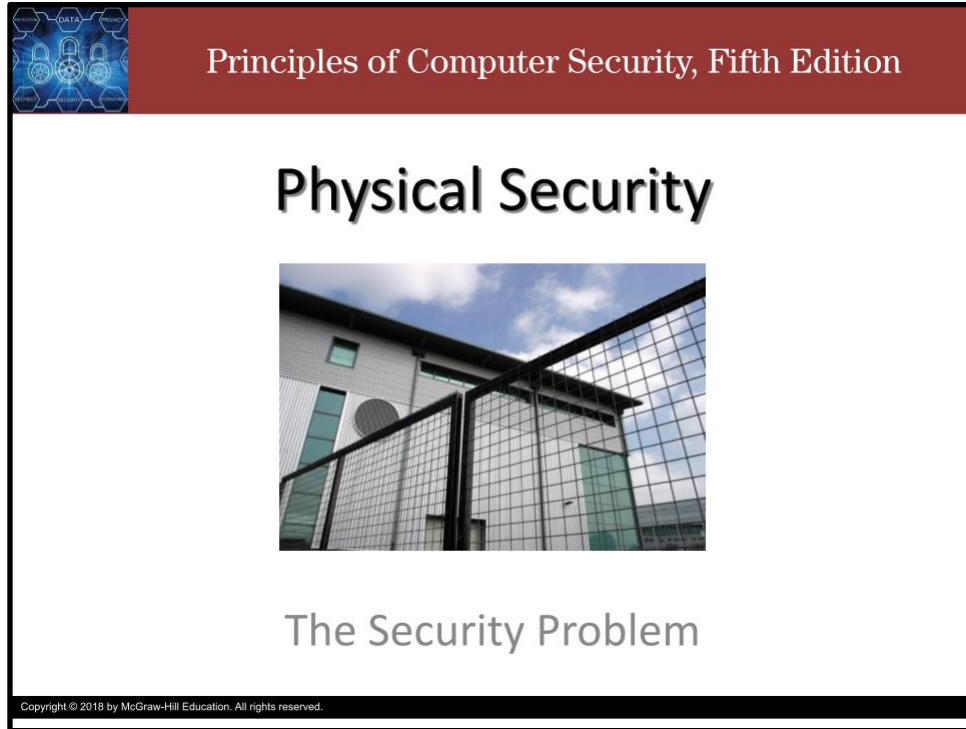



Physical Security: The Security Problem

Slide 1



Principles of Computer Security, Fifth Edition


Physical Security



The Security Problem

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! There is no security without physical security. In this video, we discuss the security problem



Principles of Computer Security, Fifth Edition

The Security Problem

- There is no security without physical security
 - “Physical access negates all other security measures.”
- More than just servers
 - Also access to entire network infrastructure
- Have I told you lately that there is no security without physical security?

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The problem that faces professionals charged with securing a company’s network can be stated rather simply:

Physical access negates all other security measures.

No matter how impenetrable the firewall and intrusion detection system, if an attacker can find a way to walk up to and touch a server, they can break into it.

But, physically securing information assets does not mean just the servers.

It also means protecting physical access to all the organization’s computers and its entire network infrastructure.

Slide 3

Principles of Computer Security, Fifth Edition

Using a lower-privilege machine to get at sensitive information

2. So the attacker physically installs malicious software on the receptionist machine that is directly connected to the servers.

1. Attacker cannot get past firewall from external connections.

Attacker remote PC

Core Corporate Servers

Receptionist machine

There is no security without physical security

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Again, physical access negates all other security measures.

Consider that most network security measures are, from necessity, directed at protecting a company from Internet-based threats. Consequently, a lot of companies allow any kind of traffic on the local area network. So, if an attacker attempts to gain access to a server over the Internet and fails, they may be able to gain physical access to the receptionist's machine and, by quickly compromising it, use it as a remotely controlled zombie to attack what they are really after.

Principles of Computer Security, Fifth Edition

A wireless bridge can allow remote access.

Attacker plugs a smartphone into an open Ethernet jack and uses 802.11 wireless to attack the network from outside the building.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Prior to handheld devices, the attacker would have to work in a secluded area with dedicated access to an Ethernet for some time. The attacker would sit down with a laptop and run a variety of tools against the network, and working internally typically put the attacker inside the firewall and IDS. Today's capable mobile devices can assist these efforts by allowing attackers to place the small device onto the network to act as a wireless bridge, as shown in the picture.

Principles of Computer Security, Fifth Edition

Bootable Media




Figure 8.3 A collection of sample LiveCDs

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Any media used to boot a computer into an operating system that is not the native OS on its hard drive is called bootable media, or simply a bootdisk

Typical boot media include CDs, DVDs, and USB drives.

Before bootable CDs or DVDs were available, a boot floppy was used to start the system and prepare the hard drives to load the operating system.

A boot source can contain a number of programs.

Typically, they include a basic utility that can be used to perform a number of tasks including mounting the hard drives and performing at least read operations.

If right access to the drive is obtained, the attacker could alter the password file or place a remote-control program to be executed automatically upon the next boot, guaranteeing continued access to the machine.

The large capacity of a CD, DVD, or USB drive means they can store an entire operating system and a complete tool set for a variety of tasks or malware.

An aside, a typical attack is to leave a disc or flash drive in an opportunistic place where members of a target organization may pick it up and insert it into their machine. Little does the victim know, the drive is loaded with malware and the act of inserting it into a computer is the trigger to release the malware. This is not a boot attack, as it requires the OS to already be up and running. The best defense is to never put media into your device of which you do not know the origin (and even then be careful). On top of that, you should disable the autorun feature and access the media in read-only mode with a low-privileged process. Better yet, do this on a virtual machine, or an air gapped machine, which is set aside for specifically this purpose. But, really. If you found it on the ground, leave it there or put it in the electronic waste bin where it belongs.

A LiveCD contains a bootable version of an entire operating system, typically a variant of Linux, complete with drivers for most devices.

LiveCDs give an attacker a greater array of tools than could be loaded onto a floppy disk.

These tools include scanners, sniffers, vulnerability exploits, forensic tools, drive imagers, password crackers, and more.

With a LiveCD, an attacker would likely have access to the hard disk and also to an operational network interface that would allow him to send the drive data over the Internet if properly connected.

These bootable operating systems could also be custom built to contain any tool that runs under Linux, allowing an attacker to build a standard bootable attack image or a standard bootable forensic image, or something customized for the tools he likes to use.

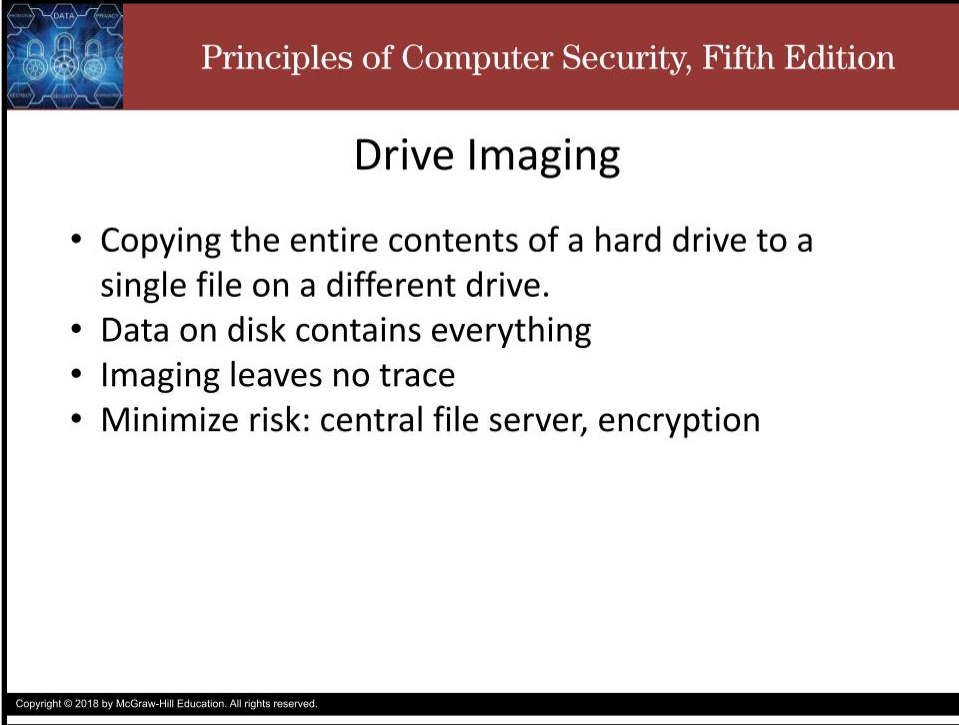
Bootable USB flash drives emulate the function of a CD/DVD and provide a device that is both physically smaller and logically larger.

Made bootable, these devices can contain entire specialized operating systems, and unlike a disk, these devices can also be written to, providing an offload point for collected data if an attacker chooses to leave the device and return later.

Given the cost and capabilities of solid state media today, USB drives are by far the preferred media for pen-testers and attacks alike. But, LiveCDs are still useful for when a system has well-secured its USB access points, but has not adequately secured its boot sequence or optical disk policies.

The most obvious mitigation for attacks that use bootable media is to tell the BIOS not to boot from removable media, but this too has issues as there are legitimate reasons to boot from a disc or USB drive, such as reinstalling the operating system. Nonetheless, the benefit of securing against an attack that uses bootable media likely outweighs the cost of the extra work to securely re-enable the use of bootable media for only the time needed to perform the required maintenance and then disabling it afterwards. This is an application of the principle of least privilege.

Slide 6



Principles of Computer Security, Fifth Edition

Drive Imaging

- Copying the entire contents of a hard drive to a single file on a different drive.
- Data on disk contains everything
- Imaging leaves no trace
- Minimize risk: central file server, encryption

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Drive imaging is the process of copying the entire contents of a hard drive to a single file on a different drive.

It is often used by people who perform forensic investigations of computers.

It uses a bootable media to start the computer and load the drive imaging software.

Then, it makes a bit-by-bit copy of the hard drive on another drive.

The process keeps the original copy exactly as it was for evidence.

From an attacker's perspective, drive imaging software is useful because it pulls all information from a computer's hard drive while still leaving the machine in its original state.

The information stored on disk contains every bit of data that is on the computer: any locally stored documents, locally stored e-mails, and every other piece of information that the hard drive contains.

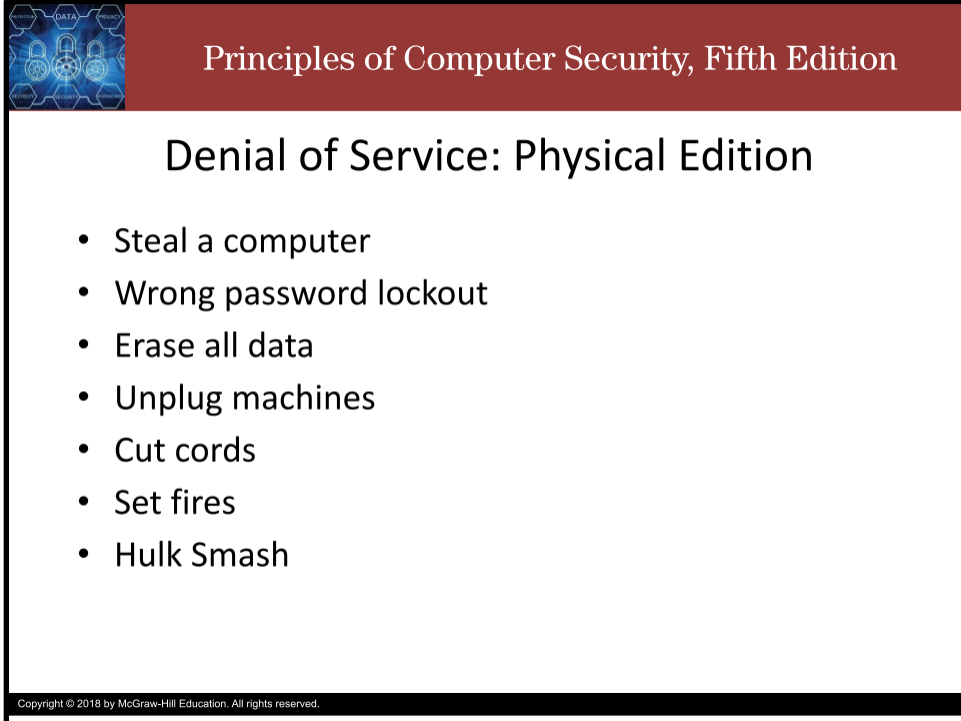
This data could be very valuable if the machine holds sensitive information about the company.

Physical access is the most common and effective way of imaging a drive.

The biggest benefit for the attacker is that physical drive imaging can leave absolutely no trace of the crime.

Besides physically securing access to your computers, you can do very little to prevent drive imaging, but you can minimize its impact. The use of encryption even for a few important files provides protection. Full encryption of the drive protects all files stored on it. Alternatively, placing files on a centralized file server keeps them from being imaged from an individual machine, but if an attacker is able to image the file server, the data will be copied.

Slide 7



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. Below the header, the title "Denial of Service: Physical Edition" is centered in black. A bulleted list of seven physical attack methods is presented on the left side. At the bottom left, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Principles of Computer Security, Fifth Edition

Denial of Service: Physical Edition


- Steal a computer
- Wrong password lockout
- Erase all data
- Unplug machines
- Cut cords
- Set fires
- Hulk Smash

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

A denial-of-service (DoS) attack can also be performed with physical access, such as by stealing a computer, using a bootdisk to erase all data on the drives, or simply unplugging computers.

Depending on the company's quality and frequency of backing up critical systems, a denial of service attack using these methods can have lasting effects.

Physical access can negate almost all the security that the network attempts to provide. Considering this, you must determine the level of physical access that attackers might obtain. Of special consideration are persons with authorized access to the building but who are not authorized users of the systems. Janitorial personnel and others have authorized access to many areas, but they do not have authorized system access. An attacker could pose as one of these individuals or attempt to gain access to the facilities through them.



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

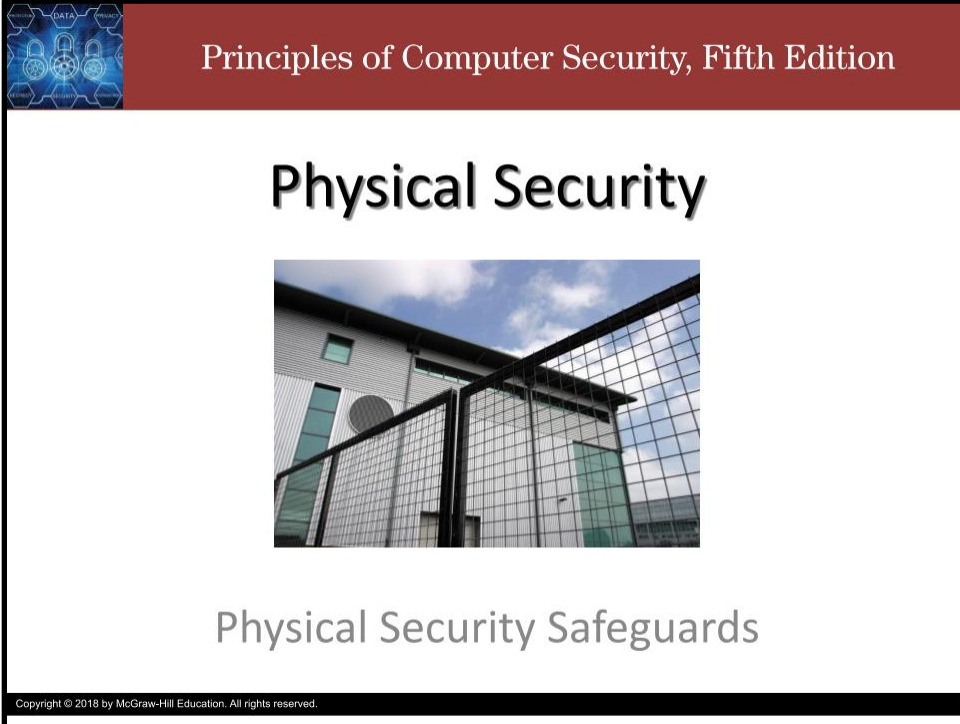
Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There is no security without physical security.

Thank you and take care.


Physical Security: Physical Security Safeguards

Slide 1



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. Below the header, the title "Physical Security" is centered in a large, bold, black font. Underneath the title is a photograph of a modern building with a glass facade and a black metal fence in the foreground. Below the photograph, the subtitle "Physical Security Safeguards" is centered in a smaller, grey font. At the bottom left of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Howdy! In this video we discuss physical security safeguards. Also, there is no security without physical security.



Principles of Computer Security, Fifth Edition

Walls and Guards

- The primary defense against a majority of physical attacks are the barriers between the assets and a potential attacker.
- Some employ private security staff to attempt to protect their assets.
- To protect the physical servers, look in all directions:

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The primary defense against a majority of physical attacks are the barriers between the assets and a potential attacker.

These include walls, fences, gates, doors.

These barriers provide the foundation upon which all other security initiatives are based, but the security must be designed carefully, as an attacker has to find only a single gap to gain access.

Some organizations employ private security staff to attempt to protect their assets.

To protect the physical servers, look in all directions:

Are doors and windows safeguarded and a minimum number of each in the server room?


Is a drop ceiling used in the server room?

Do the interior walls extend to the actual roof, raised floors, or crawlspaces?

Is there limited access to the server room, only to people who need access?

Have you made sure that there are no obvious holes in the walls?

Slide 3



Principles of Computer Security, Fifth Edition


Lighting and Signs

- Proper **lighting** is essential for physical security
 - External
 - Internal
- Signs act as informational devices and can be used in a variety of ways to assist in physical security.
 - Restricted areas
 - Visitor access

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Proper lighting is essential for physical security. This includes both External and Internal lights.

Signs act as informational devices and can be used in a variety of ways to assist in physical security, such as marking areas of restricted access and areas where visitors are allowed to be. Signs can also be deceptive. Try putting a sewage access point sign on your server room.



Principles of Computer Security, Fifth Edition

Fences

- Outside of the building's walls, many organizations prefer to have a perimeter fence as a physical first layer of defense.
- Chain-link-type fencing is most commonly used, and it can be enhanced with barbed wire.
- Anti-scale fencing, which looks like very tall vertical poles placed close together to form a fence, is used for high-security implementations that require additional scale and tamper resistance.


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Outside of the building's walls, many organizations prefer to have a perimeter fence as a physical first layer of defense.

Chain-link-type fencing is most commonly used, and it can be enhanced with barbed wire.

Anti-scale fencing, which looks like very tall vertical poles placed close together to form a fence, is used for high-security implementations that require additional scale and tamper resistance.

To increase security against physical intrusion, higher fences can be employed. A fence that is three to four feet in height will deter casual or accidental trespassers. Six to seven feet will deter a general intruder. To deter more determined intruders, a minimum height of eight feet is recommended with the addition of barbed wire or razor wire on top for extreme levels of deterrence. Other tactics include electrification, and having two fences at some short distance apart.



Principles of Computer Security, Fifth Edition

Guards and Alarms

- Provide an excellent security measure, because guards are a visible presence with direct responsibility for security
- Monitor entrances and exits and can maintain access logs of who has entered and departed the building
- Alarms serve to alert operators to abnormal conditions
 - Sensors, alarms, motion detectors, video, etc.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


Guards can provide an excellent security measure, because guards are a visible presence with direct responsibility for security

Other employees expect security guards to behave a certain way with regard to securing the facility.

Guard duties typically include monitoring entrances and exits and maintaining access logs of who has entered and departed the building

Security personnel are helpful in physically securing the machines on which information assets reside, but to get the most benefit from their presence, they must be trained to take a holistic approach to security. The value of data typically can be many times that of the machines on which the data is stored. Security guards typically are not computer security experts, so they need to be educated about the value of the data and be trained in network security as well as physical security involving users. They are the company's eyes and ears for suspicious activity, so the network security department needs to train them to notice suspicious network activity as well. Multiple extensions ringing in sequence during the night, computers rebooting all at once, or strange people parked in the parking lot with laptop computers are all indicators of a network attack that might be missed without proper training.

Alarms are also useful and serve to alert guards, operators, and others to abnormal conditions. This includes fire alarms, access alarms, environmental alarms, motion alarms, and anything else whose state is security critical.



Principles of Computer Security, Fifth Edition

Physical Access Controls and Monitoring

- **Physical access control** refers to the control of doors and entry points.
 - Physical locks
 - Layered access systems
 - Electronic access
 - Control systems closed circuit television (CCTV) systems

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


Physical access control refers to the control of doors and entry points.

This includes layered access, locks, electronic access control systems, and CCTV systems.

Slide 7

Principles of Computer Security, Fifth Edition

Layered Access



Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Layered access is an important concept in security. It is often mentioned in conversations about network security perimeters, but in this module it relates to the concept of physical security perimeters. Layered access means defense in depth.

To help prevent an attacker from gaining access to important assets, place them inside multiple perimeters.

For example, servers should be placed in a separate secure area, ideally with a separate authentication mechanism.

Access to the server room should be limited to staff with a legitimate need to work on the servers.


The area surrounding the server room should also be limited to people who need to work in that area.

The more layers, the more tedious it is for staff to move between them, but that tedium is just a song of security.

Slide 8

Principles of Computer Security, Fifth Edition

Locks



Lockpicking tools

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Although locks have been used for hundreds of years, their design has not changed much: a metal “token” is used to align pins in a mechanical device.

Only when the correct token, called the key, is inserted into the lock will the mechanism unlock.

High security locks are typically found in commercial applications.

They are designed to resist picking and drilling.

High-security locks typically have some form of key control.

Key control refers to the restrictions placed on making a copy of the key. For most residential locks, a trip to the hardware store will allow you to make a copy of the key. Key control locks use patented keyways that can only be copied at a locksmith, who will keep records on authorized users of a particular key.


They also employ mechanical means to resist a bump key attack, which is a very low-tech but surprisingly effective tactic wherein the locking mechanism is subjected to abrupt displacement, i.e. bumped, which sometimes gets lucky in also bumping the mechanism into the unlocked state.

There are many different kinds of locks in many different strengths for many different purposes. Rare is the lock which is both cheap and good. But, neither are all expensive locks good. And, a lock is not enough. If the lock can be bypassed, then it doesn't matter if it really is unpickable. If it can be bypassed, it doesn't need to be picked, it can be ignored

Slide 9

Principles of Computer Security, Fifth Edition


A high-security lock and its key



<https://www.youtube.com/watch?v=4fh6IHCr7uo>

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

This picture is a little ironic. The title is “A high security lock and its key”. The main irony is that, by taking a picture of the key, especially such a nice side-on picture like this, that particular lock is no longer secure since anyone who gets this image could make a reliable copy of the key. Another minor irony is that Medeco locks are marketed as high security and sold for a commensurate price, but despite their promotion by the company as being the “lock that cannot be picked”, they are in fact pickable by an experienced lockpicker.



Principles of Computer Security, Fifth Edition

Doors

- Doors to secured areas should have characteristics to make them less obvious.
 - Should be self-closing; have no hold-open feature; should trigger alarms if they are forcibly opened or have been held open for a long period
- There are two door design methodologies:
 - Fail-safe – the door is unlocked should power fail.
 - Fail-secure – the system will lock the door when power is lost; can also apply when door systems are manually bypassed.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Doors to secured areas should have characteristics to make them less obvious.

They should be self-closing; have a no hold-open feature; and should trigger alarms if they are forcibly opened or have been held open for a long period.

There are two door design methodologies:


Fail-safe, in which the door is unlocked should power fail. So, the door fails into a safe state: nobody gets locked in in the event of a fire.

Fail-secure, in which the system will lock the door when power is lost; this can also apply when door systems are manually bypassed. In this mode, the door fails into a secure state: nobody gets in.

Some doors should be fail-safe and some doors should be fail-secure.


There are other considerations for securing doors, such as putting the hinges on the secure side and blocking access around the sides, top, and bottom of the door. Deviant Ollam has a very good talk about doors that I highly encourage you to watch. It's called the search for the perfect door.

Slide 11



Principles of Computer Security, Fifth Edition

Cameras



Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Closed circuit television (CCTV) cameras are similar to door control systems.

They can be very effective, but implementation is an important consideration.

Traditional cameras are analog-based and require a video multiplexer to combine all the signals and make multiple views appear on a monitor.

The use of CCTV cameras for surveillance purposes dates back to at least 1961, when cameras were installed in the London Transport train station. The development of smaller and more sophisticated camera components and decreasing prices for the cameras have caused a boom in the CCTV industry since then.

CCTV cameras can be used to monitor a workplace for security purposes. These systems are commonplace in banks and jewelry stores, places with high-value merchandise that is attractive to thieves. As the expense of these systems dropped, they became practical for many more industry segments.

IP-based cameras are standalone units viewable through a web browser.

IP-based systems add useful functionality, such as the ability to check on the building from the Internet.

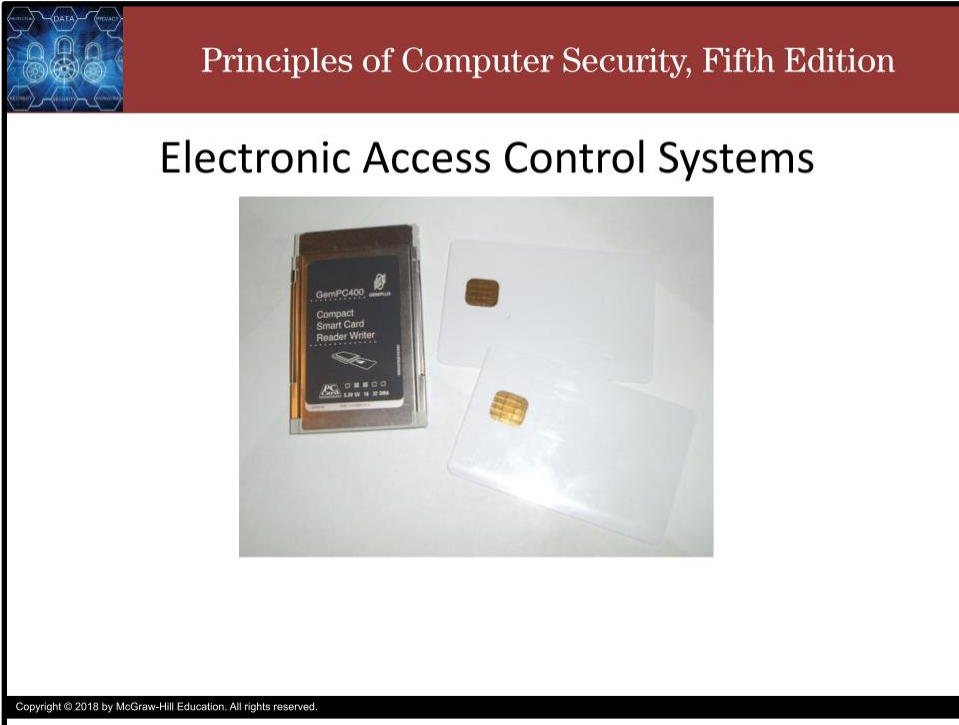
This network functionality, however, makes the cameras subject to normal IP-based network attacks.

A DoS attack launched at the CCTV system just as a break-in is occurring is the last thing that anyone would want (other than the criminals). For this reason, IP-based CCTV cameras should be placed on their own separate network that can be accessed only by security personnel. The same physical separation applies to any IP-based camera infrastructure. Older time-lapse tape recorders are slowly being replaced with digital video recorders. While the advance in technology is significant, be careful if and when these devices become IP-enabled, since they will become a security issue, just like everything else that touches the network.

If you depend on the CCTV system to protect your organization's assets, carefully consider camera placement and the type of cameras used.

Different iris types, focal lengths, and color or infrared capabilities are all options that make one camera superior to another in a specific location.

Slide 12



Principles of Computer Security, Fifth Edition

Electronic Access Control Systems

GemPC400
Compact
Smart Card
Reader/Writer

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Access tokens are frequently used for physical access solutions, just as your house key is a basic physical access token that allows you access into your home.

In the parlance of authentication factors, access tokens are an example of the “something you have” factor.

Although keys have been used to unlock devices for centuries, they do have several limitations. Keys are paired exclusively with a lock or a set of locks, and they are not easily changed. It is easy to add an

authorized user by giving the user a copy of the key, but it is far more difficult to give that user selective access unless that specified area is already set up as a separate key. It is also difficult to take away access from an individual or key holder, which usually requires a rekey of the whole system.

In many businesses, physical access authentication has moved to contactless radio frequency cards and proximity readers. When passed near a card reader, the card sends out a code using radio waves. The reader picks up this code and transmits it to the control panel. The control panel checks the code against the reader from which it is being read and the type of access the card has in its database. One of the advantages of this kind of token-based system is that any card can be deleted from the system without affecting any other card or the rest of the system. The RFID-based contactless entry card shown here is a common form of this token device employed for door controls and is frequently put behind an employee badge. In addition, all doors connected to the system can be segmented in any form or fashion to create multiple access areas, with different permissions for each one. The tokens themselves can also be grouped in multiple ways to provide different access levels to different groups of people. All of the access levels or segmentation of doors can be modified quickly and easily if building space is retasked. Newer technologies are adding capabilities to the standard token-based systems.

Smart card technology is now part of a governmental standard for physical and logical authentication.

Personal Identity Verification, or PIV, cards adhere to the FIPS 201 standard.

They include a cryptographic chip and connector, and a contactless proximity card circuit.


The cards also have a printed photo and name on front

Biometric data can be stored, providing an additional authentication factor, and if the PIV standard is followed, several forms of identification are needed to get a card.

The primary drawback of token-based authentication is that only the token is being authenticated.


Therefore, the theft of the token could grant anyone who possessed the token access to what the system protects.

Slide 13



Principles of Computer Security, Fifth Edition

Biometrics



Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Biometrics use the measurements of certain biological factors to identify one specific person from others.

These factors are based on parts of the human body that are unique.

So, biometrics is a “what you are” factor.

The most well-known of these supposedly unique biological factors is the fingerprint.

However, many other biological factors can be used, such as the retina or iris of the eye, the geometry of the hand, and the geometry of the face. When these are used for authentication, there is a two-part process: enrollment and then authentication. During enrollment, a computer takes the image of the biological factor and reduces it to a numeric value. When the user attempts to authenticate, their feature is scanned by the reader, and the computer compares the numeric value being read to the one stored in the database. If they match, access is allowed. Since these physical factors are supposed to be unique, theoretically only the actual authorized person would be allowed access.

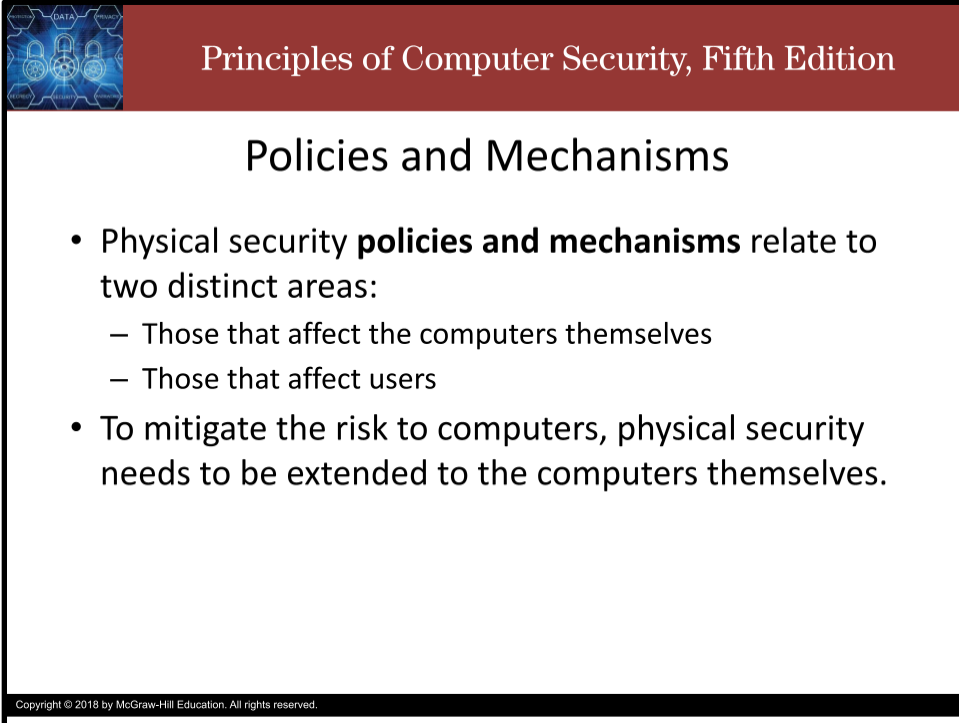
In the real world, however, the theory behind biometrics breaks down. Tokens that have a digital code work very well because everything remains in the digital realm. A computer checks your code, such as 123, against the database; if the computer finds 123 and that number has access, the computer opens the door. Biometrics, however, take an analog signal, such as a fingerprint or a face, and attempt to digitize it, and it is then matched against the digits in the database. The problem with an analog signal is

that it might not encode the exact same way twice. For example, if you came to work with a bandage on your chin, would the face-based biometrics grant you access or deny it?

Engineers who designed these systems understood that if a system was set to exact checking, an encoded biometric might never grant access since it might never scan the biometric exactly the same way twice. Therefore, most systems have tried to allow a certain amount of error in the scan, while not allowing too much.

For biometric authentication to work properly, and also be trusted, it must minimize the existence of both false positives and false negatives. To do that, a balance between precision and error must be created so that the machines allow a little physical variance - but not too much.

Slide 14



Principles of Computer Security, Fifth Edition

Policies and Mechanisms

- Physical security **policies and mechanisms** relate to two distinct areas:
 - Those that affect the computers themselves
 - Those that affect users
- To mitigate the risk to computers, physical security needs to be extended to the computers themselves.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Physical security policies and procedures relate to two distinct areas:

Those that affect the computers themselves

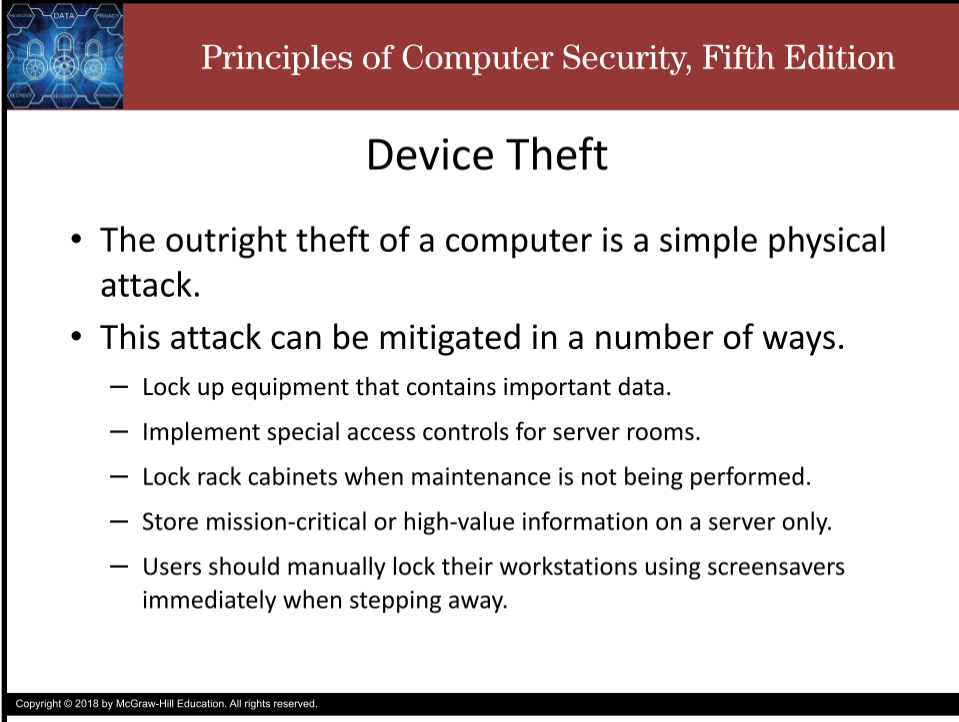
And those that affect users

To mitigate the risk to computers, physical security needs to be extended to the computers themselves.

A policy's effectiveness depends on the culture of an organization and the enforcement of the policy. Every policy should be associated with a mechanism, some functional procedure that is designed to enforce the policy.

For example, the policy that no external media should be inserted into a machine is enforced by the mechanisms of disabling autoplay, removing drivers for USB and optical disc readers, disabling booting from removable media, removing or destroying access ports, et cetera.

Slide 15



Principles of Computer Security, Fifth Edition

Device Theft

- The outright theft of a computer is a simple physical attack.
- This attack can be mitigated in a number of ways.
 - Lock up equipment that contains important data.
 - Implement special access controls for server rooms.
 - Lock rack cabinets when maintenance is not being performed.
 - Store mission-critical or high-value information on a server only.
 - Users should manually lock their workstations using screensavers immediately when stepping away.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The outright theft of a computer is a simple physical attack that can be extremely damaging.

Insurance can cover the loss of the physical equipment, but this can do little to get a business up and running again quickly after a theft.

This attack can be mitigated in a number of ways.

Lock up equipment that contains important data.

Implement special access controls for server rooms.

Lock rack cabinets when maintenance is not being performed.

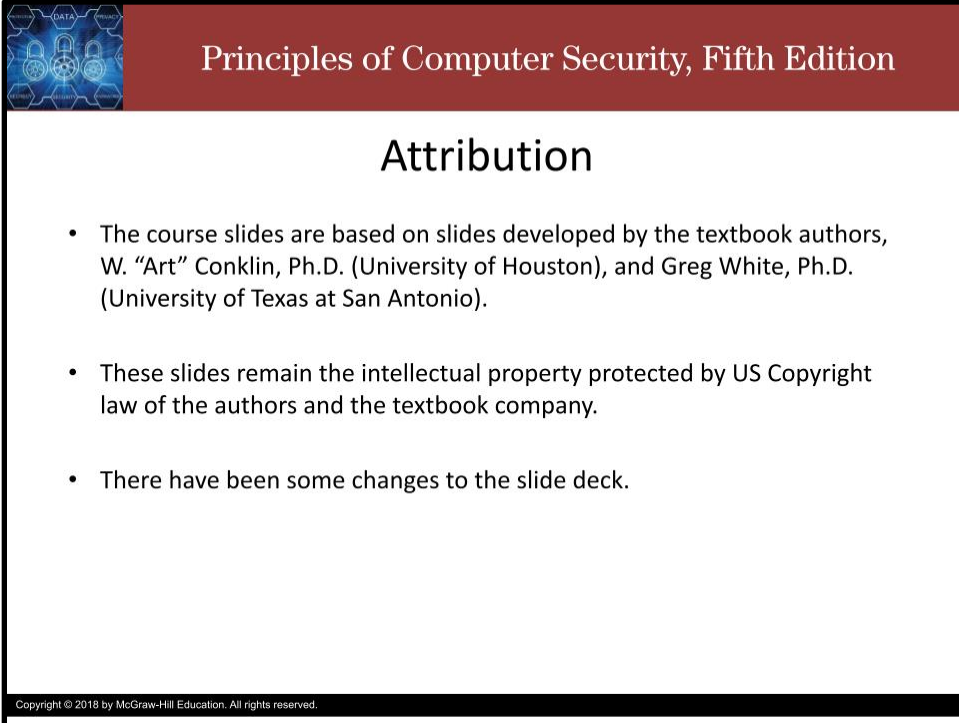
From a data standpoint, mission-critical or high-value information should be stored on a server only.

This can mitigate the risk of a desktop or laptop being stolen for the data it contains. Loss of laptops has been a common cause of information breaches.

Although use of a self-locking screensaver is a good policy, setting it to lock at any point less than 10 to 15 minutes after becoming idle is often considered a nuisance and counterproductive to active use of

the computer on the job as the computer will often lock while the employee is still actively using the computer. Thus, computers typically sit idle for at least 15 minutes before automatically locking under this type of policy. An attacker only needs to be lucky enough to catch a machine that has been left alone for a few minutes. Users can perform one of the most simple, yet important, information security tasks: lock a workstation immediately before they step away from it.

Slide 16



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. To the left of the header is a small graphic of a blue padlock surrounded by hexagonal patterns. The main content area is white with the title "Attribution" centered. Below the title is a bulleted list of three points. At the bottom of the slide, there is a small black bar containing the copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

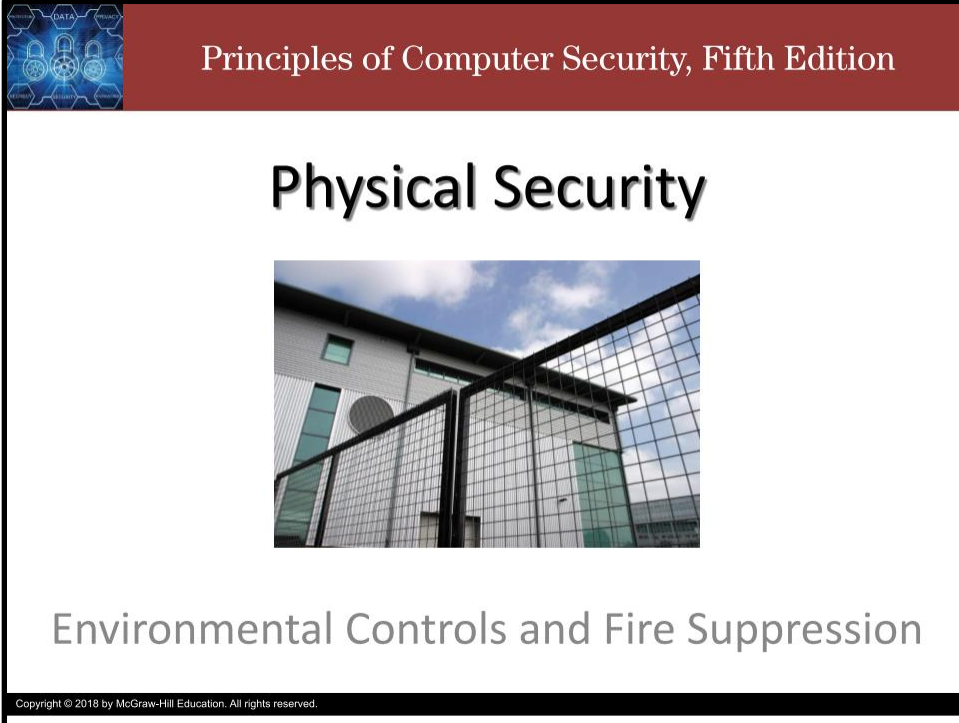
Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There is no security without physical security.

Thank you and take care.


Physical Security: Environmental Controls and Fire Suppression

Slide 1



Principles of Computer Security, Fifth Edition


Physical Security



Environmental Controls and Fire Suppression

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video we briefly discuss environmental controls and fire suppression.



Principles of Computer Security, Fifth Edition

Environmental Controls


- Sophisticated environmental controls are needed for current data centers
 - Heating ventilating and air conditioning (HVAC) systems are critical; temperature should be maintained at 70–74°F.
 - Hot aisle/cold aisle layout can alleviate increased data center density.
 - Rising copper prices have made HVAC systems the targets for thieves, and general vandalism can result in costly downtime.
 - Proper security is needed to prevent a physical DoS attack.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

While the confidentiality of information is important, so is its availability. Sophisticated environmental controls are needed for current data centers. Servers can generate large levels of heat, and managing the heat is the job of the environmental control.

Controlling a data center's temperature and humidity is important to keeping servers running. Heating ventilating and air conditioning (HVAC) systems are critical for keeping data centers cool, because typical servers put out between 1000 and 2000 BTUs of heat. The temperature of a data center should be maintained at less than about 70 degrees Fahrenheit. If the temperature is too high, it may cause equipment damage.

Multiple servers in a confined area can create conditions too hot for the machines to continue to operate. This problem is made worse with the advent of blade-style computing systems and with many other devices shrinking in size. While physically smaller, they tend to still expel the same amount of heat. This is known as increased data center density—more servers and devices per rack, putting a greater load on the cooling systems. This encourages the use of a hot aisle/cold aisle layout. A data center that is arranged into hot and cold aisles dictates that all the intake fans on all equipment face the cold aisle, and the exhaust fans all face the opposite aisle. The HVAC system is then designed to push cool air underneath the raised floor and up through perforated tiles on the cold aisle. Hot air from the hot aisle is captured by return air ducts for the HVAC system. The use of this layout is designed to control airflow, with the purpose being never to mix the hot and cold air. This requires the use of blocking plates and side plates to close open rack slots. The benefits of this arrangement are that cooling is more efficient and can handle higher density.



Principles of Computer Security, Fifth Edition

Fire Suppression

- The ability to respond to a fire quickly and effectively is critical to the long-term success of any organization.
- Addressing potential fire hazards and vulnerabilities has long been a concern of organizations in their risk analysis process.
- The goal obviously should be never to have a fire, but in the event that one does occur, it is important that mechanisms are in place to limit the damage the fire can cause.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

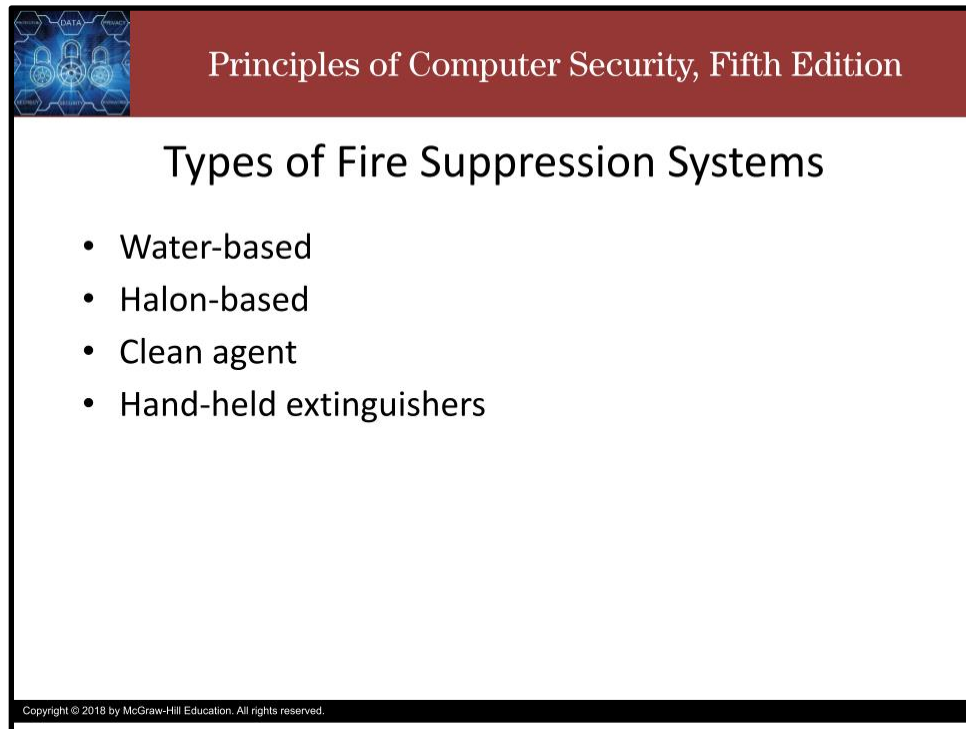
The ability to respond to a fire quickly and effectively is critical to the long-term success of any organization.

Addressing potential fire hazards and vulnerabilities is an important part of the risk analysis process.

The goal obviously should be to never have a fire, but in the event that one does occur, it is important that mechanisms are in place to limit the damage the fire can cause.

According to the Fire Suppression Systems Association (www.fssa.net), 43 percent of businesses that close as a result of a significant fire never reopen. An additional 29 percent fail within three years of the event.

Slide 4



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. To the left of the header is a small graphic of a blue padlock surrounded by hexagons and the word "DATA". The main content area is white with the title "Types of Fire Suppression Systems" in black. Below the title is a bulleted list of four items. At the bottom of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Principles of Computer Security, Fifth Edition

Types of Fire Suppression Systems

- Water-based
- Halon-based
- Clean agent
- Hand-held extinguishers

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Water-based systems have long been and still are the primary tool to address and control structural fires.

Electrical equipment does not react well to large applications of water so it is important for operators to know what to do with equipment if subjected to a water based sprinkler system.

Since water is so destructive to electronic equipment, not only because of the immediate problems of electronic shorts to the system but also because of longer-term corrosive damage water can cause, alternative fire suppression methods have been sought.

Even though halon production was banned in 1994, a number of halon-based systems still exist today. They were originally popular because halon will mix quickly with the air in a room and will not cause harm to computer systems.

Halon is dangerous to humans, especially when subjected to extremely hot temperatures (such as might be found during a fire), when it can degrade into other toxic chemicals. As a result of these dangers, and also because halon has been linked with the issue of ozone depletion, halon is banned in new fire suppression systems.

While the Environmental Protection Agency (EPA) has mandated no further production of halon, but existing systems were not required to be destroyed. Replacing the halon in a discharged system, however, will be a problem, since only existing stockpiles of halon may be used and the cost is becoming prohibitive. For this reason, many organizations are switching to alternative solutions.

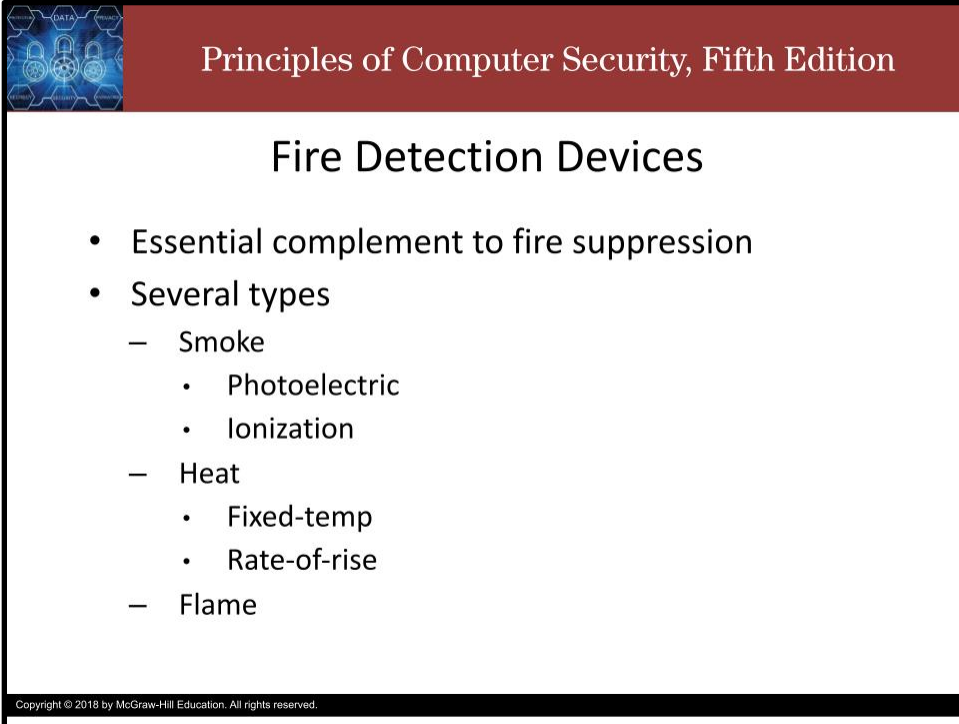
Clean-agent fire suppression systems not only provide fire suppression capabilities, but also protect the contents of the room, including people, documents, and electronic equipment. They use gasses such as carbon dioxide or Argon.

Carbon dioxide displaces oxygen so that the amount of oxygen remaining is insufficient to sustain the fire. It also provides some cooling in the fire zone and reduces the concentration of “gasified” fuel.

Argon systems extinguish fire by lowering the oxygen concentration to about 12.5%, below the 15 percent level required for combustible items to burn, but higher than the 10% below which humans suffocate too quickly.

If a fire can be caught and contained before the automatic systems discharge, it can mean significant savings to the organization in terms of both time and equipment costs. Including the recharging of the automatic system. Handheld extinguishers are common in offices, but the correct use of them must be understood or disaster can occur. There are different kinds of fires and different kinds of extinguishers to use for each fire type. Using the wrong type can result in more damage rather than less.

Slide 5



Principles of Computer Security, Fifth Edition

Fire Detection Devices

- Essential complement to fire suppression
- Several types
 - Smoke
 - Photoelectric
 - Ionization
 - Heat
 - Fixed-temp
 - Rate-of-rise
 - Flame

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Fire detectors are an essential complement to fire suppression systems and devices.

Detectors may be able to detect a fire in its very early stages.

There are several types of fire detectors.

One type detects smoke.

Another type is activated by heat.

A third type is flame activated.

There are two kinds of smoke detectors.

A photoelectric detector is good for potentially providing advance warning of a smoldering fire. This type of device monitors an internal beam of light. If something degrades the light, for example by obstructing it, the detector assumes it is something like smoke and the alarm sounds.

An ionization detector uses an ionization chamber and a small radioactive source to detect fast-burning fires.

Combinations of both are also possible.


Heat-activated detectors also come in two varieties.

Fixed-temperature or fixed-point devices activate if the temperature in the area ever exceeds some predefined level.

Rate-of-rise or rate-of-increase temperature devices activate when there is a sudden increase in local temperature that may indicate the beginning stages of a fire. Rate-of-rise sensors can provide an earlier warning but are also responsible for more false warnings.

A third type of detector is flame activated. This type of device relies on the flames from the fire to provide a change in the infrared energy that can be detected. Flame-activated devices are generally more expensive than the other two types but can frequently detect a fire sooner.

Slide 6



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

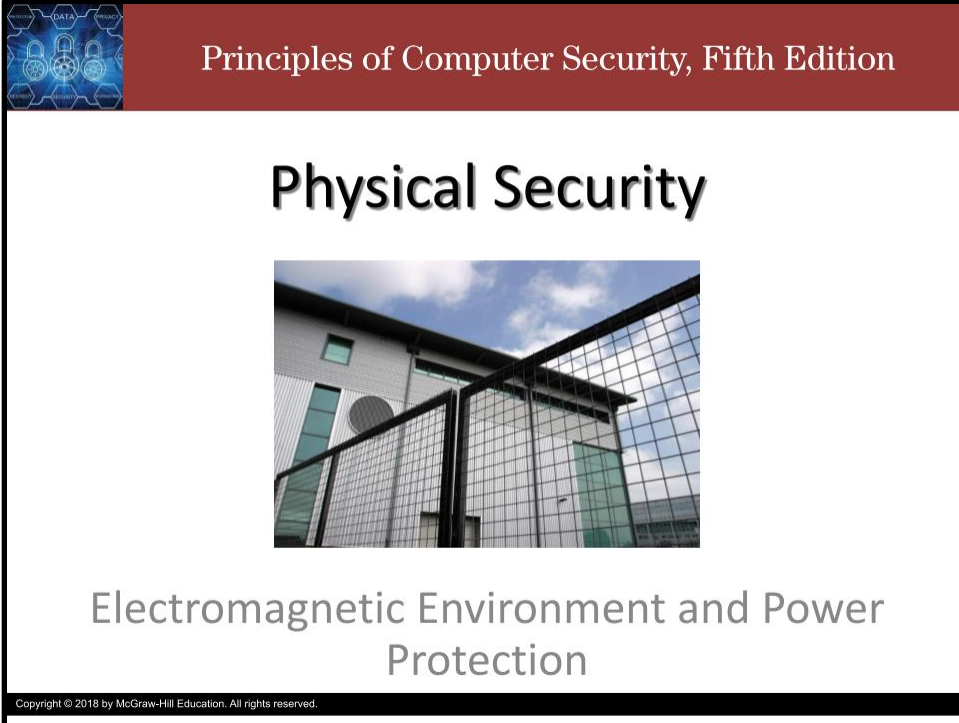
Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There is no security without physical security.

Thank you and take care.

Physical Security: Electromagnetic Environment and Power Protection


Slide 1



The image shows the cover of the book "Principles of Computer Security, Fifth Edition". The top section is a dark red banner with the text "Principles of Computer Security, Fifth Edition" in white. Below this, the title "Physical Security" is written in a large, bold, black font. Underneath the title is a photograph of a modern building with a glass facade and a metal security fence in the foreground. At the bottom of the cover, the subtitle "Electromagnetic Environment and Power Protection" is written in a smaller, grey font. A small icon in the top left corner of the cover depicts a blue digital interface with various security-related symbols like a padlock, a gear, and a shield. A copyright notice is visible at the very bottom of the cover.

Principles of Computer Security, Fifth Edition


Physical Security



Electromagnetic Environment and Power Protection

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we discuss the electromagnetic environment and power protection.



Principles of Computer Security, Fifth Edition

Electromagnetic Environment

- Electromagnetic interference, or EMI is the disturbance on an electrical circuit caused by that circuit's reception of electromagnetic radiation.
- EMI is grouped into two general types:
 - Narrowband EMI has a small frequency band.
 - Broadband EMI covers a wider array of frequencies.
- The Federal Communications Commission regulates products that produce EMI.
 - **TEMPEST**, also known as Van Eck emissions, is technology that attempts to keep EMI radiation in the circuitry.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Electromagnetic interference, or EMI, can plague any type of electronics, but the density of circuitry in the typical data center can make it a haven for EMI.

Magnetic radiation enters the circuit by induction, where magnetic waves create a charge on the circuit. The amount of sensitivity to this magnetic field depends on a number of factors, including the length of the circuit, which can act like an antenna.

EMI is grouped into two general types: Narrowband and broadband.

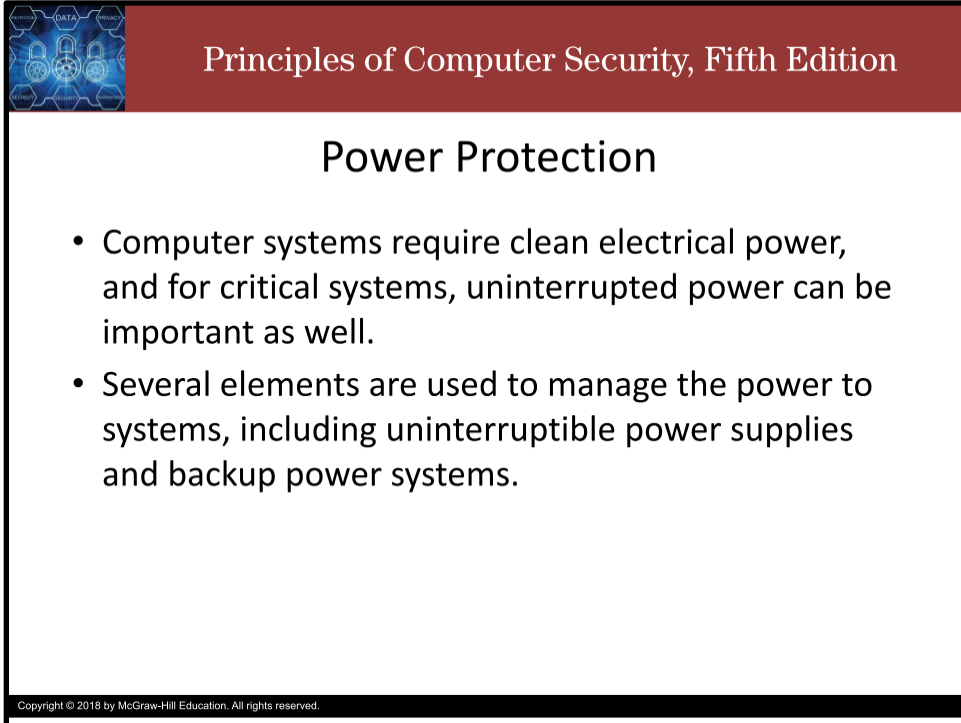
Narrowband EMI is, by its nature, electromagnetic energy with a small frequency band and, therefore, typically sourced from a device that is purposefully transmitting in the specified band.

Broadband EMI covers a wider array of frequencies and is typically caused by some type of general electrical power, such as power lines or electric motors.

In the United States, the Federal Communications Commission has responsibility for regulating products that produce EMI and has developed a program for equipment manufacturers to adhere to standards for EMI immunity. Modern circuitry is designed to resist EMI. Cabling is a good example; the twist in unshielded twisted pair, or Category 6/6a, cable is there to reduce EMI. EMI is also controlled by metal computer cases that are grounded; by providing an easy path to ground, the case acts as an EMI shield. A bigger example would be a Faraday cage or Faraday shield, which is an enclosure of conductive material that is grounded. These can be room sized or built into a building's construction; the critical element is that there is no significant gap in the enclosure material. These measures can help shield EMI, especially in high radio frequency environments.

While we have talked about the shielding necessary to keep EMI radiation out of your circuitry, there is also technology to try and help keep it in. Known by some as TEMPEST, it is also known as Van Eck emissions. A computer's monitor or LCD display produces electromagnetic radiation that can be remotely observed with the correct equipment. TEMPEST was the code word for an NSA program to secure equipment from this type of eavesdropping. While some of the information about TEMPEST is still classified, there are guides on the Internet that describe protective measures, such as shielding and electromagnetic-resistant enclosures. A company has even developed a commercial paint that offers radio frequency shielding.

Slide 3



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. To the left of the header is a small graphic with the word "DATA" and several padlock icons. The main content area is white with a black border. The title "Power Protection" is centered in black. Below the title is a bulleted list with two items. At the bottom of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Principles of Computer Security, Fifth Edition


Power Protection

- Computer systems require clean electrical power, and for critical systems, uninterrupted power can be important as well.
- Several elements are used to manage the power to systems, including uninterruptible power supplies and backup power systems.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Computer systems require clean electrical power, and for critical systems, uninterrupted power can be important as well.

Several elements are used to manage the power to systems, including uninterruptible power supplies and backup power systems.



Principles of Computer Security, Fifth Edition

Uninterruptible Power Supply (UPS)

- Used to protect against short duration power failures.
- Two types:
 - Online - in continuous use because the primary power source goes through it to the equipment.
 - Standby - has sensors to detect power failures. If there is a power failure, the load will be switched to the UPS.


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

An uninterruptible power supply (UPS) is used to protect against short duration power failures.

There are two types of UPSs: online and standby.

An online UPS is in continuous use because the primary power source goes through it to the equipment. It uses AC line voltage to charge a bank of batteries. When the primary power source fails, an inverter in the UPS will change DC of the batteries into AC.

A standby UPS has sensors to detect power failures. If there is a power failure, the load will be switched to the UPS. It stays inactive before a power failure, and takes more time than an online UPS to provide power when the primary source fails.



Principles of Computer Security, Fifth Edition

Backup Power and Cable Shielding

- Backup power sources protect against long-duration power failure
- Voltage regulator and line conditioner protect against unstable power supply and spikes
- Proper grounding is essential
- Cable shielding to avoid interference
- Power line monitoring warns of brownouts or spikes
- Emergency Power Off (EPO) for quick shutoff
- Keep electrical cables away from powerful electrical motors and lighting
- Fluorescent lighting can cause radio frequency interference

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Backup power sources, such as a motor generator, another electrical substation, and so on, are used to protect against a long-duration power failure.

A voltage regulator and line conditioner are used to protect against unstable power supply and spikes.

Proper grounding is essential for all electrical devices to protect against short circuits and static electricity.

In more sensitive areas, cable shielding can be employed to avoid interference.


Power line monitoring can be used to detect changes in frequency and voltage amplitude, warning of brownouts or spikes.

An emergency power off (EPO) switch can be installed to allow for the quick shutdown of power when required.

To prevent electromagnetic interference and voltage spikes, electrical cables should be placed away from powerful electrical motors and lighting.

Another source of power-induced interference can be fluorescent lighting, which can cause radio frequency interference.

Slide 6



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There is no security without physical security.

Thank you and take care.