CHAPTER

7

Physical Weapons

INFORMATION IN THIS CHAPTER

- How the Logical and Physical Realms are Connected
- Infrastructure Concerns
- Supply Chain Concerns
- Tools for Physical Attack and Defense

When we think of cyber warfare, we most likely envision legions of über-nerds, staring intently at banks of monitors while madly typing away at their keyboards. Although there may be some measure of truth to this particular mental picture, we also need to consider the place of conventional warfare in such conflicts.

When we look at how the physical and logical realms intersect, we find that they are very closely linked. The logical systems, such as software and applications, are entirely dependent on the physical systems and infrastructure on which they run. Changes made to either the physical or logical components can have profound effects on each other, with one sometimes rending the other completely useless.

Just as in any large conflict of a physical nature, we are concerned with the infrastructure and supply chains that make our operations possible. If either of these components is removed or subverted by opposing forces, conducting warfare becomes considerably more difficult, at best. At worst, we may find ourselves unable to act entirely, nullified by supply chain issues such as food poisoning from a batch of contaminated egg salad in a mess hall or cafeteria.

When looking at the tools we can use for physical attack and defense, we have a wide variety of options available to us. We can use conventional explosives, cut cables, jam transmissions, pick locks, and nearly anything else that come to mind. For defense, we can harden our facilities and equipment against the attacks that we consider to be the most likely, and we can take steps to ensure that those attackers that do make it through our perimeter are frustrated in their attempts and quickly detected.

http://dx.doi.org/10.1016/B978-0-12-416672-1.00007-6

HOW THE LOGICAL AND PHYSICAL REALMS ARE CONNECTED

The logical realm depends on physical hardware and network. Though the idea of the virtual world riding on the physical world is indeed a simple one, some of the second order effects of intersections between these two worlds may not be as clear or immediately obvious.

When looking at the physical network infrastructure on which such systems are maintained, we have two primary issues to consider in cyber operations: keeping our own systems and infrastructure intact and functional while rendering the opposing systems and infrastructure unable to do so.

Logical systems can also be used to make changes in the physical world. In complex items of physical hardware, software often regulates the way that the hardware functions. Changes made to the software can affect whatever the hardware interfaces with, including networks, other systems, or even people.

Logical Systems Run on Physical Hardware

The logical world runs on a variety of network infrastructure, computer systems, home automation devices, refrigerators, cars, and so on. When such a complex device loses connection to the various utilities that are critical to its functionality, mainly power and communications media, it becomes considerably less useful, often times to the point of being rendered a very expensive paperweight.

When conducting operations in a cyber conflict, whether offensive or defensive, keeping the physical hardware running that enables such activity can be challenging. Even in conventional warfare, an element of advanced technology has begun to enter the fray in the form of numerous computer systems and network-connected devices, and the intelligence provided by such technology can provide critical information on which to base cyber, as well as conventional, operations.

Many recent military actions in which the United States has participated, such as those in Iraq and Afghanistan, have taken place in desert locations that tend to be very hot and sandy, with little existing infrastructure to speak of. Operating in such bleak environments tends to be less than optimal for the continued functionality of computing equipment. The cost to environmentally harden equipment is often more than replacing off the shelf computers. In addition, such equipment may pose a tempting target for opposing forces to attack, both on a physical and a logical level. In such cases, ruggedized equipment is often required in order to have any expectation for the devices to function over a period of time.

Additionally, at a higher level, the infrastructure needs to be kept working for such systems to utilize. This type of infrastructure technology is commonly found in data centers and other areas that house critical computing equipment, although it is not commonly hardened to withstand the levels of attack that we might find in a cyber conflict. By using redundant systems, infrastructure, utilities, and other such necessities, we can make it very difficult to take systems down due to the high level of resiliency. On the other hand, because the technologies that enable resilient systems and infrastructures are generally available, we will likely find them implemented by our opponents as well.

On the reverse side of this issue is the problem of attempting to render the equipment and infrastructure of the opposing forces inoperable from a physical perspective. Particularly when physical operations are being conducted on foreign soil, those under attack may have a distinct "home court" advantage. In some situations, such as the conflict in Afghanistan, we may be dealing with an opponent that does not rely on a sophisticated technological infrastructure at all. In other cases, we may be facing well-constructed data centers that are hardened and have sufficient backup resources to provide power and communications in emergencies. These can prove to be very difficult to take offline. Often it is a mix of legacy equipment with some cutting edge technology (i.e., encrypted phones) combined with using nontraditional methods like internet-based drop boxes.

During Operation Iraqi Freedom in 2003, several rounds of cruise missiles were required to disrupt the Internet access in Baghdad. Although the civilian Internet Service Providers (ISPs) were taken down with relative ease, with much of the traffic originating from behind a single Cisco network switch, the traffic coming from the Iraqi government was not so easily silenced as it was part of a more resilient network. After direct hits on two telecommunications switching centers, several satellite dishes, and a server housed in the Iraqi Ministry of Information building, the official Iraqi government website and the associated email server were taken offline. It later appeared that communications were being carried through a satellite gateway that had been shipped to Dubai by the manufacturer and later brought into Iraq [1].

Given the ease of constructing backup systems on a variety of infrastructures, it is entirely possible that multiple systems would need to be taken down to remove the cyber capability of an opponent. Internet access can be provided over microwave, cell, ham radio, phone lines, and a variety of other solutions and can be shared through mesh networking to enable a great degree of redundancy. Given today's technologies a system could even be made to function at a minimal level from a laptop and a data connection from a cell phone. In such cases, a combination of physical and logical attacks may be required to completely take a system offline.

Logical Attacks can have Physical Effects

Just as physical attacks can affect logical systems, logical attacks can affect physical systems. To a great extent, physical computing systems are controlled by the operating systems and applications that are running on them. As a very simple example, for almost all systems that are physically connected to a network cable, changes to the network configuration can be made in such a way as to remove a device from the network.

TIP

Web administration interfaces are typically wonderful for knocking devices off of the network. They often have poor security, if the security features have been enabled on them at all. Although they have relatively limited functionality in most cases, many of them do have the capability to change basic network settings. Typically setting the IP address on such a device to 0.0.0.0 will disable its network functionality handily.

In the case of a device being removed from the network, a backup communications method could potentially be used to restore communications to the device, or a person will be required to physically travel to the device to reconfigure it. Such an attack may be very simple and ultimately very easy to fix, but using it to disrupt network infrastructure across an enterprise could bring an entire organization to a halt in very short order, and be very time consuming to fix.

Attacks on physical systems can also have effects of a much more serious nature that can go far beyond merely annoying network and system administrators. Attacks on implanted medical devices, such as pacemakers and pumps for dispensing medication, have become all too common in recent years, to the point of research being done to create firewalls for such devices [2].

Although such attacks are nontrivial to carry out, requiring considerable amounts of research and specialized hardware, but the concept is well proven. To make matters even worse for future attacks along these lines, in 2009 the first wireless and Internet connected pacemaker was installed in a patient [3]. Remotely connecting to and disabling all such devices under the control of a particular doctor, a cardiologist at the White House, for instance, might have quite a profound effect in the political world.

In addition to such concerns around generic computing devices, these attacks can also be used to affect the critical systems that control the components running industrial processes around the world. Such systems control the distribution of power and water, communications systems, manufacturing, and any number of other important processes.

INFRASTRUCTURE CONCERNS

When we mention the word infrastructure in the company of those that work in the computing and technology worlds, the common tendency is to assume that we are referring specifically to network infrastructure. Although this infrastructure is indeed important and many processes would be completely nonfunctional without it, it is only a portion of the infrastructure on which the industrial world runs.

Of chief concern when we discuss infrastructure and the associated systems are the systems that actually control these items. These control systems regulate power, water, communications, manufacturing processes, and any number of other tasks. Properly referred to, such systems are industrial control systems (ICS). ICS are made up of Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control System (DCS), Human–Machine Interfaces (HMIs), Master Terminal Units (MTUs), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), and other such items [4]. A typical SCADA layout can be seen in Figure 7.1 [5].

These categories are often grouped together under the umbrella of SCADA, rather than calling them by the less familiar term ICS. In essence, the distinction between SCADA and ICS revolves around the specifics of where and what is actually being controlled or coordinated. In many cases, such distinctions are not standard between industries, and the term SCADA is often used where ICS may be more accurate in a technical sense.

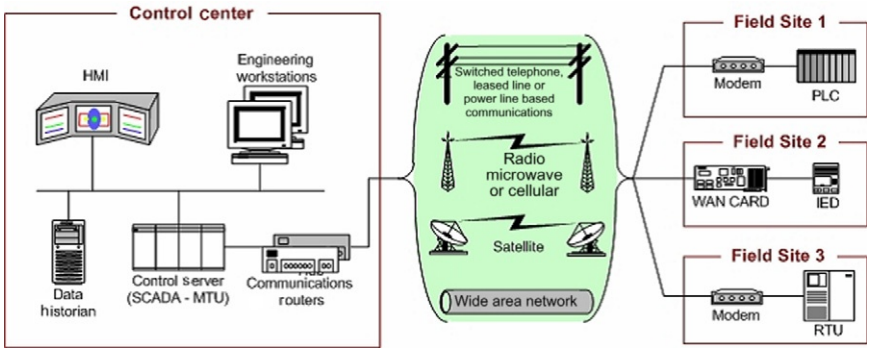

FIGURE 7.1 SCADA system general layout.

What is SCADA?

SCADA systems are used to control and monitor a variety of processes. Such processes can be industrial, infrastructure, or facility based [6]. Industrial processes can involve manufacturing facilities, generation of power, petroleum refineries, mining, or any number of similar activities that take place in factory-like environments. Infrastructure processes revolve around water and wastewater systems, pipelines used to distribute petroleum and natural gas, the transmission of electrical power, communications systems such as landline or cellular phone systems, and other systems that provide goods and services that are commonly considered utilities. Facility processes are those that regulate processes in individual facilities such as heating and air conditioning, or energy usage.

SCADA systems are integrated into nearly everything that we come into contact with. While we are putting gas in our cars, surfing the web, cooking dinner, or flushing the toilet, we are only steps away from such systems, if not directly interacting with them. Figure 7.2

FIGURE 7.2 A remote monitoring sensor for utility usage.

shows the sensor for a remote monitoring system that allows water usage to be read by a utility company. Remote sensors such as these have become increasingly common in many residential areas, as it enables utility companies to gain greater accuracy in meter reading, and does not require a person to manually visit each reader in order to collect information.

Without such systems to maintain and monitor the modern world, we would quickly be without heat, food, communications, and many other necessities. Needless to say, although such systems are designed for industrial usage and, in some critical systems, are multiply redundant, they are based on computer technology and therefore vulnerable.

What Security Issues are Present in the World of SCADA?

Many of the systems that fall under the category of SCADA depend on security through obscurity [7]. These systems use interfaces, software, operating systems, and protocols that are either proprietary or not generally well known outside of the industries in which they are implemented. In theory, in order for attackers to penetrate a SCADA system, they would either need inside knowledge of the design for the particular, and potentially unique, system, or they would need to spend the time gaining access to and learning how things worked in order to carry out attack.

Unfortunately, we are well into the information age, and a vast store of information awaits those willing to venture into the wasteland that we call the Internet. Manufacturers conveniently put manuals online for their customers to download, internal materials leak out to the public, and odd industrial systems can be bought for pennies on eBay. Although such systems do tend to be considerably more customized than the average server, we are well beyond the point of being able to depend on the obscure nature of a system conveying any large measure of protection against attackers. Indeed, systems and software that have not had the trial by fire of exposure to the Internet and outside attackers may very well be weaker for lack of having had their security flaws pointed out to the manufacturer.

As a case in point, in July of 2010 a multipart malware named Stuxnet was discovered and its main target is SCADA systems. Stuxnet is composed of a worm which spreads over USB drives via a Windows exploit, and a Trojan that specifically looks for a particular model of Siemens SCADA systems. Also included is a rootkit to prevent its discovery. If Stuxnet finds that it is on the Siemens systems, it uses a hard-coded password to access the database that the SCADA system uses as a back end. It then looks for industrial automation layout files and control files and uploads them to a remote system, as well as attempting various acts of sabotage. Stuxnet then waits for additional commands from the remote system [8].

Stuxnet has been found in SCADA systems in a number of countries, including China, India, Iran, and Indonesia, with a possible point of origination in Israel. At first it appeared that the goal of the malware was industrial espionage. It was later discovered that Stuxnet attempted to actively sabotage such systems under certain circumstances and may have been responsible for the loss of an Indian communications satellite [9]. In addition to such threats, as SCADA systems become more commonly connected to public and private networks, we are then exposed to the standard types of attacks with which many common systems are concerned. Distributed denial of service attacks (DDoS), side effects from malware attacks, patches that introduce security vulnerabilities, and a host of others now become issues for SCADA systems.

What are the Consequences of SCADA Failures?

In the case of serious SCADA failures, the potential consequences are quite far reaching. Considering that we are referring to the control systems for electrical power, communications, the flow of petroleum, and other such critical processes, a major disaster resulting from a SCADA failure seems likely indeed. We saw an example of the potential for such a failure during a large-scale power blackout in 2003.

In parts of the United States and Canada, in August of 2003, we saw the outcome from a SCADA failure that would, at first, seem to be relatively minor in nature, involving electrical distribution. Ultimately, a failure in a software monitoring system at a utility company in Ohio led to an outage at a local power plant. The failure of the power plant caused power to be drawn from other power plants in the area. Heavily loaded power lines, as seen in such outages, tend to physically sag, which several did. Sagging lines at multiple locations came into contact with improperly trimmed trees, causing these lines to also fail. While these failures were taking place, operators at the utility companies in Ohio neglected to inform controllers at utility systems in the surrounding states.

At that point, the utility systems in Ohio begin to draw power from the systems in Michigan, causing numerous issues as the system attempted to balance its load. Additional lines failed in Ohio and Michigan, causing power generating stations to go offline due to the absence of a load on them. Additional power was routed from plants on the east coast as the system continued to attempt to balance itself, causing plants on the east coast to overload and shut down. Due to the massive power grid issues, grids in Michigan and Ohio began to disconnect from each other. Connections to Canada also began to fail, and instabilities in the grid caused grids in Canada to begin disconnecting as well. Ultimately, grids in Ontario, New York, New England, Windsor, New Jersey, and Philadelphia were affected [10].

At the end of the blackout, 256 power plants were offline and 55 million customers were without power [11]. If we look all the way back at the beginning of the problem, the failure of a single monitoring system led to this enormous issue. Such situations have the potential for enormous loss of life and destruction, depending on the industry in which we see the failure. The blackout of 2003 was ultimately the result of a software bug, but was entirely accidental. Given the attention of a determined opponent, such attacks have the potential for great disruption and destruction.

SUPPLY CHAIN CONCERNS

In addition to the infrastructure concerns that we discussed earlier, awareness of our supply chain is also critical. We are now many years into a process of globalization that extends across nearly every large industry we might care to examine. Many countries import hardware and components to build infrastructure; a wide variety of foodstuffs, both processed and fresh; fuel; raw materials; clothing; and a number of other items, large and small, that are far too extensive to enumerate.

Although this has a number of benefits, it also poses severe problems, particularly when we look at the possibilities of warfare in either the conventional or cyber sense. When we look at the infrastructure that we might rely on to conduct such attacks, or in the reverse situation,

the infrastructure that might be under attack, the majority of the components, from individual items of equipment, all the way to the components from which they are constructed come from a few major manufacturing areas around the globe.

Compromised Hardware

Of major concern is the specter of hardware that has been compromised for strategic or intelligence purposes. Critical items, such as routers or switches, firewall appliances, industrial control units, or any of a number of other components may be deliberately engineered to clandestinely report information, fail given a particular signal or set of conditions, include a backdoor, or any number of other similar activities. This can place the party suffering such attacks at a distinct disadvantage, if not cripple their capacity to operate entirely.

In the late 1970s and early 1980s, the U.S. Central Intelligence Agency (CIA) learned of plans by the Russian Committee for State Security (KGB) to steal plans for a SCADA control system and its associated software from a Canadian company. Allegedly, the CIA was able to insert malware into the software for the system, which was later used in a trans-Siberian gas pipeline. In 1982 a massive explosion is reported to have taken place as a direct result of the flawed control system install [12]. There is some debate as to the validity of this report, but it does nicely illustrate the point.

To illustrate the concept of introducing such modified hardware into the market, we can look at the case of Operation Cisco Raider, a 2-year investigation run by the U.S. Federal Bureau of Investigation (FBI). In this operation, the FBI broke up a counterfeiting ring that had sold equipment to, among others, the U.S. Navy, U.S. Marine Corps, U.S. Air Force, the U.S. Federal Aviation Administration (FAA), and the FBI itself [13].

In this particular case, the aim of the counterfeiting ring was profit rather than sabotage or espionage, and the amount of equipment concerned was very large. Under more stealth-focused circumstances, it is exceedingly unlikely that a few pieces of equipment that carried modified chips would be found, even given the government programs in place to do exactly this. We will discuss this issue in further depth, as well as some of the potential solutions, in Chapter 16.

Deliberately Corrupted Components

In addition to the specifically targeted and timed attacks that we discussed earlier, a much more simple supply chain issue can be brought about with the introduction of deliberately inferior or corrupted components. Particularly when looking at equipment with electronic components, this is a relatively simple type of attack to carry out. Considering the wide variety of components found in a typical item of electronic equipment and the large number of vendors that such components come from, such failures would be very wide reaching.

A specific case of an enormous number of issues related to a single bad component is that of the “capacitor plague” [14] that started in the late 1990s. A large portion of the issue relates to industrial espionage between capacitor manufacturers. Reportedly, the formula for the electrolyte used in capacitor manufacturing was stolen from a Japanese company and resold to several Taiwanese capacitor manufacturers. Unknown to any of the thieves, the formula was

incomplete and lacked several key additives that would normally keep the capacitor from bursting. Although this allowed the capacitors to function for a short period of time, it caused them to fail at generally less than half of their expected lifetime. According to some, this problem is still being seen in the market, with devices that have been produced nearly a decade after the original issue [15].

In this particular case, the issue was caused by an effort on the part of the legitimate manufacturer of the capacitors as a defense mechanism against the theft of their intellectual property, and only got out of hand because the information was spread so widely. If this were a deliberate attempt at disrupting the supply chain of electronics components, it would be possible to produce components that were designed to fail in a very specific way, or at a particular time, as we covered in the previous section "Compromised Hardware." Such components could potentially find their way into missiles, tracking systems, aircraft avionics, or any number of other critical systems.

Nontechnical Issues

Of course when discussing supply chain issues, there are measures that could be used as attacks that do not directly relate to items of technology. Numerous issues relating to the supplies needed to conduct cyber warfare could present themselves to a sufficiently determined opponent and could prove profoundly effective at preventing such operations from being carried out. Additionally, given the potential for conducting such operations from centralized locations, such disruptions might be trivially easy to plan and implement.

In the words of Napoleon Bonaparte, "An army marches on its stomach [16]." The consumable supplies that are necessary for our forces to conduct operations whether they are toothpaste, cold medicine, drinking water, food, or other such items, are all susceptible to contamination, whether deliberate or otherwise. We have seen many examples of the outcome of such events in countries around the globe.

In October of 2012, a restaurant named Flicks in Belfast, Ireland was the source of an outbreak of food poisoning from *E. coli* contamination. Over the course of roughly 2 weeks, 293 cases of poisoning related to this incident were reported [17]. This particular case was accidental in nature, but still had very wide-reaching consequences. If such contamination were to be deliberately carried out, particularly in a centralized location such as a cafeteria, a targeted group of people could be incapacitated or worse.

Similar issues can appear with nearly any item that is required to support our forces, both conventional and cyber, particularly in locations that are not considered on the frontlines of a particular engagement. Security in a protected remote location is likely to be much more lax than that found on any battlefield. Intentionally created supply issues are more likely, when carried out carefully and subtly, to be attributed to chance, rather than an outright attack.

TOOLS FOR PHYSICAL ATTACK AND DEFENSE

As we look at some of the conventional tools or weapon systems used for offense we turn to direct fire weapons like machine guns and tanks, and indirect weapons like artillery and jets.

For defense we think of defensive minefields and dug-in troops. If we switch to reconnaissance we consider tools like satellite imaging, espionage or spies, and sending out scouts. The same concepts that apply to the physical aspects of the battlefield also apply to the cyber battlefield.

First we will explore some of the precision attack tools available during a conventional attack. Cutting cables with tools such as a wire snip or backhoe is very effective. Next is attacking the power system supporting the building housing the key network nodes. Attacks against the personnel supporting the network can be effective in preventing recovery and extend the impacts of other attacks. The goal of these attacks is to cause a denial of service. Physical attacks do not normally impact confidentiality or integrity, but rather just availability. Raids designed to capture hardware can be effective attacks against confidentiality.

Next we will examine defensive tools. At the physical plant level these include guards, gates, and guns. We need personnel monitoring and reacting to attacks and they need sufficient force to repel the attacks. This means patrolling the lines of communications (network cables and the power grid). We will need fences that have deterrent features like razor wire, force protection features to prevent vehicle attacks, and fences that are electrified. We need buildings that are built to Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST) standards, Electromagnetic Pulse (EMP) hardened, and blast reinforced. We need redundant power capabilities (uninterrupted power supply and backup generators). We need alternate communications paths to ensure connectivity.

Finally we must protect ourselves from prying eyes. This is traditionally called Operations Security (OPSEC) in military terms. Our policies and procedures are what protect us here. We need to train the workforce to not talk about work in public places or with casual acquaintances (in real life or online). We need to train them how to guard their documents, laptops, and mobile devices when outside the office. We must get them to conduct risk assessments as part of their everyday life.

Electromagnetic Attacks

Electromagnetic attacks can be very useful in an environment where cyber conflicts are taking place. As such operations often depend on relatively delicate electronics, we can use this to our advantage. Such equipment can be affected by EMP weapons, transmissions can be jammed, and emanations from such equipment can be eavesdropped upon.

Electromagnetic Pulse Weapons

EMP weapons are a somewhat common player in movies, such as *Oceans 11* and *The Matrix*, and books, but not quite as common in the real world. EMP weapons work by creating a very intense energy field which is very disruptive to nonhardened electronics. Such devices do exist in military arsenals, generally in the form of High Altitude Electromagnetic Pulse (HEMP) or High Power Microwave (HPM) weapons.

HEMP devices produce an EMP over a wide area, commonly produced by detonating a nuclear device high in the atmosphere. Obviously, if we are to the point of countries lobbing nuclear devices into the sky, things have gotten rather out of hand in the world of warfare, and we will likely have other concerns than cyber attacks in fairly short order. The more

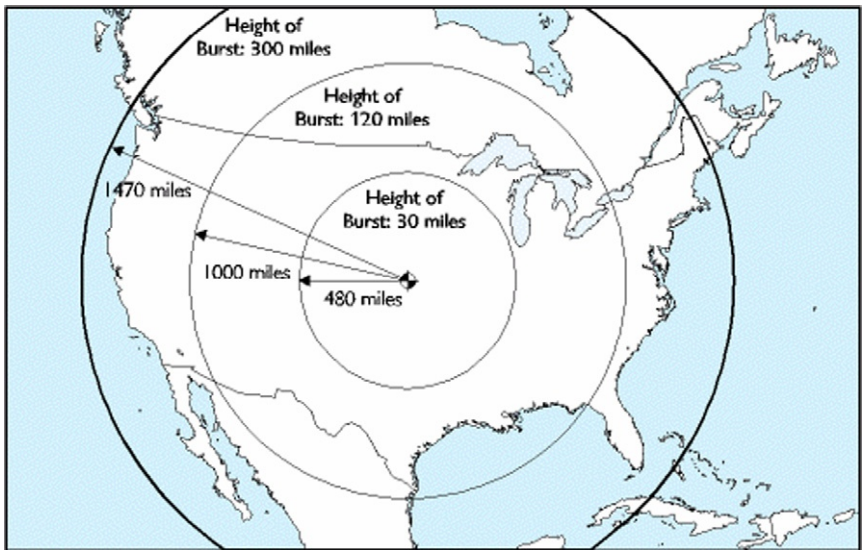

FIGURE 7.3 Estimated area affected by high altitude EMP.

realistic scenario, at present, for such a device being used is as an act of terrorism. As shown in Figure 7.3, a HEMP device triggered at 300 miles altitude over central North America would affect an area covering most of the continent [18].

HPM devices can produce a similar effect, although on a smaller scale and with smaller equipment. Instead of needing a nuclear device, a HPM can use chemical explosives or very powerful batteries, in conjunction with a type of coil called a flux compression generator, to produce a powerful pulse. HPM devices can also limit the effect of the pulse produced to a smaller area over a shorter distance. Additionally, the pulse produced by the HPM is much more effective against electronics and is more difficult to harden devices against [18].

Jamming

Particularly in many forces of a military nature, jamming technologies can be quite advanced. This set of technologies generally falls under the heading of Electronic Warfare (EW). EW systems can be used to jam nearly anything that utilizes the electromagnetic spectrum including radio, radar, sonar, infrared, laser, and a host of other technologies. Such technologies are very complex and expensive, but are common to many militaries.

On the other end of the spectrum, jamming can also be done very simply. Radio equipment can often be repurposed to interfere with transmission and receiving on other equipment, and plans for purpose-built home-brewed jamming equipment can be found on the Internet. Additionally, appliances such as portable phones, microwaves, and items that operate in the general area of the frequency to be interfered with can often be used to some effect.

Defense Against Conventional Attacks

When we are looking to defend against attacks in the physical and electromagnetic realms, there are two main areas in which we can deploy our defenses: we can harden the facilities

and equipment against expected attacks, and we can develop redundant infrastructures in place. In this way we can attempt to prevent the attack from impacting us in the first place, and we can hopefully mitigate the effects of any portion of the attack that does get through.

Redundant Infrastructure

In the case of not being able to protect our facility against attack or disaster, it is important that we have a backup site from which we can resume operations. There are three main types of backup sites: cold sites, warm sites, and hot sites [19].

Cold backup sites are the most basic and the least expensive of the three types. In a cold backup site, we basically have a facility from which we can resume operations, but not much more than that. To bring a cold site online, we might need to have utilities turned on; order, configure, and build systems; and send copies of any backups that we might need to the site. Bringing a cold site online may take weeks or more.

Warm backup sites may have some portion of the hardware and software that is needed and connectivity at a certain level, although not necessarily what is needed to operate at the full scale of the primary site. Systems may need to be configured and have software or applications installed. We may have some backups on site, but they will likely be a few days or weeks behind and will need to be restored. Warm backup sites can generally be brought online in a few days.

Hot backup sites have a completely redundant set of hardware and software, communications, and everything else needed to fully replicate the primary site. Data is usually synchronized with the primary site, so that we have very little if any data loss when switching to the backup site. The primary delay with such a site in time of disaster will usually be related to rounding up the people needed to actually work from the backup site. Hot sites themselves can generally be brought online in a matter of hours.

In the light of disasters such as those that happened at the World Trade Center and during Hurricane Katrina, the view of the technical industry on backup sites changed dramatically. Not only have organizations been made much more aware of the need for solid disaster recovery plans, but government agencies such as the Federal Communications Commission (FCC) in the United States have mandated improvements to infrastructure in order to better cope with disasters on this scale [20].

Facility and Equipment Hardening

Facilities and equipment can be hardened in a variety of ways against a broad spectrum of attacks. In many cases, such hardening involves a multilayered approach. The factors in such hardening are many and varied, depending on the physical location, potential threats, and so on. We may protect a facility against electromagnetic attacks, kinetic attacks, radiation, cold, heat, flooding, or a variety of other attacks, depending on the threats that are thought to be likely for the facility in question.

We can harden both facilities and equipment against electromagnetic attacks. In general, we are concerned with the propagation of electromagnetic energy in undesirable ways. For

purposes of HEMP, HPM, and other similar events, we want to ensure that the pulses from such events do not penetrate our facilities, and in particular our equipment.

NOTE

There is an entire field of security, known as Emissions Security (EMSEC), devoted to the prevention of intelligence-bearing emissions in the electromagnetic spectrum. Such concerns are often referred to by the name TEMPEST, which was the name of a project concerned with securing such emissions. For those interested in further reading on the subject, James Atkinson's Tempest 101 [21] gives a good overview and pointers to additional materials.

In principle, the approaches for ensuring protection for each are similar. Using a combination of shielding, faraday cages, waveguides, power and signal filters, and other similar measures, we can largely electromagnetically shield the facility or equipment in question.

Location of the facility is one of the primary layers of security. Buildings designed with security in mind are generally placed in areas that are easy to control access to, outside of flood zones and areas with frequent environmental issues, and so on. Physically hardening the facility itself might involve steps to prevent unauthorized entry to the immediate area, such as the use of fences, gates, or bollards. Inside the perimeter we may find an additional layer in the form of patrolling guards or dogs. At the facility itself, we may find structural reinforcements, locks, turnstiles or man traps, laminated glass windows, and additional physical segmentation of the facility inside.

Covert Activity

Covert activity provides the counterpoint to conventional warfare. Although in conventional warfare, our solutions generally involve overt actions with explosions and other obvious physical results, this is not necessarily the case in cyber warfare. In some situations, such activities are more damaging or more obvious than we care to be when conducting cyber warfare.

Many other alternatives are open to us when we want to carry out operations of a more subtle nature. We can use a variety of eavesdropping methods. We can jam radio-based devices, we can cut communications cables, we can pick locks, or any number of other similar methods. For a more complete discussion on some of the sneakier methods that we might want to use in such a cyber scenario, see *Ninja Hacking: Unconventional Penetration Testing Tactics and Techniques* (ISBN: 978-1-59749-588-2, Syngress).

Eavesdropping on Electromagnetic Emissions

In addition to jamming the signals of our opponents, we can also listen to the signals and eavesdrop on their emissions in the electromagnetic spectrum. Some such emissions, such as those from 802.11 wireless networks, are very trivial to eavesdrop on as they are broadcast to the world. Some emissions, such as those from keyboards or monitors, are somewhat more subtle, but are not particularly difficult to pick up either. We can even get rather esoteric and discover intelligence from the pattern of flickers on LEDs indicating network activity on servers or other such equipment.

Although it is possible that we might find our potential eavesdropping targets to be shielded against such eavesdropping, the vast majority of such devices, save a few in highly security military facilities, have absolutely no protection in this area. In the United States, the National Security Agency (NSA) is responsible for certifying facilities and equipment as being properly shielded against electromagnetic eavesdropping under the Certified TEMPEST Test Services Program (CTTSP). Such certifications indicate compliance with both the CTTSP Technical and Security Requirements Document (TSRD) and the National TEMPEST Standard, NSTISSAM TEMPEST/1-92, Compromising Emanations Laboratory Test Standard, Electromagnetics, collectively the cookbook for implementing such shielding [22].

Vandalism/Denial of Service

In the realm of technologies that depend heavily on the presence of power and communications lines, such as those used in cyber attacks, simple vandalism can be very effective. In many places, communications and power lines are buried in the ground, at best. Often access to such cables can be found by simply lifting a manhole cover. Even well-protected facilities of a military nature are often connected to public utilities, with some delay before they can revert to backup systems.

In April of 2009, exactly such an attack occurred, affecting the Santa Clara, Santa Cruz, and San Benito counties in California. Ten fiber optic cables were cut at four locations, all within easy access of manholes. In several cases, backup cables ran right next the primary cables and both were cut. Tens of thousands of phone customers using both land and cell lines were without services, as well as hospitals, police, fire departments, 911 services, and a broad variety of others [23].

Attacking Physical Access Controls

When we are looking to attack a physical access control, such as a locked door, taking a page from Occam's [24] book, going with the simplest approach will often lead to the best path. If we can avoid directly attacking a physical access control by finding an alternate way around it or by bypassing it somehow, we can often save ourselves quite a bit of pain.

Tailgating

Tailgating can be one of the easiest methods to bypass a physical access control. In a nutshell, tailgating is when we follow directly behind someone through a physical access control, generally without the person's consent, and without being authorized to pass through ourselves. In busy buildings, this is often very easy to accomplish, and, in fact, rather difficult to prevent without specific physical controls. Tailgating will beat tackling a lock every time, presuming that security at the facility in question is relatively lax.

Locks

Tackling locks directly can be very easy or very hard, depending on the environment and the lock in question. There are a number of methods that can be used to open a lock, including bypassing it or picking it.

Bypassing a lock involves working around the actual locking mechanism itself to cause the lock to open. This can commonly be done with a lower end padlock or combination lock by using a shim, a very thin piece of metal, to release the mechanism that holds the shackle closed. Similarly, a credit card can sometimes be used to slip the bolt on a door or a coat hanger can be used to unlock a car door. Such methods depend on low levels of security in the lock and the surrounding mechanism, and are generally not reliable in highly secure environments.

WARNING

Picking or bypassing locks that we don't own, or have permission to attack, is, of course, entirely illegal. In some states in the United States, merely having the tools with us can land us in a lot of trouble. That being said, learning to pick locks is a great deal of fun and can be useful for those employed in the security profession. For a great book on the topic, check out Deviant Ollam's book *Practical Lock Picking: A Physical Penetration Tester's Training Guide* (ISBN: 978-1-59749-611-7, Syngress). Additionally, a large number of demonstration videos can be found by searching for "lock picking" on YouTube.

Picking locks is a bit of a combination of art and science. The theory of lock picking is simple enough. A tool such as those shown in Figure 7.4, or even an improvised tool, in a pinch, and we use it to manipulate the mechanism of the lock, allowing the lock to open without the use of the key.

Figure 7.5 shows a view of what a lock might look like with the proper key inserted into it. In this case, because the key is in place, we see that the two parts of each pin stack, the key pins and the driver pins, are lined up so that the space where the two pins meet, called the shear line, is lined up with the edge of the plug, allowing the plug to rotate, opening the lock. This is the science piece.

Where the art comes into play is in being able to use the tool at hand to manipulate the pins in the lock in such a way as to manually line up the shear lines in the pin stacks so that the lock

FIGURE 7.4 A set of common lock picks.

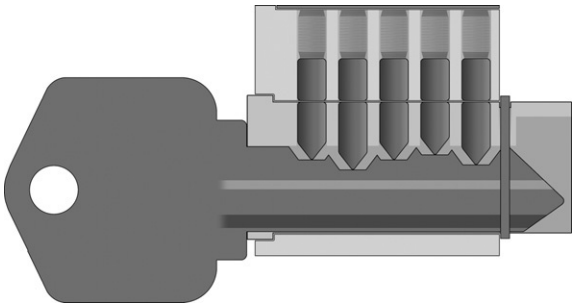

FIGURE 7.5 A key fully inserted into its lock *Courtesy of Deviant Ollam*. From *Practical Lock Picking: A Physical Penetration Tester's Training Guide* (ISBN: 978-1-59749-611-7, Syngress).

will open without the key. This is done by touch and, in some cases, by ear as well. As the pins are being manipulated with the pick, we put a small amount of pressure on the plug using a tension wrench, causing the plug to turn ever so slightly. Then, one pin at a time, we manipulate the pins until we reach the shear line. Done in the proper order, we should see the plug move a very small amount as each pin stack lines up properly. This is repeated until we are through all of the pins and the plug is able to rotate completely, hopefully opening the lock.

Picking simple pin-tumbler locks using the process that we just walked through can be relatively easy. There are several other varieties of locks, and many more in the world of high security locks, that can be much more difficult.

Defending Against Covert Attacks

Defending against covert attacks is a relatively simple, if expensive and inconvenient proposition. We can put measures into place that will keep people from tailgating, prevent locks from being bypassed, or picked, or most any other measure to subvert physical security that can be dreamed up. The problem with doing so is in the inconvenience to the people that legitimately need to pass through such controls; the trouble and expense to purchase, install, and maintain them; and the relationship to the value of what we are securing. If what we are protecting is valuable enough, then perhaps this is justified, but we can still never be 100% sure that it is completely secure.

Antitailgating measures can be relatively easy to implement, depending on the environment. On any door that we wish to absolutely prevent tailgating, we only need to install a floor to ceiling turnstile that is only big enough for one person. We can also put a guard in place, monitor the area with cameras, install a mantrap, or any of a variety of similar measures. In most cases, these types of controls are only found at government facilities with a very high level of security and are only a single layer of the physical security that is present. Additionally, we can help to mitigate tailgating through proper security awareness and training.

High security locks can contain a wide variety of measures to prevent the lock from being improperly opened or bypassed. They may contain multiple sets of pins, pins that are shaped to specifically prevent picking, specially cut keys, oddly shaped keyways, or any number of other such features. Such locks are by no means completely proof against picking or bypassing, but they will likely take a much longer period of time to do so. In the areas where such locks are used, we will often find them backed up by several layers of additional security.

Multilayered physical security may involve antitailgating measures, biometric systems, such as retina or iris scanners, guards and/or dogs, high security physical locks, proximity

badge locks, and any number of other similar controls. Such environments are generally not conducive to an intruder spending several minutes picking a high security lock open, as they are considerably less likely to enter the facility in the first place and much more likely to be caught if they do. As with almost any security system, physical, logical, or otherwise, defense in depth is the key. For those not familiar with the concept, defense in depth is the use of multiple and differing layers of security. The concept being that we will never be able to universally keep everything secure, but we can try to delay the attacker for long enough that they are detected by one of our other security measures or give up.

SUMMARY

In this chapter we discussed the use of physical weapons in cyber warfare. We talked about the intersection of the physical and logical realms and how making changes to either realm can affect the other, sometimes to a disastrous extent.

We talked about infrastructure concerns, primarily those that have to do with the SCADA systems that control the various industrial, infrastructure, and facility processes that are in constant use all over the world. We covered some of the security issues present in SCADA and the potential consequences of failures in such systems.

We covered supply chain concerns and the potential consequences of corruption or disruption in the supply chain. We discussed the potential for espionage or sabotage by either deliberately corrupting components or by adding additional functionality beyond the original design of the component. We also talked about issues in supply chains on the nontechnical side.

In the last section of the chapter, we went over tools of a physical nature that can be used for attack and defense. We talked about the use of conventional explosives, vandalism or denial of service attacks, and attacks revolving around the electromagnetic spectrum. We also discussed hardening methods to help prevent such attacks and backup strategies that might aid us if such attacks do get through.

References

[1] McWilliams B. Iraq goes offline, Salon.com, http://dir.salon.com/story/tech/feature/2003/03/31/iraq_offline/index.html; 2012 [accessed 22.03.13].
[2] Venere E. New firewall to safeguard against medical-device hacking. Purdue University News Service, http://www.purdue.edu/newsroom/research/2012/120412RaghunathanHacking.html; 2012 [accessed 22.03.13].
[3] Reuters. New York woman receives wireless pacemaker, PCMag.com, http://www.pcmag.com/article2/0,2817,2351371,00.asp; 2009 [accessed 22.03.13].
[4] Motorola, Inc. Whitepaper: SCADA systems, http://www.motorola.com/web/Business/Products/SCADA%20Products/_Documents/Static%20Files/SCADA_Sys_Wht_Ppr-2a_New.pdf; 2007 [accessed 22.03.13].
[5] Stouffer K, Falco J, Karen K. Guide to supervisory control and data acquisition (SCADA) and industrial control systems security; 2006.
[6] Juniper Networks, Inc. Architecture for secure SCADA and distributed control system networks, http://www.juniper.net/us/en/local/pdf/whitepapers/2000276-en.pdf; 2009 [accessed 22.03.13].
[7] Strategic Security. Cyber security focus in the oil and gas sector to increase significantly. Strategic Security, http://www.resilienceoutcomes.com/organisations/unpatched-control-systems-in-the-oil-and-gas-industry-predicted-to-drive-significant-increase-cybersecurity-requirements/; 2013 [accessed 22.03.13].

[8] Mills E. Details of the first-ever control system malware. Cnet News, http://news.cnet.com/8301-27080_3-20011159-245.html; 2010 [accessed 22.03.13].
[9] Woodward P. Israel: smart enough to create Stuxnet and stupidenough to use it. War in context, http://warincontext.org/2010/10/01/israel-smart-enough-to-create-stuxnet-and-stupid-enough-to-use-it/; 2010 [accessed 22.03.13].
[10] U.S.-Canada Power System Outage Task Force. Final report on the August 14, 2003 Blackout in the United States and Canada: causes and recommendations, https://reports.energy.gov/BlackoutFinal-Web.pdf; 2004 [accessed 22.03.13].
[11] Highleyman WH. The Great 2003 northeast blackout and the $6 billion software bug. s.l.: the availability digest, http://www.availabilitydigest.com/private/0203/northeast_blackout.pdf; 2007 [accessed 22.03.13].
[12] Weiss G. The farewell dossier. Central Intelligence Agency, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm; 2008 [accessed 22.03.13].
[13] Lawson S, McMillian R. FBI worried as DoD sold counterfeit Cisco gear. InfoWorld Security Central, http://www.infoworld.com/d/security-central/fbi-worried-dod-sold-counterfeit-cisco-gear-266; 2008 [accessed 22.03.13].
[14] Passalacqua C. How to identify, Badcaps.net, http://www.badcaps.net/pages.php?vid=5; 2010 [accessed 22.03.13].
[15] Moore S. Leaking capacitors muck up motherboards. IEEE spectrum. http://spectrum.ieee.org/computing/hardware/leaking-capacitors-muck-up-motherboards/0; 2003 [accessed 22.03.13].
[16] Moore R. Maxims of Napoleon bonaparte: on war. Napoleonic guide. http://www.napoleonguide.com/maxim_war.htm; 1999 [accessed 22.03.13].
[17] Marler, B. *E. coli* Poisons 293 in Belfast—someone needs to read poisoned. Centers for Marler Blog, http://www.marlerblog.com/case-news/e-coli-poisons-293-in-belfast-someone-needs-to-read-poisoned/; 2012 [accessed 23.03.13].
[18] Wilson C. High altitude electromagnetic pulse (HEMP) and high power microwave (HPM) devices: threat assessments s.l.: congressional research service, http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA529982; 2008 [accessed 22.03.13].
[19] Chapple M. Which disaster recovery site strategy is right for you? Biztech. http://www.biztechmagazine.com/article/2012/06/which-disaster-recovery-site-strategy-right-you; 2012 [accessed 23.03.13].
[20] Emmerson Network Power. Emerson network power's dusty becker addresses impact of post-katrina FCC mandate on backup power for telecom sites. Emmerson Network Power, http://www.emersonnetworkpower.com/en-US/About/NewsRoom/NewsReleases/Pages/EmersonNetworkPower%27sDustyBeckerAddressesImpactofPost-KatrinaFCCMandateonBackupPowerforTelecomSites.aspx; 2008 [accessed 22.03.13].
[21] Atkinson J. Tempest 101. Granite Island Group, http://www.tscm.com/TSCM101tempest.html; 2010 [accessed 22.03.13].
[22] National Security Agency. TEMPEST company POCs. National Security Agency/Central Security Service, http://www.nsa.gov/applications/ia/tempest/tempestPOCs.cfm; 2010 [accessed .22.03.13].
[23] Sabotage attacks knock out phone service. San Francisco Chronicle. http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/04/10/MNP816VTE6.DTL&tsp=1; 2010 [accessed 22.03.13].
[24] Hiroshi S. What is Occam's razor? Phys.ncku.edu.tw, http://www.phys.ncku.edu.tw/mirrors/physicsfaq/General/occam.html; 1997 [accessed 22.03.13].