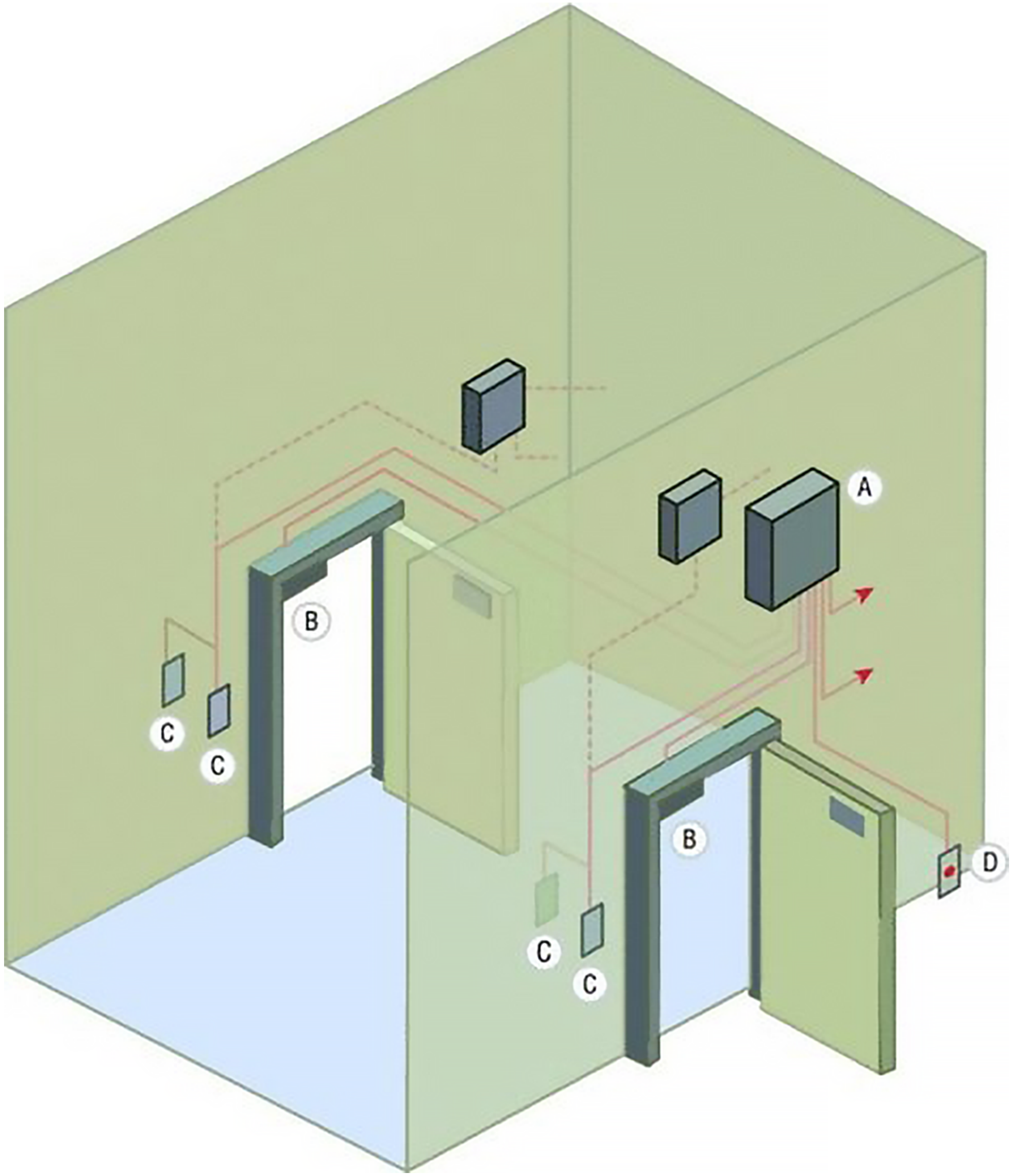
Security Zone

An area of a network that deploys specific security policies.

1c. Access Control Vestibules

An **access control vestibule** is a series of two doors with a small room between them. A person accessing the area is authenticated at the first door and then allowed into the room. At that point, additional verification will occur (such as a guard visually identifying the person) and then they are allowed through the second door. These doors are typically used only in very high-security situations. They can help prevent tailgating, which is two people entering the area on a single authentication.

An access control vestibule design is shown in the diagram below.



TERM TO KNOW

Access Control Vestibule

A small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens, used to restrict access.

1d. Network Closets

While much of the network equipment should be locked securely in the server room, there are frequent cases where it is also stored in a smaller location or closets. If that is the case, these locations should be locked as securely as the server room, and access to them should be controlled through mechanisms such as cipher doors or proximity locks.

1e. Video Monitoring

In many high-security scenarios it may be advisable to visually monitor the area 24 hours a day. When this is the case, it will make sense to deploy video monitoring. We will look at two options, IP cameras and CCTV systems. Internet Protocol (IP) video systems are a good example of the benefits of networking applications. These systems can be used both for surveillance of the facility and for facilitating collaboration.

Whereas an **IP camera** is a type of digital video camera commonly employed for surveillance, analog **closed-circuit television (CCTV)** cameras are unable to send their images across IP networks. CCTV cameras record directly to a medium such as video tape or hard drive. It is possible to convert the signal to digital in cases where you need to send it across an IP network.

TERMS TO KNOW

Internet Protocol (IP) Camera
A webcam used specifically for surveillance as a security measure.

Closed-Circuit Television (CCTV)
A network of one or more television cameras and television receivers connected together with no provision for broadcasting.

1f. Door Access Controls

While access control vestibules may justify their cost in some high-security scenarios, not all situations require them. Door controls should be used to prevent physical access to important infrastructure devices such as routers, switches, firewalls, and servers. The following are some of the most common door access controls.

Proximity readers are door controls that read a card from a short distance and are used to control access to sensitive rooms. These devices can also provide a log of all entries and exits. Usually, a card contains the user information required to authenticate and authorize the user to enter the room.

A **key fob**, on the other hand, is a type of security token: a small hardware device with built-in authentication mechanisms. The mechanisms in the key fob control access to network services and information. An advantage of a key fob is that it can support multi-factor authentication.

> EXAMPLE A user may have a personal identification number (PIN), which authenticates them as a device’s owner; after the user correctly enters their PIN, the device displays a number that allows them to open a door or log on to the network.

Biometric authentication systems are designed to operate using characteristic and behavioral factors. While knowledge factors (password, PIN, or something you *know*) are the most common authentication factors used, characteristic factors represent something that you *are* (fingerprint, iris scan), while behavioral factors represent something that you *do* (signature analysis).

Multi-factor authentication is achieved by combining authentication factors. When two factors are combined, such as a retina scan (characteristic factor) and a password (knowledge factor), dual-factor authentication is required. When three factors are combined, such as a retina scan (characteristic factor), a password (knowledge factor), and signature analysis (behavioral factor), then multi-factor authentication is in effect.

HINT

One of the issues with **biometrics** is the occurrence of false positives and false negatives. A false positive is when a user that should not be allowed access is indeed allowed access. A false negative, on the other hand, is when an authorized individual is denied passage by mistake.

Cipher locks that use a keypad require a user to know the key code. These devices can also come with additional security features. The lock can be combined with a set time for opening the door as well as a battery standby system. Three types of alarm systems are available. A burglar alarm interface is available to indicate when the door is breached. An error alarm can reveal someone who tries to guess the code. Finally, a hostage alarm can be triggered to indicate that entry was made under duress.

In cases where judgment may be required to control entry, a human **Security Guard** may be advisable. While the cost is generally higher than with an automated system, there are advantages to this. This offers the most flexibility in reacting to whatever occurs. One of the keys to success when using guards is to ensure that they are trained with a response to every conceivable eventuality. Finally, the biggest advantage is that guards can use discriminating judgment in a situation, which an automated system cannot.

TERMS TO KNOW

Proximity Reader
A reader device that senses the presence of a contactless smart card.

Key Fob
A passive wireless electronic device that uses RFID technology to control access to buildings, data centers, and computers by being placed near a detector.

Biometric Authentication
Body measurements and calculations used in as a form of identification and access control, for example fingerprint, facial recognition, iris scan, and retina scan.

Multi-Factor authentication
An electronic authentication method in which a user is granted access to a resource only after successfully presenting two or more pieces of evidence to an authentication mechanism.

Biometrics
Body measurements and calculations related to human characteristics.

Cipher Lock
A lock that uses a programmable keypad to control access to a secure area.

SUMMARY

In this lesson, you learned about the **physical security** of network devices, including physical barriers, security zones, access control vestibules, network closets, video monitoring, and various door access control mechanisms.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Access Control Vestibule

A small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens, used to restrict access.

Biometric Authentication

Body measurements and calculations used in as a form of identification and access control, for example fingerprint, facial recognition, iris scan, and retina scan.

Biometrics

Body measurements and calculations related to human characteristics.

Cipher Lock

A lock that uses a programmable keypad to control access to a secure area.

Closed-Circuit Television (CCTV)

A network of one or more television cameras and television receivers connected together with no provision for broadcasting.

Internet Protocol (IP) Camera

A webcam used specifically for surveillance as a security measure.

Key Fob

A passive wireless electronic device that uses RFID technology to control access to buildings, data centers, and computers by being placed near a detector.

Multi-Factor Authentication

An electronic authentication method in which a user is granted access to a resource only after successfully presenting two or more pieces of evidence to an authentication mechanism.

Multiple Barrier System

A security system designed with multiple points of access control.

Proximity Reader

A reader device that senses the presence of a contactless smart card.

Security Zone

An area of a network that deploys specific security policies.