3

NETWORK SECURITY

## LEARNING OBJECTIVES

By the end of this chapter, you should be able to:

* Describe the threat environment, including types of attacks and types of attackers.
* Explain how to protect dialogues by cryptography, including encryption for confidentiality, electronic signatures, and host-to-host virtual private networks (VPNs).
* Evaluate alternative authentication mechanisms, including passwords, smart cards, biometrics, digital certificate authentication, and two-factor authentication.
* Describe firewall protection, including stateful packet inspection, next-generation firewalls, and related intrusion prevention systems.
* Describe the role of antivirus protection.

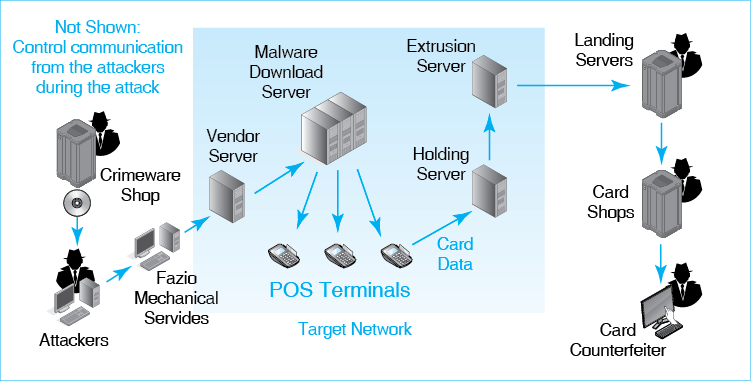
# The Target Breach

Near the end of the 2013 holiday season, Target announced that thieves had stolen data from 40 million credit cards scanned at Target stores in preceding weeks.[[1]](#footnote-1) The attackers had downloaded malware to nearly all point-of-sale (POS) systems in American Target stores. This malware captured magnetic stripe information and sent it to data thieves.[[2]](#footnote-2) Target did not reveal in its first announcement that thieves were already committing fraud with the stolen card data. A month later, Target announced that a separate but related theft had occurred during roughly the same period. Attackers had stolen personal information on roughly 70 million Target customers.[[3]](#footnote-3) Consumers were shocked and worried by these thefts. Many cancelled their charge cards and demanded new cards from their banks. Within weeks, a barrage of lawsuits began. Based on past megabreaches, such as the TJX breach described in Chapter 7, the final cost to Target will be hundreds of millions of dollars.

## The POS Attack

Target released little information about either compromise, but analysts gradually constructed a likely picture of how the credit card number theft had occurred. News reports naturally focused on the POS systems, but the theft involved a complex series of steps inside and outside Target. Figure 3-1 shows the most important of these steps.

Figure 3-: The Target Breach



The theft did not begin with a direct attack on Target. Rather, it began with an attack on Fazio Mechanical Services, which did work for Target in the Mid-Atlantic region.[[4]](#footnote-4) Fazio had credentials on a vendor server that handled electronic billing and other matters. The attackers probably sent an employee a spear phishing e-mail that tricked the employee into loading malware onto his or her machine. The malware captured the Fazio credentials on the vendor server and sent it back to the attackers. The attackers then used these credentials to get access to the vendor server. From this initial foothold, they were able to move more deeply into the Target network.

Now inside the Target network, thieves uploaded point-of-sale (POS) malware, which they had purchased from an online crimeware shop, to a malware download server within Target. There is suspicion that the thieves actually took over Target’s internal server that downloaded updates to the point-of-sale systems.[[5]](#footnote-5) In any case, the malware was downloaded to a few POS systems initially and then to nearly all Target point-of-sale systems in the United States.[[6]](#footnote-6)

The malware was a variant of the BlackPOS malware that had been in existence for almost a year.[[7]](#footnote-7) It was readily available at online crimeware shops for a price of about $2,000.[[8]](#footnote-8) The attackers probably modified the software to attack Target’s specific POS terminals.[[9]](#footnote-9) They probably also modified it so that existing antivirus programs would not detect it.[[10]](#footnote-10) It is common for hackers to maintain small server farms to test malware against popular antivirus products.

The malware collected magnetic stripe data from every card swiped at the terminal. This occurred before the information was encrypted and sent over the Target network. Most sources called the malware a *RAM scraper*, indicating that it sent everything in the POS terminal’s memory to the attackers.[[11]](#footnote-11) Actually, it was more selective, stealing only data on the magnetic stripes of swiped cards.[[12]](#footnote-12) This included the primary account number, the expiration date, the name of the card owner, and optional information. Stolen data did not include the card security code, which is a 3-digit or 4-digit number printed on a credit card. Companies ask you for this number when you cannot present your card physically. For credit cards, there was sufficient information on the magnetic stripe to create counterfeit credit cards. For debit cards, the theft included encrypted PINs, but there is no indication at the time of this writing that these PINs were decoded.[[13]](#footnote-13)

Data collected at the POS terminal went, as usual, to legitimate Target servers. However, the malware also sent the data to a compromised holding server where the data from all of the POS terminals was stored temporarily.[[14]](#footnote-14) For data extrusion, the attackers compromised another server that would deliver the data to the attackers outside the Target network.[[15]](#footnote-15) This extrusion server pulled batches of card data sets from the holding server and transmitted them to landing servers in Russia, Brazil, Miami, and other locations.[[16]](#footnote-16) The thieves could not conceal the IP addresses of the landing servers, so they probably moved the data quickly to other servers.

Now the attackers monetized their stolen data. They wholesaled batches of data to online *card shops* that then sold the data to counterfeiters. Data on individual cards was stored in a searchable database. For example, thieves know that using a credit card in a city that is not the owner’s may result in a credit freeze. Consequently, card shops allowed customers to search by zip code. Counterfeiters also refined their purchases in other ways, based on such factors as whether the card had a high debt limit. Based on the characteristics of each card, counterfeiters paid from $20 to more than $100 per card. The first customers received a money-back guarantee that 100% of the card data was useable.[[17]](#footnote-17) Over time, the guaranteed percentage fell, and prices declined.

The counterfeiters used the card data to create fake credit cards that looked legitimate down to the graphics used by individual banks. They then copied data from a single legitimate card onto the magnetic stripe on each counterfeit card. This allowed them to purchase high-end merchandise and then sell the merchandise to traditional fences.

The attacks needed to transmit control messages frequently into the Target network, in order to compromise servers and take actions to direct actions on these servers during the attack. All of these messages had to go through Target’s firewalls. Showing this information in Figure 3-1 would create an unintelligible spider web of arrows. However, it was critical for the attackers to maintain a hole in the victim’s firewalls during the entire attack process.

Test Your Understanding

1. a) List the steps taken by the attackers. b) How did the attackers gain access to Target’s network? c) List the internal Target servers the attackers compromised. d) How did the attackers exfiltrate the card data? e) List the criminal groups, besides the main attackers, who were involved in the overall process. f) What benefit did the attackers seek to obtain from their actions? g) Critique (positively or negatively) the fact that Target knew that fraud was already occurring with the stolen card data but did not reveal this when it announced the breach.

## Damages

It may take years before we will understand the damage from the Target breach fully. However, it is easy to identify victims in the case. One was Target itself. In the period from the breach revelation to February 2014, Target sales fell 5.3% from the previous year, and profits fell 46%.[[18]](#footnote-18) This profit decline was roughly $500 million. In addition, Target will probably pay out several hundred million dollars due to lawsuits brought by commercial and governmental organizations. The company’s Chief Technical Officer resigned fairly soon after the breach.[[19]](#footnote-19) The company’s CEO resigned in May 2014.[[20]](#footnote-20)

Consumers are protected against fraudulent credit card purchases—but only if they notify their credit card company quickly of fraudulent charges on their bills. Credit card companies will drop these transactions from bills. However, this process entails time loss and frustration. It sometimes even involves disagreements about whether charges are truly fraudulent. There is even more time lost if the consumer cancels the credit card and gets a new card to get better peace of mind. Finally, the prospects of credit card fraud and identity fraud created psychological costs for many cardholders.

Banks and credit card processors will not lose money in the case of reported fraudulent purchases. Just as the customer does not pay them, banks and credit card processors do not pay the retail stores in which the fraudulent purchases were made. These financial services companies will face substantial costs in the replacement of compromised cards. However, they are likely to recover these costs successfully in lawsuits against Target based on precedents set in the TJX breach discussed in Chapter 7.

Fraud will hit retailers the hardest. They rarely recover merchandise purchased fraudulently. However, there is one thing that physical retailers can do. Counterfeiters normally only create a single card master from which all counterfeit cards in a batch are made. All counterfeit cards in the batch have the same printed name, credit card number, expiration date, and other information. The magnetic stripe data, however, will be specific to a single compromised credit card. This is why store clerks look at the last four digits on the card number on the physical credit card. If this is different from information on the magnetic stripe, the card is fraudulent.

Test Your Understanding

2. a) How was Target damaged by the breach? b) Were banks and credit card bureaus damaged by the breach? c) How were consumers damaged by the breach? d) How were retailers damaged by the breach? e) What can retailers do to defend themselves against counterfeit credit cards? f) What individual victim or group of individual victims suffered the most harm?

## Perspective

The Target breach was not an isolated incident. Surveys have found that most firms suffer at least one compromise each year. Successful attacks are becoming ever more frequent, sophisticated, and damaging. In 2012, the director of the Federal Bureau of Investigation Robert Mueller made the following statement: “Terrorism remains the FBI’s top priority. But in the not too distant future, we anticipate that the cyber threat will pose the number one threat to our country.”[[21]](#footnote-21) In 2014, the Center for Strategic and International Studies, estimated global damage from cybercrime.[[22]](#footnote-22) It concluded that cybercrime reduced the entire world’s gross domestic product by almost one percent. Cybercrime is not a distant threat.

“Terrorism remains the FBI’s top priority. But in the not too distant future, we anticipate that the cyber threat will pose the number one threat to our country.”

Robert Mueller, Director of the FBI

# Introduction

Networks give us access to almost anything, anytime, anywhere. Unfortunately, they give the same access to criminals, national governments, terrorists, and just plain jerks. Wherever there has been opportunity, there has been crime and vandalism. Networks are no exception. Security is the snake in the network garden.

Network thinking focuses on software bugs, and mechanical breakdowns. In contrast, security thinking must anticipate the actions of intelligent adversaries who will try many things to succeed and adapt to the defenses you put in place.

Network thinking focuses on software bugs and mechanical breakdowns. In contrast, security thinking must anticipate the actions of intelligent adversaries who will try many things to succeed and adapt to the defenses you put in place.

Giving you even a broad view of security is too much for one chapter. The next chapter looks at how to manage security as part of overall network management. As security expert Bruce Schneier has said in many of his writings, “Security is a process, not a product.”

Test Your Understanding

3. How does security thinking differ from network thinking?

# TYPES OF ATTACKS

We will begin by looking at the threat environment that corporations face. The threat environment consists of the types of attacks that companies face and the types of attackers who engage in these attacks. We will begin by looking at *types of attacks*.

## Malware Attacks

Malware is a generic name for evil software. It includes viruses, worms, Trojan horses, and other dangerous attack software. Malware attacks are the most frequent attacks that companies face. Nearly every firm has one or more significant malware compromises each year.

Malware is any evil software.

Test Your Understanding

4. a) What is malware? b) What are the most frequent attacks on companies?

Figure 3-: Malware and Vulnerabilities (Study Figure)

Malware

A general name for evil software

Vulnerabilities and Patches

Vulnerabilities are security flaws in specific programs

Vulnerabilities enable specific attacks against these programs

Vendors release patches to close vulnerabilities

However, users do not always install patches promptly or at all, so continue to be vulnerable

Also, zero-day attacks occur before the patch is released for the vulnerability

Social Engineering

When there is no vulnerability

Trick the user into doing something that will compromise security, such as opening an e-mail attachment

Phishing makes an e-mail message appear to be legitimate to a group of people (bank customers)

Spear phishing is aimed at individuals or a few individuals (more effective)

Going to a website and being tricked into downloading malware

## **Vulnerabilities and Patches**

Most types of malware can only succeed if a program under attack has a security vulnerability. A vulnerability is a flaw in a program that permits a specific attack or set of attacks to succeed against the program. Vulnerabilities are found in popular application programs frequently.[[23]](#footnote-23)

A vulnerability is a flaw in a program that permits a specific attack or set of attacks against this program to succeed.

When a software vendor discovers a vulnerability, the company issues a patch, which is a small program designed to fix the security vulnerability. After patch installation, the program is safe from attacks based on that particular vulnerability. Too often, however, users fail to install patches, so their programs continue to be vulnerable. Even if they do install patches, furthermore, they may delay, giving the attacker a long window of opportunity.

Of course, if attacks begin before the program vendor creates a patch (or even learns about the attack), then all attacks against vulnerable computers will succeed. A vulnerability-specific attack that occurs before a patch is available is called a zero-day attack. In such cases, there would be no signature yet to check for. On the security black market, well-funded adversaries can often purchase information that allows them to create zero-day attacks.

A vulnerability-specific attack that occurs before a patch is available is called a zero-day attack.

Test Your Understanding

5. a) What is a vulnerability? b) How can users eliminate vulnerabilities in their programs? c) What name do we give to attacks that occur before a patch is available?

## Social Engineering: No Vulnerability Necessary

Even if the software being attacked has no vulnerabilities, attackers can succeed if they can get the user to take an action that compromises security. This is called social engineering. A prime example of social engineering is an e-mail phishing attack. A phishing attack pretends to be from a company the user does business or from other seemingly trustworthy source. The next of the e-mail message is also convincing. Using HTML, it may look exactly like e-mail messages the source usually sends.

In spear phishing attacks via e-mail, the attacker personalizes the e-mail message to a particular person, such as the chief executive officer of the company. Spear phishing e-mails are even more convincing. They typically appear to come from a specific trusted person and contain information that only that person is likely to know. For example, it may mention specific projects or locations while traveling.

In some cases, a social engineering attack entices the user to click on a link that will take the victim to a site that asks the person to download a program to view a particular attachment. This downloaded program will actually be malware. In fact, the e-mail may contain the malware directly, in the form of an attachment.

## Social Engineering: No Vulnerability Necessary

5a. a) What kind of attack may succeed against a system with no technological vulnerabilities? b) What is the goal of social engineering? c) What is a phishing attack? d) Distinguish between phishing and spear phishing attacks.

## Types of Malware

There are many types of malware. Figure 3-3 lists three common types.

Figure 3-: Common Types of Malware

Viruses

Small pieces of code that must attach themselves to legitimate programs

This makes them difficult to detect

When the program executes, the virus infects other programs on the computer

Self-propagate to other computers by attaching themselves to e-mail messages, software downloaded from websites, peer-to-peer file transfer networks, social networks, RAM sticks, and so forth

Worms

Stand-alone malware programs that do not have to attach themselves to legitimate programs

Self-propagate like viruses

In some cases, a vulnerability will allow worms to jump directly to another computer with no human interaction

This can spread an infestation very quickly across many hosts

Trojan Horses

Replace an existing file, taking its name

Consequently, it appears to be “legitimate”

This makes it hard to detect

Cannot propagate by itself

Must be delivered to the computer by a hacker or other malware

Viruses. The first common type of malware was the virus. A virus attaches itself to a legitimate program, just as a human virus attaches itself to a person’s cells. If the victim runs the program, the virus will spread to other programs on the computer.

Typically, the virus will then try to propagate to other computers. It cannot do this directly. Instead, it propagates through e-mail attachments, peer-to-peer file transfer networks, social networks, and websites that ask the visitor to download a special program to experience their contents. They also propagate through USB RAM sticks. In Afghanistan, the Taliban left infected USB RAM sticks in public places. When U.S. forces found these drives and inserted them into their USB ports, they spread the infection throughout their networks.

Worms. Worms are similar to viruses. However, instead of attaching themselves to other programs, worms are full programs. Normally, they propagate between computers with the same mechanisms that viruses use.

However, some worms are able to jump directly between computers without human intervention. This means that no social engineering is necessary. However, directly propagating worms have a major limitation. They must be written to exploit a particular vulnerability on the receiving host, and that host must have the vulnerability. Humans are often gullible, but propagation through social engineering takes time. Worms that propagate directly can do so in milliseconds, and each worm that succeeds will launch itself against many more victims. In 2003, the Slammer worm infected 90% of all vulnerable computers attached to the Internet within 10 minutes.

Trojan Horses. In *The Iliad*, the Trojan horse was supposed to be a gift offering. It was really a trap. The Greeks left it at the gate because only the Trojans could get it inside. In malware, a Trojan horse is similar.

* First, it disguises itself as a legitimate file. This makes it difficult to detect.
* Second, in contrast to viruses, worms, and mobile code, a Trojan horse cannot propagate to another computer on its own initiative. It must be placed there by another piece of malware, by a human hacker, or by a user downloading the program voluntarily.

A Trojan horse cannot spread from one computer to another by itself.

Test Your Understanding

6. a) How do viruses and worms differ? b) How do viruses and worms propagate using social engineering? c) What other propagation method do some worms use? d) Why is it especially dangerous? e) What are Trojan horses? f) How do Trojan horses propagate to computers?

## Payloads

In war, when a bomber aircraft reaches its target, it releases its payload of bombs. Similarly, after they spread, viruses, worms, and other types of malware may execute pieces of code called payloads. Malicious payloads can do extensive damage. Figure 3-4 gives some example of this.

Figure 3-: Payloads

After propagation, malware may execute payloads

Code that does damage

Malicious payloads intend to do damage

Can erase your hard drive

Can send you to a pornography site if you mistype a URL

Can make your computer into a spam source or pornography distribution site

Spyware can steal information from your computer and send it to attackers

Keystroke loggers capture what you type

Data miners search your storage for social security numbers, bank account numbers, etc.

Ransomware encrypts your files, forcing you to pay ransom to be able to read them.

Credit card number theft

Steal credit card numbers, make unauthorized purchases

Credit card companies will reimburse, but the process can be painful

Identity theft

Steal enough information to impersonate the victim in large financial transactions

No reimbursement for stolen funds

Repairing credit can be difficult

Spyware. One concern on the list is Spyware can steal information from your computer and send it to attackers. Keystroke logger spyware captures what you type, analyzes it for login credentials and other “interesting” data. At a more sophisticated level, data miners search your storage for social security numbers, bank account numbers, etc.

Credit Card Number Theft. Two payloads are very common. One is malware to do credit card number theft. The thief can use this information to make unauthorized purchases. Credit card firms will refund money spent on purchases by the thief, but this can be a painful process.

Identity Theft. In some cases, thieves collect enough data about a victim (name, address, Social Security number, driver’s license number, date of birth, etc.) to impersonate the victim in complex crimes. This impersonation is called identity theft. Thieves commit identity theft in order to purchase expensive goods, take out major loans using the victim’s assets as collateral, obtain prescription drugs, get a job, enter the country illegally, and do many other things. Identity theft is more damaging than credit card theft because it can involve large monetary losses that are not reimbursed by anyone. In addition, correcting the victim’s credit rating can take months. Some victims have even been arrested for crimes committed by the identity thief.

Test Your Understanding

7. a) What are payloads? b) What is spyware? c) What is the difference between the two types of spyware mentioned in the text? d) What is ransomware? e) Discuss your choices are if you are hit by ransomware. f) Distinguish between credit card number theft and identity theft. g) Which is more harmful to the victim? Why?

## Human Break-Ins (Hacking)

A virus or worm typically has a single attack method. If that method fails, the attack fails. However, human adversaries can attack a company with a variety of different approaches until one succeeds. This flexibility makes human break-ins much more likely to succeed than malware break-ins.

Figure 3-: Human Break-Ins (Hacking) (Study Figure)

Humans Can Use Many Attack Methods

This makes them more dangerous than malware, which usually has only one or two attack methods

Hacking

*Intentionally* using a computer resource

*without authorization* or

*in excess of authorization*.

If an Action Fits the Definition, it Is Hacking

For example, if you find username and password on a piece of paper negligently left around, you are still not authorized to use the account, so to use it would be hacking

Irrelevant Considerations

Not properly protected: does not excuse hacking

Just testing the resource’s security: does not excuse hacking

Penalties Depend on the Amount of Damage Done

Easy to do damage accidentally

What is Hacking? Breaking into a computer is called hacking. Legally, Hacking is defined as *intentionally* using a computer resource *without authorization* or *in excess of authorization*. The key issue is authorization.[[24]](#footnote-24) If you see a password written on a note attached to a computer screen, this does not mean that you have authorization to use it. Also, note that it is hacking even if a person has legitimate access to an account but uses the account for unauthorized purposes.

Hacking is intentionally using a computer resource without authorization or in excess of authorization.

All hacking is illegal. Penalties differ by the type of asset that is hacked and by the amount of damage done, but it is very easily to do enough harm accidentally to merit a jail term, and “intentionally” only applies to intending to use the asset, not intending to damage.

Test Your Understanding

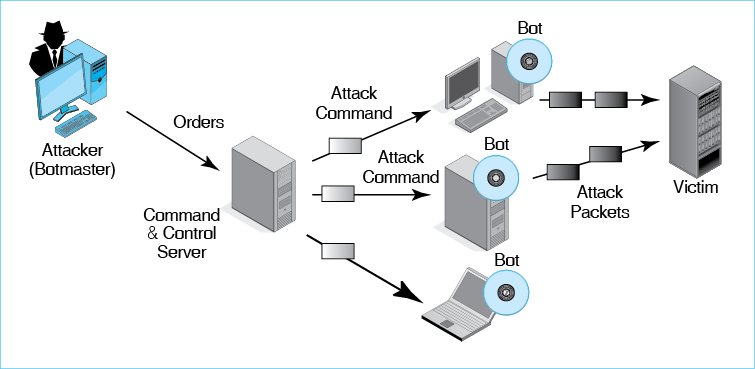
8. a) What is the definition of hacking? b) If you see a username and password on a Post-It note on a monitor, is it hacking if you use this information to log in? Explain in terms of the definition. c) You discover that you can get into other e-mail accounts after you have logged in under your account. You spend just a few minutes looking at another user’s mail. Is that hacking? Explain in terms of the definition. d) If you click on a link expecting to go to a legitimate website but are directed to a website that contains information you are not authorized to see. Is that hacking? Explain in terms of the definition.

## Denial-of-Service (DoS) Attacks

The goal of denial-of-service (DoS) attacks is to make a computer or entire network unavailable to its legitimate users. As Figure 3-6 shows, most DOS attacks involve flooding the victim computer with attack packets. The victim computer becomes so busy processing this flood of attack packets that it cannot process legitimate packets. The overloaded host may even fail.

The goal of denial-of-service (DoS) attacks is to make a computer or entire network unavailable to its legitimate users.

Figure 3-: Distributed Denial of Service (DDoS) Attack Using Bots



More specifically, the attack shown in the figure is a distributed DOS (DDoS) attack. In this type of DoS attack, the attacker first installs programs called bots on hundreds or thousands of PCs or servers. This collection of compromised computers is called a botnet, and the attacker is called the botmaster. When the user sends these bots an attack command, they all begin to flood the victim with packets.

Typically, the adversary does not communicate with bots directly. Rather, he or she sends orders to a command and control server, which then sends attack commands to the bots. In effect, the attacker is two levels removed from the attack, making the botmaster difficult to identify.

Test Your Understanding

9. a) What is the purpose of a denial-of-service attack? b) Which programs directly attack the victim in a distributed denial-of-service attack? c) What is a collection of compromised computers called? d) What is the person who controls them called? e) To what computer does the attacker send messages directly? f) Explain the steps of a distributed DoS attack.

## Advanced Persistent Threats (APTs)

In the past, criminal attacks were brief and limited—the electronic equivalent of smash-and-grab thefts in jewelry stores. Increasingly, however, we are experiencing advanced persistent threats (APTs) in which the adversaries has multiple objectives that they continue to pursue for days, weeks, months, or even years. These are true nightmares for corporations.

Figure 3-: Advanced Persistent Threats [Study Figure]

Prolonged Attack

Days, weeks, months, sometimes years

Initial foothold, then move to other systems

Plenty of time to learn systems and do damage

Advanced

Uses attack techniques well beyond typical hacks

Although often begins with a relatively simple spear phishing attack

Difficult and Expensive

Only worth it form major objectives

Once done only by nation states, now done by criminal hackers (e.g., Target)

The adversary must first break into the firm. In a large majority of cases, he or she does this through an extremely well-crafted spear phishing attack that gives the attacker access to critical authentication credentials. (This was probably the case in the Target breach case at the beginning of this chapter.) “The adversary uses the initial foothold to explore and break into other parts of the firm’s IT infrastructure. The attacker may also install Trojan horses and other exploitation programs. In each of these steps, the attacker uses advanced penetration and exploitation methods. This is the origin of “advanced.”

APTs are expensive to mount. Consequently, they were only done by national governments in the past. However, if there are good prospects for a large theft, criminal groups often may launch them. This was the case with the Target attack.

Test Your Understanding

10. a) Explain “advanced” in the term *advanced persistent threat*. b) Explain “persistent” in the context of APTs. c) How do adversaries often enter the system and then expand to other parts of it? d) Who mounts APTs today?

# TYPES OF ATTACKERS

The threat environment consists of types of attacks and types of attackers. As Figure 3-8 shows, there are many different types of attackers facing organizations today.

Figure 3-: Types of Attackers

Cybercriminals

Most attackers today are motivated by money

Often attack as sophisticated gangs with ranges of skills

Can buy crimeware to help in attacks

Black markets for stolen credit cards and other valuable information

Employees, Ex-Employees, and Other Insiders

Current employees: Revenge or theft

Dangerous

Already have access

Know the systems

Know how to avoid detection

Are trusted

IT employees and security employees are the most dangerous

Ex-employees are dangerous, so all access must be terminated before their leaving

Contractors with access permissions are also “insiders”

Nonmalicious insiders: Unware or aware but consider their violations minor

On the Horizon

Cyberwar by nations: Espionage and Damage

Cyberterror by terrorists

Hacktivists attack for political motives

Dangerous because tend to be sophisticated

Dangerous because want to do widespread damage

## Cybercriminals

When most people think of attackers, they normally have two pictures in their minds. The first is the old-school hacker driven by curiosity, the thrill of the break-in, and the desire to increase one’s reputation among other old-school hackers. They were seen as annoying but not too damaging.

This view is completely out of date. Hackers today are overwhelmingly cybercriminals who attack to make money. This has been true since the beginning of this century.

Today, most hackers are cybercriminals

Cybercriminals often work in loosely structured gangs. Funded by their crimes, many criminals can afford to hire the best hackers and to enhance their own skills. Consequently, criminal attacks are not just growing in numbers; they also are growing very rapidly in technical sophistication.

Criminal attackers have access to a vast online cybercrime community that gives them access to crimeware programs with slick user interfaces and prepaid annual updates. There are black markets for them to buy and sell credit card numbers and identity information. Many elements of this black market are in countries where regulation is minimal at best.

Test Your Understanding

11. a) What type of adversary are most hackers today? b) Why is this type of attacker extremely dangerous? c) What resources can they purchase and sell over the Internet?

## Employees, Ex-Employees, and Other Insiders

A large number of attacks are undertaken not by outsiders but by employees. Often, they are disgruntled employees who attack for revenge. However, they can also be employees who simply want to steal. Employees are especially dangerous for four reasons:

* They are knowledgeable about corporate systems,
* They typically have access to key systems,
* They have knowledge about how to avoid detection, and
* They tend to be trusted.

The most dangerous employees are IT staff members and especially IT security staff members. An ancient Roman question, “Quis custodiet ipsos custodes?” means “Who guards the guardians?” It is a serious question in security.

For ex-employees, revenge is a common motive. Another is stealing trade secrets that the employee worked on and believes are “his” or “hers.” It is important to terminate all ex-employee access to internal resources after they leave. In fact, even *before* employees leave, it is important to monitor their access for signs that they are infiltrating company intellectual property.

Often, contractors and service providers are given access credentials. This makes them insiders, and they must be considered dangerous as a consequence. When Edward Snowden stole files from the National Security Agency in early 2013, he was an employee of contractor Booz Allen Hamilton in Hawaii. In the Target breach, the account that thieves used to break into Target’s computers was that of an air conditioning service company performing services for Target.

Malicious insiders have garnered the most attention in the past. However, companies also need to be concerned with nonmalicious insiders who commit security violations through ignorance or because they consider the violation to be a one violation that will do little or no damage. The Target breach and many other breaches begin with unsafe acts my nonmalicious insiders.

Test Your Understanding

12. a) Why may employees attack? b) For what four reasons are employees especially dangerous? c) Who are the most dangerous employees? d) Why may ex-employees attack? e) What should be done when an employee leaves the firm? f) Why are contractor firms more dangerous than other outside firms?

## Cyberterrorists and National Governments

On the horizon is the danger of far more massive cyberterror attacks by terrorists and even worse cyberwar attacks by national governments. These could produce unprecedented damages in the hundreds of billions of dollars.

The United States has acknowledged that it has long had cyberwar capabilities, and it established a consolidated Cyberwar Command in 2009. It is clear that several other countries have these capabilities as well (especially China). Countries could use IT to do espionage to gather intelligence, conduct attacks on opponents’ financial and power infrastructures, or destroy enemy command and control facilities during physical attacks.[[25]](#footnote-25)

Cyberterror attacks by terrorists are also likely. During physical attacks, terrorists might disable communication systems to thwart first responders and to spread confusion and terror among the population. Cyberterrorists could also conduct purely IT-based attacks. While nation states are concerned about the side effects of cyberwar attacks, terrorists have no such qualms.

Cyberwar and cyberterror are particularly dangerous for three reasons. First, funding allows them to be extremely sophisticated. Second, they focus on doing damage instead of committing thefts. Third, they are dangerous because they are likely to be directed against many targets simultaneously for massive damage.

Espionage has more limited objectives than destructive attacks. In spying, the goal is to learn an enemy’s secrets. Several countries are doing this on a massive scale. In many cases, they are also targeting commercial enterprises to steal trade secrets useable to firms in their countries. The Chinese have been very effective in penetrating classified U.S. defense resources in recent years.

Hactivists attack for political motives. They do so to embarrass corporations or governments. Edward Snowden’s publication of secret programs in the U.S. National Security Agency (NSA) was an example of hacktivism.

Test Your Understanding

13. a) What are cyberterror and cyberwar attacks? b) Why are cyberwar attacks especially dangerous?

# PROTECTING DIALOGUES CRYPTOGRAPHY

Having looked at the threat environment, we will now begin to look at the tools that companies use to attempt to thwart attackers. One of these is cryptography. Formally, cryptography is the use of mathematics to protect information.

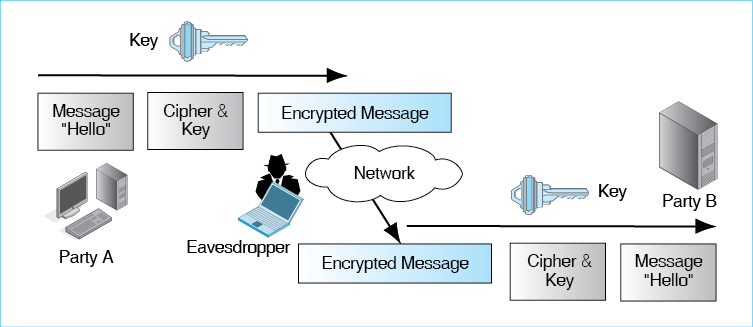
Cryptography is the use of mathematics to protect information.

Cryptography is important in and of itself. We begin with “crypto,” however, because it is part of many other security protections. A knowledge of cryptography is necessary to understand how they work.

## Encryption for Confidentiality

Encryption for Confidentiality. When most people think of cryptography, they think of encryption for confidentiality, which Figure 3-9 illustrates. Confidentiality means that even if an eavesdropper intercepts a message, he or she will not be able to read it. The sender uses an encryption method, called a cipher, to create a message that an eavesdropper cannot read. However, the receiver can decrypt the message in order to read it.

Figure 3-: Encryption for Confidentiality



Key Length. Encryption keys can be cracked by the attacker’s trying all possible keys. The way to defeat exhaustive key searches is to use long keys, which are merely binary strings. For most encryption ciphers, key lengths must be 128 bits or greater to be considered strong.

Keys are long strings of bits.

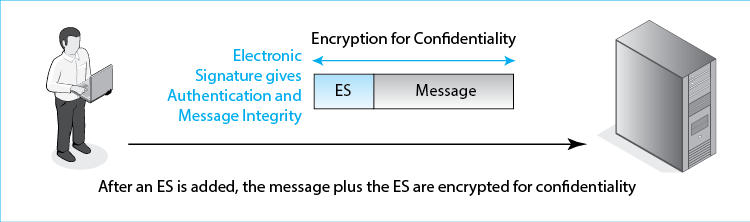
Test Your Understanding

14. a) What is a cipher? b) What protection does confidentiality provide? c) What is the minimum size for encryption keys to be considered strong in most encryption ciphers?

## Electronic Signatures: Message Authentication and Integrity

In addition to encrypting each packet for confidentiality, cryptographic systems normally add electronic signatures to each packet. This is illustrated in Figure 3-10. Electronic signatures are small bit strings that provide message-by-message authentication, much as people use signatures to authenticate individual written letters. Authentication means proving a sender’s identity. An electronic signature allows the receiver to detect a message added to the dialogue by an impostor.

Figure 3-: Electronic Signature for Authentication (and Message Integrity)



Electronic signatures also provide message integrity, meaning that the receiver will be able to detect if the packet is altered by an attacker while the packet is in transit. Consequently, cryptographic systems provide three protections to every packet. Encryption for confidentiality provides message-by-message confidentiality, while electronic signatures provide message-by-message authentication and message integrity.[[26]](#footnote-26)

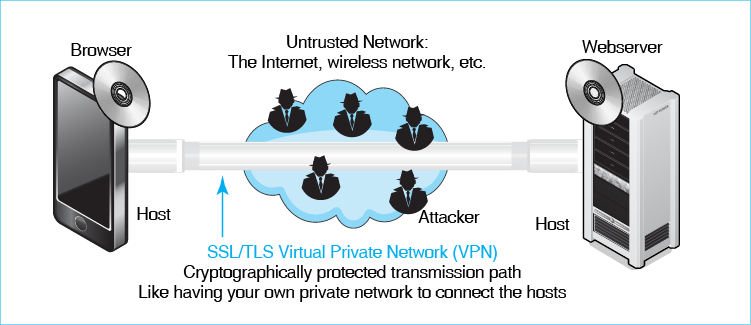
Test Your Understanding

15. a) What two protections do electronic signatures provide? b) What three protections are typically given to each packet?

## Host-to-Host Virtual Private Networks (VPNs)

Sometimes, transmission through untrusted networks is necessary. One of these is the Internet, which has no built-in security and is full of attackers. Another untrusted network is a wireless network because anyone can intercept your transmissions. The way to address a lack of security is to communicate with cryptographic protections. This is said to give you a host-to-host virtual private network (VPN). Figure 3-11 illustrates this concept. Of course, transmissions actually pass through a real network. In terms of security, however, the hosts are effectively communicating via a private network that connected just them.

Figure 3-: SSL/TLS Host-to-Host Virtual Private Network (VPN)



A common cryptographic system for VPNs is SSL/TLS. SSL/TLS was created as Secure Sockets Layer (SSL) by Netscape. The Internet Engineering Task Force then took over the standard, renaming it Transport Layer Security (TLS). It is called by both names today, so we call it SSL/TLS.[[27]](#footnote-27)

SSL/TLS is an attractive cryptographic system for webservice because SSL/TLS is built into every webserver and browser today, so the cost of adding SSL/TLS protection is negligible. Given security threats on the Internet, SSL/TLS should be used whenever possible.

Test Your Understanding

16. a) Distinguish between private networks and virtual private networks. b) Why is SSL/TLS attractive for VPNs to connect browsers to webserver?

# OTHER FORMS OF AUTHENTICATION

Electronic signatures provide message-by-message authentication. However, there are many types of authentication in use today, each with strengths and weaknesses. Authentication is crucial to controlling access to resources so that adversaries can be prevented from reaching them.

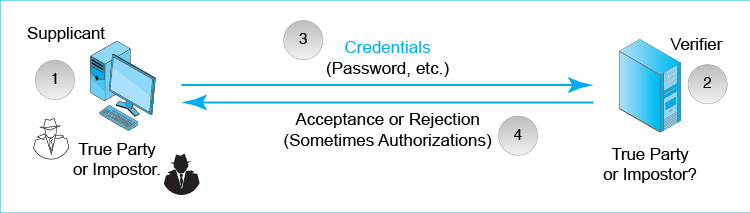
## Terminology and Concepts

The specific question that all authentication methods ask is whether the supplicant’s credentials prove that he or she is the true party.

Figure 3-12 illustrates the main terminology and concepts in authentication. The user trying to prove his or her identity is the supplicant. The party requiring the supplicant to prove his or her identity is the verifier. The supplicant claims to be a particular user, the true party. The supplicant tries to prove that he or she is the true party by providing credentials (proofs of identity) to the verifier.

The specific question that all authentication methods ask is whether the supplicant’s credentials prove that he or she is the true party.

Figure 3-: General Authentication Concepts



The type of authentication tool that is used with each resource must be *appropriate for the risks to that particular resource*. Sensitive personnel information should be protected by very strong authentication methods. However, strong authentication is expensive and often inconvenient. For relatively nonsensitive data, weaker but less expensive authentication methods may be sufficient.

The type of authentication tool that is used with each resource must be appropriate for the risks to that particular resource.

Test Your Under[[28]](#footnote-28)standing

17. a) What is authentication? b) Distinguish between the supplicant and the verifier. c) What are credentials? d) Who is the true party? e) What is the specific goal of authentication? f) Is the supplicant the true party or is the supplicant an impostor? g) Why must authentication be appropriate for risks to an asset?

## Reusable Passwords

The most common authentication credential is the reusable password, which is a string of characters that a user types to gain access to the resources associated with a certain **username** (account) on a computer. These are called reusable passwords because the user types the same password each time he or she needs access to the resource. Unfortunately, the reusable password is the weakest form of authentication, and it is appropriate only for the least sensitive assets.

The reusable password is the weakest form of authentication, and it is appropriate only for the least sensitive assets.

Figure 3-: Reusable Password Authentication (Study Figure)

Reusable Passwords

Passwords are strings of characters

They are typed to authenticate the use of a username (account) on a computer

They are used repeatedly and so are called reusable passwords

Benefits

Ease of use for users (familiar)

Inexpensive because they are built into operating systems

Often Weak (Easy to Crack)

Passwords that are words, proper nouns, or common passwords such as 12345678

They can be cracked quickly with dictionary attacks

Dictionary attacks catch common variants (Capitalize first letter only, add a single digit to the end)

No password that can be cracked by a dictionary attack is acceptably strong, even if it is very long

Passwords Should Be Complex

Should mix case, digits, and other keyboard characters ($, #, etc.)

Complex passwords can be cracked only with brute force attacks (trying all possibilities)

Passwords Also Should Be Long

Should have a minimum of ten to twelve characters

Big gain for using uppercase and lowercase letters (unless just the first letter is capitalized)

Smaller gains by using digits (0-9) and other keyboard characters (/, %, @, etc.)

Only passwords that are long and complex are adequately strong

Each added character increases the brute force search time by a factor of about 70 if case change, digits, and other keyboard characters are used.

For case change alone, each character increases search time by a factor of 52

If people are forced to use long and complex passwords, they tend to write them down

Ease of Use and Low Cost The popularity of password authentication is hardly surprising. For users, passwords are familiar and relatively easy to use. For corporate IT departments, passwords add no cost because operating systems and many applications have built-in password authentication.

Password Dictionary Attacks The main problem with passwords is that most users pick very weak passwords.[[29]](#footnote-29) To break into a host by guessing weak passwords, hackers often use password dictionaries. Password dictionaries typically have three types of entries:

* A list of common passwords, such as *12345678*. *Letmein*, or *password*.
* Common words, such as words in dictionaries, names of sports teams, pets, and so forth
* Hybrid versions of words such as capitalizing the first letter and perhaps adding a digit at the end. An example is *Processing1*. Others include the following.
* replacing the letter 0 with a zero, s with $, and to do other look-similar replacements. An example is *pa$$w0rd*.
* repeating the password, for example *pizzapizza*.
* alternating uppercase and lowercase letters, as in *PaSsWoRd*.

Password stealing programs have dictionaries with the characteristics we have just seen. If a password can be cracked by a dictionary attack, which tries all passwords in a password dictionary, then it will only take seconds to find the password. Consequently, no password that is in a cracker’s dictionary is adequately strong, no matter how long it is. Supercalifragilisticexpialidocious is not an adequately strong password.

No password that is in a cracker’s dictionary is adequately strong, no matter how long it is.

Long, Complex Passwords and Brute-Force Attacks Fortunately, good passwords cannot be broken by dictionary attacks. Good passwords have two characteristics. First, they are complex. It is essential to have a mix of upper and lower case letters that does not have a regular pattern. It is also good—and some would say necessary—to include non-letter keyboard characters such as the digits (0 through 9) and other keyboard characters (&, #, /, ?, etc.).

If a password is complex, it can only be cracked by a brute-force attack, in which the cracker first tries all combinations of one-character passwords, then all combinations of two-character passwords, and so forth, until the attacker finds one that works.

Complexity is not enough, however. Complex passwords must also be long. For short complex passwords, brute force attacks will still succeed. Beyond about 10 to 12 characters, however, there are too many combinations to try in a reasonable period of time.

Ever-Smaller Scope of Usefulness. Overall, while long complex passwords can defeat determined attacks, most users select passwords that can be cracked with dictionary attacks. Reusable passwords are no longer appropriate in an era when password-cracking programs can reveal most passwords in seconds or minutes. Passwords are only useful for nonsensitive assets.

Test Your Understanding

18. a) Why are passwords widely used? b) What three types of passwords are susceptible to dictionary attacks? c) Can a password that can be broken by a password dictionary attack be adequately strong if it is very long? d) What types of passwords can be broken only by brute-force attacks? e) What are the two characteristics of passwords that are safe from even brute-force attacks? f) Why is it undesirable to use reusable passwords for anything but the least sensitive assets?

## Other Forms of Authentication

Companies are beginning to look for stronger types of authentication for most of their resources. This will allow them to replace most or all of their reusable password access systems. We have space to mention only the few types of authentication shown in Figure 3-14.

Figure 3-: Other Forms of Authentication

Perspective

Goal is to replace reusable passwords

Access Cards

Permit door access

Need to control distribution and disable lost or stolen access cards

Biometrics

Biometrics uses body measurements to authenticate you

Vary in cost, precision, and susceptibility to deception

Fingerprint scanning

Inexpensive but poor precision, deceivable

Sufficient for low-risk uses

For a notebook, may be better than requiring a reusable password

Iris scanning

Based on patterns in the colored part of your eye

Expensive but precise and difficult to deceive

Facial scanning

Based on facial features

Controversial because can be done surreptitiously—without the supplicant’s knowledge

Digital Certificate Authentication

See Figure 3-15.

Two-Factor Authentication

Supplicant needs two forms of credentials

Example: debit card and pin

Strengthens authentication

Fails if attacker controls user’s computer or intercepts authentication communication

**Access Cards** To get into your hotel room, you may have to swipe an **access card** through a card reader. Many bus systems let riders purchase access cards to pay for their travel. Many companies use access cards for door access control. In addition, simple access card readers can be plugged into USB ports on computers for computer access.

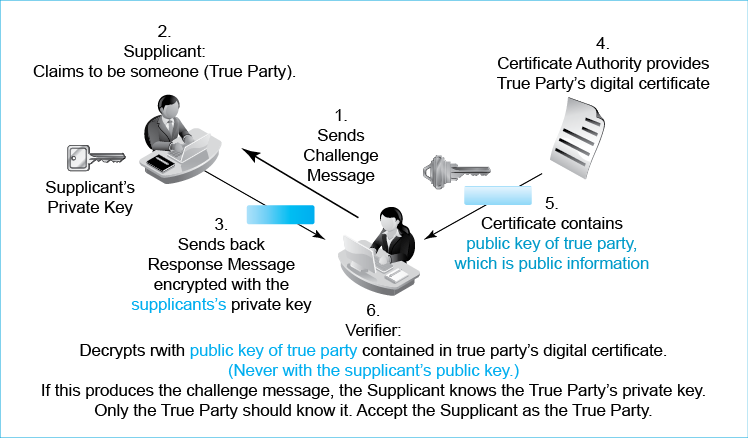
Biometrics In biometric authentication, access control is granted based on something you always have with you—your body. **Biometrics** is the use of bodily measurements to authenticate you. There are several types of biometrics. They differ in cost, precision, and susceptibility to deception by someone wishing to impersonate a legitimate user.

Biometrics is the use of body measurements to authenticate you.

* At the low end on price, precision, and the ability to reject deception is **fingerprint recognition**, which looks at the loops, whorls, and ridges in a finger. Although not a strong form of authentication, its price makes it acceptable for low-risk resources such as most tablets, and smart phones. For such devices, fingerprint recognition may acceptable, given the tendency of people to pick poor passwords and forget them.
* At the high end of the scale on price, precision, and the ability to reject deception is **iris recognition**,[[30]](#footnote-30) which looks at the pattern in the colored part of your eye. They are normally used for access to sensitive rooms. However, as the processing power on small devices like tablets and smartphones improves, we may begin to see iris scanning on them.
* A controversial form of biometrics is **facial recognition**, in which an individual is identified by his or her facial features. Facial recognition can be done **surreptitiously**—without the knowledge of the person being scanned. This raises privacy issues. We are beginning to see facial recognition scanning on tablets and smartphones.

**Digital Certificate Authentication** The strongest form of authentication is **digital certificate authentication**.[[31]](#footnote-31) Figure 3-15 illustrates this form of authentication.

Figure 3-: Digital Certificate Authentication



* In this form of authentication, each party has a secret **private key** that only he or she knows.
* Each party also has a **public key**, which anyone can know. It is not kept secret.
* The public key of a person in a document called a **digital certificate**.[[32]](#footnote-32) A digital certificate is cryptographically protected for message integrity, so that it cannot be changed without this change being obvious in a way that causes the verifier to reject it.

The supplicant claims to be someone, the true party. To test this claim, the verifier sends the subject a challenge message (1). This is just a random stream of bits. It is not even encrypted for confidentiality.

To prove its claim to being the true party, the supplicant encrypts the challenge message *with his or her private key* and sends this response message to the verifier (3). Again, there is no encryption for confidentiality.

The verifier gets the true party’s digital certificate (4), which contains the true party’s public key (5). The verifier tests the response message by decrypting it with the *public key of the true party*, which is contained in the digital certificate. If the decryption produces the original challenge message, then the supplicant has proven that he or she knows the private key of the true party (6). Only the true party should know this key. Therefore, it is reasonable to authenticate the supplicant as the true party. If the decrypted response message is not a match for the original challenge message, the supplicant is treated as an impostor.

Note that the verifier uses the public key of the true party—not the supplicant’s public key. If the verifier used the supplicant’s public key, the test would always succeed. The supplicant’s public key would decrypt the message correctly. Impostors would *always* be authenticated.

Note that the verifier uses the public key of the true party—not the supplicant’s public key.

There are three parties involved—the supplicant, the verifier, and the true party. Each has a public key and a private key. Therefore, you should never say *the* private key or *the* public key. So always say the supplicant’s public or private key, the verifier’s public or private key, or the true party’s public or private key.

Two-Factor Authentication. Debit cards are potentially dangerous because if someone finds a lost debit card, the finder might be able to use it to make purchases. Consequently possession of the debit card is not enough to use it. To use a debit card, the user must type a **personal identification number (PIN)**, which usually is four or six digits long. Requiring two credentials for authentication is called **two-factor authentication**. Two-factor authentication is more difficult to defeat because the attacker must obtain both sets of credentials.[[33]](#footnote-33)

Two-factor authentication requires two forms of authentication.

Test Your Understanding

19. a) How do you authenticate yourself with an access card? b) What is biometrics? c) Why may fingerprint recognition be acceptable for user authentication to a laptop? d) Why is iris recognition desirable? e) Why is face recognition controversial?

20. a) In digital certificate authentication, what does the supplicant do? b) What does the verifier do? c) Does the verifier decrypt with the true party’s public key or the supplicant’s public key? Why is this important? d) How does the verifier get the true party’s public key?

21. a) What characteristic of the true party is used in access card authentication, iris authentication, and digital certificate authentication. b) Which form of authentication that we looked at depends on the verifying proving that it knows something that only the true party should know? c) What if this information is learned by an attacker? d) Why is two-factor authentication desirable?

# FIREWALLS

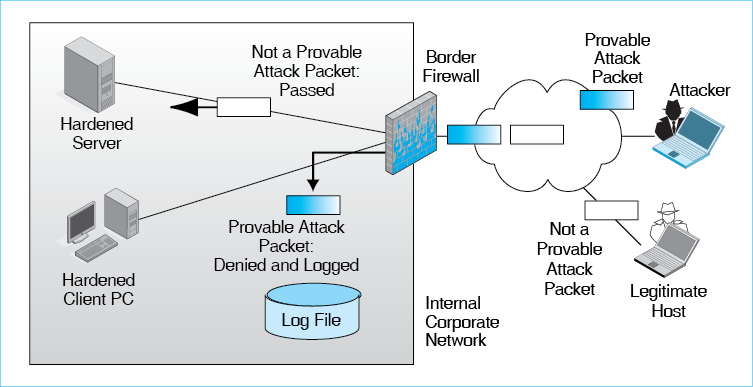
In hostile military environments, travelers must pass through checkpoints. At each checkpoint, guards will examine their credentials. If the guards find the credentials insufficient, the guard will stop the traveler from proceeding and note the violation in a checkpoint log.

## Dropping and Logging Provable Attack Packets

Figure 3-16 shows that firewalls operate the same way. When a packet arrives, the **firewall** examines it. If the firewall identifies a packet as a **provable (definite) attack packet**, the firewall discards it.[[34]](#footnote-34) (Synonyms for provable are definite, certain, etc.) On the other hand, if the packet is not a provable attack packet, the firewall allows it to pass.

If a firewall identifies a packet as a provable attack packet, the firewall discards it.

Figure 3-: General Firewall Operation



The firewall copies information about each discarded packet into a **firewall log file**. Firewall managers should read their firewall log files every day to understand the types of attacks coming against the resources that the firewall is protecting.

Note that firewalls pass *all* packets that are not provable (certain) attack packets, even if they are suspicious. By analogy, police cannot arrest someone unless they have probable cause, which is a reasonably high standard of proof. They cannot arrest someone for being suspicious.

Consequently, firewalls never stop all attack packets. It is important to harden all internal hosts against attacks by adding firewalls, adding antivirus programs, installing all patches promptly, and taking other precautions. This chapter focuses on network security, rather than host security, so we will not consider host hardening.

Test Your Understanding

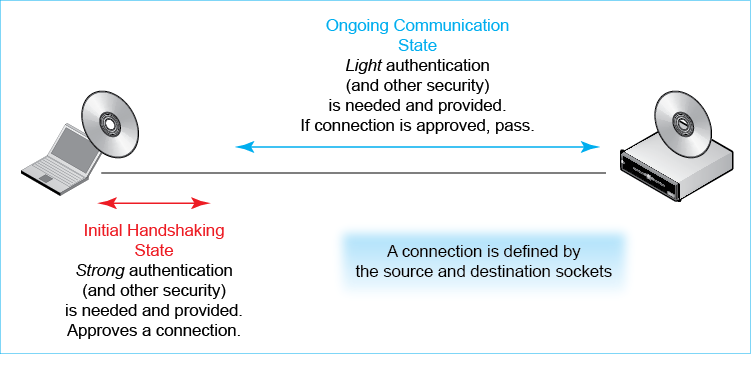
22. a) What does a firewall do when a provable attack packet arrives? b) Does a firewall drop a packet if it probably is an attack packet? c) Why is it important to read firewall logs daily?

## Stateful Packet Inspection (SPI) Firewalls

How do firewalls examine packets to see if they are attack packets? Actually, there are several firewall filtering mechanisms. We will only look at two—stateful packet inspection (SPI) and Next-Generation Firewalls.

Figure 3-17 shows that stateful packet inspection (SPI) firewalls act as if there are two *states* (stages) in a dialogue between two parties. The first is initial handshaking, which is the initial interactions that take place to authenticate the other party and other activities. This is crucial to security, so SPI firewalls spend a great deal of time on this and require high-quality authentication. If a connection between the two sides is not authenticated at this stage, the connection is terminated.

Figure 3-: Stateful Packet Inspection (SPI) Firewall



After this intense but brief handshaking state, everything else is ongoing communication. If a packet arrives that is part of an approved connection arrives, it is given only cursory examination because authentication had been proven initially. Connections involve an application program on each machine, which also has an IP address. In other words, a connection consists of source and destination sockets. If an arriving packet has the expected source and destination sockets, it is passed through with little or no additional inspection.

Think of a telephone conversation. When someone calls you, you want to ensure that you know who you are talking to. Once you establish that, you ignore authentication for the remainder of the call. This is what SPI firewalls do with network connections.

Stateful packet inspection firewalls provide a good balance of security and economy. For the most sensitive part of a connection, SPI firewalls provide strong security. For ongoing communication, where less intense security is needed, SPI firewalls only do enough security for the situation. This saves money. Thanks to this balance of strong security when it is needed and economical operation most of the time, most main border firewalls today are stateful packet inspection firewalls.

However, SPI firewalls are limited in the attacks they can stop. Most importantly, they act primarily on the basis of socket information: source and destination IP addresses and port numbers. This does not allow them to know what application is generating the traffic. For example, if an application uses Port 80 on the server, this seems to indicate that HTTP is the protocol used by the applications. However, if attackers run another protocol but still use Port 80, an SPI firewall cannot determine this. This kind of “port spoofing” is becoming more common in attacks, and many firms now feel that SPI firewalls are no longer sufficient.

Test Your Understanding

23. a) Why are stateful firewalls attractive? b) What type of firewalls do most corporations use for their main border firewalls? c) What are the two states in connections for SPI firewalls? d) Which state needs the most security protection? e) Which state gets the most security? f) What is the big limitation of stateful packet inspection firewall? Don’t just name it. Explain it.

## Next-Generation (Application Aware) Firewalls (NGFWs)

The newest type of firewall is the next-generation firewall (NGFW). The most important capability of NGFWs is that they are application aware. This means that, unlike stateful packet inspection firewalls, NGFWs can determine the specific application that is sending and receiving messages over a connection.

To do this, they look at all of the application traffic in a connection. This requires them to collect application traffic and then to look for traffic characteristics specific to individual applications. Application awareness allows firewall administrators to create rules for individual applications. For example, companies may not permit YouTube traffic or may limit it to avoid overloading the network. And, of course, if malware traffic is identified, it can be stopped automatically. By providing visibility into application traffic patterns, NGFWs also provide information for better network management.

Application-aware firewalls need a great deal of processing power to analyze application traffic. This means that they are expensive per packet filtered. They are also more expensive to manage. Companies have hundreds of applications and must protect against even more malware applications. They must create a policy that specified how each application will be handled, and they must implement these rules on all firewalls.

Figure 3-: Next-Generation (Application Aware) Firewalls [Study Figure]

Next-Generation Firewalls are Application-Aware

Can base decisions on the actual application that is creating traffic

Advantages of Being Application Aware

Detects port spoofing.

Create accept/reject rules based on specific applications.

Recognize specific malware applications, providing laser-focused firewall decisions.

For network and security management, can see which applications are using which percentages of network traffic

Tradeoffs

Processing requirements make NGFWs more expensive than SPI firewalls per packet

Richer information requires greater management effort to create and implement policies and rules

Test Your Understanding

24. a) Why are SPI firewalls limited in their ability to detect attack packets? b) How do NGFWs address this problem? c) Give specific examples of how application information can be used to increase security. d) Why are NGFWs expensive.?

## **Intrusion Detection System (IDSs)**

It would be naïve to expect firewalls to stop all attack packets. Most obviously, they do not drop suspicious packets—only definite attack packets. Intrusion detection systems (IDSs) were created to address this limitation by focusing specifically on identifying *suspicious* transmissions. When they find suspicious packet streams that may create a problem, they log them for security administrators to examine. If a threat appears to be very serious, the IDS will send an alarm to security administrators. Next-generation firewall processing grew out of IDS processing methods, but NGFWs are still limited to stopping definite attacks. NGFWs are like locks, while IDSs are like burglar alarms.

Figure 3-19: Intrusion Detection and Prevention Systems [Study Figure]

The Need for Intrusion Detection

Firewalls only stop provable attack packets

Some way is needed to address suspicious transmissions

Intrusion Detection System (IDSs) Characteristics

Like car alarms for security

If detect suspicious activity, send a warning

Problem of many false alarms (false positives)

False Positives (False Alarms). Unfortunately, intrusion detection systems generate many false alarms, which are called false positives. An IDS sends the average business about 10,000 security alerts per day, only a handful of which are real threats. Finding these real attacks is literally like finding a needle in a haystack.[[35]](#footnote-35)Companies must invest sufficient human resources into handling alarms and reading log files. Even then, finding the one or two true attacks in a long stream of false alarms leads to frustration and flagging vigilance. In the case of the Target security breach, the FireEye IDS detected the attack, but Target security personnel did not follow up on the alarm.

No Alternatives. Although IDSs create many problems, firms today realize that it is impossible to prevent breaches automatically and that they must be able to identify and stop attacks if they succeed initially. Learning to look for meaningful patterns in IDS alerts and log files is enormously difficult, but there is no alternative.

Test Your Understanding

25. a) Do IDSs stop packets? b) Why are they painful to use? c) How do they offer a broader picture of the threat environment than NGFWs?

# Box: Antivirus Protection

Both firewalls and antivirus programs attempt to stop attacks. However, they work at different levels. Firewalls examine packets and groups of packets. Antivirus (AV) programs, in contrast, examine entire files. When an e-mail message arrives at a mail server, the server may pass any attachment to an AV program for vetting.

Firewalls examine packets and groups of packets. Antivirus (AV) programs, in contrast, examine entire files.

Figure 3-: Antivirus Protection (Study Figure)

Firewalls versus Antivirus Programs

Firewalls analyze packets and streams of packets

Antivirus programs analyze files

Search for All Malware, Not Only Viruses

Signatures versus Behavior

Traditionally looked for signatures (characteristic bit patterns) for specific malware

Malware writers now create code that mutates slightly each time it runs

Defeats most signature detection

Now, also look at behavioral patterns: What programs do

Antivirus programs do not simply check for viruses. They also examine the attached file for worms, Trojan horses, and other forms of malware. These programs were named antivirus programs when “malware” was roughly synonymous with “virus.” Although the scope of detection has broadened, the name antivirus has stuck.

Traditionally, AV programs only looked for malware signatures, which are snippets of code that let the antivirus program identify particular malware programs. Signature detection is still widely used, but it is no longer sufficient. First, the number of malware programs is now so large that the processing power to detect all known malware via signature detection would drive any computer to its knees. More fundamentally, many malware programs now mutate constantly, rewriting their code in a way that maintains functionality while making the matching of strings of characters useless.

Today, AV programs also look for behavioral patterns—things the file is attempting to do. To give an extreme example, if the file is a program that will try to reformat a computer’s hard drive, that is an undeniable indication that the program is malware. Some AV programs even run the suspect program in a sandbox (environment it cannot escape from) to watch it operate.

Test Your Understanding

26. a) Distinguish between what firewalls look at and what antivirus programs look at. b) Are AV programs used to detect more than viruses? Explain. c) Distinguish between signature detection and behavioral pattern detection. d) Why is signature detection not enough?

# CONCLUSION

## Synopsis

Security is now an integral part of every network project from requirements to ongoing operations. It is important to design security into networks up front instead of trying to add it later at far higher cost and at a substantially lower rate of success. We discuss network security throughout the book. In this chapter and the next, we look at security in depth.

We began with a discussion of the threat environment—the types of people and organizations that attack you and the types of attacks they use. Attackers include hackers, insiders, terrorists, national governments, and hacktivists. Hackers today are mainly cybercriminals, who are dangerous because they are well-funded, work in gangs, and can buy crimeware software on the Internet. Insider attacks are common and tend to be damaging because insiders have access to systems, know systems well, know how to avoid detection, and tend to be trusted. Attacks by cyberterrorists and national governments tend to be very dangerous because these adversaries can afford to engage in highly sophisticated attacks, focus on doing damage instead of committing isolated crimes, and execute their attacks against many targets all at once.

There are many attack methods. Malware is a generic name for evil software, including viruses, worms, and Trojan horses, to name only three. Malware often propagates between computers and then executes a payload, which is a program that does damage to the victim’s computer. Malware often takes advantages of security vulnerabilities in user software to break in. If there are no technical vulnerabilities, the attacker will attempt to trick the user into doing something that permits the attacker to succeed. A typical example is opening an e-mail attachment containing malware. This type of trickery is called social engineering. Spear-phishing attacks, in which the user receives a convincing looking e-mail message with information that pertains directly to them, are very often successful.

Hackers break into a computer resource and then can do a wide range of damage. We discussed the specific definition of hacking, which is intentionally using a computer resource without authorization or in excess of authorization.

In distributed denial-of-service attack, a botmaster builds an army of bot programs on compromised computers. The botmaster then overwhelms a selected victim with a flood of attack packets. Bots can be upgraded to fix bugs or to equip them to do a different kind of attack.

Advanced persistent threats last for days, weeks, months or years. As their name suggests, they involve the use of highly sophisticated attack methods. APTs are extremely difficult to detect and stop and can do a great deal of damage over a long period of time.

Companies defend against attacks in many ways. One is cryptography, which is the use of mathematics to provide security. For example, a company may encrypt all transmissions for confidentiality, so that an attacker cannot read them. This normally uses symmetric key encryption. Messages can also be given electronic signatures so that their authenticity can be checked and to provide message integrity—assurance that the message has not been tampered with en route. Virtual private networks (VPNs) combine different forms of security to give a secure transmission path that travels through a nonsecure network.

Knowing whom you are communicating with can reduce risks. In authentication, a supplicant presents credentials to prove its identity as the true party it claims to be to a verifier. Traditionally, authentication meant reusable passwords, and passwords are widely used today. However, companies are trying to move away from them because they are not very secure. Dictionary attacks can break most passwords in seconds or minutes. Long complex passwords can defeat dictionary attacks, but they are typically written down or forgotten. Today, companies increasingly are using physical access cards, biometrics (such as fingerprint, iris, and face recognition), and cryptographic methods using digital certificate authentication. Using two forms of authentication—two-factor authentication—provides stronger authentication in most circumstances.

Firewalls stop definite attack packets from entering or leaving the firm. They do not stop suspicious packets, so they are not a panacea for stopping attacks. Most firewalls today use stateful packet inspection (SPI), in which the intensity of packet examination depends on the state of the conversation. Packets attempting to open a new connection are particularly dangerous and are given extensive scrutiny. In contrast, packets that do not attempt to open a new connection are given only cursory scrutiny. By focusing expensive filtering resources on comparatively rare but risky connection-opening packets, SPI firewalls can provide very good security at reasonable cost.

SPI firewalls are now being superseded by next-generation firewalls. NGFWs look beyond IP addresses and port numbers. They collect many packets, reintegrate fragmented application messages, compare reintegrated application messages to a database to identify the application, and follow rules specific to particular applications. Application awareness brings a host of benefits, but it is expensive

Firewalls do not drop packets just because they are suspicious, but this does not mean that suspicious packets are safe. Intrusion detection systems look specifically for suspicious patterns. If a pattern looks especially dangerous, the IDS will notify the security administrator. Unfortunately, IDSs generate mostly false alarms, and this makes them painful to use.

Firewalls look at packets and groups of packets. In contrast, antivirus programs look at entire files. Despite the name “antivirus,” they check for all forms of malware. Traditionally, they used signature detection based on byte patterns that characterize specific malware programs. Malware has become good at evading signature detection, so antivirus programs now use behavioral analysis to see what a program is attempting to do.

## END-OF-CHAPTER QUESTIONS

### Thought Questions

3-1. a) What form of authentication would you recommend for relatively unimportant resources? Justify your answer.

b) What form of authentication would you recommend for your most sensitive resources?

3-2. What is the promise of newer authentication systems?

3-3. In digital certificate authentication, the supplicant could impersonate the true party by doing the calculation with the true party’s private key. What prevents impostors from doing this?

3-4. What are the implications for digital certificate authentication if the true party’s private key is stolen?

3-5. a) If someone in your firm gives you their password and you log into their account, is this hacking? Go back to the definition. b) If you think someone in your office is sending slanderous e-mail about you, is it hacking if you break into their e-mail account to see if this is true? Go back to the definition. c) If you log into a server at your bank to test their security, is this hacking. Go back to the definition.

Harder Thought Questions (You May Not Get These, but Try)

3-6. When a sales clerk accepts a credit card payment, he or she should type the last four digits of the credit card into the terminal in or der for the terminal to verify that the last four digits on the card are the same as on the magnetic stripe. How do you think sales clerks may enter the last four digits yet still make the crosscheck worthless?

3-7. Keys and passwords must be long. Yet most personal identification numbers (PINs) that you type when you use a debit card are only four or six characters long. Yet this is safe. Why?

Perspective Questions

3-8. What was the most surprising thing you learned in this chapter?

3-9. What was the most difficult part of this chapter for you?

1. Alastair Jamieson and Erin McClam, “Millions of Target Customers' Credit, Debit card Accounts May Be Hit by Data Breach,” NBC News, December 19, 2013. http://www.nbcnews.com/business/consumer/millions-target-customers-credit-debit-card-accounts-may-be-hit-f2D11775203. [↑](#footnote-ref-1)
2. Jaikumar Vijayan, “Security Firm IDs Malware Used in Target Attack,” Computerworld.com. <http://www.computerworld.com/s/article/9245491/Security_firm_IDs_malware_used_in_Target_attack>. [↑](#footnote-ref-2)
3. Target, “Target Provides Update on Data Breach and Financial Performance,” January 10, 2014. http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance. [↑](#footnote-ref-3)
4. Fazio Mechanical Services, “Statement on Target Data Breach,” date viewed April 26, 2014.http://faziomechanical.com/Target-Breach-Statement.pdf. Brian Krebs, “Target Hackers Broke in Via HVAC Company,” KrebsOnSecurity.com, February 5, 2014. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company. [↑](#footnote-ref-4)
5. Brian Krebs, “These Guys Battled BlackPOS at a Retailer,” KrebsonSecurity.com, February 14, 2014. http://krebsonsecurity.com/2014/02/these-guys-battled-blackpos-at-a-retailer/. [↑](#footnote-ref-5)
6. Brian Krebs, “Target Hackers Broke in Via HVAC Company,” KrebsOnSecurity.com, February 5, 2014. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/. [↑](#footnote-ref-6)
7. Jaikumar Vijayan, “Security Firm IDs Malware Used in Target Attack,” Computerworld.com. <http://www.computerworld.com/s/article/9245491/Security_firm_IDs_malware_used_in_Target_attack>. [↑](#footnote-ref-7)
8. Jaikumar Vijayan, “Security Firm IDs Malware Used in Target Attack,” Computerworld.com. <http://www.computerworld.com/s/article/9245491/Security_firm_IDs_malware_used_in_Target_attack>. [↑](#footnote-ref-8)
9. Jaikumar Vijayan, “Security Firm IDs Malware Used in Target Attack,” Computerworld.com. <http://www.computerworld.com/s/article/9245491/Security_firm_IDs_malware_used_in_Target_attack>. [↑](#footnote-ref-9)
10. Jaikumar Vijayan, “Security Firm IDs Malware Used in Target Attack,” Computerworld.com. <http://www.computerworld.com/s/article/9245491/Security_firm_IDs_malware_used_in_Target_attack>. [↑](#footnote-ref-10)
11. Target, “Target Provides Update on Data Breach and Financial Performance,” January 10, 2014. <http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance>. [↑](#footnote-ref-11)
12. Brian Krebs, “These Guys Battled BlackPOS at a Retailer,” KrebsonSecurity.com, February 14, 2014. <http://krebsonsecurity.com/2014/02/these-guys-battled-blackpos-at-a-retailer>. [↑](#footnote-ref-12)
13. Adam Greenberg, “Hackers Seek to Decrypt PIN Codes Likely Stolen in Target Breach,” *SC Magazine*, January 8, 2014. http://www.scmagazine.com/hackers-seek-to-decrypt-pin-codes-likely-stolen-in-target-breach/article/328529/. [↑](#footnote-ref-13)
14. Keith Jarvis and Jason Milletary, “Inside a Targeted Point-of-Sale Data Breach,” Dell SecureWorks, January 24, 2014. http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf. [↑](#footnote-ref-14)
15. Keith Jarvis and Jason Milletary, “Inside a Targeted Point-of-Sale Data Breach,” Dell SecureWorks, January 24, 2014. http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf. [↑](#footnote-ref-15)
16. Brian Krebs, “[Non-US Cards Used at Target Fetch Premium](http://krebsonsecurity.com/2013/12/non-us-cards-used-at-target-fetch-premium/),” KrebsonSecurity.com, December 13, 2014, http://krebsonsecurity.com/2013/12/non-us-cards-used-at-target-fetch-premium/. [↑](#footnote-ref-16)
17. Brian Krebs, “[Cards Stolen in Target Breach Flood Underground Markets](http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/),” KrebsonSecurity.com, December 20, 2014. http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/. [↑](#footnote-ref-17)
18. BBC.com. “Target Profits Plunge 46% after holiday Security Breach,” February 26, 2014. http://www.bbc.com/news/business-26358556. [↑](#footnote-ref-18)
19. Anne D'Innocenzio, “Target’s Chief Information Officer Resigns,” The Associated Press, March 5, 2014. http://www.nytimes.com/2014/03/06/business/targets-chief-information-officer-resigns.html?\_r=0. [↑](#footnote-ref-19)
20. Clare O’Connor, “Target CEO Gregg Steinhafel Resigns in Data Breach Fallout,” Forbes, May 5, 2014. http://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/. [↑](#footnote-ref-20)
21. Federal Bureau of Investigation Press release. Speech by Robert S. Mueller III, Director, Federal Bureau of Investigation, RSA Cyber Security Conference, San Francisco, California, March 1, 2012. [↑](#footnote-ref-21)
22. Center for Strategic and International Studies, “Net Losses: Estimating the Global Cost of Crime,” June 2014. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2-summary.pdf. [↑](#footnote-ref-22)
23. A 2014 study by Cenzic found that 96% of all applications tested had at least one vulnerability. The median number of flaws per application was 14. Andy Patrizio, “Nearly all Apps are Vulnerable in Some Way,” NetworkWorld, March 3, 2014. http://www.networkworld.com/article/2226448/microsoft-subnet/nearly-all-apps-are-vulnerable-in-some-way--report-says.html. [↑](#footnote-ref-23)
24. Note also that the unauthorized access must be intentional. Proving intentionality is almost always necessary in criminal prosecution, and hacking is no exception. [↑](#footnote-ref-24)
25. A 2009 article in the *New York Times* reported that before the 2003 invasion of Iraq, the United States considered an attack that would shut down Iraq’s entire financial infrastructure (John Markoff, and Thom Shanker, “ ‘03 Plan Displays Cyberwar Risk,” *New York Times*, August 1, 2009. www.msnbc.msn.com/id/3032619/%2328368424). This attack was not approved, but not because it was infeasible. It was held back because its impact might have spread beyond Iraq and might even have damaged the U.S. financial system. More recently, attacks by the United States and Israel used the Stuxnet worm to damage a specific group of nuclear centrifuges in a specific factory in Iran. The researchers who discovered Stuxnet were amazed by its complexity and by the scope of the operation that produced and tested it. It even involved forged digital certificates for important firms. [↑](#footnote-ref-25)
26. Another common protection is anti-replay. In some cases, an attacker may be able to do damage by capturing an encrypted message. Although the attacker cannot read the encrypted message, he or she may be able to accomplish objectives by simply retransmitting the message later. Anti-replay protections prevent this. [↑](#footnote-ref-26)
27. When you use SSL/TLS, the URL begins with https://. Although you will not notice it, the port number in TCP changes from 80 to 443, which indicates HTTP over SSL/TLS. [↑](#footnote-ref-27)
28. [↑](#footnote-ref-28)
29. In a study of 10,000 passwords, Mark Burnett at xato.net found that almost 10 percent were “password,” “123456,” or “12345678.” Also in the top 20 were “111111,” “abc123,” “1234,” “12345,” “football,” and “letmein.” Trying just the top 100 passwords would allow a hacker to get into 40 percent of accounts. Trying the top 1,000 would get into 91 percent. One weakness in this study is that password case was not considered. However, given the lax attitude of most users toward passwords, separating different strings with different case patterns probably would not have made a difference. [↑](#footnote-ref-29)
30. In science fiction movies, eye scanners are depicted as shining light into the supplicant’s eye. This does not happen. Iris scanners merely require the supplicant to look into a camera. In addition, science fiction movies use the term retinal scanning. The retina is the back part of the eye; it has distinctive vein patterns. Retinal scanning is not used frequently because the supplicant must press his or her face against the scanner. [↑](#footnote-ref-30)
31. It also good for authenticating software processes, which have no heads or fingers and have a difficult time swiping access cards. [↑](#footnote-ref-31)
32. Digital certificates are created by organizations called Certificate Authorities. [↑](#footnote-ref-32)
33. However, if a user’s computer is compromised, the attacker typically controls both credentials, so two-factor authentication gives no security. Two-factor authentication may also fail if an eavesdropper can intercept authentication communication between the supplicant and the verifier. Two-factor authentication is desirable, but factors that limit its use must be understood. [↑](#footnote-ref-33)
34. Synonyms for provable are certain, etc. The point is that there is no doubt. [↑](#footnote-ref-34)
35. John E. Dunn, “Average US Business Fields 10,000 Security Alerts per Day, Damballa Analysis Finds,” Terchworld.com, May 13, 2014. http://news.techworld.com/security/3516426/average-us-business-fields-10000-security-alerts-per-day-damballa-analysis-finds/. [↑](#footnote-ref-35)