

Defending Endpoints

MANY PEOPLE THINK OF traditional information security designs from the outside in—as providing protection at a network edge or some other logical separation between organizations and the rest of the world. Each layer deeper inside the organization provides additional defenses until the workstations, laptops, and other endpoint devices are reached. Those individual systems and devices can be difficult to secure. Each system may be slightly different due to functional requirements, unique software or hardware configurations, or even individual user behavior. The large number of individual endpoints in an organization, as well as the endless variety of systems and devices that can be added to a network, makes protecting them a constant struggle.

Those individual systems and devices provide an excellent target for attackers, who typically seek to exploit vulnerabilities in the systems, their software, and the people who use them. Once an attacker succeeds with a single system or device, he or she can then use that system to explore the network around it, to steal data using the system or user's rights, or to launch further attacks against other parts of the network that may trust the compromised system. Although successfully attacking a single computer may not provide attackers with everything they need to successfully take over an organization's infrastructure, a single vulnerable computer is often their starting point. Like a breach in a medieval castle's wall, a single gap in the defenses of an organization can allow attackers in.

The past few years have offered many examples of attacks against endpoints using sophisticated malware and a deep understanding of the infrastructure and systems that their targets used. This evidence shows that attackers are talented, well supported, and patient. As more nation-states develop advanced cyberwarfare capabilities, the complexity of threats against individual systems and networks will continue to increase. Targeting endpoint systems is an attractive option for attackers who know that there are hundreds, and sometimes thousands, of opportunities for them to find a system that is weaker than the others around it—

or a user who will fall for an attack and allow the attacker into the network through the user's own actions.

In addition to traditional cyberattacks, pairing advanced intelligence-gathering capabilities with nation-state-level resources creates an environment where a single flaw open to exploit can provide the way in for an attacker. This is true even if traditional security measures have been put in place. Intelligence operations in cyberwar are increasingly focused on acquiring digital data. Penetrating computer systems or other network-connected devices can provide intelligence operatives with an amazing amount of information. Networked devices not only store digital documents, designs, blueprints, and photos, but they also monitor the environment, run utility grids, control factories, and even provide direct medical care and monitoring for individuals.

The Stuxnet attack demonstrated that even systems that are not connected directly to the Internet can be reached by a clever and determined attacker. Stuxnet's use of a human factor to transfer the malware from infected laptops carried by engineers to the protected systems that it was meant to finally attack provides another reason to carefully consider how endpoint systems and networks can be protected. A single gap in an organization's defensive design can be exploited by attackers, and can result in exposure of data or significant damage to systems and the infrastructure they control.

In cyberwar, the endpoint system is the final line of defense between attackers and defenders. Defenders must understand the complete list of endpoints that they are responsible for, and how attackers are likely to target those devices and systems. Attackers must understand the multitude of options they have and how those systems are likely to be protected. In either case, cyberwar creates a challenging environment for individual systems to operate safely in.

Chapter 11 Topics

This chapter covers the following topics and concepts:

- What the role of endpoint systems and devices in cyberwar is
- What the types of endpoint systems are
- Which attacks are commonly used against endpoints in cyberwar
- What common endpoint protection concerns and strategies to protect against them are

Chapter 11 Goals

When you complete this chapter, you will be able to:

- Explain the role of endpoint devices in cyberwarfare
- Describe types of endpoint systems and devices
- Describe common attacks against endpoints
- Describe current U.S. Department of Defense endpoint protection goals
- Explain endpoint protection strategies and designs

Cyberwarfare Endpoints

Modern computer networks are often composed of hundreds, if not thousands, of devices that connect through the same network and services infrastructure. When those computer networks are owned or managed by an organization, central management systems often control the devices on the network. Typically, these devices are held to some form of configuration and management standards. When individuals or small groups control the devices on the network, the level of control applied to them often varies more. In both cases, large numbers of devices provide a huge number of potential targets that attackers can probe to find a flaw.

The sheer number of systems found on a typical large network means that attackers are likely to find a neglected system, a system with an easily fooled user who will click on a malware-infected file in an e-mail, or a system that has not been updated with critical patches and updates. The same techniques that non-cyberwar attackers use to compromise systems provide a means for cyberattacks as part of cyberwarfare. Even systems that are not on a network can be attacked, either by directly accessing the system in person or tricking a person who has access into admitting your attack tools.

Success in cyberwar frequently requires that attackers first identify vulnerabilities in protected systems and networks. Once they have found a gap in the layers protecting their target, they must then use that vulnerability to make their way deeper and deeper through defensive layers until they reach their final goal. That goal varies depending on the reason for the attack. It may be intended to provide information about the enemy, to provide a foothold for future attacks, or to allow the attacker to translate his or her electronic success into the physical world by disabling critical systems or causing them to act in ways they are not intended to.

Attackers in cyberwarfare also target systems that are not part of the typical set of computer network devices that traditionally motivated attackers seek out. Cyberwar targets include military systems like targeting and command-and-control systems, drones,

NOTE

The United States has explored ever-increasing levels of network connectivity for its forces, including individual soldiers through the Land Warrior project and other network-connected soldier technology projects. These technologies and others were demonstrated via the Future Force Warrior project. The Future Force Warrior design included individual soldier computer systems that provided monitoring of individual soldiers with health sensors, communications, sensor systems, and helmet-mounted displays.

communication systems, and even the control systems of significant military assets like naval vessels and satellites. They can also include the infrastructure that supports military operations, such as weapons production, utilities, and the infrastructure support system. As the control systems for military and other assets increasingly rely on computer systems, they also become targets for cyberattacks. The potential to take them over or to make them inoperable with a cyberattack becomes more likely.

The broad array of network-connected devices and computer-based systems used for targets that nation-states may attack—as part of a computer network attack or an intelligence-gathering operation—is incredibly diverse. Fortunately, most of these targets can be broken down into a few major categories of endpoints, whose critical features can then be studied.

Types of Endpoints

Although there are a huge number of possible endpoint systems on networks, most of them can be broken down into a handful of common types. The most common type from a cybersecurity perspective is the traditional PC. Whether it is a server, a laptop, or a desktop, a Windows, a Linux, or a Mac computer, the same basic cybersecurity concepts for attack and defense apply. The fastest-growing components of many networks are mobile devices, such as tablets, mobile phones, e-readers, and related devices. In addition to these, networks often contain building and utility control systems, network-enabled phones, and network devices. Computer network attack and defense also target military devices and systems, such as drones, weapons systems, and command-and-control systems, adding to the potential endpoints defenders must consider in their design.

Computers

Personal computers and servers are the most frequently attacked endpoint systems, and thus are the focus of many endpoint defense plans. The sheer number of possible variations of software, hardware, drivers, firmware, and other components that make up computers results in a challenge for defenders. Computers are also the way that most employees interact with data and networks, meaning that defenders must ensure that employees and computer users are part of the defensive plan.

Cyberwarfare attacks like Stuxnet have demonstrated the important role that individual computers can have in a large-scale, carefully planned attack. Thousands of computers around the world were infected with the Stuxnet malware using a variety

of attacks against vulnerable software. The Stuxnet attack used attacks against those thousands of computers to finally get its attack tools into specific systems in Iran. If the attacks had failed at any point before they got to the laptops used by engineers in Iranian nuclear production facilities, or if the laptops themselves had been able to detect and stop the malware from transferring to the USB drives those engineers used, the attack might have failed.

Personal computers provide attackers with a multitude of options when they look for a way to attack. Because the software they run is usually commercially available, attackers have the option of buying the same hardware and software, then practicing their attacks or developing new tools without actually attacking their potential victims. This means that a skilled and well-funded attacker, such as a nation-state's computer network attack team, can develop advanced tools without opponents being aware of those tools before they are used.

Mobile Devices

Mobile devices might appear to simply be another type of small computer at first glance. In fact, mobile devices like tablets and smartphones add a new set of challenges for organizations that are designing a defense strategy for their networked devices. Not only are many mobile devices personally owned, and thus difficult to centrally manage, they also come in a huge number of varieties. Mobile devices might use Apple's iOS, Google's Android, Microsoft's Windows Mobile operating system, or some other version that administrators might not be familiar with. They can also run any of a multitude of various versions and releases of those operating systems. Much like the challenges organizations face with desktop PCs, the massive number of possible configurations and software versions can make securing mobile devices a challenge.

Organizations that choose to centrally purchase and manage only a limited selection of mobile devices still must face the limitations of the devices themselves. Operating system patches, vendor configurations, and even the basic security capabilities of the mobile devices' operating systems can limit what defenders can do with them. Many high-security organizations limit or even prohibit the use of mobile devices in their networks due to these challenges. More-open organizations must face the risk that mobile devices can create a path into their network they cannot easily control.

Industrial Control Systems

An **industrial control system (ICS)** includes the devices and systems that control industrial production and operation. ICSs include systems that monitor electrical, gas, water, and other utility infrastructure and production operations, as well as the systems that control sewage processing and control, irrigation, and other processes. Commonly recognized types of ICS systems include **supervisory control and data acquisition (SCADA)** systems, **distributed control systems (DCSs)**, and **programmable logic controllers (PLCs)**.

ICS systems are a particularly attractive target for cyberwarfare attackers who want to disable a nation's power grid or damage or destroy parts of its utility infrastructure. ICS systems are often not as well secured as traditional computing infrastructure. Their high requirements for stability and continuous operations mean that they are less likely to be consistently patched and updated. In fact, some ICS systems manufacturers advise their customers to not update the control systems and sensor devices. This makes protecting SCADA and DCS systems an even greater challenge requiring additional planning to overcome.

Supervisory Control and Data Acquisition Systems

SCADA systems are used to monitor and control remote equipment. SCADA systems like those shown in Figure 11-1 are very common in industries that require remote monitoring of their infrastructure and production systems, such as natural gas pipelines, power production and distribution infrastructure, and water supply control systems. SCADA systems typically include individual remote sensors known as remote telemetry units, which provide reports back to the central data collection system and provide some level of local control. The central system then uses the information provided by the remote units to control the entire grid or pipeline of production and control systems. Attacks against SCADA systems can target the feedback provided to the central control system. Or they can cause the local sensor and control unit to perform an incorrect action.

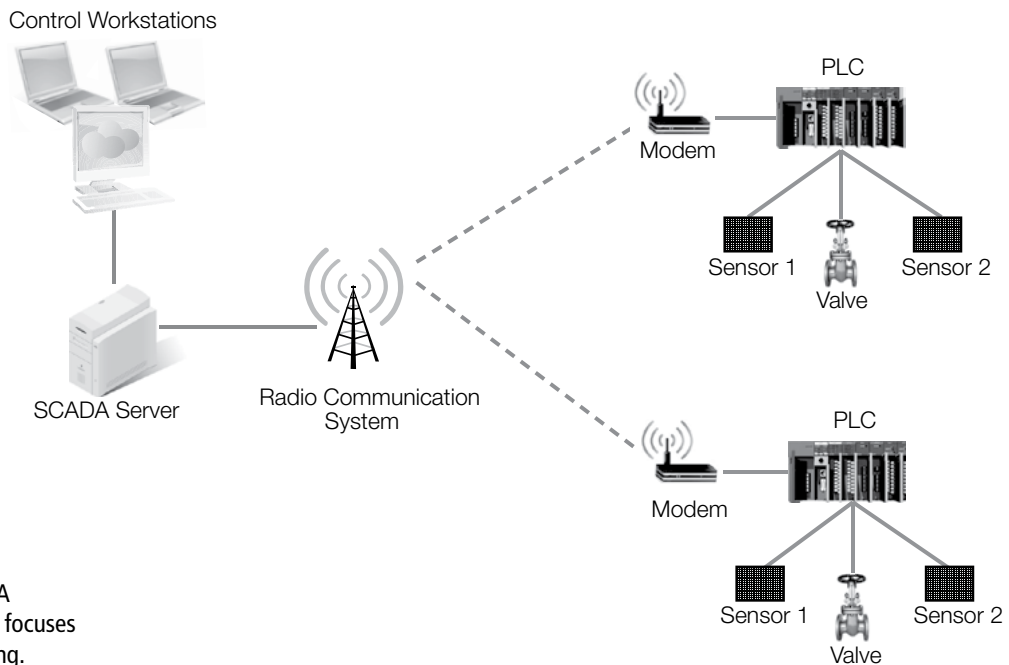
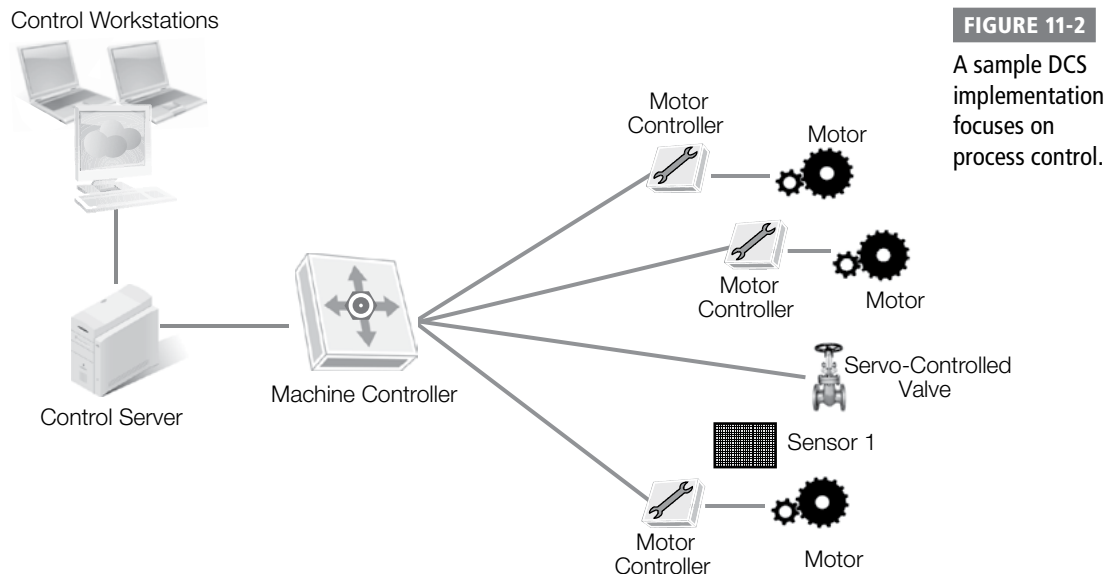


FIGURE 11-1

A sample SCADA implementation focuses on data gathering.

**FIGURE 11-2**

A sample DCS implementation focuses on process control.

Distributed Control Systems

Distributed control systems like those shown in Figure 11-2 are frequently used to control water and wastewater treatment and distribution systems, power generation plants, refineries, and production facilities like those that make cars, electronics, and food products throughout the world. DCS systems use a combination of sensors and feedback systems to control and adjust processes as they receive feedback. Much like SCADA systems, an attack against a DCS system could be as simple as providing incorrect feedback, resulting in a shutdown, overproduction, or delay in the system at a critical time.

Programmable Logic Controllers

Programmable logic controllers (PLCs) are special-purpose computers designed to handle specialized input and output systems. They are typically designed to handle difficult environments with special temperature, vibration, or other requirements while still functioning. PLCs are designed to handle and respond to their specialized input and output requirements reliably to ensure that the processes they support occur without interruption or delay. PLCs connect to a Human Machine Interface (HMI) to provide

FYI

PLCs normally use a specialized operating system known as a *real-time operating system (RTOS)*, which prioritizes inputs to ensure that they are handled appropriately. Like desktop operating systems, exploits exist for common real-time operating systems, but most real-time operating systems do not receive the same level of security scrutiny that desktop operating systems do.

Targeting SCADA and ICS Endpoints

Attacks against SCADA systems aren't new. In early 2000, a former employee in Queensland, Australia, used his knowledge about the water treatment software and systems to release 800,000 gallons of raw sewage into local parks, rivers, and the grounds of a local hotel. The spill killed marine life and polluted the local creek and surrounding area. An investigation showed that neither cybersecurity defenses nor security policies or procedures were in place.

Attacks against SCADA systems are a popular topic at security conventions and conferences. A 2013 demonstration at the Black Hat security conference showed how the underlying Modbus communication protocol between programmable logic controllers and their controllers could be attacked, allowing the attackers to disable protective controls and then make the system work in ways it was not intended to.

With ever-increasing interest in SCADA, DCS, and PLC attacks, reports of successful attacks against poorly configured or unpatched systems are common. In 2013, researchers at Cylance discovered that they could access the air conditioning system at Google's Wharf 7 facility. Other attacks have allowed access to building-entry systems, elevator control systems, and other internal infrastructure for buildings.

NOTE

Later in this chapter you will learn about the U.S. Department of Defense cybersecurity strategy and the stance that the DoD takes on protecting military endpoint devices and systems.

interfaces that can interact with human operators. Typical PLCs don't have a monitor or other interface beyond buttons or lights built in to them.

Military Systems

The term *military systems* describes a range of devices and platforms. Some use common civilian operating systems and software; others are built using custom-designed software and hardware. Due to the diversity of military systems, defenders must carefully evaluate the defensive capabilities of the endpoint devices they have to protect, and then design appropriate layers of defense based on those capabilities.

Drones and Remote Platforms

Electronic attacks against drones have demonstrated that drone platforms and their command against drones' use of the Global Positioning System (GPS) and those aimed at capturing video feeds from drones deployed in active combat. According to leaked NSA documents, al-Qaeda-sponsored research has primarily been aimed at jamming GPS and infrared marker systems, as well as the use of lasers to dazzle drone sensors.

FYI

At the time of writing, attacks against drones have been targeted at drones that were in active use. They have not succeeded in taking over control of drone-based weapons systems. Reports of civilian drones being jammed and control over drones being seized by unknown parties have surfaced, but have not been confirmed.

Because drone command-and-control system links are encrypted, drones' software and the systems used to control them are a more likely target.

Weapons Systems

Military weapons systems have integrated an ever-increasing amount of computer hardware and software into their design. Table 11-1 shows the published increase in the use of software in the avionics and flight control systems of major U.S. aircraft since the 1960s. Each successive generation has seen a significant amount of additional control by computer-based systems. As additional capabilities for communications and command and control have been added, warplanes and other systems have become more likely targets for cyberattacks.

Modern military aircraft provide an excellent example of the increasing use of software-controlled systems. They use flight control, navigation, intelligence, and communication systems that not only have software-based controls—they can also frequently receive in-flight updates and data, providing a potential means of attack or deception.

TABLE 11-1 Percentage of aircraft function handled by software.

AIRCRAFT	YEAR INTRODUCED	PERCENTAGE OF FUNCTION HANDLED BY SOFTWARE
F-4	1960	8
A-7	1964	10
F-111	1970	20
F-15	1975	35
F-16	1982	45
B-2	1990	65
F-22	2000	80

FYI

In 2007, reports surfaced that F-22 Raptors attempting to cross the International Date Line on their way to Asia had to turn back due to a software bug that crashed their onboard computers. Although this wasn't a cyberattack, it demonstrates the potential that a carefully designed and implemented attack could have on aircraft or other weapons systems heavily controlled by software. Fortunately, the F-22 fighters were able to follow their in-air refueling tankers back to base for a safe landing. A different software issue in early 2014 caused air traffic controllers to ground flights in Los Angeles, California, to avoid a collision with a U-2 reconnaissance aircraft. Analysis later showed that multiple waypoints and altitude changes between control zones had resulted in a software error.

Command and Control

Military command-and-control systems are a particularly attractive target in cyberwar. As the U.S. Department of Defense continues to integrate computing capabilities into a broader and broader array of military systems, it references this as **Command, Control, Communications, Computers, and Intelligence (C4I)**. C4I systems provide situational awareness—the ability to know where both friendly and enemy forces are—and to react and respond. C4I systems include capabilities like weapons targeting, including the data that is passed to weapons as they are en route to their target. The links and control systems of active weapons, or the real-time data that soldiers and commanders use to decide what they should do and where they should be in a combat situation, are obvious targets for cyberattack.

Due to their critical role in battlefield control, C4I systems are a very important part of current and future combat strategies. Defending C4I systems while they are in use is very important. The endpoint devices that individual soldiers carry into combat, the sensor systems that provide information, and the control systems for weapons platforms and smart weapons themselves all must be protected, in addition to the more traditional computer networks and devices used by command staff.

Embedded Systems

The growth of devices built in to many of the technologies that surround people's daily lives creates a new type of target for cyberattack. Embedded systems like telephone switches, traffic light controls, vehicle-based computers, consumer electronics, computers built in to buildings, and even appliances with network access all provide a target for attackers. Such a target can provide a useful launching point for further attacks or access to disrupt lives and productivity.

Some embedded systems use traditional operating systems, but many use specialized versions that are designed to meet the specialized needs of the devices or systems they are built into. Much like the SCADA and ICS systems examined earlier in this chapter, embedded systems are far less likely to be patched or to have strong security models in place, because they are focused on performing specialized tasks. Designers didn't expect them to be exposed to network attacks or other threats.

Embedded systems create a number of unique challenges for defenders, as security standards and other common tools are rare or nonexistent for most embedded systems. Military and defense-specific embedded systems often receive special attention to help them be more resilient than civilian and commercial systems. But the resulting tradeoff is evident in the U.S. Department of Defense cybersecurity strategy: Faster, more nimble acquisition and update strategies are necessary to help ensure that outdated and devices known to be vulnerable do not remain in service.

Attacks like the Stuxnet attack demonstrate that motivated nation-states can research and exploit embedded systems as well as ICS and SCADA technologies. Embedded systems in critical locations require both awareness and dedicated security designs to ensure that they don't create a path for an attacker or an exploitable weakness in an organization's capabilities.

Medical Devices

A type of endpoint that most defenders would never have considered until recently became highly visible in 2013, when former U.S. Vice President Dick Cheney revealed that his doctors had disabled the wireless control capabilities of his pacemaker. Like many other computerized devices, modern pacemakers support wireless updates to their settings and can provide information about their current status to a nearby receiver.

Researchers reverse engineered pacemaker radio controls as early as 2008, with findings published in an IEEE symposium paper titled "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses." Similar research in 2011 demonstrated vulnerabilities in insulin pumps that could inject users with fatal doses of insulin, revealing yet another potential attack method.

Although so far no one has documented attacks against implantable or wearable medical devices, the possibility of attacks against heads of state or others who use wirelessly accessible devices expands the boundaries of cyberwarfare to include direct physical harm. It is possible that an attacker could take even subtler action to speed up or slow down a diplomat's heart rate or modify his or her blood sugar levels.

Despite a push by the FDA, no standards for the security of medical devices have been created or widely adopted. Nor have best practices for how to secure them while providing access for medical professionals and emergency responders been implemented. Medical device manufacturers, like the creators of many other specialized systems, continue to provide unique solutions and thus can create unexpected challenges for endpoint protection in an unexpected place.

Attacking Endpoints

In both computer network defense and traditional information security practice, one of the best ways to understand endpoint defense requirements is to learn to think like an attacker. Attackers analyze endpoints, their management practices, their design, and their administrators and users all as potential targets, looking for gaps in defenses. Once they find a way in, either through vulnerabilities, misconfigurations, mistakes, or simply the helpful nature of the staff who use the systems, they can conduct further attacks as a springboard into a network. They can use the device for its intended purpose, but to their own ends. Or they can just gather data from the endpoint they have under control.

The huge number of endpoint types leads to an even larger number of possible types of attacks against them. It helps to categorize the attacks into a few useful groups to match defensive techniques against the attacks themselves. A few of the ways to categorize attacks are:

- Attacks that require physical access, such as inserting a hardware keyboard logger into a system, or making a physical copy of a drive by capturing the encryption key from live memory without remote access to the machine
- Attacks that require network access, such as denial of service attacks, or attacks against services that the system provides, such as a Web server or file server
- Attacks that require the user or an administrator to take action, such as phishing attacks or other forms of social engineering that lead a user to compromise the machine by inadvertently helping an attacker
- Attacks that target the hardware or firmware of the device, which often require access to the design or manufacturing process of the device to compromise the design or to insert a vulnerability or Trojan into the firmware before the system is sold
- Attacks against application software, such as Web browsers; most application software attacks require the attacker to discover a vulnerability, either through vulnerability testing or by software vulnerability analysis using the actual code that makes up the program
- Attacks that use the endpoint's normal function against it, such as those that provide fake feedback to intrusion detection systems, causing them to block legitimate traffic, or the GPS attacks against U.S. drones that allegedly have caused the drones to try landing in the wrong place

Other categories can be created to match specific types of endpoints, with the primary goal in mind of grouping attacks in a way that allows an organization to determine which defenses are appropriate and which can reasonably be put in place. Some defenses, such as awareness, can help against attacks by both detecting and helping to prevent attacks, whereas other defensive techniques and designs will only be effective against a specific type of attack or scenario.

FYI

Firmware is the software that has been stored in read-only memory, which is part of the hardware system. Firmware typically contains the basic operating processes of a device, such as the basic input/output system (BIOS) of a PC or the software that operates a pacemaker. The Stuxnet malware was specifically designed to attack the Siemens Simatic S7-300 PLC's firmware, which had one of two very specific variable frequency drive units attached to it, allowing it to target specific uses of that PLC.

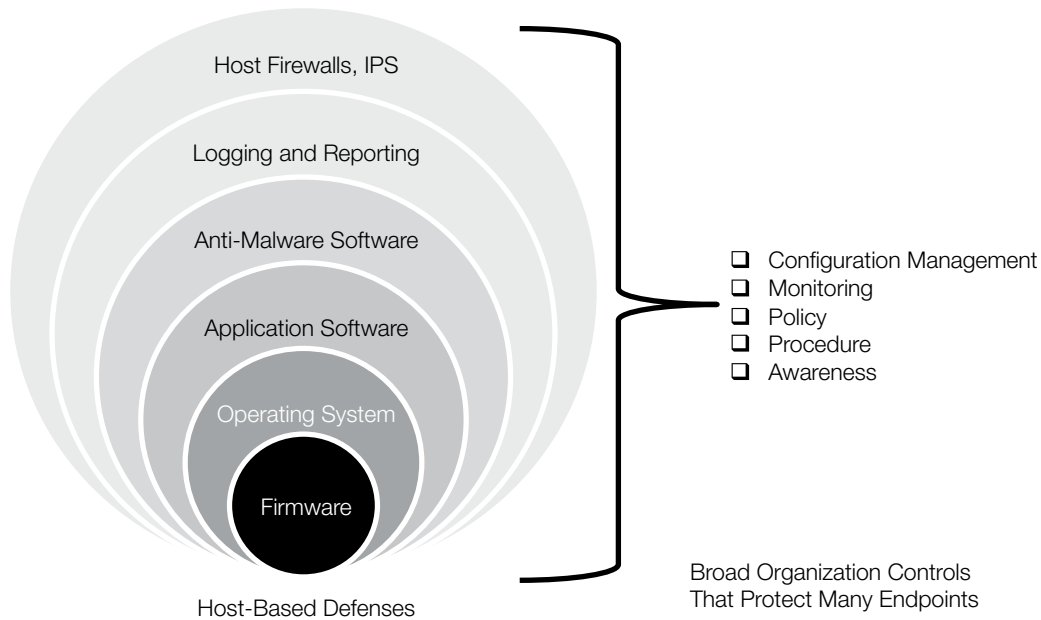
Protecting Endpoints

Computer network defense strategies for endpoint protection require assessment of the threats that the endpoint systems and devices will face. Once defenders have assessed the likely threats and which methods would be effective against them, they can balance the costs of the defenses and their ability to implement them against the need of their organization to provide that level of defense.

Typical defense-in-depth strategies for endpoints include a number of common layers:

- Physical security
- Policy and procedures
- Configuration standards
- Central management
- Awareness and information sharing
- Anti-malware and antivirus software
- Configuration management, patching, and updates
- Whitelisting and blacklisting
- Testing, including penetration testing and the use of red teams

Figure 11-3 shows many of the typical layers of defense for a computer workstation. Defenses start at the firmware and hardware level, which provides the underlying environment that the rest of the software and defenses reside on. The computer's operating system and the application software that it runs provide the next layers of defense, as the operating system must be properly secured, and the application software must prevent attackers from using it to compromise the system. Anti-malware software works to detect infections, whereas logging and reporting capabilities provide status information about the system. Finally, most network-attached systems now use some form of system-level firewall or other network protection that filters and sometimes monitors the network's connection to other systems and networks for attacks.

**FIGURE 11-3**

Defense in depth in endpoint protection designs.

Endpoint protection also relies on non-system-specific control capabilities, such as configuration management, central monitoring, and the human side of controls via policy, procedures, and awareness. These defenses reside outside individual systems, and are typically common to a larger group of systems or devices, rather than providing unique controls for each computer.

The following sections explore each of the major defensive concepts. There are many specific techniques, and each system or device may require unique designs or special capabilities to properly protect it. Defensive techniques for common operating systems and frequently used devices are broadly available, but relatively uncommon systems or those that are not part of a typical organizational cyberdefense strategy will need special attention to understand their defensive needs.

U.S. Department of Defense Strategy

The U.S. Department of Defense's cyberspace operations strategy provides some insight into the DoD's views on endpoint protection. It states that "Cyber hygiene and defensive posture" are critical to the strategy. **Cyberhygiene**, in this context, includes awareness on the part of individuals in the DoD, software and operating system updates, cybersecurity practices for users and administrators, and configuration management. It further includes practices that are not endpoint centered, such as network security and network

management techniques. The strategy notes that “intrusions may not always be stopped at the network boundary,” emphasizing the need to provide endpoint security as well as monitoring and response capabilities.

The Department of Defense has a four-point process to provide this defense:

- Improve cyberhygiene, including traditional and developing information security techniques and strategies, such as patching, awareness, continuous renewal processes that help avoid out-of-date devices and software, and design and maintenance standards and behaviors.
- Strengthen workforce communications to deter and mitigate insider threats. This strategy emphasizes both the role of humans and a “culture of information assurance”—with individual responsibility and changes in behaviors and attitudes due to more significant penalties for malicious activities.
- Employ an active cyberdefense capability, a real-time ability to “discover, detect, analyze, and mitigate threats and vulnerabilities.”
- Develop new defense operating concepts and computing architectures, with an emphasis on mobile and cloud computing.

The Department of Defense doesn’t provide in-depth information on its implementation strategy for each element of its overall strategy. This ensures that attackers can’t simply use publicly available information to craft their attacks or to find potential holes in DoD’s defensive strategy.

Defense in Depth in Endpoint Security

The concept of defense in depth remains important when deploying endpoint defenses. Each endpoint can become its own virtual castle, with protective layers providing defenses against a variety of attacks. Designing standards around how devices should be protected in various situations and configurations can provide a good baseline to give organizations with new types of endpoints a starting point to work from.

The process of designing endpoint layers for protection in a variety of situations can also be important, particularly for systems that travel. Laptops, mobile devices, and other systems that will leave their normally secure locations must be protected against threats beyond the normal attacks a workstation in an office or a server in a data center might face. Devices that attackers could access need even more protection to ensure that they haven’t been modified, accessed, or had their hardware replaced while they were out of their owner’s hands.

Much like a medieval castle under siege, endpoints also shouldn’t have to stand alone against attacks for a long period of time. A strong management system, reporting and logging capabilities, testing processes, and capable administrators and defenders are all necessary to keep even a well-defended system secure in the long term.

FYI

Attackers in Afghanistan planted a USB thumb drive loaded with malware in the parking lot of a Department of Defense facility. When the thumb drive was plugged into a laptop, it infected the laptop with a worm that spread through military networks. No information has been released on what data was exposed during the time the infection was active on military networks. The 14-month-long defense against the attack is known as Operation Buckshot Yankee.

Physical Security

Although it might seem obvious, the need to protect endpoints from falling into the hands of attackers is one of the most basic requirements of endpoint security. If attackers have physical control of a system and enough time, they can almost always compromise the system or the data it contains. If they have less time with the device, they might copy its data or insert software or hardware bugs to capture keyboard input—or even record conversations that happen near the device. Some attacks even rely on replacing the device or system with an apparently identical system that is sent on to the original owner or new purchaser of the gear.

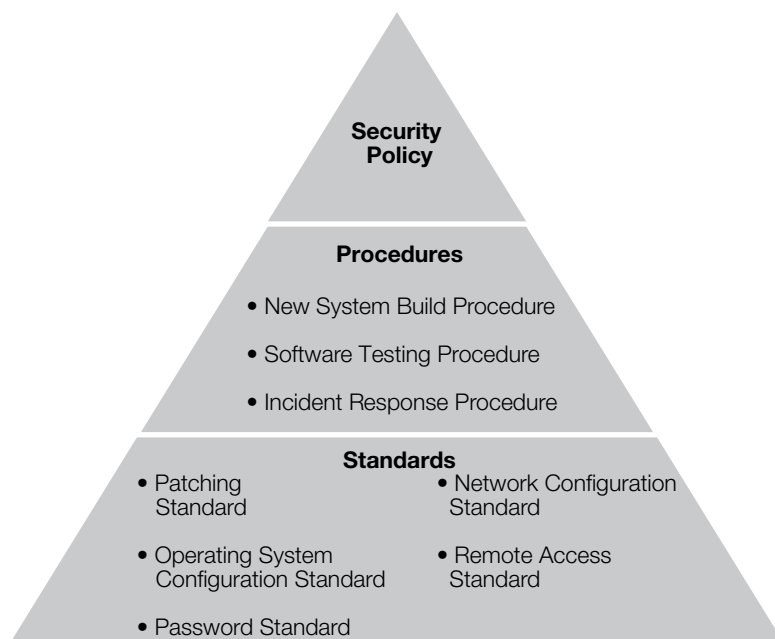
Physical security also plays a role in the devices brought into secure environments. The civilian sector concern about staff bringing their own devices and connecting them to internal networks is even more critical for military and governmental organizations. Insecure, untrusted devices connected by staff to a sensitive network can provide a bridge into it for attackers. Even bringing in a simple USB thumb drive can cause problems if that device contains malware.

Policy

The root of most defensive strategies is a cyberdefense policy. Policies assign responsibility and set the overall tone for computer network defense activities. Well-written policies don't specify specific technologies or processes. Instead they focus on the organization's strategic direction. Once a policy has been created, organizations will then create procedures and standards to ensure that their staff can implement the policy effectively. Policies are typically authorized by the highest levels in an organization to ensure that they are both appropriate to the organization and that they have support when policy issues come up.

FYI

The U.S. Department of Defense includes a deputy assistant secretary of defense for cyber policy. The position is tasked with providing support to the DoD by "formulating, recommending, integrating, and implementing policies and strategies to improve the DoD's ability to operate in cyberspace."

**FIGURE 11-4**

Relationship of policy, procedures, and standards.

Figure 11-4 shows the relationship between policies, procedures, and standards. A broad security policy provides the core guidance to develop procedures. Those procedures are used to guide the development of standards for specific configurations and actions. Together, policies, procedures, and standards make up the set of guidance that helps to ensure that people involved in endpoint protection act appropriately.

Procedures

An organization's procedures for endpoint defense in depth are based on the policy or policies the organization has in place. Procedures typically describe things like how the organization acquires systems or develops new systems, how the organization assesses risks, or how it responds to attacks. Formalized processes that define what, when, who, and how the organization takes action ensure that responses are predictable and reliable, and that the staff who are responsible take appropriate action.

The U.S. Department of Defense has defined a number of requirements for its own procedures in response to the increasing threat of cyberattack. The DoD's acquisition strategy says that the "DoD will take a security in depth approach to design, acquisition, and implementation of trustworthy systems." This results in four major concepts that the DoD intends to apply in its procedures:

- First, speed is a critical priority. The DoD's acquisition processes and regulations must match the technology development life cycle. With information technology, this means cycles of 12 to 36 months, not seven or eight years.
- Second, DoD will employ incremental development and testing rather than a single deployment of large, complex systems.
- Third, DoD will be willing to sacrifice or defer some customization to achieve speedy incremental improvements.
- Fourth, DoD's information technology must adopt differing levels of oversight based on the priorities it assigns to critical systems.

The DoD is taking advantage of procedural changes to help ensure that each stage of its acquisition process is appropriate to modern cyberwarfare requirements. It demonstrates an awareness of historical issues with slow acquisition and updates, which resulted in out-of-date and often vulnerable systems, as well as issues with slow, long-term development cycles that made software hard to fix and difficult to update when problems were found. Similarly, the DoD is showing a willingness to simplify procedures to improve responsiveness.

NOTE

The National Security Agency provides configuration guides and other security management information for applications, operating systems, and wireless devices at http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/.

Configuration Standards

Configuration standards define the settings and options a system, application, or other part of an endpoint system has in place. Common operating systems and devices often have publicly available configuration standards that have been published by the manufacturer, groups of experts, or specialized organizations. Standards help to set expectations for what a given system can be expected to do, how it will respond to attacks, and how it is secured.

Organizational requirements drive configuration standards. Even when industry standards exist, organizations will typically modify the standards before adopting them to their specific needs. Systems that comply with specific configurations can also be *certified*

in those standards, proving that they have reached a specific level of security compliance through a combination of their configuration and capabilities.

Central Management

Central management systems provide the ability to enforce configuration standards, report on the status of systems, and make changes and updates to those systems from a single, central location. This allows management of large numbers of endpoints rather than requiring each individual endpoint to receive individual maintenance. Central management is a critical part of large-scale endpoint defense strategies because it helps maintain compliance with standards. A system that no longer meets those standards may be compromised or have problems that must be addressed.

Central management can also create a threat to endpoint systems due to the level of control it has over endpoint systems. A compromised central management system can allow attackers to modify configurations or to ensure that defenders are not notified of issues with their systems. Thus, central management systems must have extra layers of defense included in their own endpoint defense design.

Configuration Management

The basis for most central management systems is configuration management. Although configuration management systems for individual endpoints also exist, most networked systems rely on a central management system to provide configuration management.

Configuration management systems typically apply one or more prebuilt configuration templates to a device, which provide control over a variety of settings and capabilities, such as:

- Security settings
- Software versions
- Network settings
- User rights management
- User interface settings

Patches and Updates

Many central management systems provide another critical service for endpoint protection: patch and update management. A typical computer in use today will have an operating system; numerous hardware drivers that make video, audio, and other devices work; application software such as word processing and spreadsheet software; Web browsers; and a variety of other software packages. It is critical to the security of computers and other devices to have current software versions and patches that provide security fixes.

Patch and update management is often a challenge in complex environments. New software patches and versions might not be compatible with older software or might have flaws. Individual endpoints might not properly install the software update, leaving them vulnerable. Despite potential flaws, without central management capabilities for configuration and patch management, it is nearly impossible to manage and update large numbers of systems in a reasonable amount of time.

FYI

One danger of patch management systems is the reliance on the system to ensure patch installation. Some patches can fail without the patch management and configuration management systems being aware of it. In fact, some will even show the correct version when asked, but the patch itself will not have installed properly, leaving the system vulnerable. Although patch management and configuration management helps, it isn't always a guarantee of correct configuration and updates.

Awareness

The Department of Defense noted in its cybersecurity strategy that “it is just as important for individuals to be focused on protecting themselves as it is to keep security software and operating systems up to date.” It’s critical for endpoint protection that system users—along with the administrators and security personnel who build, support, maintain, and defend those systems—be aware of both the status and typical behavior of their systems. They must also be alert to the threats and attacks they are likely to experience.

NOTE

In March of 2011, attackers used an e-mail phishing attack to persuade staff at a defense contractor to run malware. The final estimate of data exposure was 24,000 files, including sensitive data from the defense contractor. Phishing is one of the most common types of social engineering attacks, which focus on human weaknesses, and is a frequent focus of awareness efforts.

Awareness as a defensive measure requires that staff know about threats and attacks, and be inclined to use that knowledge. Most awareness programs use training in various forms as their basis, but training isn’t the only option. More-advanced awareness programs often combine experience or testing-based experiences for participants, including simulated attacks that allow feedback on which issues are detected and how participants respond.

Awareness also means that those who are responsible for administration of endpoints, including their hardware, software, and configuration, must monitor information sources for recently released updates and active exploits that target vulnerable parts of their systems. An organization that has a great level of user security awareness, but that does not remain up to date on software patches, may detect a breach, but will likely not have acted to stop it.

Information Sharing

Awareness of attacks and new techniques for defending and attacking systems often relies on sharing knowledge between organizations. Information-sharing organizations include organizations such as the U.S. government’s U.S. Computer Emergency Readiness Team (US-CERT) and Information Sharing and Analysis Centers (ISACs). Information sharing as an awareness strategy is a key part of the DoD and U.S. government’s information security strategy. Information-sharing controls are in place to ensure that information about actual attacks and vulnerabilities is distributed only to appropriate individuals and organizations.

Anti-Malware and Antivirus

Many of the most successful attacks against endpoints in cyberwar have been malware-based. The Stuxnet and Flame attacks both focused on malware-based infections, and the Aurora attacks and other advanced persistent threats (APTs) use malware as a key element of their ongoing control of systems. Anti-malware technologies are therefore an important layer in the defense-in-depth strategy for cyberwar.

FYI

In May 2014, antivirus manufacturer Symantec publicly noted that antivirus software is no longer an effective solution by itself.

Anti-malware software uses two primary techniques to detect malware:

- **Signature-based detection**, which focuses on knowing the digital fingerprint of a malware package. These signatures are packaged into frequent detection package updates, which anti-malware vendors release to their customers. Unfortunately, modern malware uses a variety of techniques to help ensure that their tools don't have the same fingerprint across different installations, making signature-based detection less likely to work. Anti-malware vendors continue to develop additional capabilities in an attempt to overcome this, but attackers have an advantage when signatures are the only line of defense.
- **Heuristics**, which involves behavior-based detection techniques. This provides defenders with the ability to observe what a program is doing and then to determine whether that activity looks like malware activity. This offers a better chance to detect otherwise harmless-looking malware, but it also runs the risk of detecting a legitimate program that takes actions that malware might also take.

Unfortunately, traditional techniques for detecting malware have become less effective over the past decade as malware creators have used increasingly advanced techniques to hide their tools from defenders. Now defenders must use alternate techniques to protect systems, whereas traditional signature-based defenses used to provide strong protection.

Network Protection

Much of the protection that endpoint devices require against network attacks is handled as part of the design of the networks they connect to. But endpoint devices still must be able to protect themselves against the traffic that reaches them past those network filters and protective systems. Therefore, many systems provide their own host-based protections. For most devices, those take the form of two types of network protection:

- Firewalls, which block communication both to and from the system based on a set of rules.
- Intrusion prevention systems, which are software-based filters that use behavior- and signature-based detection capabilities. These capabilities are like those used for malware defense to recognize and stop attacks both against the system itself and those that might come from within the system on which they are installed.

The Failure of Anti-Malware Software

Traditional antivirus applications are a familiar tool to computer users, and are typically considered a necessary part of a well-designed security infrastructure. Unfortunately, the effectiveness of traditional antivirus methods that use signature-based detection techniques has been steadily decreasing. Next-generation malware packages, particularly those used by advanced persistent threat organizations like those operating the Aurora attacks, are nearly invisible to antivirus and anti-malware tools.

Researchers studying the malware applications used to compromise machines in APT attacks have discovered evidence that APT tool writers use common antivirus packages to test their applications. Once they're sure that the attack won't be caught by those protective applications, they can deploy the malware with the expectation they won't be caught. They can even continue to use publicly available updates from the vendor to continue to test their malware, and can change it if and when it is detected.

This doesn't mean that anti-malware software doesn't have a place in endpoint defense strategy. Malware that isn't as advanced as that employed by highly advanced actors remains a threat that network defenders must take seriously. Less-advanced threats often recycle existing malware, or make relatively minor modifications, allowing traditional detection methods to work. Thus, much like a flu shot, traditional antivirus tools can help protect against the known threats and can have some success against unknown threats—even if they're not a complete solution.

Encryption

Encryption for endpoint defense typically involves full disk encryption intended to prevent theft of the data that resides on the system or device if it is stolen or is outside its owner's possession. This doesn't prevent theft of system data when the system is in use, so encryption isn't as useful against attackers who compromise the system using a vulnerability in the operating system or software applications.

Full disk encryption for many secure systems is assisted with a **Trusted Platform Module (TPM)** chip. This is a cryptographic processor built in to the motherboard of the device. TPM modules are unique to each system. They allow the system to prove that it is the system that should be unlocking a given hard drive or other storage device. Systems without TPM chips must rely on other ways to verify their identity. Sometimes systems do this by providing a digital certificate stored on a USB flash drive and matched with a password that only the system's owner should know.

Unfortunately for those tasked with defending systems, most disk encryption systems that aren't built in to the disk itself are vulnerable to a variety of attacks. These attacks use techniques to recover keys stored in memory, or **side-channel attacks**.

FYI

In 2012, NASA lost a laptop with the algorithms required to control the International Space Station. The laptop was not encrypted, meaning that whoever ended up in control of the system could access the algorithms directly.

These target other ways to recover the keys to the drive, such as capturing keyboard input, or even recording the sounds of typing on the keyboard to determine which keys were pressed.

Although full disk encryption is one of the most important parts of endpoint protection using encryption, encryption also plays an important role in communication between endpoints. It's also key in the processes used to provide updates and patches that are verifiably the originals from the manufacturer or another trusted organization.

Due to the extensive use of encryption techniques to secure and protect both data at rest and in transit between systems, attacks on cryptography are increasingly a focus for nation-states. The additional resources, technological tools for drive analysis, and advanced intelligence acquisition techniques that nation-states can bring to bear on individual devices mean that encryption is useful, but cannot be considered impervious to attack.

Whitelisting and Blacklisting

The ability to choose which software, Web sites, services, or access a system provides can be very useful when designing endpoint security. Whitelisting and blacklisting provide this capability, allowing administrators and security staff to ensure that the decisions that they make and the policies they must enforce can be successfully put into place.

Whitelisting

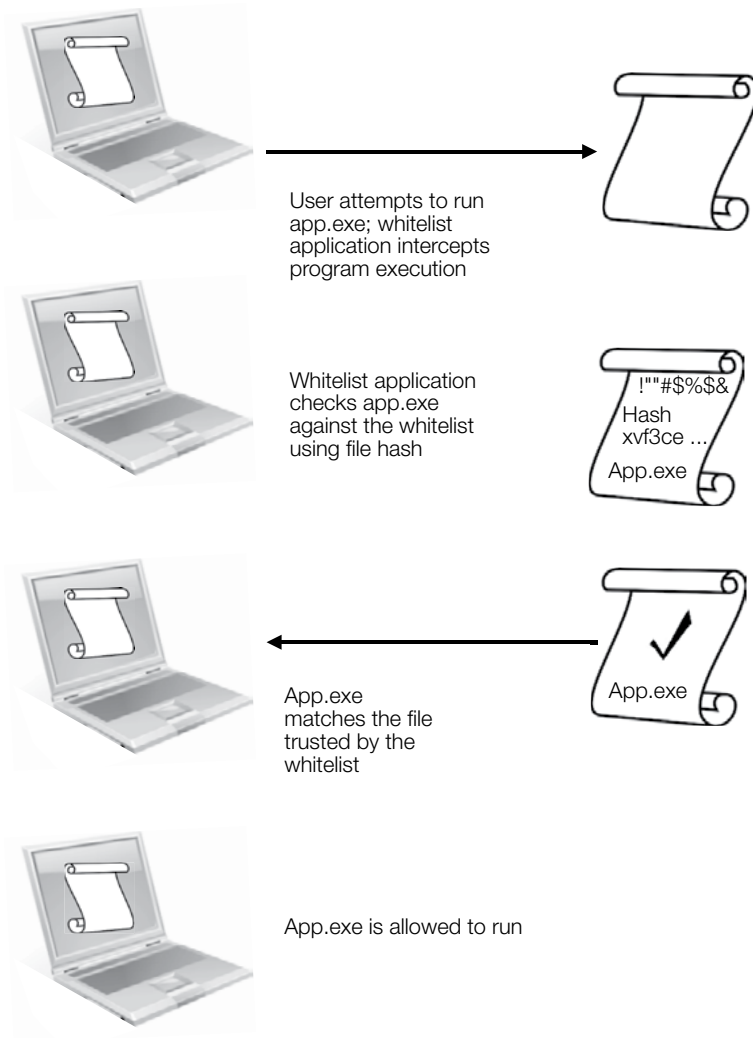
Whitelisting relies on the ability to build a list of trusted software, systems, networks, or other resources. Once a whitelist is built and implemented, it's checked each time a request is made to use that type of resource. If the resource is on the whitelist and matches it, access to the resource is allowed. If the resource is not on the list, access isn't allowed, and further action must be taken to access it. A number of types of commonly used whitelisting are available, including software or application whitelisting, Web site whitelisting, and even user whitelisting that allows specific users access to systems.

NOTE

Whitelisting is trust-centric, whereas blacklisting is threat-centric. This means that whitelisting is often used when it is reasonable to know every item that should be on the whitelist, without updates and maintenance becoming unmanageable. Blacklisting is used when a list of threats can be built and maintained more effectively, or when access should be allowed in most cases unless it is intentionally blocked by the blacklist.

FIGURE 11-5

Whitelist check process for a software application.



Whitelisting has a number of advantages in a high-security environment:

- It allows administrators to prevent running of unauthorized software.
- It can provide a very strict set of requirements for Web sites or other resources.
- It does not require administrators to think of every possible alternative or workaround.

Figure 11-5 shows a typical application whitelisting scenario. When a user attempts to run a program, the whitelisting application intercepts the request and checks the program against its list. The whitelist program verifies that the application being run is actually the whitelisted application by checking the file, its location on the workstation,

and other details about the program. If it matches properly, which it does in this example, it is then allowed to run. If the application did not match, or had been modified, the whitelisting program would prevent the user from running it, and would notify an administrator if it were configured to do so.

Blacklisting

Blacklisting reverses the technique used in whitelisting and builds a list of prohibited applications, files, sites, or other data or access. Figure 11-6 shows a blacklist check for a sample endpoint system using a blacklist application that tracks known malicious Web sites. When the system attempts to access a blacklisted site, the access is stopped or, as the example shows, it can be redirected to an awareness Web site.

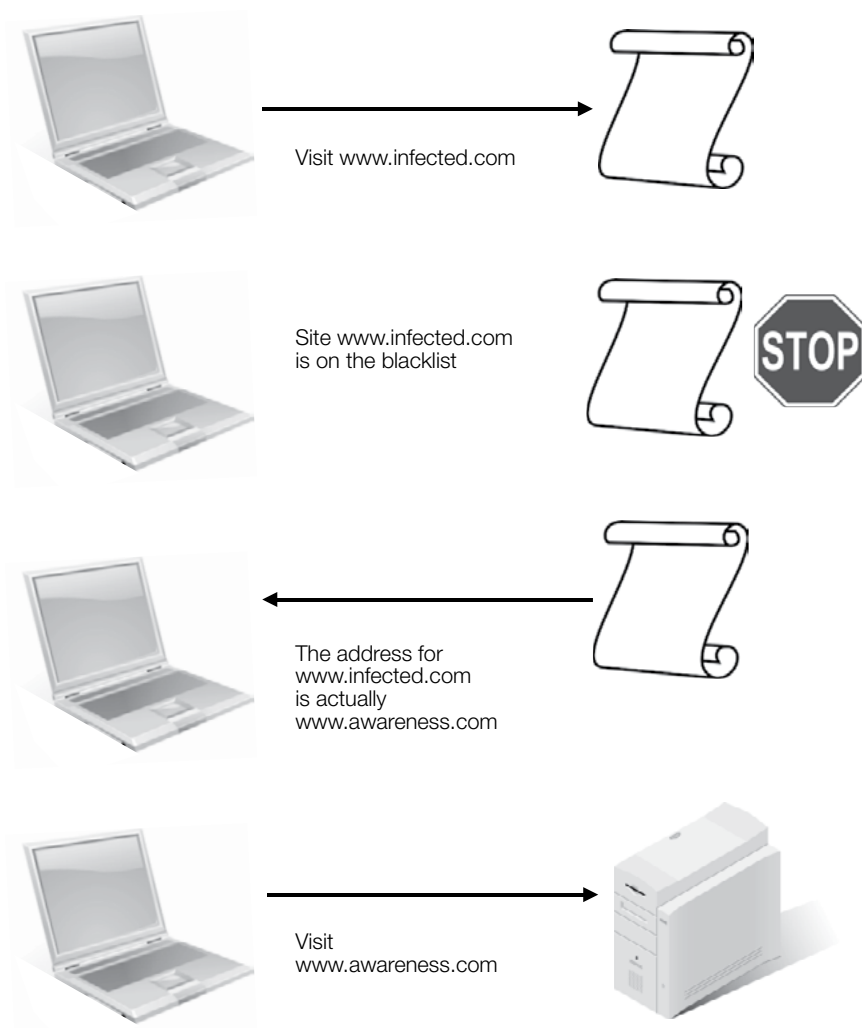


FIGURE 11-6

Blacklist checking for a blacklisted Web site.

FYI

Whitelisting is typically considered a more secure solution than blacklisting because it works on a foundation of trust. Unfortunately, the difficulty of keeping a whitelist up to date means that blacklisting is more commonly used in most environments.

Blacklisting offers advantages when specific accesses must be blocked, or when the list of known files or data is well known. Blacklists can also be useful for quick responses, as adding a known problem Web site or file to a blacklist distributed to endpoint systems can stop those systems from suffering the same issues other systems already have.

Blacklisting can also create a number of problems:

- Blacklisting can result in legitimate resources being blocked.
- Some blacklisting can be overly broad, resulting in useful resources being blocked at the same time as threats.
- Blacklists require updates and maintenance to ensure that new threats are added.
- Blacklisting becomes increasingly difficult as the size of the blacklist grows.

Testing

Once endpoint defenses are in place, they must be tested to ensure they are performing as expected. Computer network defense plans typically include a variety of testing methods that verify settings and technical configurations as well as procedures, practices, and the awareness of staff who use and support the endpoint systems. Military and government agencies use a variety of testing methods and often have access to methods and resources beyond those used for typical civilian information security operations. A few of the most common testing techniques include:

- **Software testing** is commonly used both during the development of software and when software is deployed using automated and manual testing methods. Automated, software-based testing applications allow defenders to validate new software's resistance to common attacks. The actual underlying code that makes up software can also be tested for common problems using source code validation and testing tools and techniques.
- **Certification** to standards such as the Common Criteria provides extensive testing guidelines, against which certification organizations can test computer systems.
- **Port scanning** tests systems and network devices to see what network ports they have accessible. Port scanning is often used to quickly verify if a system is providing the services it is expected to provide, or if it responds in unexpected ways.

- **Vulnerability scanning** is used to test the services that a system or device provides and to check those services for vulnerabilities either by checking the version information it responds with or by attempting to exploit vulnerabilities known to exist in the service.
- **Configuration management systems** can provide useful testing and reporting capabilities that allow administrators to verify that the systems under their control have the settings, software, and policies applied that they were intended to have.
- **Penetration testing** is a broad discipline that uses attacks and exploits against an organization to verify whether and how its security controls, systems, and staff respond to attacks. Two major categories of penetration tests are typically conducted. The first type is *white box penetration testing*, which provides the testers full information about the targets. White box testing is also sometimes known as *crystal box penetration testing* because it provides a complete view of the target. The second common type is *black box penetration testing*, which provides the testers no prior knowledge, requiring them to act like an attacker who doesn't know the internal workings of the organization and its systems.
- **Simulations** and **war games** are used by organizations to test their processes by creating a scenario for their staff to practice what and how they would react in the event an issue occurred. Simulations are often used to test procedures and to identify issues with processes.

Red Teams and Tiger Teams

Testing that goes beyond simulation into active tests of defenses as part of planned exercises often uses specialized teams of trained and skilled attackers. These teams, sometimes known as **tiger teams**, use the same tactics and tools as the actual attackers an organization is likely to face. This provides a better test of the defenses put in place and can reveal much more than a simulation or internal testing might.

The U.S. National Security Agency's Cyber Defense tiger team is known as a **Red Cell** or **red team**, part of a group of organizations that serve as the opposing force during simulations and exercises. The NSA's Red Cell team participates with elements of the U.S. Department of Defense's cyberwarfare teams in live-fire training exercises that help to build additional strength for the U.S. Naval Academy and other groups.

Some organizations are beginning to use *purple teams*, which are combinations of aggressor red teams and defender blue teams. Their intention is to use the combination of teams to better understand how defense and attacks can work together, and to allow shared knowledge in both scenarios.



CHAPTER SUMMARY

This chapter examined the concept of endpoint defense. There are many types of endpoints, including computers, mobile devices, ICS and SCADA systems, military endpoints such as weapons systems and command-and-control devices, and embedded systems. The existence of many types of endpoints makes defending them a challenge—configurations and capabilities vary widely between them. Due to the wide variety of endpoints and the ways they can be targeted, attacks on endpoints may consist of anything from social engineering that targets users to complex attacks that require access to systems’ supply chain and design process.

This chapter also explained that endpoints are common cyberwarfare targets because they contain data and can provide access to other parts of a computer network. Defenses against attacks on endpoints often focus on a defense-in-depth strategy that combines physical security, policy, procedures, standards, configuration management, central management systems, awareness, and technical controls. All of these protections must be tested, and many organizations do so by conducting penetration tests and using red teams—groups of experts who help validate the protections their defenders put in place.



KEY CONCEPTS AND TERMS

Blacklisting	Heuristics	Simulations
Certification	Industrial control system (ICS)	Software testing
Command, Control, Communications, Computers, and Intelligence (C4I)	Penetration testing	Supervisory control and data acquisition (SCADA)
Configuration management systems	Port scanning	Tiger teams
Cyberhygiene	Programmable logic controllers (PLCs)	Trusted Platform Module (TPM)
Distributed control systems (DCSS)	Red Cell	Vulnerability scanning
	Red team	War games
	Side-channel attacks	Whitelisting
	Signature-based detection	