Physical & Facility Security

Surveillance

- CCTV
  - Wired
  - Wireless
- PTZ
- Heat sensor
- Sound

Door Locks

Now, door locks, again, come in many different varieties. Some use a key. Some use a PIN number. Some use wireless signals. And some even use biometrics, like a thumbprint, to open and shut the lock. Now, better security does exist as you move up the ladder, but so does cost.

At the bottom of the ladder, we have a basic office door lock. Another type of door lock is known as a cipher lock. Now, a cipher lock provides excellent protection using a mechanical locking mechanism with push buttons that are numbered that require a person to enter the correct combination in order to open that door. These are often used on server rooms, network closets, and other high security locations. Next, we have electronic access systems.

These electronic access control systems have become quite popular in recent years as the price has been falling. These can use an RFID reader to scan an employee's badge and grant them access based on those credentials. Some of these will actually be combined with a badge and a PIN number, to create multi-factor authentication that allows for logging and auditing, as well. In addition to these door locks, we also might use something called a mantrap.

Now, a mantrap is an area between two doorways that holds people until they're identified and authenticated. Sometimes, these are automated, like using that electronic badge and PIN system we talked about. And sometimes, they are manned by security personnel who actually look at your ID badge to verify that you are who you claim to be.

Biometric Readers

It’s your eye, it’s your fingerprint, it’s your voice, it's something that is innately part of your ability and part of your person. Now, when we talk about fingerprints, fingerprints have become a very common identification system. At this point, it's even gone beyond door locks, and it's now integrated into our smartphones and our laptops for log in. Now, the newest iPhones have done away with touch ID in favor of face ID. So, if you have an iPhone X or newer, they actually have the front-facing camera scan your face and measure the distance between different areas of your face to uniquely identify you. The crossover error rate uses a measure of the effectiveness of a given biometrics system. So, when you're looking to purchase one, you can use this as a factor in your decision-making process. You want one that doesn't have a huge error to the positive side or a huge error to the negative side. If you can get one that has a good crossover error rate, that's going to make sure that your people are getting authenticated when you should be and rejected when they should be.

Fire Suppression

Now, there are three types of fire suppression that we have to discuss for the Security+ exam. There's:

1. handheld fire extinguishers
2. sprinkler systems
3. special hazard protection systems that we use especially in our server rooms

Fires are broken down into five different categories: Class A, B, C, D, and K.

A

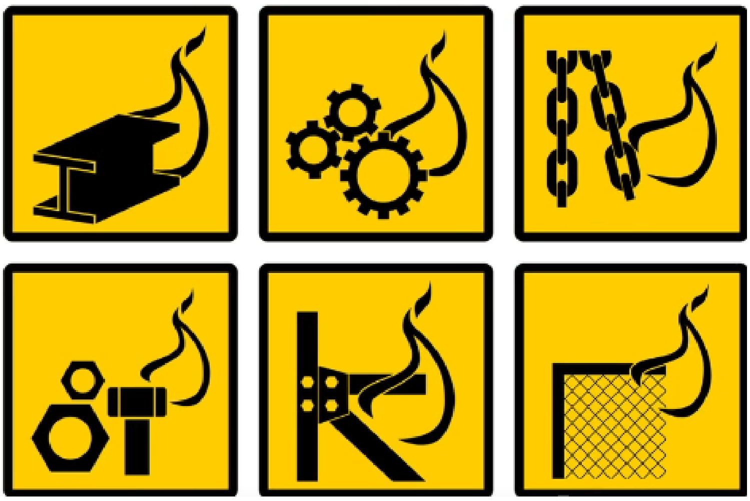
Ordinary combustibles : wood, paper, rubber, fabrics, and many plastic

B

Flammable Liquids and Gases : gasoline, oils, paint, lacquer, and tar

C	Fire involving Live Electrical Equipment

D	Combustible metals or Combustible Metal Alloys



K
Fire in Cooking Appliance that involve
Combustible Cooking Media :
Vegetable or Animal Oils and Fats

The first is an ABC extinguisher, which uses dry chemicals to put out fires. If possible, you should avoid using this on computer equipment, though, because the dry chemical is corrosive and destructive to computer and electrical components.

INSTRUCTIONS
1. PULL PIN, HOLD UNIT UPRIGHT
2. FREE HOSE. STAND BACK 8 FEET AIM AT BASE OF FIRE
3. SQUEEZE LEVER AND SWEEP SIDE TO SIDE
ABC

The second and probably most common type you're going to see is called a BC extinguisher, which is used on B and C fires. This most often uses CO2 to put out a fire. This is useful for both gas fires, Class B, and electrical fires, Class C, and it's also safe to use on computers.

CO2
FIRE EXTINGUISHER
2 KG CARBON DIOXIDE
1 USE UPRIGHT. REMOVE SAFETY PIN.
2 AIM NOZZLE AT BASE OF FIRE.
3 SQUEEZE LEVERS.
DO NOT USE OUTSIDE TEMPERATURE RANGE
PROTECT THE HAND AGAINST COOLING DURING USE

The third type is a yellow extinguisher and these bottles are used for Class D or metal fires. These are less common but you should be aware of where they are in case you need one inside your organisation.

HVAC

Over time, though, the room will become hotter and hotter and hotter if we didn't have a good HVAC system to cool it down. Now, to best circulate the air around the server room, you should design it with hot and cold aisles. This allows all of the front of the server racks to be facing each other, making designated cold aisles where you'll be working, while expending all of their heat out the rear of their cabinets to what we call the designated hot aisle. Now, by focusing on the hot and cold aisles, this allows us to set up better ventilation systems, using our raised floors in a server room, and dissipating that heat much more effectively. Now, another use of an HVAC system is to maintain the right humidity level in that server room. After all, if there's too little humidity, static electricity can build up and cause electrostatic discharge that can damage your components. Now, many HVAC systems are also connected to your organization's ICS, or industrial control systems, or your SCADA systems, your supervisory control and data acquisition systems. This is a specialized network that's going to control all of your manufacturing and facility systems.

Shielding

First, to reduce EMI in your network cables, you should be opting for STP, or Shielded Twisted Pair cables, instead of using unshielded twisted pair, or UTP. These cables do cost a little bit more money, but they do provide a nice foil wrapping around the twisted pairs that's inside the cable itself. You need to make sure you put some shielding around that HVAC because it's basically a large motor or a large generator, and anything with a large motor or generator is going to put off EMI. Another type of shielding used in high-security environments is the use of a Faraday cage.

Now, this type of shielding is usually installed around the entire room so that electromagnetic energy cannot get into the room or get out of it. In fact, the U.S. government created a standard called the TEMPEST standard that certifies facilities that meet its stringent requirements for shielding. If your organisation is going to work for the U.S. government as a contractor, your facility may have undergone this level of security inspection to determine if your facility has the appropriate shielding to ensure that it isn't subject to emissions or interference. These TEMPEST-certified buildings are usually used to process classified, secret, and top secret government information and so they want to make sure nothing is leaking in and nothing is leaking out.
Another side benefit of a TEMPEST-certified building is that it's resistant to the effects of an electromagnetic pulse. An EMP is a high-energy pulse that could otherwise destroy the electronics that are within range of that EMP. And so, this is a

nice side benefit that we get if we happen to work inside a TEMPEST-certified building.

Vehicular Vulnerabilities

These systems all have to connect some way. And so we take all these different subsystems, like the HVAC and the steering and the cruise control and all of these different functions, and they all get passed over what's called a Controller Area Network or a CAN.

Now, when you talk about a Controller Area Network, this is a digital serial data communications network that's used within a vehicle. Now, if you look at an airplane, for instance, they have miles and miles of cabling and all that cabling connects together. That is a CAN. In your car, the same thing, just not as large or not as big of an extent.

Well, they have to get to the CAN bus and there's really three ways to do it.

One is they can do it locally. They can attach an exploit locally to the OBD-II. Now you might think, well, that means you have to be in the car with you. Well, not necessarily. You can create a plug that plugs into the OBD-II. And most OBD-IIs are underneath the dashboard where somebody doesn't see it visibly. So let's say you went to a local restaurant and you actually handed your car off to some valet. While you're in there, he could have a plugged in something to the OBD-II, and now he has a connection that they can run an exploit from.

Now, another thing they can do is they can actually exploit over the onboard cellular. If your car has a cell modem built into it, that means you have a connection to the outside world, which means they have a connection to you. Now, most cars have two networks. They have the entertainment network and the vehicular CAN network and they are separated. For instance, I have a Tesla that I drive. It has a cell modem built in that runs through the entertainment system, so I can listen to the radio, I can listen to songs over Pandora and Spotify and things like that. That is one system. And then there's the system that controls the driving of the car. They've built that as two separate systems because of this vulnerability. But if you have a manufacturer who doesn't have a clear separation of the two, that could be an issue.

And then the third, you can have an exploit over the onboard wifi. Again, a lot of cars have onboard wifi as a feature that was added within the last five to 10 years. And so if I'm driving close to you and I can reach your wifi, and there's a link between that wifi and the CAN, I can then get messages into your can and cause issues. So again, this isn't a big area that we as cyber security analysts are really going to work in, except to know that this vulnerability exists. For the exam, if you can remember these three vulnerabilities, you'll do fine when it comes to vehicle questions.

IOT Vulnerabilities

It can be things like trains, planes, and automobiles. It can be shopping carts. It can be your Smart TV. It can be your cell phone. Pretty much anything that can connect to the Internet could be considered an Internet of Things. For instance, there's some refrigerators out there right now that have the ability of connecting to the Internet and using things like Alexa to be able to add things or take things away from your shopping list. All of that is part of the Internet of Things. So, when we define the Internet of Things, or IoT, we're really just talking about a group of objects, and they could be electronic or not, and they all have to be connected to the wider Internet by using embedded electronic components. But the biggest problem with these things is they're not always secure, and security is most often an afterthought to convenience when we start talking about smart devices. Now, most of our smart devices are going to use an embedded version of Linux or Android as their operating system. And so, because they have Linux or Android as their operating system, they are vulnerable to attack. If there's a Linux vulnerability out there and you're using a Linux version on that smart device, and that vulnerability matches, it can actually attack your Smart speaker, for instance. And so, these are things you have to think about as you start looking at your network, because if they're connected to your network, 'cause you have a Smart TV in the conference room, that could be an attack vector for somebody to get into your network. And that is one of the most common places I see people getting into a network through, is things like smart devices that are now connected to the corporate network.

Embedded system vulnerabilities

Now, when we talk about an embedded system, this is a computer system that is designed to perform a specific and dedicated function. Now, oftentimes, when we talk about an embedded system, we're talking about things more in the manufacturing space or automation space. So, we might have a microcontroller in a medical drip system that has one job, it's to measure the amount of volume of fluid that goes through that machine and into your IV so you can give the patient what they need.

Now, when we talk about embedded systems, there's a term called PLC, which is a programmable logic controller. This is a type of computer that is designed for deployment in industrial or outdoor setting, and it can automate and monitor mechanical systems. Now, when you think about a PLC, I want you to think of something like manufacturing that's going to open or shut a valve to let more or less water come in. That's the idea of a PLC. It is a programmable logic controller. Now, these PLCs run on firmware, because again, these are embedded systems. So, the

firmware which is software at a chip can be patched and reprogrammed to fix vulnerabilities when they occur, but again, there's a very specific process and there's usually limited support from the manufacturer.
Now, another way we can do this is using what's called a system on a chip. This is another form of embedded systems. This is where our processor integrates the platform functionality of multiple logical controllers onto a single chip. So, instead of having all these big PLCs all over the place, we can get all that down to one single chip. Now, this system on a chip can be very power efficient, and therefore, they're often used with smaller devices that need to have an embedded system.

Now, the other thing we want to talk about is some of these operating systems they use. So, there's this thing known as an RTOS, which is a real-time operating system. Now, this is a type of operating system that prioritizes deterministic execution of operations. And this will help us to ensure consistent response for time-critical tasks. Now, think about this. If you're running something that has to open or shut a valve inside of a nuclear plant, can you have the ability for that to be offline at any time? Probably not, right? Well, that's the idea of where we would use an RTOS, a real-time operating system. This is because a lot of our embedded systems typically can't tolerate reboots or crashes, and they have to have these response times that are predictable within milliseconds.

Now, the last thing I want to talk about is an FPGA, which is a field programmable gate array. This is a type of processor that can be programmed to perform a specific function by a customer, rather than at the time of manufacture. So, if I'm going to use something like a system on a chip, that is going to be programmed by the manufacturer and whatever it's programmed to do, that's what it's going to do. But with a field programmable gate array, I, as the customer, can actually program what I want it to do. This is really useful if I have a more generic function like open or shut a valve, but I need to tell it what time I want it to do it. Or if I want to tell it how many seconds it should be open for and how many seconds it should be closed for.

Now, the end customer here has the ability to program these things by configuring the programming logic. And we can do this to run a specific application instead of using an application-specific integrated circuit, like I was talking about a system on a chip design would. When you burn a system on a chip, that is the program you're going to have. When you're dealing with a field programmable gate array, you have the ability to change that.

ICS and SCADA vulnerabilities

But when we start talking about ICS and SCADA, we are talking about OT, which is operational technology. This is a communications network that's designed to implement an industrial control system rather than data networking. So, here, we're really not talking about end-user machines. We're not talking about having a Windows 10 host sitting on this network. Instead, with OT, we're talking about things that's using technology and computers to be able to do things in the physical world, like open or shut a valve, like do manufacturing, like create power generation in a power plant, things like that. So, if I look here, for instance, this is what OT looks like. Usually, they look like big cabinets with dials and gauges and buttons.

ICS

Now, let’s start with ICS. ICS is an Industrial Control System. When you hear ICS, this is essentially just a network that manages embedded devices. So, if I work in some place like an electrical power station or a water supplier, or I work in a hospital doing health services, I might work in telecommunications in the backbones. Now, one of the things that ICS uses is what's known as Fieldbus. Fieldbus is a digital serial data communications that are used in operational technology networks to link different PLCs together. So, we talked about those PLCs in a previous lesson, right? I might have a PLC that opens and shuts this valve to let more gas into the engine, so that we can go faster on a ship, for instance. Well, that is just one PLC, but I might have another PLC that opens and shuts a breaker that allows electricity to go to a different part of the ship. And if I want to connect all those things together, I need a way to do it. And that's what we use Fieldbus for. It's this digital serial data communications that we use to link all these things together. Now, another thing we have to be able to do is we need to be able to talk to these machines and tell them what to do. And that's where we use an HMI: a Human Machine Interface. This is the input and output controls on a PLC that allows a user to configure and monitor the system. So, when I'm trying to tell the system to do something, like open a valve, I need a way to give it that input. I can do that by pushing a button. That could be a Human Machine Interface. And so, as a cybersecurity analyst, one of the things you want to look for is the data historian. Now, the data historian is a software that aggregates and catalogs data from multiple sources within an industrial control system. Now, again, as an analyst, this is important for you to know because if you're working in a place that has an industrial control system, you want to find out where the data historian is and how you can use it, because that's going to have valuable information for you.

SCADA

SCADA is a Supervisory Control and Data Acquisition. This is a type of industrial control system. So, it's a type of ICS that manages large-scale, multi-site devices and equipment spread over a geographic region. So, when I'm talking about ICS, I'm looking at one plant. When I talk about SCADA, I'm talking about multiple plants. That's really the way I like to distinguish these two. So, when you deal with SCADA, this typically runs a software on ordinary computers and it gathers data and manages it across the different plant devices and the different equipment that has embedded PLCs. So, when you're dealing with SCADA, it typically is going to use some kind of a wide area network connection. So, I mentioned earlier, I have a smart meter on my house. They don't have to come out once a month and read my electrical meter to know how much to bill me. Why don't they have to do that? Because it's part of a SCADA network, and all the houses in my area are part of that SCADA network. They have a cellular chip in there, and it takes that reading once a month, sends it back over cellular as a text message or data format, whatever they use, to their SCADA server, collates that information, passes it to the billing system, and then I get a bill.

Modbus

Now, the third part of this we need to talk about was Modbus. Now, because ICS and SCADA are really focused on operational technology, they don't have to use things that we'd only use in the IT world. But they have to have a way to communicate with each other. And Modbus is that way. Modbus is a communications protocol that's used in operational technology networks. So, in our IT networks, what do we usually use? TCP/IP, right? Well, we don't have to use that inside these OT networks. And often, we don't. Modbus is instead what we use. So, Modbus is going to give the control servers and the SCADA host the ability to query and change configurations of each PLC. Now, this is important to know. Because this is more of a proprietary protocol, it looks different than TCP/IP. So, if you're trying to do an incident response, and you think somebody's in your ICS SCADA network, and you've been studying how to do TCP/IP your entire life, are you going to know what you're looking at? Most likely not. And that's why there are experts in ICS and SCADA systems. Because it is a different way of thinking. It is a different way of communicating, and they use a different protocol.

Mitigating Vulnerabilities

Well, the go-to guide for this is going to be the NIST Special Publication 800-82. Now, again, this is a good read if you happen to work in a manufacturing environment or someplace that uses ICS and SCADA.

Now, the first thing we want to talk about is how you can establish administrative control over operational technology networks. The best way to do this is by recruiting staff who have expertise with these things. Because, as I said, these are not your normal IT networks.

The second big tip, you want to make sure you're implementing the minimum network links by disabling any unnecessary links, services, and protocols. Essentially, when you have an operational technology network, you want to eliminate it from all of the rest of the networks, as much as possible.

The third thing we want to talk about is how we can develop and test a patch management program for operational technology networks. Again, these OT networks are different than our information technology networks. You can't just go ahead and use your Microsoft SCCM servers. That's not going to work for you. So, you want to make sure you understand what options you have and how you're going to do a patch management program. Remember, these are things unlike PLCs, they have firmware that needs to be upgraded sometimes, that's going to require maintenance windows, that's going to require downtime.

And then, the fourth thing we need to think about is how we're going to perform regular audits of logical and physical access to these different systems so that we can detect possible vulnerabilities and intrusions.

Premise System Vulnerabilities

Well, a premise system is a system used for building automation and physical access security. And these are a different type of network, as well. Oftentimes, you'll have this as a third network in your organization. When you're dealing with this and you go to your front door of your building and you try to get in and use your card and your PIN, that has to go through some kind of an access control system. Now, in addition to this, we also have building automation systems. Now, building automation systems, they have components and protocols that facilitate the centralized configuration and monitoring of your different mechanical and electrical systems within offices or data centers. Now, the final thing I want to talk about in this lesson is the idea of PACS, which is the Physical Access Control System.

Now, the Physical Access Control System is all of the components and protocols that facilitate the centralized configuration and monitoring of security mechanisms within offices and data centers. So, when we start talking about all the security cameras and the access control to badge in and badge out of your building, that is all part of your Physical Access Control Systems.