Chapter 8

Monitoring and Detecting Deviations

Solutions in this Chapter:

- Looking at the Difference
- Monitoring Something Completely Different
- Detection by Watching, Listening, or Kicking

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

Introduction

As mentioned previously when looking at hardware devices in general, I said that detection and monitoring were two completely different processes. Here we look at these two areas of devices, how they differ, and how attacks focus on specifically one or the other.

This chapter covers the details of physical monitoring devices. This includes the standard streaming video, or always-on cameras, and those that take time-indexed snapshot photography or even turn on and off based on other means of detection. In the new age of data representation, we begin to worry less about how the information was originally gathered and more about how it is presented or stored before entered into a court of law. They say that a picture is worth a thousand words. As digital as photography is these days, and how being digital inherently introduces the ability to modify that data, I personally trust digital images less than those produced through the original processes. A Polaroid camera produced an instant image that was developed instantly on a physical medium that you could touch. Physical ownership and protection of that image, that picture, was possible. Digital imaging falls under the category of modification after the fact. In fact, photographic studios today will make you look slimmer, taking a few pounds off should you pay a little extra for some Photoshop work, and people who we see in magazines are rarely the real thing. Digital tools allow us to make anything seem what it is not. While some of these tools make up for a not-so-great photographer, or the bad lighting during a wedding, it is not those uses that spoil security. The problem is that images that are seen are believed, and for some reason, the change in photography hasn't resulted in a change in the trust in photography. Is what you are seeing real or just a dream?

This chapter also covers how detection mechanisms work in physical-based detection systems. We look at these processes and talk about how they could potentially be bypassed. Because the process of physical detection requires physical presence, and the state of the world is changed through that presence, it is often difficult or not feasible to trick a detection system. Although we could talk about all the crazy brainstorm ideas of how to create arbitrary tools that might help us bypass these devices by exploiting the way they were integrated, such as elevating a person using some type of wall grip method to avoid touching a pressure-plated floor, those exploits do not exploit the device itself, and thus are left out.

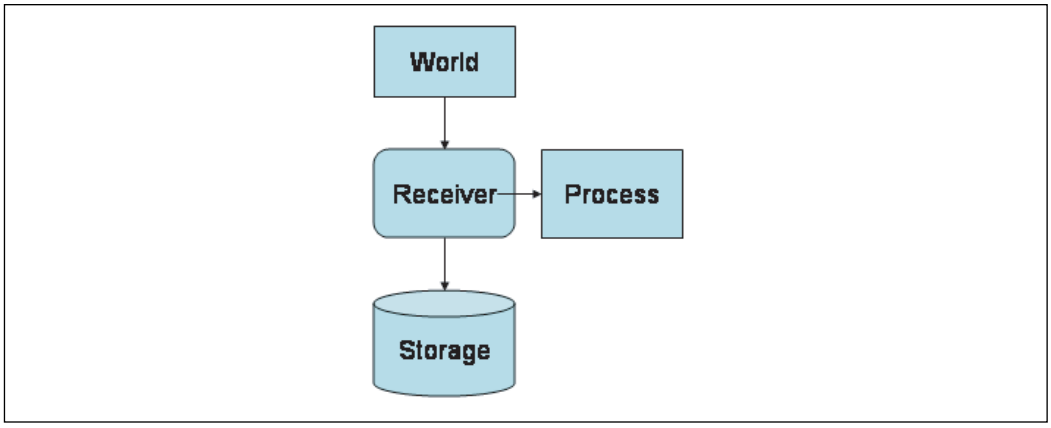
Looking at the Difference

In the course of determining how to show you the difference between these two very important concepts in security, I found that the definitions of the words them-

selves lead people to believe otherwise, and it is almost the language that fails to allow the correct representation of function.

First, let's review the *Webster*'s online definition of the word *monitoring*. The definition describes devices used to record, regulate, and/or control the process of a system. This is really more like a nuclear reactor type of monitor, as obvious action is taken based on specific events. The closest definition to what we need for security is from the supervisor variation that defines it as the process of keeping a close watch or to supervise. However, a security camera that records raw video data to disk, in itself, is providing absolutely no supervision. I looked through many variations of words, and ended up with *watch*. Still, watching suggests that you are looking for something. In the case of a bank robbery, you won't know what you are looking for until after the fact. In fact, most audio and video monitoring systems don't necessarily integrate any configurable process of detection except by that which is defined specifically by the user and/or configuration company. When we consider the process of monitoring, we must review Figure 8.1 to understand exactly what a monitoring system does as integrated for security. When someone says he is monitoring data, Figure 8.1 is what he may be suggesting.

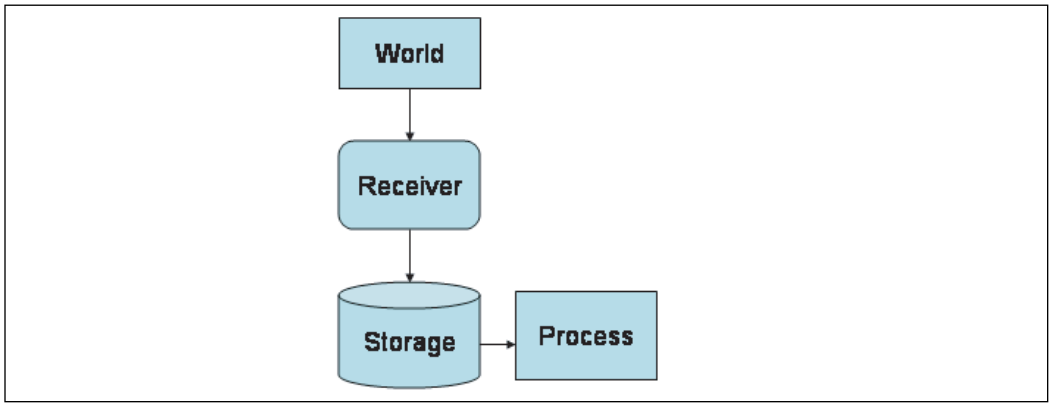
Figure 8.1 Suggestive Monitoring



We are going to classify the standard monitoring process as the method of recording real-time information from any possible source. This in itself is *demodulation*. Demodulation is defined as extracting information from a carrier. Cameras store information from light that is received. A network monitor demodulates information from a network wire (electricity) and records that information. Audio recording is storing interpreted data from waves carried via air and vibrations. Figure 8.2 describes a process of taking data and storing it for reviewing by other processes or

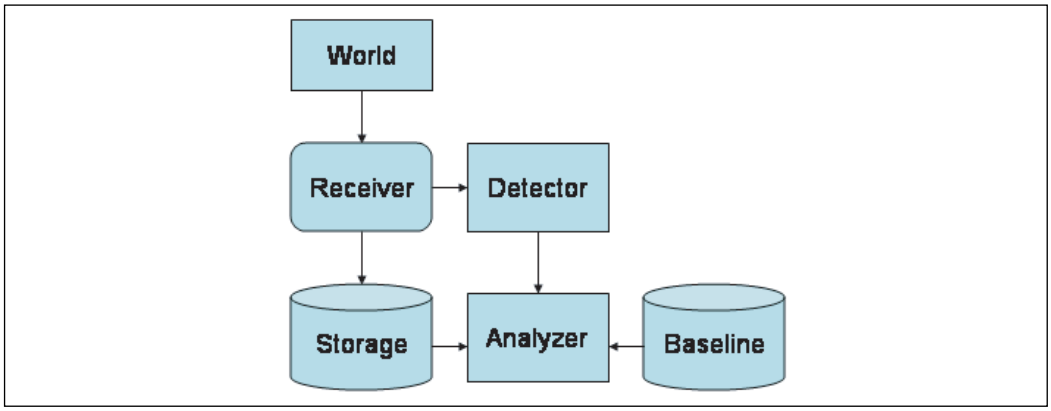
for reviewing in real time by a person. However, purely monitored data we regard as demodulated data that may or may not be saved for future reference. The possibility of a purely demodulating system to detect anything at all is zero.

Figure 8.2 Actual Monitoring (Demodulation)



As we see in Figure 8.2, a real monitoring system will have an after-the-fact type of processing. These systems allow for historical data, whether video or audio, to be checked later for possible legal or other auditing reasons. We know that since a monitoring system is purely demodulation, we can possibly attack the process of demodulation itself, and with computer networks today, we can see that demodulation of information from carriers is a significant problem. The data must be demodulated before it is validated. However, before we get to that, let's jump back to how detection fits into this. Detection denotes that you are looking at something, but it doesn't decide the difference between watching for an event through demodulated data or not. Therefore, we will classify detection in two ways. The first way is as Figure 8.3 suggests, an integrated process used with a monitoring system.

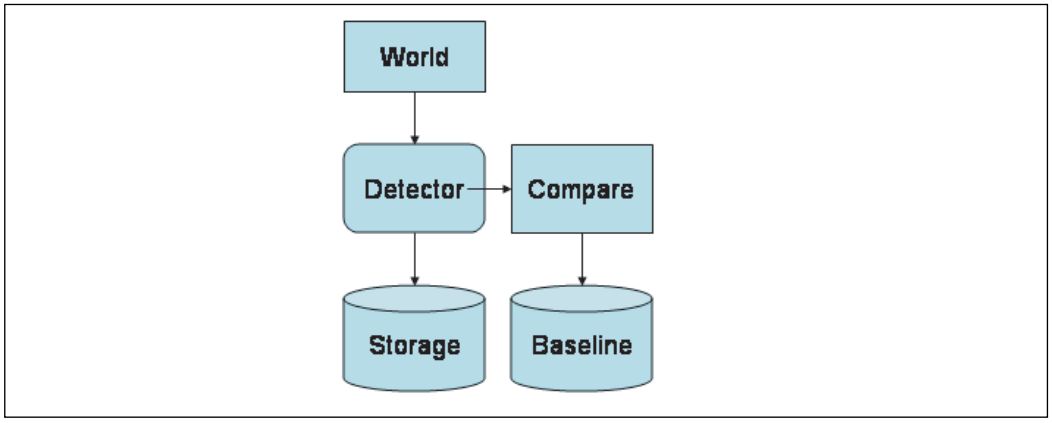
Figure 8.3 Demodulation and Integrated Detection



Obviously here, the demodulation process will deliver data into the storage location and signal the detection system that new data has arrived. The detection system will pull comparative data from the baseline configuration and analyze the data for deviations. Network-based intrusion detection systems (IDSs) work this way. All network data is reviewed, demodulated from the network into a logical format, and then verified via a comparison mechanism for invalid data. These systems look for bad data as opposed to what is considered good data. When the data set is so large for logical data structures, these systems are required to only check for bad data, often called *signatures*, for reasons of performance. The amount of bad data is largely considered less than the amount of good data.

The second type of detection is based on the constant comparison against a known state. Motion and sound detection are prime examples. Here, a constant stream of information is received by the detection device. The baseline in formation is in constant comparison, but until a change of state occurs, there is no need to record any information, thus defining it as detection and not as a monitoring system. The monitoring system would record constant data and not just the variations. Figure 8.4 illustrates the second variation of detection.

Figure 8.4 Detecting without Monitoring



In Figure 8.4, the only information stored is events determined through the comparison as deviations from the baseline data.

Damage & Defense…

Recording Can Help Determine Denial of Service

Pure detection systems that do not use any form of monitoring for information storage purposes are more susceptible to denial-of-service (DoS) attacks. They don't allow information to be analyzed over a period of time to determine patterns of activity or deviations of those patterns.

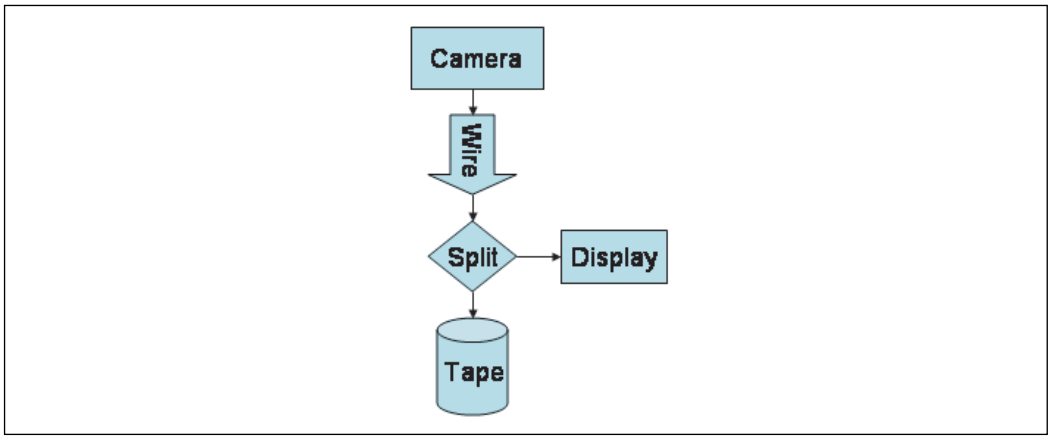
Monitoring Something Completely Different

Of all the generic monitoring exposures that exist, the most commonly seen is the injection and/or man-in-the-middle (MITM) attacks. If we take any monitoring system with a camera and a storage or viewing device and look at the independent components, we can see how these exposures can occur.

We look first at a standard camera system. We see that we have the device that receives the raw input, the camera. This device could be a cheap camera or an expensive one. The dependency on the accuracy of the recorded information isn't

just the quality of the camera lens or whether it is digital or analog in nature, but rather due to the nature of the entire recording and monitoring system (Figure 8.5).

Figure 8.5 Wired Camera System



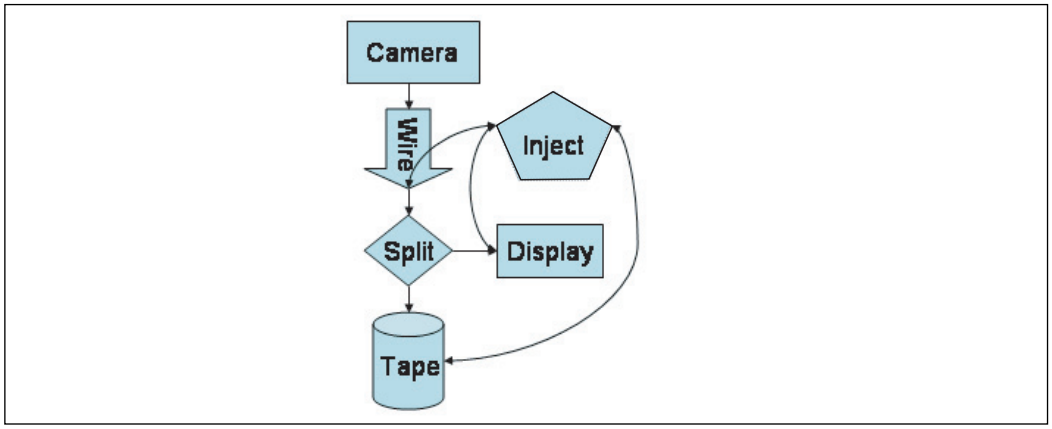
A typical camera may have a wire that goes from the camera to the controller box. For many systems, this controller will split the video so that it can be viewed while it is being recorded. Even if the input is not predictable, it won't be a problem to find out what the correct video feed format is. Every camera will freely distribute this data, so the exact details of the wire current may change, but we can extrapolate that in our example we have a simple NTSC video feed. We know that over this wire will travel a current specific to the input allowance, which for this case could be 75 ohm, 120 volts at 60Hz. Since we know these details, it is simply a matter of buying a similar device to the one we want to control and develop a method to inject our own data stream, but splitting off the real feed, and perhaps even modifying that video feed. It's not enough to just create a bridge, but also boost the strength so that we don't lose quality based on the new resistance and processing that we will add. Most likely, we will need a repeater so that the change in signal strength is as good.

In Figure 8.6, we can see the injection occurring within a wired system by tapping into the wires directly available. The process of cutting and tapping, or bridging our device into the video system so we can inject one of any of these positions may depend on the availability of those wires, and thus the risk for performing such an exploit can be determined, but the ability for the injection to work is high.

We can even take this type of control a step further. If we know what the monitoring system is watching, which we would, and we know what the monitoring system is looking for, we can create our bridged modules to control the content of

the video stream, and it could even be dynamic per the time of day, or based on an event that is triggered by the attacker.

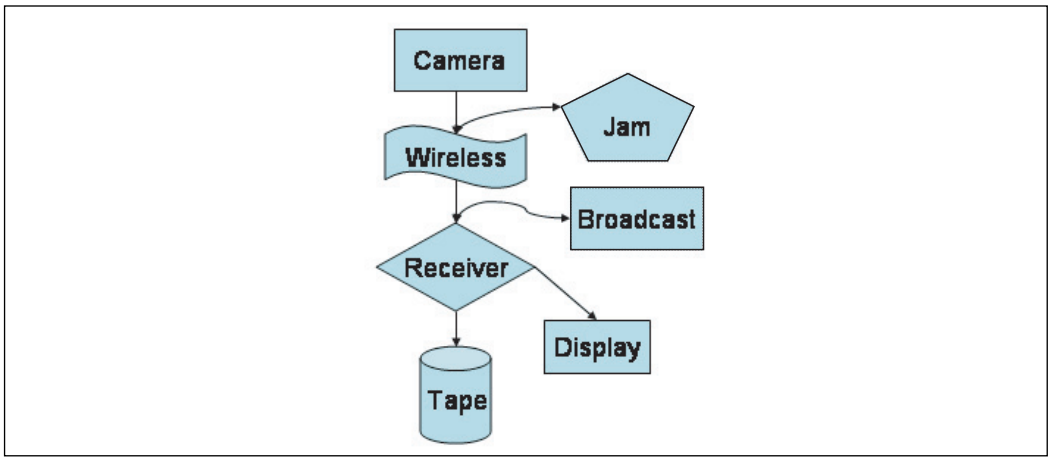
Figure 8.6 Injecting into a Wired System



The information seen by the display or recorded on tape could all be different from the information being input into the recording lens of the camera. In fact, it would be most beneficial for short scams to dump the fraudulent information only to the display, while dumping complete garbage to the splitter, so the tape system records nothing. For long-term exploits, both the display and tape feeds might require exploitation so they can be injected at will at specific times.

Figure 8.7 demonstrates the same concepts behind attacking a wireless variation of a monitoring system. A low-power (while still being enough power) jamming device correctly placed to jam the broadcast signal of the camera would stop the video feed. Then, the attacker places a new broadcast device within distance of the receiver so that the video stream isn't interrupted. What's interesting about this type of scenario is that wireless systems are used for rapid deployment (no worries about wiring), and we know that the receiver is going to be a good distance away from the camera. This actually makes it easy in some respects. We just have to get our new broadcast device close to the receiver.

Figure 8.7 Injecting into a Wireless System



Most attacks such as this one would be created using the same equipment. It wouldn't be hard for an engineer to modify a real camera from the same vendor. In fact, this would ensure that the compatibility between the receiver and camera transmitter remains constant. As long as wireless devices are prone to interference as defined and required by the FCC, this device must accept all interference (sound familiar?). Then, the security guards (if they are paying attention) most likely won't think anything of a glitch or two on the display. Moreover, before deploying this type of injection device, we would likely cause glitches on purpose so that this one glitch didn't cause any special interest or attention.

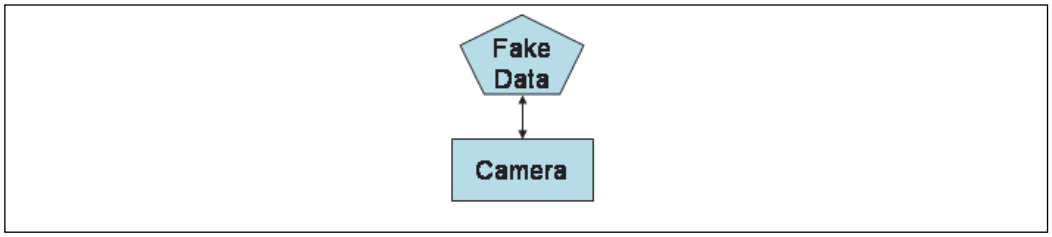
Notes from the Underground…

Jamming Devices

Jamming devices, diagrams, and blueprints are downloadable from the Internet and also covered in the basics of signal processing in many books. Jamming GPS, cellular, and other wireless devices, although illegal, is still absolutely possible—where there is a will, there is also a documented way.

Of course, the most fun that you didn't see in this trick is just placing a picture or some type of fake data feed into the camera system directly. Depending on the reaction time of the victims, a nicely chewed stick of chewing gum will fit over the lens just fine, as in Figure 8.8.

Figure 8.8 Injecting Natural Fake Data



There isn't much difference between communicating devices such as camera systems and a network. Even a wired monitoring system has the same problems of communication and authentication that two computers attempting to communicate from across the world have. Without authentication, you cannot be sure who is communicating to you, regardless of whether you believe that the wire that goes from point A to point B is secure from being tapped or manipulated.

Monitoring Injections

Of course, we could just monitor the monitoring systems. Then, we could have monitoring systems that monitor the monitoring systems that are monitoring the monitoring systems. If I lost you just now, good. It's pointless to monitor a situation that is prone to injections, when by that same process, you can be injected upon.

The best thing to do would be to establish a secure channel of communication between the camera device and the recording input location, whether at a switch or controller, and long before the data is written to tape or other storage, or displayed to a user. Only through device-to-device authentication and cryptographic exchange is it possible for the transmitting device to identify itself to the receiving device, and likewise, this ensures that the receiver authenticates to the transmitting device. This will require a higher level communication protocol than raw voltage. Raw data feeds can never be trusted based on the simple laws of injection and MITM attacks that can be used against them. If you need to know how this is possible, review Chapter 3, "Information Security," and establishing secure tunnels of communication.

Just Turn It Off

The FlexWATCH line of Internet available camera systems from Seyeon Technology still gets the claim to fame for possibly the most insecure camera system whose purpose is to ensure security. I mentioned in a previous chapter about this line of integrated monitoring stations that allows you to browse to it directly—no matter where you are in the world. It appears that the first exploits to come out were authorization bypass methods, where requesting the administration page by applying two forward slashes "//" instead of one for your URL request of the administration page allowed you to bypass all authentication. This may seem like a simple mistake, but for a security device to have such a backdoor is unthinkable. Even worse is that they patched the bug, but the following method using a Unicode character of %2F, which is the Unicode variation of the forward slash "/", still works, thus giving you administrative access to any of the devices.

Damage & Defense…

Want a Secure Device?

Looking for a secure solution? It's going to cost you more money than you may think, because before you buy that nifty gadget, you need a third party to perform an audit of it. You must ensure the security of the device before trusting it to ensure the security of your data and personnel. Of course, you could just take their word for it… that it is secure. What about risk management?

Why worry about security cameras when you can just browse to them and turn them off? */%2Fadmin/aindex.htm* is the offending URL that still works. Is this a backdoor left there on purpose that security analysts have just magically found, or just a small oversight? This is the second time it has occurred. How can we trust security corporations to create solid products with technology such as embedded Web servers that are not secure?

Detection by Watching, Listening, or Kicking

All the detection devices that exist can be broken into two categories, passive and active. Passive devices wait for input. They sit there constantly waiting for input. These types of devices include sound detection, light detection, gas detection (carbon monoxide detection is a common application), or any number of other input possibilities. Active devices send signals and listen for responses. Bats are good examples of animals that navigate using active radar, which is a polling method of active detection. All detection devices are implementations of the concept of radar using various physical methods or levels of technology.

There are many examples of active detection methods. Infrared scanning could be used with point-to-point connections that communicate between each other via multiple listen and transmit devices. Lasers, like in many movies, are blasted around a room and sensors watch for possible fluctuation. All of these active methods are ways of kicking. It is a way of kicking your foot into the hall with your eyes shut and your ears plugged to determine if someone is there. You must continually kick, and hopefully, between kicks no one slips through. If you just put your foot out, the criminal may just crawl under it or jump over it. Most active methods have predictable patterns, and although some may offer 100-percent coverage, they may not be 100-percent secure if the criminal knows they are there. Most detection mechanisms perform differential analysis against their configuration data for the most effective coverage possible.

Passive methods also exist such as that employed by thermography, which allows for the detection and imagery of thermal radiation, or heat. Militaries have invested lots of money to research and implement thermography as low-visibility radar to detect and track objects that radiate heat, such as people and/or vehicles. Thermography can be active, although the active portion has more to do with doing analysis on the characterization of the entity being imaged or mapped to determine quantitative values, rather than just to observe the existence or presence of an entity.

Passive Detection

Passive detection mechanisms are very common. Not unlike most devices, a smoke alarm (you know - the detection device that is supposed to wake you up should a fire occur), is still only as good as the batteries that are powering the device. Security based integrated detection devices will have a main power feed and a battery backup should the main power fail. Given response times for power loss, it is unlikely that just killing the power to a location will allow you to bypass detection systems. Those

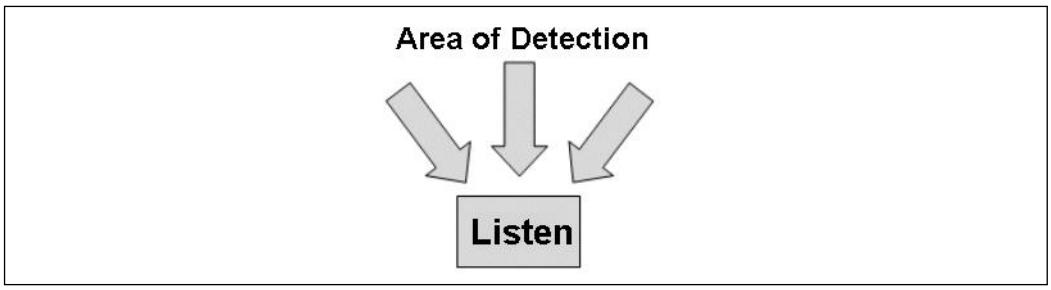
situations are considered highly probable to be attacks in the first place. Sure, timing a penetration ready to go at a moments notice during the yearly windstorm may seem brilliant, but it is also predictable and something that the police and corporations assume is possible.

Most detection devices are self-contained, and despite their communicative abilities, they are a very difficult hurdle to jump when attempting to access a physical location.

Physical weight pressure, air pressure and temperature, or *thermography*, are just a few types of passive detection methods that you are not going to be able to bypass directly without breaking the notification systems that those devices use.

We can however fall back on our favorite pastime to cause the faith in these devices to be lacking when we desire to actually perform the penetration. Figure 8.9 simply describes a passive detection sensor.

Figure 8.9 Passive Detection



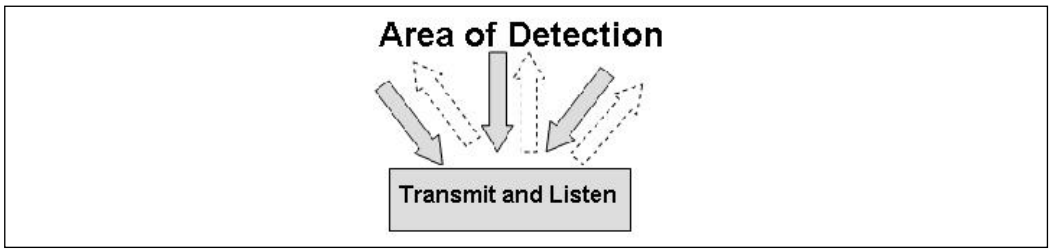
Passive mechanisms are commonly found in car alarms. These little gadgets sense a physical bump, dectecting the necessary force that breaking a window or kicking a door will entail. The sensor reacts, firing the loud car alarm that we hear so often in parking lots and apartment complexes. It's not really the detector itself that is being exploited; as the alarm is continually set off, frustrating the owner until he or she eventually doesn't turn on the alarm at all. At that time the thief steals the car since the owner has lost trust in the detection mechanism. Denial of service attacks are about all that is possible with passive detection devices unless physical access can be made to the mechanism to possibly sabotage the device.

A detection device that detects light can likely be triggered by various degrees of ease by using light. Street lamps can be turned off for ten to fifteen minutes at a time by shining a bright flashlight beam at the sensor that turns the light off during daytime hours, when the amount of light given by the sun, even on cloudy days, is present.

Active Detection

Active detection devices, while hard to bypass, are also easy to cause denial of service attacks against. A store that has a door locked with a magnetic strip and an internal active motion detection device, perhaps laser-based, contains something you desire. You determine a method to bypass the magnetic strip by entering through the window instead, but you know that the motion detection device will activate the alarm. You know that a watching agency is signaled internally by phone when the alarm sounds. Triggering this alarm many times to cause denial of service is required, and also needed to check the response times. It may be as simple as slipping a piece of paper underneath the door to cause the motion detection mechanisms to trigger the alarms. Figure 8.10 illusatrates a basic active detection device as it sends out signals that are then retrieved and validated.

Figure 8.10 Active Detection



Detection devices generally create a baseline configuration at the time the alarm is armed and that configuration is used to determine changes in the state of the world. Any changes in the state will trigger the device to notify the alarm system to trigger.

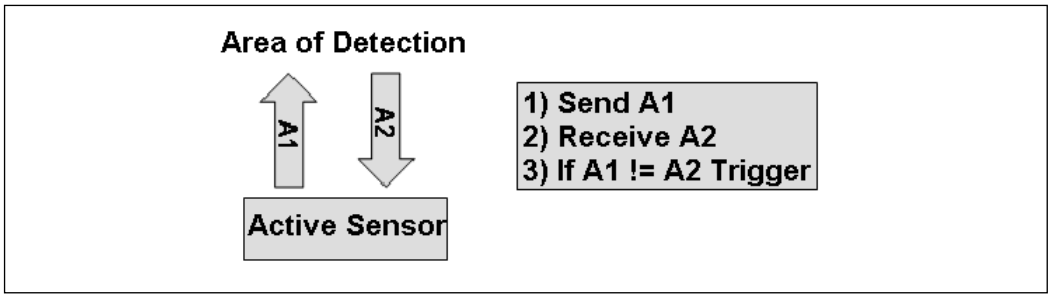
Blinding Detection Devices

Can detection devices be blinded? It's possible. All you need to do is purchase the detection device you wish to attack and test it in the comfort of your own home. We know that active detection devices use signals to determine deviations in the state of the world. To mask yourself completely from these devices means you must either change the state of the world so that you can move freely within that world and not be detected, or you must change the configuration of the device. Having access to change the configuration is the easiest method, but most detection devices reinitialize their configuration each time they are activated, depending on the type of device. A thermography-based detection device will have a preset heat signature,

while a laser-based device will remap the target area upon initialization, since someone could have moved the couch since after it was enabled last.

As you'll see in Figure 8.11, a device will possible trigger if the data that is sent is not the data that is returned. Objects that block or cause deviations in the patterns of output to input will cause the device to notify the alarm system to trigger.

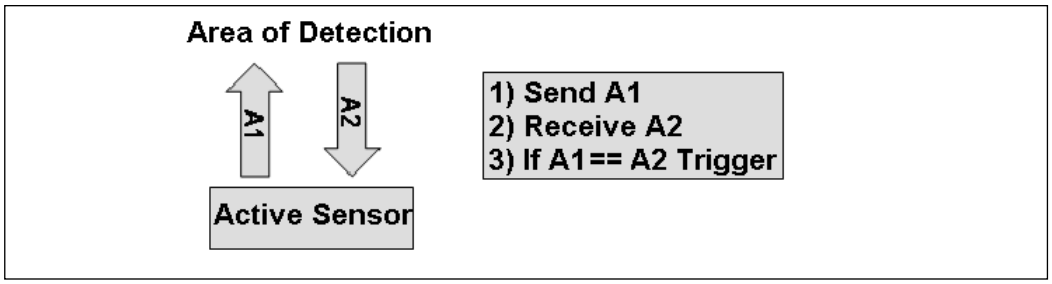
Figure 8.11 Expecting Matches



Other types of devices will trigger when a deviation occurs. These types of devices are the infrared lasers that cause the garage door to close, since it knows that the transmitted data from one side of the garage is reaching the other side. Obviously there is nothing blocking the path and it is okay for the garage door to be shut. A system such as this is prone to an injection attack by placing a new transmission sensor very close to the reception sensor, thus allowing the door to close on top of your car before it can safely enter the garage.

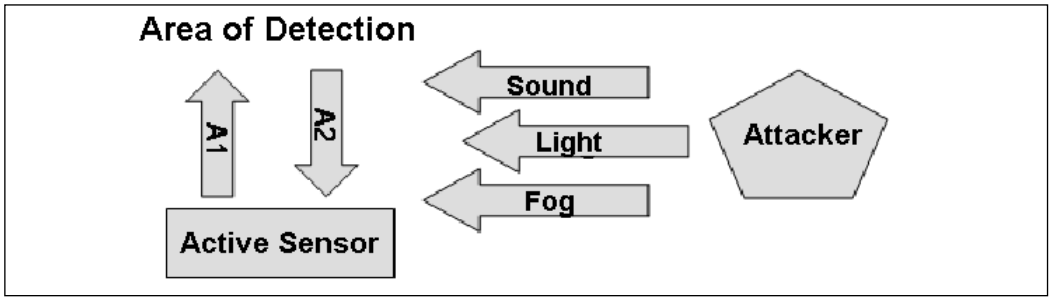
Often these types of system will have a feedback system where the sender of the information tells the receiver through a backchannel so that the receiver has state information to assert that the sender is sending the signal. Exploiting that scenario would only require a second receiver to be placed, causing the sender to believe that the receiver is actually there both through the detection channel and through the backchannel. In Figure 8.12 we see an example of a sensor that expects data to change and if the data doesn't change then it triggers an alarm.

Figure 8.12 Expecting Deviations



Since detection mechanisms are performed via physical methods, over air, via light sound and changes in physical properties of sent and received data we know that changing the state of the world can lead to possible exploitation of these detection methods.

Figure 8.13 Injection Deviations



Any possible injections directly into the state of the world or to the sensor's receiver mechanism could directly cause the sensor to operate incorrectly, thus causing the trigger to not fire, or fail in the detection of objects or changes in the state of the world.

Most devices do not necessarily communicate directly to the triggering controller, signaling that they are still active. It may even be possible to use electromagnetic fields induced into the devices strategically to cause them to fail.

Metal Detection: Searching For Lost Treasures

Metal detection is an amazing process, built from pure ingenuity. Having studied it in preparation for this section, I can grasp quite easily how it works, and yet until I reviewed it, I hadn't a clue exactly why it worked. It makes perfect sense, and also presents some possible perspectives for exploits. There are multiple methods for basic metal detection, and I'm going to present some basics. We have telemarketing commercials on television that show people finding coins or jewelry from a hundred years ago. As kids, or even still as adults, we wanted to find some lost treasure, maybe through experiences read in a book, or after seeing *Goonies*. Metal detection devices aren't often considered for purposes other than in airports corporate headquarters, or governments for the detection of weapons.

Metal objects have specific properties-they can conduct electricity, and electricity flowing through any material will create an electromagnetic field.. Basic metal detectors use electromagnetic fields to induce electricity in metal objects and then look for the electromagnetic field that would be created by that inductance. These devices are set to allow for specific levels of *phase shifting*. Phase shifting occurs on the basis that the detection mechanism never stops. However, the receiver that is checking for induced electromagnetic fields may receive an input after the inductance of electricity into an object, because it isn't instantaneous. Obviously there will never be an instant response as metal objects have resistance and the change of the flow of electricity called *inductance* will delay the shift. This could be based upon what they consist of, the amount of induced electricity, or the amount of resistance or any number of modifiers.

The detection of ferrous materials (those that contain Iron (Fe)) is not required, nor wanted, by the average gold seeker. ThOver-the-counter metal detectors will have various settings that allow the detector to ignore small detections and focus on larger objects such as gold that consists of good inductive properties.

Tools & Traps…

Swabbing for Compounds

Swabbing is done for detection of explosives or explosive-type compounds for multiple reasons. First, the potential induction of electricity, using large metal detectors looking for materials, could cause any random device to detonate. Second, depending on the makeup of the compounds, they may not be detectable via basic induction mechanisms, based on the power and accuracy of those detection methods. Third, the test may indicate that specific compounds or residues that exist on your person or luggage are drug-based, and have nothing to do with weapons whatsoever.

The largest problem with the detection of metal objects is that we are looking for something bad among a massive amount of items that are harmless. We present the question again - What is bad? To walk through a metal detector, we place our belongings into a scanner first. The idea is that the person reviewing the scanner will find large objects or things that look dangerous, while any hidden metal objects on our person will be detected using the metal detector. While this process may seem intensive, it really is not. Bypassing such a system can be done merely by testing the process and determining what levels of conductivity occur within the metal detector. Since the person walking through isn't often padded down, or strip-searched, the possession of one or more items that bypass the laws of metal detectors is possible. Since the conductivity of materials is based on many factors—current compound makeup, temperature, resistance, strength and frequency of the induction field—it is feasible to both determine these extents and bypass them. Buy a metal detector to test with, and then bypass the detection method if possible.

It is feasible that the accuracy of these devices is such that the amounts of materials that could be smuggled are negligible, and not considered a threat.

Summary

Monitoring and detection systems should be integrated to each other. The communication between the devices should be expected at all times. If one sub-system becomes lost or doesn't communicate in a timely fashion, then it can be assumed that the system is under attack. Even a power failure or battery failure could cause this type of apparent false alarm, and yet the same attitudes would be seemingly visible when a real attack occurs. The monitoring systems that allow for the recording of events in real time and for historical purposes allows the deviation of attitudes in detection devices to be validated and potential attacks mitigated based on the analysis of what, when and how detection devices signal alarms.

Detection devices sense changes in the state of the world. If the state of the world can be changed to reflect the comparative nature of how the analysis is performed, the device can be bypassed by slowly changing the state of the world to reflect the configuration of the device. Detection devices must not be accessible at any time by a person other than authenticated maintenance security personnel, or else they could be tampered with.

Solutions Fast Track

Looking At the Difference

- ☑ Monitoring is the process of recording aspects of the state of the world to a recorded medium that can be used for analysis or review.
- ☑ Detection allows for the finding of deviations in the state of the world, possibly in real time or based on the analysis of the data recorded by a monitoring system.
- ☑ Monitoring and detection systems rely on each other, and one without the other offers many possibilities of exploitation and repudiation.

Monitoring Something Completely Different

- ☑ Monitoring systems stream data from an input mechanism to a storage device.
- ☑ The data that is transferred is vulnerable to injection and theft without requiring device-to-device authentication and cryptographic tunnels.

- ☑ All devices should implement high-level logical streams of data so the state of the communicative process can be asserted and audited.

Detection by Watching, Listening or Kicking

- ☑ Detection systems are prone to denial of service attacks.
- ☑ Monitoring integration is required to determine whether denial of service attacks are real attacks or just bugs or flaws in the detection systems.
- ☑ Complete security systems should maintain communication at all times with the detection components since the mitigation of a single detection sub-system mitigates the entire security system. Autonomous processing within the detection device is required, in addition to assertions performed remotely about the state of the world at a central processing location.

Metal Detection: Searching For Lost Treasures

- ☑ Deviations in electromagnetic fields are used to detect metals of various properties.
- ☑ It is curious how effective 3rd party penetration tests against the test base, and the metal detection units themselves could be.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form. You will also gain access to thousands of other FAQs at ITFAQnet.com.

Q: If we place high-level communication processes within our devices, isn't that creating more problems then simply plugging wires that carry raw signals into these devices?

A: Obviously the properties of networking apply, and if each of the devices within a security system were objects on a network with logical identification it would be easier to communicate. But it does introduce other problems such as protocols, cryptographic dependencies and so on. While keeping it simple is always a good rule, the communication between the devices in a security system can be completely faked without the mathematical complexity of cryptography.

Q: Are you suggesting here that all devices authenticate to each other? That seems the only way for a security device to be able to identify the difference between an attacker injecting data or a device into the security system architecture.

A: This entire book really focuses on a few specific instances of scale-free networking. When I say scale-free networking, I refer to independent devices or people attempting to prove that they should have access to a given entity. Your thumb authenticates you to your computer, your password authenticates your to your email, and so on. We look at people attempting to authenticate to computers, and motion detectors attempting to assert that the control system they are telling to sound an alarm is really there. These two situations are exactly the same from the perspective of sending information and asserting the trust between the sender and the receiver. We need a method for each independent agent to authenticate within the scope of the larger system. Security devices lack these fundamental qualities. Many devices that attempt to develop these qualities are not audited and fail in their attempts.