



CHAPTER 5

E-commerce Security and Payment Systems

LEARNING OBJECTIVES

After reading this chapter, you will be able to:

- Understand the scope of e-commerce crime and security problems, the key dimensions of e-commerce security, and the tension between security and other values.
- Identify the key security threats in the e-commerce environment.
- Describe how technology helps secure Internet communications channels and protect networks, servers, and clients.
- Appreciate the importance of policies, procedures, and laws in creating security.
- Identify the major e-commerce payment systems in use today.
- Describe the features and functionality of electronic billing presentment and payment systems.

Cyberwar:

MAD 2.0

From the earliest of days, humans have warred against each other, with the tools of warfare evolving over time from sticks and stones, to arrows and spears, to artillery and bombs. Physical warfare and weaponry are familiar and readily recognizable. But today, there is also another type of warfare that is becoming increasingly common, a type that is conducted by hidden armies of hackers wielding weaponry that consists of algorithms and computer code. Cyberspace has become a new battlefield, one that often involves nations against other nations, and nations against corporations. The targets include defense installations, nuclear facilities, public infrastructure, banks, manufacturing firms, and communications networks. There are two primary objectives of this kind of warfare: obtaining intellectual property (a kind of economic warfare) and attacking the ability of other nations to function.

One of the problems of warfare is that your enemy may possess the same weapons as you do. In the context of thermonuclear warfare, politicians have negotiated treaties based on the so-called doctrine of mutually assured destruction (MAD): the recognition that even a first attacker would ultimately perish in the counterattack. Today, cyberwarfare has some striking similarities: an attack by a nation against its enemy's cyberinfrastructure might unleash a counterattack so powerful that critical infrastructure in both nations would be heavily damaged and shut down.

The United States, China, Russia, and many other nations are preparing today for such a cyberwar, hoping it won't happen, but developing new weapons and practicing defensive techniques. For example, in April 2016, NATO, an alliance of countries from North America and Europe, brought together 550 military and corporate leaders from 26 nations for the 7th annual Locked Shields cyberwar games, the largest such games in the world. Using the Estonian Cyber Range, a sort of firing range for cyberwarriors, the national Blue Teams had to defend their countries against an all-out Red Team cyberattack, with the emphasis on defensive strategies and keeping the infrastructure of their countries working. The U.S. Department of Defense conducted its 5th Cyber Guard cyberwar games exercise in August 2016. Over 100 organizations and 800 people, from both armed forces and private corporations, participated in the games.

A cyberarms race has already started. The big countries in cyberwar are the United States, Great Britain, China, Russia, Iran, Israel, Pakistan, and India, but many smaller



© Rafal Olechowski / Fotolia

SOURCES: "Cyber Warfare: Who Is China Hacking Now?," by Kristie Lu Stout, Cnn.com, September 29, 2016; "Hacking the US Election: How the Worlds of Cyberwarfare and Politics are Colliding Spectacularly," by Kalev Leetaru, Forbes.com, September 11, 2016; "Governments and Nation States Are Now Officially Training for Cyberwarfare: An Inside Look," by Steve Ranger, Techrepublic.com, September 2, 2016; "How America Could Go Dark," by Rebecca Smith, *Wall Street Journal*, July 14, 2016; "NATO Recognizes Cyberspace as New Frontier in Defense," by Julian Barnes, *Wall Street Journal*, June 14, 2016; "'Dark Territory: The Secret History of Cyber War,' by Fred Kaplan," by P.W. Singer, *New York Times*, March 1, 2016; "Gen. Michael Hayden Gives an Update on the Cyberwar," *Wall Street Journal*, Feb. 9, 2016; "Pentagon Chief: 2017 Budget Includes \$7B for Cyber," by Sean Lyngaas, *Fcw.com*, February 2, 2016; "The First Cyber Battle of the Internet of Things May Have Just Happened," by Kalev Leetaru, Forbes.com, January 5, 2016; "Ukraine: Cyberwar's Hottest Front," by Margaret Coker and Paul Sonne, *Wall Street Journal*, November 9, 2015; *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*, by Brian M. Mazanec, Potomac Books (November 1, 2015); "Cyberwar Ignites a New Arms Race," by Damian Paletta, Danny Yardon, and Jennifer Valentino-Devries, *Wall Street Journal*, October 11, 2015; "Cataloging the World's Cyberforces," by Jennifer Valentino-Devries and Danny Yardon, *Wall Street Journal*, October 11, 2015; "Obama and Xi Jinping of China Agree to Steps on Cybertheft," by Julie Davis and David Sanger, *New*

countries like Denmark, the Netherlands, Estonia, and tiny Belarus are building their arsenals. Unlike nuclear weapons, cyberwar is so inexpensive that even small nations can afford it. A recent report documented 29 countries with formal military and intelligence units dedicated to offensive cyberwar, 49 that have purchased off-the-shelf hacking software, and 63 currently engaged in electronic surveillance of their own and other populations. Countries are developing cyberarsenals that include collections of malware for penetrating industrial, military, and critical civilian infrastructure controllers, e-mail lists and text for phishing attacks on important targets, and algorithms for denial of service (DoS) attacks. The computer code has been tested and ready to go for offensive purposes to surprise and cripple enemy systems.

Cyberattacks on information systems have also been on the rise over the past few years. Such attacks, while not real cyberwar in the sense of incapacitating infrastructure, nevertheless illustrate the ease with which corporate and government systems can be penetrated. Some of these attacks were likely undertaken by nation states that were practicing their offensive techniques. For instance, in 2014, Sony Pictures' computer system was hacked, revealing information on 47,000 individuals, much of it e-mail correspondence among executives. About 70% of the firm's computers were incapacitated, and confidential e-mails were published by the hackers in an effort to embarrass executives of the firm. North Korea remains a major suspect, although North Korean officials denied this. In the biggest attack on U.S. government systems thus far, in July 2015, the White House announced that the Office of Personnel Management, the government's human resources agency and database, had been hacked and complete records on over 21 million people were copied, including the names of people in the defense sector. The likely source of the hack was the Chinese government. In 2016, U.S. intelligence agencies have reportedly expressed suspicions that the hacks into various e-mail accounts of Democratic National Committee officials and others associated with the Clinton campaign have been part of an orchestrated campaign by Russia to influence the 2016 presidential race. The Russian government has denied any involvement.

Attacks against physical infrastructure have been less frequent. Infrastructure attacks require detailed knowledge of the infrastructure, which usually requires insider knowledge of industrial controllers (computers that control valves and machines). The most well-known and best documented infrastructure attack was Stuxnet, malware allegedly created by Israeli and American intelligence services in 2010 in an effort to cripple thousands of Iranian nuclear centrifuges. Stuxnet was a malware virus program planted in industrial controller modules of Iranian nuclear fuel centrifuges, causing them to destroy themselves. Stuxnet was precedent-setting: it was the first large-scale cyberattack on infrastructure. In response, the Iranian government sponsored a cyberattack against the Saudi-Aramco company using a virus called Shamoon that wiped out 30,000 computers at the company. More recently, Russian hackers, allegedly employed by the Russian government, have picked up the spirit of Stuxnet and have targeted oil and gas firms. Using a "watering hole attack," the hackers launched a massive e-mail campaign to employees of these firms in an attempt to trick them into visiting a website where malware can be downloaded to their computers. While the emphasis of the attackers has been industrial

espionage, the same software could be used in a cyberwar attack against oil and gas production and transmission facilities just like the Stuxnet software that crippled Iranian nuclear centrifuges. Other infrastructure attacks include weapons known as Flame, which is thought to have caused Iran to disconnect its oil terminals from the Internet, and Snake, a malware tool kit believed to be from Russia that infected many Ukrainian civilian and industrial computer systems and networks. Snake gives attackers full access to remote systems, acts as a two-way conduit that can siphon information from systems, and provides a path for installing additional malware. Using these cyberweapons, Russia has led a three-year campaign against Ukrainian infrastructure and government systems, most recently in December 2015, when power was lost across multiple cities in Western Ukraine.

Security analysts believe the United States has developed the most powerful cyberwarfare defense and offense capabilities in the world. U.S. efforts are concentrated in the United States Cyber Command located in Fort Meade, Maryland. USCYBERCOM's stated mission is to coordinate and direct the operations and defense of Department of Defense (DoD) information networks and to prepare for military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace, and deny the same to adversaries. In early 2016, the DoD detailed a \$35 billion five-year cyberbudget aimed at furthering DoD's network defenses, building more cybertraining ranges for its cyberwarriors, and developing cybertools and infrastructure to provide offensive cyberweapons.

A number of diplomatic efforts have been undertaken by American planners to reach some sort of understanding with its cyberenemies that would set limits on cyberwar and prevent civilian casualties. These efforts are similar to nuclear arms treaties. In 2015, the Pentagon announced a new cyberstrategy outlining the conditions under which the United States would engage in a cyberweapons attack on an adversary. Routine attacks against companies will be defended by companies themselves, but attacks on U.S. government systems, infrastructure systems, defense systems, and intelligence systems that involve significant loss of life, destruction of property, or lasting economic damage, will be grounds for launching a major counterattack that will threaten similar losses to the enemy. This new policy is aimed at Russia, China, Iran, and North Korea, each of whom have been implicated in state-sponsored attacks on U.S. government and corporate systems for several years. Announcing this new policy raises the potential cost of hacking critical American systems, and is the beginning of a deterrence strategy based on the concept of mutual assured destruction.

In September 2015, the Obama administration finally reached an understanding with Chinese leaders. The presidents of both countries announced their pledge to refrain from computer-enabled theft of intellectual property for commercial gain, and attacks on their country's critical infrastructure, but there was no agreement to limit the use of cybertools for traditional espionage. A pledge is hardly a commitment and is certainly not a treaty. There is no verification protocol to ensure compliance. Nevertheless, this was the first agreement of any kind expressing the goal of restraining cyberwarfare, and since then, it appears that China has shifted its cyberespionage focus away from the United States and Western organizations to other areas of the world.

York Times, September 25, 2015; "U.S. and China Seek Arms Deal for Cyberspace," by David Sanger, *New York Times*, September 19, 2015; "Cyberthreat Posed by China and Iran Confounds White House," by David Sanger, *New York Times*, September 15, 2015; "U.S. vs. Hackers: Still Lopsided Despite Years of Warnings and a Recent Rush," by Michael Shear and Nicole Perlroth, *New York Times*, July 18, 2015; "Hacking of Government Computers Exposes 21.5 Million People," by Julie Hirschfield, *New York Times*, July 9, 2015; "Defense Infrastructure: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning," Government Accountability Office, July 2015; "Here's What a Cyber Warfare Arsenal Might Look Like," by Larry Greenemeier, *Scientific American*, May 6, 2015; "Pentagon Announces New Strategy for Cyberwarfare," by David Sanger, *New York Times*, April 23, 2015; "Deterrence Will Keep Lid on Cyberwar, Former Spy Chief Says," by Tim Hornyak, *Computerworld.com*, April 14, 2015; "Document Reveals Growth of Cyberwarfare Between the U.S. and Iran," by David Sanger, *New York Times*, February 22, 2015; "NATO Set to Ratify Pledge on Joint Defense in Case of Major Cyberattack," by David Sanger, *New York Times*, August 31, 2014; "Chinese Hackers Extending Reach to Smaller U.S. Agencies, Officials Say," by Michael Schmidt, *New York Times*, July 15, 2014; "Chinese Hackers Pursue Key Data on U.S. Workers," by Michael Schmidt, David Sanger, and Nicole Perlroth, *New York Times*, July 9, 2014; "Russian Hackers Targeting Oil and Gas Companies," by Nicole Perlroth, *New York Times*, June 30, 2014; "2nd China Army Unit Implicated in Online Spying," by Nicole Perlroth, *New York Times*, June 9, 2014; "5 in China Army Face U.S. Charges of Cyberattacks," by Michael Schmidt and David Sanger, *New York Times*, May 19, 2014; "Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government," by David Sanger and Steven Erlanger, *New York Times*, March 8, 2014.

As *Cyberwar: MAD 2.0* illustrates, the Internet and Web are increasingly vulnerable to large-scale attacks and potentially large-scale failure. Increasingly, these attacks are led by organized gangs of criminals operating globally—an unintended consequence of globalization. Even more worrisome is the growing number of large-scale attacks that are funded, organized, and led by various nations against the Internet resources of other nations. Anticipating and countering these attacks has proved a difficult task for both business and government organizations. However, there are several steps you can take to protect your websites, your mobile devices, and your personal information from routine security attacks. Reading this chapter, you should also start thinking about how your business could survive in the event of a large-scale “outage” of the Internet.

In this chapter, we will examine e-commerce security and payment issues. First, we will identify the major security risks and their costs, and describe the variety of solutions currently available. Then, we will look at the major payment methods and consider how to achieve a secure payment environment. **Table 5.1** highlights some of the major trends in online security in 2016–2017.

TABLE 5.1**WHAT'S NEW IN E-COMMERCE SECURITY 2016–2017**

- Large-scale data breaches continue to expose data about individuals to hackers and other cybercriminals.
- Mobile malware presents a tangible threat as smartphones and other mobile devices become more common targets of cybercriminals, especially as their use for mobile payments rises.
- Malware creation continues to skyrocket and ransomware attacks rise.
- Distributed Denial of Service (DDoS) attacks are now capable of slowing Internet service within entire countries.
- Nations continue to engage in cyberwarfare and cyberespionage.
- Hackers and cybercriminals continue to focus their efforts on social network sites to exploit potential victims through social engineering and hacking attacks.
- Politically motivated, targeted attacks by hacktivist groups continue, in some cases merging with financially motivated cybercriminals to target financial systems with advanced persistent threats.
- Software vulnerabilities, such as the Heartbleed bug and other zero day vulnerabilities, continue to create security threats.
- Incidents involving celebrities raise awareness of cloud security issues.

5.1 THE E-COMMERCE SECURITY ENVIRONMENT

For most law-abiding citizens, the Internet holds the promise of a huge and convenient global marketplace, providing access to people, goods, services, and businesses worldwide, all at a bargain price. For criminals, the Internet has created entirely new—and lucrative—ways to steal from the more than 1.6 billion Internet consumers

worldwide in 2016. From products and services, to cash, to information, it's all there for the taking on the Internet.

It's also less risky to steal online. Rather than rob a bank in person, the Internet makes it possible to rob people remotely and almost anonymously. Rather than steal a CD at a local record store, you can download the same music for free and almost without risk from the Internet. The potential for anonymity on the Internet cloaks many criminals in legitimate-looking identities, allowing them to place fraudulent orders with online merchants, steal information by intercepting e-mail, or simply shut down e-commerce sites by using software viruses and swarm attacks. The Internet was never designed to be a global marketplace with billions of users and lacks many basic security features found in older networks such as the telephone system or broadcast television networks. By comparison, the Internet is an open, vulnerable-design network. The actions of cybercriminals are costly for both businesses and consumers, who are then subjected to higher prices and additional security measures. The costs of malicious cyberactivity include not just the cost of the actual crime, but also the additional costs that are required to secure networks and recover from cyberattacks, the potential reputational damage to the affected company, as well as reduced trust in online activities, the loss of potentially sensitive business information, including intellectual property and confidential business information, and the cost of opportunities lost due to service disruptions. Ponemon Institute estimates that the average total cost of a data breach to U.S. corporations in 2016 was \$4 million (Ponemon Institute, 2016).

THE SCOPE OF THE PROBLEM

Cybercrime is becoming a more significant problem for both organizations and consumers. Bot networks, DDoS attacks, Trojans, phishing, ransomware, data theft, identity fraud, credit card fraud, and spyware are just some of the threats that are making daily headlines. Social networks also have had security breaches. But despite the increasing attention being paid to cybercrime, it is difficult to accurately estimate the actual amount of such crime, in part because many companies are hesitant to report it due to the fear of losing the trust of their customers, and because even if crime is reported, it may be difficult to quantify the actual dollar amount of the loss. A 2014 study by the Center for Strategic and International Studies examined the difficulties in accurately estimating the economic impact of cybercrime and cyberespionage, with its research indicating a range of \$375 billion to \$575 billion worldwide. Further research is planned to try to help determine an even more accurate estimate (Center for Strategic and International Studies, 2014).

One source of information is a survey conducted by Ponemon Institute of 58 representative U.S. companies in various industries. The 2015 survey found that the average annualized cost of cybercrime for the organizations in the study was \$15 million, representing a 20% increase from the previous year, and an 82% increase since the first survey in 2009. The average cost per attack was more than \$1.9 million, a 22% increase from the previous year. The number of successful cyberattacks also increased, by over 15%. The most costly cybercrimes were those caused by denial of service, malicious insiders, and malicious code. The most prevalent types of attacks were viruses, worms, and Trojans, experienced by 100% of the companies surveyed, followed by malware

(97%), web-based attacks (76%), botnets (66%), phishing and social engineering attacks (59%), and malicious code (52%) (Ponemon Institute, 2015a).

Reports issued by security product providers, such as Symantec, are another source of data. Symantec issues a semi-annual *Internet Security Threat Report*, based on 57.6 million sensors monitoring Internet activity in more than 157 countries. Advances in technology have greatly reduced the entry costs and skills required to enter the cybercrime business. Low-cost and readily available web attack kits enable hackers to create malware without having to write software from scratch. In addition, there has been a surge in polymorphic malware, which enables attackers to generate a unique version of the malware for each victim, making it much more difficult for pattern-matching software used by security firms to detect. According to Symantec, the number of data breaches increased 23% in 2015, over half a billion personal records were stolen, the number of spear-phishing attacks increased by 55%, malware increased by 36%, and ransomware attacks grew by 35% (Symantec, 2016). However, Symantec does not attempt to quantify actual crimes and/or losses related to these threats.

Online credit card fraud is one of the most high-profile forms of e-commerce crime. Although the average amount of credit card fraud loss experienced by any one individual is typically relatively small, the overall amount is substantial. The overall rate of online credit card fraud is estimated to be about 0.8% of all online card transactions, including both mobile and web transactions (Cybersource, 2016). The nature of credit card fraud has changed greatly from the theft of a single credit card number and efforts to purchase goods at a few sites, to the simultaneous theft of millions of credit card numbers and their distributions to thousands of criminals operating as gangs of thieves. The emergence of identity fraud, described in detail later in this chapter, as a major online/offline type of fraud may well increase markedly the incidence and amount of credit card fraud, because identity fraud often includes the use of stolen credit card information and the creation of phony credit card accounts.

The Underground Economy Marketplace: The Value of Stolen Information

Criminals who steal information on the Internet do not always use this information themselves, but instead derive value by selling the information to others on the so-called underground or shadow economy market. Data is currency to cybercriminals and has a “street value” that can be monetized. For example, in 2013, Vladislav Horohorin (alias “BadB”) was sentenced to over 7 years in federal prison for using online criminal forums to sell stolen credit and debit card information (referred to as “dumps”). At the time of his arrest, Horohorin possessed over 2.5 million stolen credit and debit card numbers. There are several thousand known underground economy marketplaces around the world that sell stolen information, as well as malware, such as exploit kits, access to botnets, and more. **Table 5.2** lists some recently observed prices for various types of stolen data, which typically vary depending on the quantity being purchased, supply available, and “freshness.” For example, when credit card information from the Target data breach first appeared on the market, individual card numbers went for up to \$120 each. After a few weeks, however, the price dropped

TABLE 5.2 THE CYBER BLACK MARKET FOR STOLEN DATA

DATA	PRICE *
Individual U.S. card number with expiration date and CVV2 (the three-digit number printed on back of card) (referred to as a CVV)	\$5–\$8
Individual U.S. card number with full information, including full name, billing address, expiration date, CVV2, date of birth, mother's maiden name, etc. (referred to as a Fullz or Fullzinfo)	\$30
Dump data for U.S. card (the term "dump" refers to raw data such as name, account number, expiration data, and CVV encoded on the magnetic strip on the back of the card)	\$110–\$120
Online payment service accounts	\$20–\$300
Bank account login credentials	\$80–\$700
Online account login credentials (Facebook, Twitter, eBay)	\$10–\$15
Medical information/health credentials	\$10–\$20
1,000 e-mail addresses	\$1–\$10
Scan of a passport	\$1–\$2

SOURCES: Based on data from McAfee, 2016; Intel Security, 2015; Symantec, 2015; Maruca, 2015; Infosec Institute, 2015; RAND Corporation, 2014.

*Prices vary based on supply and quality (freshness of data, account balances, validity, etc.).

dramatically (Leger, 2014). Experts believe the cost of stolen information has generally fallen as the tools of harvesting have increased the supply. On the demand side, the same efficiencies and opportunities provided by new technology have increased the number of people who want to use stolen information. It's a robust marketplace.

Finding these marketplaces and the servers that host them can be difficult for the average user (and for law enforcement agencies), and prospective participants are typically vetted by other criminals before access is granted. This vetting process takes place through Twitter, Tor, and VPN services, and sometimes e-mail exchanges of information, money (often Bitcoins, a form of digital cash that we discuss further in Section 5.5 and in the *Insight on Business* case study on pages 315–316), and reputation. There is a general hierarchy of cybercriminals in the marketplace, with low-level, nontechnical criminals who frequent "carder forums," where stolen credit and debit card data is sold, aiming to make money, a political statement, or both, at the bottom; resellers in the middle acting as intermediaries; and the technical masterminds who create malicious code at the top.

So, what can we conclude about the overall size of cybercrime? Cybercrime against e-commerce sites is dynamic and changing all the time, with new risks appearing often. The amount of losses to businesses is significant and growing. The managers of e-commerce sites must prepare for an ever-changing variety of criminal assaults, and keep current in the latest security techniques.

WHAT IS GOOD E-COMMERCE SECURITY?

What is a secure commercial transaction? Anytime you go into a marketplace you take risks, including the loss of privacy (information about what you purchased). Your prime risk as a consumer is that you do not get what you paid for. As a merchant in the market, your risk is that you don't get paid for what you sell. Thieves take merchandise and then either walk off without paying anything, or pay you with a fraudulent instrument, stolen credit card, or forged currency.

E-commerce merchants and consumers face many of the same risks as participants in traditional commerce, albeit in a new digital environment. Theft is theft, regardless of whether it is digital theft or traditional theft. Burglary, breaking and entering, embezzlement, trespass, malicious destruction, vandalism—all crimes in a traditional commercial environment—are also present in e-commerce. However, reducing risks in e-commerce is a complex process that involves new technologies, organizational policies and procedures, and new laws and industry standards that empower law enforcement officials to investigate and prosecute offenders. **Figure 5.1** illustrates the multi-layered nature of e-commerce security.

To achieve the highest degree of security possible, new technologies are available and should be used. But these technologies by themselves do not solve the problem. Organizational policies and procedures are required to ensure the technologies are not subverted. Finally, industry standards and government laws are required to enforce payment mechanisms, as well as to investigate and prosecute violators of laws designed to protect the transfer of property in commercial transactions.

FIGURE 5.1 THE E-COMMERCE SECURITY ENVIRONMENT



E-commerce security is multi-layered, and must take into account new technology, policies and procedures, and laws and industry standards.

The history of security in commercial transactions teaches that any security system can be broken if enough resources are put against it. Security is not absolute. In addition, perfect security of every item is not needed forever, especially in the information age. There is a time value to information—just as there is to money. Sometimes it is sufficient to protect a message for a few hours or days. Also, because security is costly, we always have to weigh the cost against the potential loss. Finally, we have also learned that security is a chain that breaks most often at the weakest link. Our locks are often much stronger than our management of the keys.

We can conclude then that good e-commerce security requires a set of laws, procedures, policies, and technologies that, to the extent feasible, protect individuals and organizations from unexpected behavior in the e-commerce marketplace.

DIMENSIONS OF E-COMMERCE SECURITY

There are six key dimensions to e-commerce security: integrity, nonrepudiation, authenticity, confidentiality, privacy, and availability.

Integrity refers to the ability to ensure that information being displayed on a website, or transmitted or received over the Internet, has not been altered in any way by an unauthorized party. For example, if an unauthorized person intercepts and changes the contents of an online communication, such as by redirecting a bank wire transfer into a different account, the integrity of the message has been compromised because the communication no longer represents what the original sender intended.

Nonrepudiation refers to the ability to ensure that e-commerce participants do not deny (i.e., repudiate) their online actions. For instance, the availability of free e-mail accounts with alias names makes it easy for a person to post comments or send a message and perhaps later deny doing so. Even when a customer uses a real name and e-mail address, it is easy for that customer to order merchandise online and then later deny doing so. In most cases, because merchants typically do not obtain a physical copy of a signature, the credit card issuer will side with the customer because the merchant has no legally valid proof that the customer ordered the merchandise.

Authenticity refers to the ability to identify the identity of a person or entity with whom you are dealing on the Internet. How does the customer know that the website operator is who it claims to be? How can the merchant be assured that the customer is really who she says she is? Someone who claims to be someone he is not is “spoofing” or misrepresenting himself.

Confidentiality refers to the ability to ensure that messages and data are available only to those who are authorized to view them. Confidentiality is sometimes confused with **privacy**, which refers to the ability to control the use of information a customer provides about himself or herself to an e-commerce merchant.

E-commerce merchants have two concerns related to privacy. They must establish internal policies that govern their own use of customer information, and they must protect that information from illegitimate or unauthorized use. For example, if hackers break into an e-commerce site and gain access to credit card or other information, this violates not only the confidentiality of the data, but also the privacy of the individuals who supplied the information.

integrity

the ability to ensure that information being displayed on a website or transmitted or received over the Internet has not been altered in any way by an unauthorized party

nonrepudiation

the ability to ensure that e-commerce participants do not deny (i.e., repudiate) their online actions

authenticity

the ability to identify the identity of a person or entity with whom you are dealing on the Internet

confidentiality

the ability to ensure that messages and data are available only to those who are authorized to view them

privacy

the ability to control the use of information about oneself

TABLE 5.3 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY		
DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmitted or received been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

availability
the ability to ensure that an e-commerce site continues to function as intended

Availability refers to the ability to ensure that an e-commerce site continues to function as intended.

Table 5.3 summarizes these dimensions from both the merchants' and customers' perspectives. E-commerce security is designed to protect these six dimensions. When any one of them is compromised, overall security suffers.

THE TENSION BETWEEN SECURITY AND OTHER VALUES

Can there be too much security? The answer is yes. Contrary to what some may believe, security is not an unmitigated good. Computer security adds overhead and expense to business operations, and also gives criminals new opportunities to hide their intentions and their crimes.

Ease of Use

There are inevitable tensions between security and ease of use. When traditional merchants are so fearful of robbers that they do business in shops locked behind security gates, ordinary customers are discouraged from walking in. The same can be true with respect to e-commerce. In general, the more security measures added to an

e-commerce site, the more difficult it is to use and the slower the site becomes. As you will discover reading this chapter, digital security is purchased at the price of slowing down processors and adding significantly to data storage demands on storage devices. Security is a technological and business overhead that can detract from doing business. Too much security can harm profitability, while not enough security can potentially put you out of business. One solution is to adjust security settings to the user's preferences. A recent McKinsey report found that when consumers find authentication at websites easy, they purchased 10% to 20% more. About 30% of the Internet population prioritizes ease of use and convenience over security, while 10% prioritize security. The report suggests it is possible to have both ease of use and security by adjusting the authentication process for each customer, providing options from automatic login (low security), to downloadable one-time passwords (high security) (Hasham, et al., 2016).

Public Safety and the Criminal Uses of the Internet

There is also an inevitable tension between the desires of individuals to act anonymously (to hide their identity) and the needs of public officials to maintain public safety that can be threatened by criminals or terrorists. This is not a new problem, or even new to the electronic era. The U.S. government began tapping telegraph wires during the Civil War in the mid-1860s in order to trap conspirators and terrorists, and the first police wiretaps of local telephone systems were in place by the 1890s—20 years after the invention of the phone (Schwartz, 2001). No nation-state has ever permitted a technological haven to exist where criminals can plan crimes or threaten the nation-state without fear of official surveillance or investigation. In this sense, the Internet is no different from any other communication system. Drug cartels make extensive use of voice, fax, the Internet, and encrypted e-mail; a number of large international organized crime groups steal information from commercial websites and resell it to other criminals who use it for financial fraud. Over the years, the U.S. government has successfully pursued various “carding forums” (websites that facilitate the sale of stolen credit card and debit card numbers), such as Shadowcrew, Carderplanet, and Cardersmarket, resulting in the arrest and prosecution of a number of their members and the closing of the sites. However, other criminal organizations have emerged to take their place.

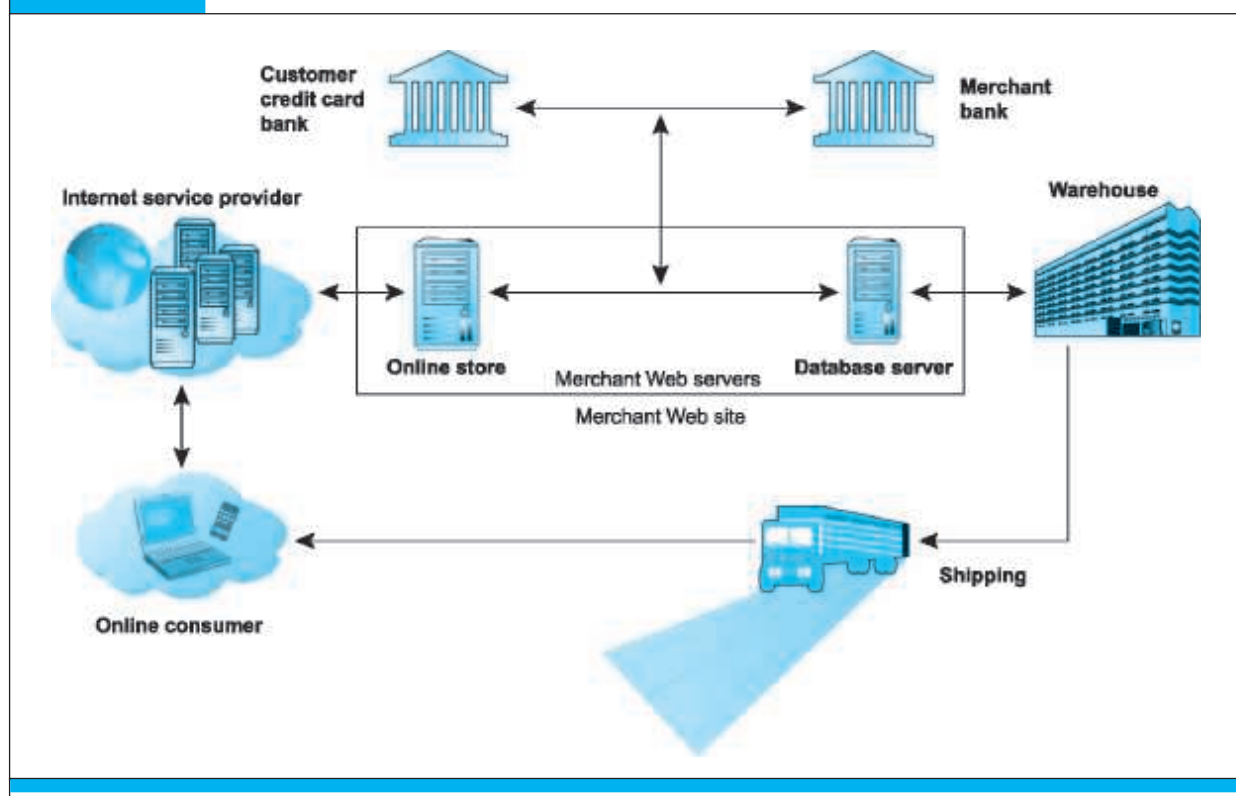
The Internet and mobile platform also provide terrorists with convenient communications channels. Encrypted files sent via e-mail were used by Ramzi Yousef—a member of the terrorist group responsible for bombing the World Trade Center in 1993—to hide plans for bombing 11 U.S. airliners. The Internet was also used to plan and coordinate the subsequent attacks on the World Trade Center on September 11, 2001. The case of Umar Farouk Abdulmutallab further illustrates how terrorists make effective use of the Internet to radicalize, recruit, train, and coordinate youthful terrorists. Abdulmutallab allegedly attempted to blow up an American airliner in Detroit on Christmas Day 2009. He was identified, contacted, recruited, and trained, all within six weeks, according to a Pentagon counterterrorism official. In an effort to combat such terrorism, the U.S. government has significantly ramped up its surveillance of communications delivered via the Internet over the past several years. The extent of that surveillance created a major controversy with National Security Agency contrac-

tor Edward Snowden's release of classified NSA documents that revealed that the NSA had obtained access to the servers of major Internet companies such as Facebook, Google, Apple, Microsoft, and others, as well as that NSA analysts have been searching e-mail, online chats, and browsing histories of U.S. citizens without any court approval. Security agencies have shifted from mass surveillance to smaller, targeted surveillance of terrorists and terrorist groups, and the use of predictive algorithms to focus their efforts (N.F. Johnson, et al., 2016). The proper balance between public safety and privacy in the effort against terrorism has proven to be a very thorny problem for the U.S. government.

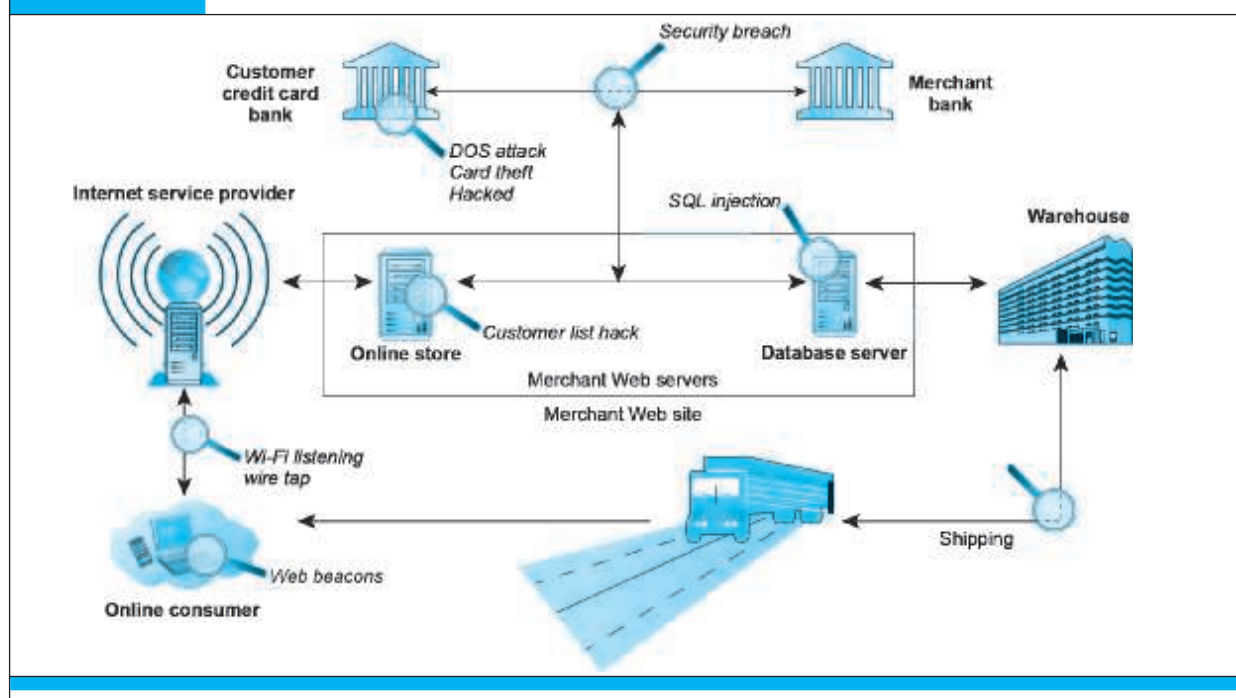
5.2 SECURITY THREATS IN THE E-COMMERCE ENVIRONMENT

From a technology perspective, there are three key points of vulnerability when dealing with e-commerce: the client, the server, and the communications pipeline. **Figure 5.2** illustrates a typical e-commerce transaction with a consumer using a credit

FIGURE 5.2 A TYPICAL E-COMMERCE TRANSACTION



In a typical e-commerce transaction, the customer uses a credit card and the existing credit payment system.

FIGURE 5.3 VULNERABLE POINTS IN AN E-COMMERCE TRANSACTION

There are three major vulnerable points in e-commerce transactions: Internet communications, servers, and clients.

card to purchase a product. **Figure 5.3** illustrates some of the things that can go wrong at each major vulnerability point in the transaction—over Internet communications channels, at the server level, and at the client level.

In this section, we describe a number of the most common and most damaging forms of security threats to e-commerce consumers and site operators: malicious code, potentially unwanted programs, phishing, hacking and cybervandalism, credit card fraud/theft, spoofing, pharming, spam (junk) websites (link farms), identity fraud, Denial of Service (DoS) and DDoS attacks, sniffing, insider attacks, poorly designed server and client software, social network security issues, mobile platform security issues, and finally, cloud security issues.

MALICIOUS CODE

Malicious code (sometimes referred to as “malware”) includes a variety of threats such as viruses, worms, Trojan horses, ransomware, and bots. Some malicious code, sometimes referred to as an *exploit*, is designed to take advantage of software vulnerabilities in a computer's operating system, web browser, applications, or other software components. **Exploit kits** are collections of exploits bundled together and rented or sold as a commercial product, often with slick user interfaces and in-depth analytics functionality. Use of an exploit kit typically does not require much technical skill, enabling novices

malicious code (malware)

includes a variety of threats such as viruses, worms, Trojan horses, and bots

exploit kit

collection of exploits bundled together and rented or sold as a commercial product

to become cybercriminals. Exploit kits typically target software that is widely deployed, such as Microsoft Windows, Internet Explorer, Adobe Flash and Reader, and Oracle Java. In 2014, according to Cisco, Angler, an exploit kit that uses Flash, Java, Microsoft Internet Explorer, and Microsoft Silverlight vulnerabilities, was one of the exploit kits most observed “in the wild” (Cisco, 2016). According to Symantec, more than 430 million new variants of malware were created in 2015, an average of more than a million strains a day, up 36% in one year (Symantec, 2016). In the past, malicious code was often intended to simply impair computers, and was often authored by a lone hacker, but increasingly it involves a small group of hackers or a nation-state supported group, and the intent is to steal e-mail addresses, logon credentials, personal data, and financial information. It's the difference between petty crime and organized crime.

Malware is often delivered in the form of a malicious attachment to an email or embedded as a link in the email. Malicious links can also be placed in innocent-looking Microsoft Word or Excel documents. The links lead directly to a malicious code download or websites that include malicious code (Symantec, 2016). One of the latest innovations in malicious code distribution is to embed it in the online advertising chain (known as **maladvertising**), including in Google, AOL, and other ad networks (Goodin, 2016). As the ad network chain becomes more complicated, it becomes more and more difficult for websites to vet ads placed on their sites to ensure they are malware-free. A 2014 research study indicated that as many as 1% of all ads served may be maladvertising (Zarras et al., 2014). The largest advertising malware infection occurred at Yahoo where more than 6.9 million daily visitors were exposed to malicious pop-up ads (Blue, 2016). These malicious ads can be stopped by turning on pop-up blockers in users' browsers. Much of the maladvertising in the recent years has been in the form of drive-by downloads that exploited the frequent zero-day vulnerabilities that have plagued Adobe Flash, which is often used for online advertisements. As a result, the Internet Advertising Bureau has urged advertisers to abandon Adobe Flash in favor of HTML5, and Mozilla Firefox, Apple's Safari, and Google's Chrome browser all now block Flash advertisements from autoplaying. Amazon has also stopped accepting Flash ads (see the Chapter 3 *Insight on Technology* case, *The Rise of HTML5*). A **drive-by download** is malware that comes with a downloaded file that a user intentionally or unintentionally requests. Drive-by is now one of the most common methods of infecting computers. For instance, websites as disparate as the New York Times, MSN, Yahoo, and AOL have experienced instances where ads placed on their sites either had malicious code embedded or directed clickers to malicious sites. According to Symantec, drive-by download exploit kits, including updates and 24/7 support, can be rented for between \$100 to \$700 per week. Malicious code embedded in PDF files also is common. Equally important, there has been a major shift in the writers of malware from amateur hackers and adventurers to organized criminal efforts to defraud companies and individuals. In other words, it's now more about the money than ever before.

A **virus** is a computer program that has the ability to replicate or make copies of itself, and spread to other files. In addition to the ability to replicate, most computer viruses deliver a “payload.” The payload may be relatively benign, such as the display of a message or image, or it may be highly destructive—destroying files, reformatting the computer's hard drive, or causing programs to run improperly.

maladvertising

online advertising that contains malicious code

drive-by download

malware that comes with a downloaded file that a user requests

virus

a computer program that has the ability to replicate or make copies of itself, and spread to other files

Viruses are often combined with a worm. Instead of just spreading from file to file, a **worm** is designed to spread from computer to computer. A worm does not necessarily need to be activated by a user or program in order for it to replicate itself. The Slammer worm is one of the most notorious. Slammer targeted a known vulnerability in Microsoft's SQL Server database software and infected more than 90% of vulnerable computers worldwide within 10 minutes of its release on the Internet; crashed Bank of America cash machines, especially in the southwestern part of the United States; affected cash registers at supermarkets such as the Publix chain in Atlanta, where staff could not dispense cash to frustrated buyers; and took down most Internet connections in South Korea, causing a dip in the stock market there. The Conficker worm, which first appeared in November 2008, is the most significant worm since Slammer, and reportedly infected 11 million computers worldwide (Microsoft, 2015). Originally designed to establish a global botnet, a massive industry effort has defeated this effort, but Conficker still resides on over 800,000 Internet devices in 2016. It is the most widely detected malware on the Internet.

Ransomware (scareware) is a type of malware (often a worm) that locks your computer or files to stop you from accessing them. Ransomware will often display a notice that says an authority such as the FBI, Department of Justice, or IRS has detected illegal activity on your computer and demands that you pay a fine in order to unlock the computer and avoid prosecution. One type of ransomware is named CryptoLocker. CryptoLocker encrypts victims' files with a virtually unbreakable asymmetric encryption and demands a ransom to decrypt them, often in Bitcoins. If the victim does not comply within the time allowed, the files will not ever be able to be decrypted. Other variants include CryptoDefense and Cryptowall. Ransomware attacks increased by over 400% in 2016, and the U.S. Department of Justice reports that there are over 4,000 ransomware attacks daily, up from 1,000 daily in 2015 (U.S. Department of Justice, 2016). Crypto-ransomware infections often take place via a malicious e-mail attachment that purports to be an invoice (Symantec, 2016). The growth of ransomware is also related to the growth of the virtual currency Bitcoin. Hackers often demand victims pay using Bitcoin so their transactions are hidden from authorities (McMillan, 2016).

A **Trojan horse** appears to be benign, but then does something other than expected. The Trojan horse is not itself a virus because it does not replicate, but is often a way for viruses or other malicious code such as bots or *rootkits* (a program whose aim is to subvert control of the computer's operating system) to be introduced into a computer system. The term *Trojan horse* refers to the huge wooden horse in Homer's *Iliad* that the Greeks gave their opponents, the Trojans—a gift that actually contained hundreds of Greek soldiers. Once the people of Troy let the massive horse within their gates, the soldiers revealed themselves and captured the city. In today's world, a Trojan horse may masquerade as a game, but actually hide a program to steal your passwords and e-mail them to another person. Miscellaneous Trojans and Trojan downloaders and droppers (Trojans that install malicious files to a computer they have infected by either downloading them from a remote computer or from a copy contained in their own code) are a common type of malware. According to Panda Security, Trojans accounted for over 50% of all malware created in 2015, and over 60% of all malware infections (Panda Security, 2016). In 2011, Sony experienced the largest data

worm

malware that is designed to spread from computer to computer

ransomware (scareware)

malware that prevents you from accessing your computer or files and demands that you pay a fine

Trojan horse

appears to be benign, but then does something other than expected. Often a way for viruses or other malicious code to be introduced into a computer system

breach in history up to that time when a Trojan horse took over the administrative computers of Sony's PlayStation game center and downloaded personal and credit card information involving 77 million registered users (Wakabayashi, 2011). Trojan horses are often used for financial malware distributed via botnets. One example is Zeus, which steals information by keystroke logging and has infected over 10 million computers since it first became known in 2007. Other examples include SpyEye, a Trojan that can steal banking information via both a keylogging application and the ability to take screenshots on a victim's computer; Torpig, a botnet that is spread by a Trojan horse called Meboot; and Vawtrak, a Trojan that spreads via social media, e-mail, and FTP, and is able to hide evidence of fraud by changing bank balances shown to the victim on the fly (Cyphort, 2015).

backdoor

feature of viruses, worms, and Trojans that allows an attacker to remotely access a compromised computer

bot

type of malicious code that can be covertly installed on a computer when connected to the Internet. Once installed, the bot responds to external commands sent by the attacker

botnet

collection of captured bot computers

A **backdoor** is a feature of viruses, worms, and Trojans that allows an attacker to remotely access a compromised computer. Downadup is an example of a worm with a backdoor, while Virut, a virus that infects various file types, also includes a backdoor that can be used to download and install additional threats.

Bots (short for robots) are a type of malicious code that can be covertly installed on your computer when attached to the Internet. Once installed, the bot responds to external commands sent by the attacker; your computer becomes a "zombie" and is able to be controlled by an external third party (the "bot-herder"). **Botnets** are collections of captured computers used for malicious activities such as sending spam, participating in a DDoS attack, stealing information from computers, and storing network traffic for later analysis. The number of botnets operating worldwide is not known but is estimated to be well into the thousands, controlling millions of computers. Bots and bot networks are an important threat to the Internet and e-commerce because they can be used to launch very large-scale attacks using many different techniques. In 2011, federal marshals accompanied members of Microsoft's digital crimes unit in raids designed to disable the Rustock botnet, at that time the leading source of spam in the world with nearly 500,000 slave PCs under the control of its command and control servers located at six Internet hosting services in the United States. Officials confiscated the Rustock control servers at the hosting sites, which claimed they had no idea what the Rustock servers were doing. The actual spam e-mails were sent by the slave PCs under the command of the Rustock servers (Wingfield, 2011). In 2013, Microsoft and the FBI engaged in another aggressive botnet operation, targeting 1,400 of Zeus-derived Citadel botnets, which had been used in 2012 to raid bank accounts at major banks around the world, netting over \$500 million (Chirgwin, 2013). In April 2015, an international cybersquad took down the Beebone botnet, made up of 12,000 computers that had been infecting about 30,000 computers a month around the world via drive-by downloads with Changeup, a polymorphic worm used to distribute Trojans, worms, backdoors, and other types of malware (Constantin, 2015). In 2015, the FBI and British police were also able to stop a botnet that had stolen over \$10 million from banks (Pagliery, 2015). As a result of efforts such as these, the number of bots has significantly declined, especially in the United States (Symantec, 2016).

Malicious code is a threat at both the client and the server levels, although servers generally engage in much more thorough anti-virus activities than do consumers. At

TABLE 5.4 NOTABLE EXAMPLES OF MALICIOUS CODE		
NAME	TYPE	DESCRIPTION
Cryptolocker	Ransomware/Trojan	Hijacks users' photos, videos, and text documents, encrypts them with virtually unbreakable asymmetric encryption, and demands ransom payment for them.
Citadel	Trojan/botnet	Variant of Zeus Trojan, focuses on the theft of authentication credentials and financial fraud. Botnets spreading Citadel were targets of Microsoft/FBI action in 2012.
Zeus	Trojan/botnet	Sometimes referred to as king of financial malware. May install via drive-by download and evades detection by taking control of web browser and stealing data that is exchanged with bank servers.
Reveton	Ransomware worm/Trojan	Based on Citadel/Zeus Trojans. Locks computer and displays warning from local police alleging illegal activity on computer; demands payment of fine to unlock.
Ramnit	Virus/worm	One of the most prevalent malicious code families still active in 2013. Infects various file types, including executable files, and copies itself to removable drives, executing via AutoPlay when the drive is accessed on other computers
Sality.AE	Virus/worm	Most common virus in 2012; still active in 2013. Disables security applications and services, connects to a botnet, then downloads and installs additional threats. Uses polymorphism to evade detection.
Conficker	Worm	First appeared November 2008. Targets Microsoft operating systems. Uses advanced malware techniques. Largest worm infection since Slammer in 2003. Still considered a major threat.
Netsky.P	Worm/Trojan	First appeared in early 2003. It spreads by gathering target e-mail addresses from the computers, then infects and sends e-mail to all recipients from the infected computer. It is commonly used by bot networks to launch spam and DoS attacks.
Storm (Peacomm, NuWar)	Worm/Trojan	First appeared in January 2007. It spreads in a manner similar to the Netsky.P worm. May also download and run other Trojan programs and worms.
Nymex	Worm	First discovered in January 2006. Spreads by mass mailing; activates on the 3rd of every month, and attempts to destroy files of certain types.
Zotob	Worm	First appeared in August 2005. Well-known worm that infected a number of U.S. media companies.
Mydoom	Worm	First appeared in January 2004. One of the fastest spreading mass-mailer worms.
Slammer	Worm	Launched in January 2003. Caused widespread problems.
CodeRed	Worm	Appeared in 2001. It achieved an infection rate of over 20,000 systems within 10 minutes of release and ultimately spread to hundreds of thousands of systems.
Melissa	Macro virus/worm	First spotted in March 1999. At the time, the fastest spreading infectious program ever discovered. It attacked Microsoft Word's Normal.dot global template, ensuring infection of all newly created documents. It also mailed an infected Word file to the first 50 entries in each user's Microsoft Outlook Address Book.
Chernobyl	File-infecting virus	First appeared in 1998. It wipes out the first megabyte of data on a hard disk (making the rest useless) every April 26, the anniversary of the nuclear disaster at Chernobyl.

the server level, malicious code can bring down an entire website, preventing millions of people from using the site. Such incidents are infrequent. Much more frequent malicious code attacks occur at the client level, and the damage can quickly spread to millions of other computers connected to the Internet. **Table 5.4** lists some well-known examples of malicious code.

potentially unwanted program (PUP)

program that installs itself on a computer, typically without the user's informed consent

adware

a PUP that serves pop-up ads to your computer

browser parasite

a program that can monitor and change the settings of a user's browser

spyware

a program used to obtain information such as a user's keystrokes, e-mail, instant messages, and so on

social engineering

exploitation of human fallibility and gullibility to distribute malware

phishing

any deceptive, online attempt by a third party to obtain confidential information for financial gain

POTENTIALLY UNWANTED PROGRAMS (PUPS)

In addition to malicious code, the e-commerce security environment is further challenged by **potentially unwanted programs (PUPs)** such as adware, browser parasites, spyware, and other applications that install themselves on a computer, such as rogue security software, toolbars, and PC diagnostic tools, typically without the user's informed consent. Such programs are increasingly found on social network and user-generated content sites where users are fooled into downloading them. Once installed, these applications are usually exceedingly difficult to remove from the computer. One example of a PUP is System Doctor, which infects PCs running Windows operating systems. System Doctor poses as a legitimate anti-spyware program when in fact it is malware that, when installed, disables the user's security software, alters the user's web browser, and diverts users to scam websites where more malware is downloaded.

Adware is typically used to call for pop-up ads to display when the user visits certain sites. While annoying, adware is not typically used for criminal activities. A **browser parasite** is a program that can monitor and change the settings of a user's browser, for instance, changing the browser's home page, or sending information about the sites visited to a remote computer. Browser parasites are often a component of adware. In early 2015, Lenovo faced a barrage of criticism when it became known that, since September 2014, it had been shipping its Windows laptops with Superfish adware preinstalled. Superfish injected its own shopping results into the computer's browser when the user searched on Google, Amazon, or other websites. In the process, Superfish created a security risk by enabling others on a Wi-Fi network to silently hijack the browser and collect anything typed into it. Lenovo ultimately issued a removal tool to enable customers to delete the adware. Microsoft and legitimate security firms have redefined adware programs to be malware and discourage manufacturers from shipping products with adware programs (Loeb, 2016).

Spyware, on the other hand, can be used to obtain information such as a user's keystrokes, copies of e-mail and instant messages, and even take screenshots (and thereby capture passwords or other confidential data).

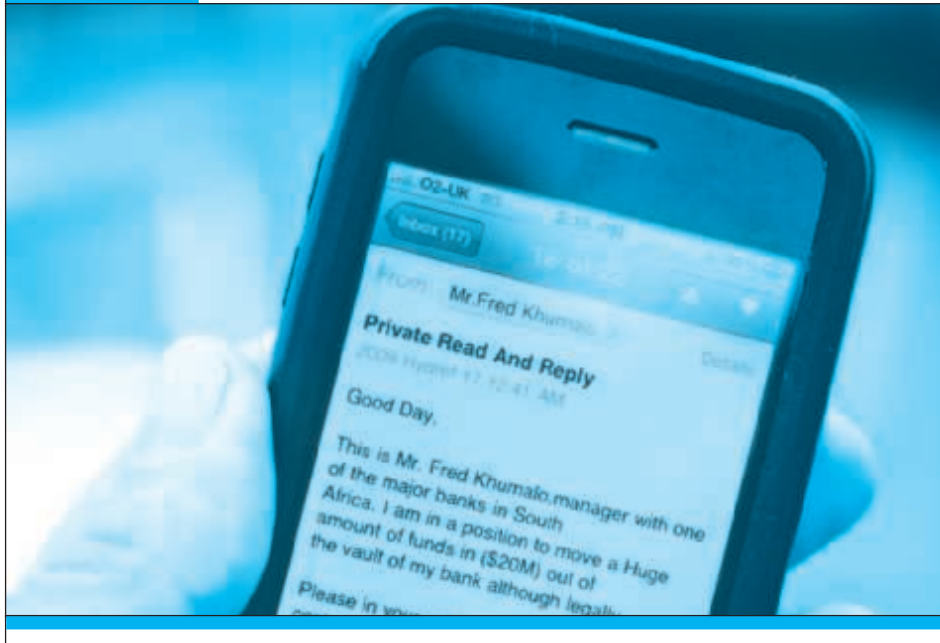
PHISHING

Social engineering relies on human curiosity, greed, and gullibility in order to trick people into taking an action that will result in the downloading of malware. Kevin Mitnick, until his capture and imprisonment in 1999, was one of America's most wanted computer criminals. Mitnick used simple deceptive techniques to obtain passwords, social security, and police records all without the use of any sophisticated technology (Mitnick, 2011).

Phishing is any deceptive, online attempt by a third party to obtain confidential information for financial gain. Phishing attacks typically do not involve malicious code but instead rely on straightforward misrepresentation and fraud, so-called "social engineering" techniques. One of the most popular phishing attacks is the e-mail scam letter. The scam begins with an e-mail: a rich former oil minister of Nigeria is seeking a bank account to stash millions of dollars for a short period of time, and requests your bank account number where the money can be deposited. In return, you will receive

FIGURE 5.4

AN EXAMPLE OF A NIGERIAN LETTER E-MAIL SCAM



This is an example of a typical Nigerian letter e-mail scam.

© keith morris / Alamy

a million dollars. This type of e-mail scam is popularly known as a “Nigerian letter” scam (see **Figure 5.4**).

Thousands of other phishing attacks use other scams, some pretending to be eBay, PayPal, or Citibank writing to you for account verification (known as *spear phishing*, or targeting a known customer of a specific bank or other type of business). Click on a link in the e-mail and you will be taken to a website controlled by the scammer, and prompted to enter confidential information about your accounts, such as your account number and PIN codes. On any given day, millions of these phishing attack e-mails are sent, and, unfortunately, some people are fooled and disclose their personal account information.

Phishers rely on traditional “con man” tactics, but use e-mail to trick recipients into voluntarily giving up financial access codes, bank account numbers, credit card numbers, and other personal information. Often, phishers create (or “spoof”) a website that purports to be a legitimate financial institution and cons users into entering financial information, or the site downloads malware such as a keylogger to the victim’s computer. Phishers use the information they gather to commit fraudulent acts such as charging items to your credit cards or withdrawing funds from your bank account, or in other ways “steal your identity” (identity fraud). Symantec reported that in 2015, about 1 in every 1,875 e-mails contained a phishing attack. The number of spear-phishing campaigns in 2015 increased by 55%, but the number of attacks, recipients within each campaign, and the average duration of the campaign all declined, indi-

cating that perpetrators are becoming stealthier about them, since campaigns that target fewer recipients and are smaller and shorter are less likely to arouse suspicion. In 2015, according to Symantec, 43% of spear-phishing e-mails were directed at small businesses with less than 250 employees, and 35% of large organizations reported they were targeted in spear-phishing campaigns (Symantec, 2016). According to Verizon, 30% of phishing emails were opened by their targets, and 12% were clicked on to open attachments (Verizon, 2016).

To combat phishing, in January 2012, leading e-mail service providers, including Google, Microsoft, Yahoo, and AOL, as well as financial services companies such as PayPal, Bank of America, and others, joined together to form DMARC.org, an organization aimed at dramatically reducing e-mail address spoofing, in which attackers use real e-mail addresses to send phishing e-mails to victims who may be deceived because the e-mail appears to originate from a source the receiver trusts. DMARC offers a method of authenticating the origin of the e-mail and allows receivers to quarantine, report, or reject messages that fail to pass its test. Yahoo and AOL have reported significant success against email fraud as a result of using DMARC, and, effective as of June 2016, Google joined them in implementing a stricter version of DMARC, in which e-mail that fails DMARC authentication checks will be rejected (Vijayan, 2015).

HACKING, CYBERVANDALISM, AND HACKTIVISM

hacker

an individual who intends to gain unauthorized access to a computer system

cracker

within the hacking community, a term typically used to denote a hacker with criminal intent

cybervandalism

intentionally disrupting, defacing, or even destroying a site

hacktivism

cybervandalism and data theft for political purposes

A **hacker** is an individual who intends to gain unauthorized access to a computer system. Within the hacking community, the term **cracker** is typically used to denote a hacker with criminal intent, although in the public press, the terms hacker and cracker tend to be used interchangeably. Hackers and crackers gain unauthorized access by finding weaknesses in the security procedures of websites and computer systems, often taking advantage of various features of the Internet that make it an open system that is easy to use. In the past, hackers and crackers typically were computer aficionados excited by the challenge of breaking into corporate and government websites. Sometimes they were satisfied merely by breaking into the files of an e-commerce site. Today, hackers have malicious intentions to disrupt, deface, or destroy sites (**cybervandalism**) or to steal personal or corporate information they can use for financial gain (data breach).

Hacktivism adds a political twist. Hacktivists typically attack governments, organizations, and even individuals for political purposes, employing the tactics of cybervandalism, distributed denial of service attacks, data thefts, and doxing (gathering and exposing personal information of public figures, typically from emails, social network posts, and other documents). The most prominent hacktivist organization is Wikileaks, founded by Julian Assange and others, which released documents and e-mails of the U.S. Department of State, U.S. Department of Defense, and Democratic National Committee in 2016. LulzSec and Anonymous are two other prominent hacktivist groups. In 2015, another hacktivist group called the Impact Team allegedly hacked the Ashley Madison website to call attention to its weak security, and after its owner Avid Life Media refused to shut it down as they demanded, the group released millions of sensitive customer records. See the *Insight on Society* case study, *The Ashley Madison Data Breach*, for a more in-depth look at implications of this high-profile hack.



INSIGHT ON SOCIETY

THE ASHLEY MADISON DATA BREACH

As the Internet continues to permeate even the most intimate aspects of our lives, the stigma attached to online dating has largely disappeared. Online dating has grown into a \$2.2 billion industry annually in the United States, led by companies like eHarmony, OKCupid, and Match. There are also a number of smaller niche sites that cater to people with more specific interests or lifestyles. One such site is Ashley Madison.

Based in Canada and launched in 2001 by its parent company, Avid Life Media, Ashley Madison specifically markets itself to people in marriages or committed relationships, which has earned the site a tawdry reputation. Users purchase credits, rather than a monthly subscription, and then redeem the credits to participate in conversations with other members, which can be through messages or real-time chat. Women are not charged money to create a profile on the site, nor are they charged to send or receive messages, while men are charged for both. Even with those incentives, the ratio of men to women on the site skews dramatically toward men, which led Ashley Madison to create fictitious female profiles to create the appearance of balance.


The perception of secrecy is critical for prospective users of Ashley Madison. But in 2015, that veil of secrecy came crashing down. The site was hacked by a group known as The Impact Team, which stated that its motivations were to harm the site and its unethical business model, as well as to protest the site's use of a \$19 data deletion fee for users seeking to close their accounts. The Impact Team stated that after creating a plan to make an undetectable breach, they discovered they were easily able to access the entire cache of company data. They released the data in two batches of 10 and 12 gigabytes, and the data is

now easily searchable on the Web. Names, street addresses, and dates of birth were all stolen and made public, as well as other personal information. They also stole company documents, including the e-mails of CEO Noel Biderman, many of which caused further damage to the company's shattered reputation. For example, Biderman's e-mails revealed that the CTO of Ashley Madison had hacked a competitor's database, revealing key security flaws (perhaps he should have been paying more attention to his own company's security systems). Partial credit card information of Ashley Madison users was also leaked, but not enough for identity thieves to use.

Demographic information gleaned from the data dump shows that of the site's 36 million users, 31 million were males, but only 10 million actively used the site. The other 5 million profiles were female, but less than 2,500 of those were involved in chats with other users, suggesting that fake female profiles were the overwhelming majority of female profiles on the site. A full third of the accounts on the site were created with dummy e-mail addresses. North Americans had the highest number of accounts as a percentage of population, with the United States coming in at 5.1%. E-mail addresses associated with government accounts were well-represented, as were big banks, large tech companies, and other high-powered industries. This stands in stark demographic contrast to a service like Tinder, which consists of much younger members; Ashley Madison users tended to be more established financially and willing to pay for what they perceived to be a discreet and upscale service. After the hack, researchers found that companies with a disproportionately high number of Ashley Madison members took bigger financial risks and had poor scores in corporate responsibility.

Ashley Madison's own corporate profile suggests risk-taking of its own. How could a site

(continued)



that advertises the ability to discreetly have an affair allow its data to be breached and stolen so easily? Security experts reviewing Ashley Madison's setup claimed that the site lacked even simplistic security measures. For example, all of the data belonging to users who paid the \$19 data deletion fee persisted on Ashley Madison servers and was obtained in the hack. Additionally, none of the data was encrypted. Encryption would have incurred hefty additional expense for the company, but it might have saved it considerable embarrassment during a breach like this one.

Most data breaches allow criminals to engage in identity theft and other types of online fraud. But in this case, the Ashley Madison hack has even more significant ramifications on the personal lives of its users. There are already multiple reported incidents of suicides committed by former users, and a handful of notable public figures have been publicly embarrassed by the release of their profile data. The hack has the potential to ruin the marriages and personal lives of thousands of people. Although many of Ashley Madison's users were engaged in infidelity, these people were still the victims of a crime and an invasion of privacy that goes beyond typical data breaches. Spammers and blackmailers have used the now-public data to extort users, demanding Bitcoin in exchange for silence and threatening to share Ashley Madison data with users' families and social media contacts.

As a result of the hack, Biderman quickly stepped down from his post as CEO, and in 2016

a new executive team was installed and immediately began distancing themselves from the previous regime. Going forward, the revelations about fake profiles, impending lawsuits, and overall negative coverage of the breach will likely derail plans for growth. Ashley Madison had already struggled to market its business and raise funds in the past, despite its very solid financial profile. The company had been growing so fast that Biderman had started investigating launching an IPO in England to fuel its expansion. Not only are those plans on hold indefinitely, but the Federal Trade Commission has begun investigating Ashley Madison's usage of bots and other fake profiles. Ashley Madison has also begun to receive what may become a barrage of lawsuits alleging negligence and personal damages, though many potential plaintiffs may be unwilling to reveal their identities, which they must do to be included in any suit after a judge ruled in 2016 that plaintiffs could not use aliases such as John Doe. And the results of a joint investigation by the Canadian and Australian governments completed in 2016 confirmed that the company had fabricated a "trusted security award" displayed on its homepage. The investigation also confirmed the company's failure to delete profile information of users who canceled their accounts.

Despite the turmoil, the company estimates that its membership base has actually grown over the past year. However, a third-party analysis showed that traffic to the site has dropped by 82% since the breach, calling the site's self-reported numbers into question.

SOURCES: "Ashley Madison Blasted Over Fake Security Award as Lawsuit Moves Forward," by Jeff John Roberts, *Fortune*, August 25, 2016; "You Blew It, Ashley Madison: Dating Site Slammed for Security 'Shortcomings,'" by Claire Reilly Cnet.com, August 23, 2015; "Ashley Madison Parent, Under FTC Investigation, Launches Turnaround Plans," by Maria Armentel and Austen Hufford, *Wall Street Journal*, July 5, 2016; "Infidelity Website Ashley Madison Facing FTC Probe, Apologizes," Alastair Sharp and Allison Martell, by Reuters.com, July 5, 2016; "Ashley Madison Hacking Victims Face Big Decision," by Robert Hackett, *Fortune*, April 20, 2016; "The Ashley Madison Effect on Companies," by Justin Lahart, *Wall Street Journal*, March 6, 2016; "Life After the Ashley Madison Affair," by Tom Lamont, *Theguardian.com*, February 27, 2016; "It's Been Six Months Since the Ashley Madison Hack. Has Anything Changed?" by Caitlin Dewey, *Washington Post*, January 15, 2016; "Ashley Madison Hack Victims Receive Blackmail Letters," BBC, December 15, 2015; "Ashley Madison Hack: 6 Charts That Show Who Uses the Infidelity Website," by Zachary Davies Boren, *Independent.co.uk*, August 21, 2015; "Ashley Madison Hackers Speak Out: 'Nobody Was Watching'," by Joseph Cox, *Motherboard.vice.com*, August 21, 2015; "The Ashley Madison Hack, Explained," by Timothy B. Lee, *Vox.com*, August 19, 2015; "Who Is Ashley Madison," by Paul R. LaMonica, *CNN Money*, July 20, 2015.

Groups of hackers called *tiger teams* are sometimes used by corporate security departments to test their own security measures. By hiring hackers to break into the system from the outside, the company can identify weaknesses in the computer system's armor. These "good hackers" became known as **white hats** because of their role in helping organizations locate and fix security flaws. White hats do their work under contract, with agreement from the target firms that they will not be prosecuted for their efforts to break in. Hardware and software firms such as Apple and Microsoft pay bounties of \$25,000 to \$200,000 to white hat hackers for discovering bugs in their software and hardware (Perlroth, 2016).

In contrast, **black hats** are hackers who engage in the same kinds of activities but without pay or any buy-in from the targeted organization, and with the intention of causing harm. They break into websites and reveal the confidential or proprietary information they find. These hackers believe strongly that information should be free, so sharing previously secret information is part of their mission.

Somewhere in the middle are the **grey hats**, hackers who believe they are pursuing some greater good by breaking in and revealing system flaws. Grey hats discover weaknesses in a system's security, and then publish the weakness without disrupting the site or attempting to profit from their finds. Their only reward is the prestige of discovering the weakness. Grey hat actions are suspect, however, especially when the hackers reveal security flaws that make it easier for other criminals to gain access to a system.

DATA BREACHES

A **data breach** occurs whenever organizations lose control over corporate information to outsiders. According to Symantec, the total number of data breaches in 2015 grew by only 2% compared to 2014, which was a record year for breaches. There were nine mega-breaches in 2015, up from eight in 2014. The total identities exposed reached 429 million, up 23%, with over 190 million identities exposed in a single breach (Symantec, 2016). The Identity Theft Resource Center is another organization that tracks data breaches. It recorded 780 breaches in 2015, the second highest total on record. Breaches involving the medical/healthcare industry had the highest impact, representing 35% of all breaches and almost 70% of all records exposed. Hackers were the leading cause of data breaches, responsible for almost 40% of breaches, followed by employee error/negligence (15%), accidental e-mail/Internet exposure (14%) and insider theft (11%). The number of breaches involving social security numbers involved almost 165 million people (Identity Theft Resource Center, 2016). Among the high profile breaches that occurred in 2015 were those affecting the Office of Personnel Management and the Internal Revenue Service, as well as others against health-care insurers such as Anthem and Premera, retailers such as CVS and Walgreens, and the credit rating agency Experian. In 2016, the trend has continued with the Yahoo data breach, which is believed to be the largest breach at a single company in history, exposing the records of 500 million. Compared to others like Google and Microsoft, Yahoo management was reportedly slow to invest in security measures (Perlroth and Goel, 2016).

white hats

"good" hackers who help organizations locate and fix security flaws

black hats

hackers who act with the intention of causing harm

grey hats

hackers who believe they are pursuing some greater good by breaking in and revealing system flaws

data breach

occurs when an organization loses control over its information to outsiders

CREDIT CARD FRAUD/THEFT

Theft of credit card data is one of the most feared occurrences on the Internet. Fear that credit card information will be stolen prevents users from making online purchases in many cases. Interestingly, this fear appears to be largely unfounded. Incidences of stolen credit card information are actually much lower than users think, around 0.8% of all online card transactions (CyberSource, 2016). Online merchants use a variety of techniques to combat credit card fraud, including using automated fraud detection tools, manually reviewing orders, rejection of suspect orders, and requiring additional levels of security such as email address, zip code, and CCV security codes.

In addition, federal law limits the liability of individuals to \$50 for a stolen credit card. For amounts more than \$50, the credit card company generally pays the amount, although in some cases, the merchant may be held liable if it failed to verify the account or consult published lists of invalid cards. Banks recoup the cost of credit card fraud by charging higher interest rates on unpaid balances, and by merchants who raise prices to cover the losses. In 2016, the U.S. credit card system is in the midst of a shift to EMV credit cards, also known as smart cards or chip cards. Already widely used in Europe, EMV credit cards have a computer chip instead of a magnetic strip that can be easily copied by hackers and sold as dump data (see Table 5.2). While EMV technology cannot prevent data breaches from occurring, the hope is that it will make it harder for criminals to profit from the mass theft of credit card numbers that could be used in commerce.

In the past, the most common cause of credit card fraud was a lost or stolen card that was used by someone else, followed by employee theft of customer numbers and stolen identities (criminals applying for credit cards using false identities). Today, the most frequent cause of stolen cards and card information is the systematic hacking and looting of a corporate server where the information on millions of credit card purchases is stored. For instance, in 2010, Albert Gonzalez was sentenced to 20 years in prison for organizing one of the largest thefts of credit card numbers in American history. Along with several Russian co-conspirators, Gonzalez broke into the central computer systems of TJX, BJ's, Barnes & Noble, and other companies, stealing over 160 million card numbers and costing these firms over \$200 million in losses (Fox and Botelho, 2013).

International orders have a much higher risk of being fraudulent, with fraud losses twice those of domestic orders. If an international customer places an order and then later disputes it, online merchants often have no way to verify that the package was actually delivered and that the credit card holder is the person who placed the order. As a result, most online merchants will not process international orders.

A central security issue of e-commerce is the difficulty of establishing the customer's identity. Currently there is no technology that can identify a person with absolute certainty. For instance, a lost or stolen EMV card can be used until the card is cancelled, just like a magnetic strip card. Until a customer's identity can be guaranteed, online companies are at a higher risk of loss than traditional offline companies. The federal government has attempted to address this issue through the Electronic Signatures in Global and National Commerce Act (the "E-Sign" law), which gives digital

signatures the same authority as hand-written signatures in commerce. This law also intended to make digital signatures more commonplace and easier to use. Although the use of e-signatures is still uncommon in the B2C retail e-commerce arena, many businesses are starting to implement e-signature solutions, particularly for B2B contracting, financial services, insurance, health care, and government and professional services. DocuSign, Adobe eSign, RightSignature, and Silanis eSignLive are currently among the most widely adopted e-signature solutions. They use a variety of techniques, such as remote user identification through third-party databases or personal information verification such as a photo of a driver's license; multi-factor user authentication methods (user ID and password, e-mail address verification, secret question and answer); and public/private key encryption to create a digital signature and embedded audit trail that can be used to verify the e-signature's integrity (Silanis Technology, 2014). The use of fingerprint identification is also one solution to positive identification, but the database of print information can be hacked. Mobile e-signature solutions are also beginning to be adopted (DocuSign, 2015).

IDENTITY FRAUD

Identity fraud involves the unauthorized use of another person's personal data, such as social security, driver's license, and/or credit card numbers, as well as user names and passwords, for illegal financial benefit. Criminals can use such data to obtain loans, purchase merchandise, or obtain other services, such as mobile phone or other utility services. Cybercriminals employ many of the techniques described previously, such as spyware, phishing, data breaches, and credit card theft, for the purpose of identity fraud. Data breaches, in particular, often lead to identity fraud.

Identity fraud is a significant problem in the United States. In 2015, according to Javelin Strategy & Research, 13 million U.S. consumers suffered identity fraud. The total dollar losses as a result of identity fraud were approximately \$15 billion (Javelin Research & Strategy, 2016).

SPOOFING, PHARMING, AND SPAM (JUNK) WEBSITES

Spoofing involves attempting to hide a true identity by using someone else's e-mail or IP address. For instance, a spoofed e-mail will have a forged sender e-mail address designed to mislead the receiver about who sent the e-mail. IP spoofing involves the creation of TCP/IP packets that use someone else's source IP address, indicating that the packets are coming from a trusted host. Most current routers and firewalls can offer protection against IP spoofing. Spoofing a website sometimes involves **pharming**, automatically redirecting a web link to an address different from the intended one, with the site masquerading as the intended destination. Links that are designed to lead to one site can be reset to send users to a totally unrelated site—one that benefits the hacker.

Although spoofing and pharming do not directly damage files or network servers, they threaten the integrity of a site. For example, if hackers redirect customers to a fake website that looks almost exactly like the true site, they can then collect and process orders, effectively stealing business from the true site. Or, if the intent is to disrupt rather than steal, hackers can alter orders—inflating them or changing prod-

identity fraud

involves the unauthorized use of another person's personal data for illegal financial benefit

spoofing

involves attempting to hide a true identity by using someone else's e-mail or IP address

pharming

automatically redirecting a web link to an address different from the intended one, with the site masquerading as the intended destination

spam (junk) websites

also referred to as link farms; promise to offer products or services, but in fact are just collections of advertisements

sniffer

a type of eavesdropping program that monitors information traveling over a network

ucts ordered—and then send them on to the true site for processing and delivery. Customers become dissatisfied with the improper order shipment, and the company may have huge inventory fluctuations that impact its operations.

In addition to threatening integrity, spoofing also threatens authenticity by making it difficult to discern the true sender of a message. Clever hackers can make it almost impossible to distinguish between a true and a fake identity or web address.

Spam (junk) websites (also sometimes referred to as *link farms*) are a little different. These are sites that promise to offer some product or service, but in fact are just a collection of advertisements for other sites, some of which contain malicious code. For instance, you may search for “[name of town] weather,” and then click on a link that promises your local weather, but then discover that all the site does is display ads for weather-related products or other websites. Junk or spam websites typically appear on search results, and do not involve e-mail. These sites cloak their identities by using domain names similar to legitimate firm names, and redirect traffic to known spammer-redirection domains such as topsearch10.com.

SNIFFING AND MAN-IN-THE-MIDDLE ATTACKS

A **sniffer** is a type of eavesdropping program that monitors information traveling over a network. When used legitimately, sniffers can help identify potential network trouble-spots, but when used for criminal purposes, they can be damaging and very difficult to detect. Sniffers enable hackers to steal proprietary information from anywhere on a network, including passwords, e-mail messages, company files, and confidential reports. For instance, in 2013, five hackers were charged in another worldwide hacking scheme that targeted the corporate networks of retail chains such as 7-Eleven and the French retailer Carrefour SA, using sniffer programs to steal more than 160 million credit card numbers (Voreacos, 2013).

E-mail wiretaps are a variation on the sniffing threat. An e-mail wiretap is a method for recording or journaling e-mail traffic generally at the mail server level from any individual. E-mail wiretaps are used by employers to track employee messages, and by government agencies to surveil individuals or groups. E-mail wiretaps can be installed on servers and client computers. The USA PATRIOT Act permits the FBI to compel ISPs to install a black box on their mail servers that can impound the e-mail of a single person or group of persons for later analysis. In the case of American citizens communicating with other citizens, an FBI agent or government lawyer need only certify to a judge on the secret 11-member U.S. Foreign Intelligence Surveillance Court (FISC) that the information sought is relevant to an ongoing criminal investigation to get permission to install the program. Judges have no discretion. They must approve wiretaps based on government agents’ unsubstantiated assertions. In the case of suspected terrorist activity, law enforcement does not have to inform a court prior to installing a wire or e-mail tap. A 2007 amendment to the 1978 Foreign Intelligence Surveillance Act, known as FISA, provided new powers to the National Security Agency to monitor international e-mail and telephone communications where one person is in the United States, and where the purpose of such interception is to collect foreign intelligence (Foreign Intelligence Surveillance Act of 1978; Protect America Act of 2007). The FISA Amendments Reauthorization Act of 2012 extends the provisions of FISA for five more

years, until 2017. NSA's XKeyscore program, revealed by Edward Snowden, is a form of "wiretap" that allows NSA analysts to search through vast databases containing not only e-mail, but online chats, and browsing histories of millions of individuals (Wills, 2013).

The Communications Assistance for Law Enforcement Act (CALEA) requires all communications carriers (including ISPs) to provide near-instant access to law enforcement agencies to their message traffic. Many Internet services (such as Facebook and LinkedIn) that have built-in ISP services technically are not covered by CALEA. One can only assume these non-ISP e-mail operators cooperate with law enforcement. Unlike the past where wiretaps required many hours to physically tap into phone lines, in today's digital phone systems, taps are arranged in a few minutes by the large carriers at their expense.

A **man-in-the-middle (MitM) attack** also involves eavesdropping but is more active than a sniffing attack, which typically involves passive monitoring. In a MitM attack, the attacker is able to intercept communications between two parties who believe they are directly communicating with one another, when in fact the attacker is controlling the communications. This allows the attacker to change the contents of the communication.

DENIAL OF SERVICE (DOS) AND DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

In a **Denial of Service (DoS) attack**, hackers flood a website with useless pings or page requests that inundate and overwhelm the site's web servers. Increasingly, DoS attacks involve the use of bot networks and so-called "distributed attacks" built from thousands of compromised client computers. DoS attacks typically cause a website to shut down, making it impossible for users to access the site. For busy e-commerce sites, these attacks are costly; while the site is shut down, customers cannot make purchases. And the longer a site is shut down, the more damage is done to a site's reputation. Although such attacks do not destroy information or access restricted areas of the server, they can destroy a firm's online business. Often, DoS attacks are accompanied by attempts at blackmailing site owners to pay tens or hundreds of thousands of dollars to the hackers in return for stopping the DoS attack.

A **Distributed Denial of Service (DDoS) attack** uses hundreds or even thousands of computers to attack the target network from numerous launch points. DoS and DDoS attacks are threats to a system's operation because they can shut it down indefinitely. Major websites have experienced such attacks, making the companies aware of their vulnerability and the need to continually introduce new measures to prevent future attacks. According to Akamai, the number of DDoS attacks in the 2nd quarter of 2016 increased by about 130% compared to the same period in 2015. One new technique increasingly being used targets insecure routers and other home devices such as webcams that use UPnP (Universal Plug and Play) to amplify the attacks (Akamai, 2016a). With the growth of the Internet of Things (IoT), billions of Internet-connected things from refrigerators to security cameras can be used to launch service requests against servers. In October 2016, a large scale DDoS attack using Internet devices such as these was launched against an Internet domain resolving firm, Dyn. Twitter, Amazon, Netflix, Airbnb, the New York Times, and many other sites across the

man-in-the-middle (MitM) attack

attack in which the attacker is able to intercept communications between two parties who believe they are directly communicating with one another, when in fact the attacker is controlling the communications

Denial of Service (DoS) attack

flooding a website with useless traffic to inundate and overwhelm the network

Distributed Denial of Service (DDoS) attack

using numerous computers to attack the target network from numerous launch points

country were affected. Hackers were able to guess the administrator passwords of common devices (often set to factory defaults like admin, or 12345), and then insert instructions to launch an attack against Dyn servers (Sanger and Perlroth, 2016). DDoS attacks are typically isolated to a single firm, but in the Dyn attack, the firm attacked happened to be one of the switchboards for a large part of the Internet in the United States. In another measure of the prevalence of DDoS attacks, in an Arbor Networks survey of 354 ISP and network operators around the world, respondents noted that DDoS attacks against customers constituted the number one operational threat, with over 50% of respondents experiencing DDoS attacks during the survey period. Arbor Networks also reported that the size of reported DDoS attacks in terms of bandwidth consumed continued to increase in 2015, with attackers using reflection/amplification techniques to create attacks reaching 500 Gpbs (Arbor Networks, 2016). Another trend is DDoS smokescreening, in which attackers use DDoS as a distraction while they also insert malware or viruses or steal data. A 2016 survey of 760 security and IT professionals in companies in North America and Europe, the Middle East, and Africa conducted by Neustar found that 45% reported that a virus or malware was installed as a result of the DDoS attack, while 57% also experienced a theft of data or funds (Neustar, 2016). And not surprisingly, now that mobile data connections have become faster and more stable, hackers are beginning to harness mobile devices for mobile-based DDoS attacks. A recent attack originating from China used malicious ads loaded inside mobile apps and mobile browsers as the attack mechanism (Majkowski, 2015).

China also appears to have been behind another major DDoS attack in 2015 against the software development platform GitHub, aimed specifically at two Chinese anti-censorship projects hosted on the platform. Researchers say the attack was an example of a new tool they have nicknamed the Great Cannon. Although originally thought to be part of China's Great Firewall censorship system, further investigation revealed that the Great Cannon is a separate distinct offensive system that is co-located with the Great Firewall. The Great Cannon enables hackers to hijack traffic to individual IP addresses and uses a man-in-the-middle attack to replace unencrypted content between a web server and the user with malicious Javascript that would load the two GitHub project pages every two seconds (Kirk, 2015b; Essers, 2015).

INSIDER ATTACKS

We tend to think of security threats to a business as originating outside the organization. In fact, the largest financial threats to business institutions come not from robberies but from embezzlement by insiders. Bank employees steal far more money than bank robbers. The same is true for e-commerce sites. Some of the largest disruptions to service, destruction to sites, and diversion of customer credit data and personal information have come from insiders—once trusted employees. Employees have access to privileged information, and, in the presence of sloppy internal security procedures, they are often able to roam throughout an organization's systems without leaving a trace. Research from Carnegie Mellon University documents the significant damage insiders have done to both private and public organizations (Software Engineering Institute, 2012). Survey results also indicate that insiders are more likely to be the source of cyberattacks than outsiders, and to cause more damage to an organization

than external attacks (PWC, 2015). In some instances, the insider might not have criminal intent, but inadvertently exposes data that can then be exploited by others. For instance, a Ponemon Institute study found that negligent insiders are a top cause of data breaches (Ponemon Institute, 2015b). Another study based on an analysis of the behavior of 10 million users during 2015 estimated that 1% of employees are responsible for 75% of cloud-related enterprise security risk, by reusing or sending out plain-text passwords, indiscriminately sharing files, using risky applications, or accidentally downloading malware or clicking phishing links (Korolov, 2015).

POORLY DESIGNED SOFTWARE

Many security threats prey on poorly designed software, sometimes in the operating system and sometimes in the application software, including browsers. The increase in complexity and size of software programs, coupled with demands for timely delivery to markets, has contributed to an increase in software flaws or vulnerabilities that hackers can exploit. For instance, **SQL injection attacks** take advantage of vulnerabilities in poorly coded web application software that fails to properly validate or filter data entered by a user on a web page to introduce malicious program code into a company's systems and networks. An attacker can use this input validation error to send a rogue SQL query to the underlying database to access the database, plant malicious code, or access other systems on the network. Large web applications have hundreds of places for inputting user data, each of which creates an opportunity for an SQL injection attack. A large number of web-facing applications are believed to have SQL injection vulnerabilities, and tools are available for hackers to check web applications for these vulnerabilities.

Each year, security firms identify thousands of software vulnerabilities in Internet browsers, PC, Macintosh, and Linux software, as well as mobile device operating systems and applications. According to Microsoft, vulnerability disclosures across the software industry in the second half of 2015 increased by 9% compared to the same period in 2014. Over 3,300 vulnerabilities were identified (Microsoft, 2016). Browser vulnerabilities in particular are a popular target, as well as browser plug-ins such as for Adobe Reader. A **zero-day vulnerability** is one that has been previously unreported and for which no patch yet exists. In 2015, 54 zero-day vulnerabilities were reported, up from 24 in 2014 (Symantec, 2016). The very design of the personal computer includes many open communication ports that can be used, and indeed are designed to be used, by external computers to send and receive messages. Ports that are frequently attacked include TCP port 445 (Microsoft-DS), port 80 (WWW/HTTP), and 443 (SSL/HTTPS). Given their complexity and design objectives, all operating systems and application software, including Linux and Macintosh, have vulnerabilities.

In 2014, a flaw in the OpenSSL encryption system, used by millions of websites, known as the **Heartbleed bug**, was discovered (see Section 5.3 for a further discussion of SSL). The vulnerability allowed hackers to decrypt an SSL session and discover user names, passwords, and other user data, by using OpenSSL in combination with a communications protocol called the RFC6520 heartbeat that helps a remote user remain in touch after connecting with a website server. In the process a small chunk of the server's memory content can leak out (hence the name heartbleed), potentially large

SQL injection attack

takes advantage of poorly coded web application software that fails to properly validate or filter data entered by a user on a web page

zero-day vulnerability

software vulnerability that has been previously unreported and for which no patch yet exists

Heartbleed bug

flaw in OpenSSL encryption system that allowed hackers to decrypt an SSL session and discover user names, passwords, and other user data

enough to hold a password or encryption key that would allow a hacker to exploit the server further. The Heartbleed bug also affected over 1,300 Android apps. Later in 2014, another vulnerability known as ShellShock or BashBug that affected most versions of Linux and Unix, as well as Mac OS X, was revealed. ShellShock enabled attackers to use CGI (see Chapter 4) to add malicious commands (Symantec, 2015). In 2015, researchers announced that they had discovered a new SSL/TLS vulnerability that they named FREAK (Factoring Attack on RSA-Export Keys) that allows man-in-the-middle attacks that enable the interception and decryption of encrypted communications between clients and servers, which would then allow the attackers to steal passwords and other personal information. More than 60% of encrypted websites were reportedly open to attack via this security vulnerability, including those for the White House, the FBI, and the National Security Agency (Hackett, 2015; Vaughan-Nichols, 2015). A recent study found over 1,200 of the largest firms' websites have not fixed the problem entirely.

SOCIAL NETWORK SECURITY ISSUES

Social networks like Facebook, Twitter, LinkedIn, Pinterest, and Tumblr provide a rich and rewarding environment for hackers. Viruses, site takeovers, identity fraud, malware-loaded apps, click hijacking, phishing, and spam are all found on social networks. According to Symantec, the most common type of scam on social media sites in 2015 were manual sharing scams, where victims unwittingly shared videos, stories, and pictures that included links to malicious sites. Fake offerings that invite victims to join a fake event or group with incentives such as free gift cards and that require a user to share his or her information with the attacker were another common technique. Other techniques include fake Like buttons that, when clicked, install malware and post updates to the user's Newsfeed, further spreading the attack, and fake apps (Symantec, 2016). By sneaking in among our friends, hackers can masquerade as friends and dupe users into scams.

Social network firms have thus far been relatively poor policemen because they have failed to aggressively weed out accounts that send visitors to malware sites (unlike Google, which maintains a list of known malware sites and patrols its search results looking for links to malware sites). Social networks are open: anyone can set up a personal page, even criminals. Most attacks are social engineering attacks that tempt visitors to click on links that sound reasonable. Social apps downloaded from either the social network or a foreign site are not certified by the social network to be clean of malware. It's "clicker beware."

MOBILE PLATFORM SECURITY ISSUES

The explosion in mobile devices has broadened opportunities for hackers. Mobile users are filling their devices with personal and financial information, and using them to conduct an increasing number of transactions, from retail purchases to mobile banking, making them excellent targets for hackers. In general, mobile devices face all the same risks as any Internet device as well as some new risks associated with wireless network security. For instance, public Wi-Fi networks that are not secured are very susceptible to hacking. While most PC users are aware their computers and websites may be hacked and contain malware, most cell phone users believe their cell

phone is as secure as a traditional landline phone. As with social network members, mobile users are prone to think they are in a shared, trustworthy environment.

Mobile cell phone malware (sometimes referred to as malicious mobile apps (MMAs) or rogue mobile apps) was developed as early as 2004 with Cabir, a Bluetooth worm affecting Symbian operating systems (Nokia phones) and causing the phone to continuously seek out other Bluetooth-enabled devices, quickly draining the battery. The iKee.B worm, first discovered in 2009, only two years after the iPhone was introduced, infected jailbroken iPhones, turning the phones into botnet-controlled devices. An iPhone in Europe could be hacked by an iPhone in the United States, and all its private data sent to a server in Poland. iKee.B established the feasibility of cell phone botnets.

In 2015, Symantec analyzed 10 million apps and found 3 million were malware. Symantec expects the growth in mobile malware to continue in 2016 and become more aggressive in targeting mobile payment and mobile banking applications. The majority of mobile malware still targets the Android platform. For instance, Symantec has already discovered Android malware that can intercept text messages with bank authentication codes and forward them to attackers, as well as fake versions of legitimate mobile banking applications. However, the Apple iPhone platform is beginning to be increasingly targeted as well, and in 2015, Chinese hackers infected Xcode, Apple's integrated suite of development tools for creating iOS apps, and as a result, unsuspecting Chinese iOS developers unknowingly created thousands of apps with the malicious code (Keizer, 2015). And it is not just rogue applications that are dangerous, but also popular legitimate applications that simply have little protection from hackers. For instance, in 2014, security researchers revealed that the Starbucks mobile app, the most used mobile payment app in the United States, was storing user names, e-mail addresses, and passwords in clear text, in such a way that anyone with access to the phone could see the passwords and user names by connecting the phone to a computer. According to researchers, Starbucks erred in emphasizing convenience and ease of use in the design of the app over security concerns (Schuman, 2014).

Vishing attacks target gullible cell phone users with verbal messages to call a certain number and, for example, donate money to starving children in Haiti. *Smishing* attacks exploit SMS/text messages. Compromised text messages can contain e-mail and website addresses that can lead the innocent user to a malware site. Criminal SMS spoofing services have emerged, which conceal the cybercriminal's true phone number, replacing it with a false alpha-numeric name. SMS spoofing can also be used by cybercriminals to lure mobile users to a malicious website by sending a text that appears to be from a legitimate organization in the From field, and suggesting the receiver click on a malicious URL hyperlink to update an account or obtain a gift card. A small number of downloaded apps from app stores have also contained malware. *Madware*—innocent-looking apps that contain adware that launches pop-up ads and text messages on your mobile device—is also becoming an increasing problem. An examination of 3 million apps in 2015 that Symantec classified as grayware (programs that do not contain viruses and are not overtly malicious, but which can be annoying or harmful) found that 2.3 million of those ads were madware (Symantec, 2016).

Read the *Insight on Technology* case, *Think Your Smartphone Is Secure?* for a further discussion of some of the issues surrounding smartphone security.



INSIGHT ON TECHNOLOGY

THINK YOUR SMARTPHONE IS SECURE?

So far, there have been few publicly identified, large-scale, smartphone security breaches, but just because it hasn't happened yet doesn't mean it won't. With about 210 million smartphone users in the United States, business firms increasingly switching their employees to the mobile platform, and consumers using their phones for financial transactions and paying bills, the size and richness of the smartphone target for hackers is growing.

Many users believe their smartphones are unlikely to be hacked because Apple and Google are protecting them from malware, and that Verizon and AT&T can keep the cell phone network secure just as they do the land-line phone system. Telephone systems are "closed" and therefore not subject to the kinds of attacks that occur on the open Internet.

But hackers can do to a smartphone just about anything they can do to any Internet device: request malicious files without user intervention, delete files, transmit files, install programs running in the background that can monitor user actions, and potentially convert the smartphone into a robot that can be used in a botnet to send e-mail and text messages to anyone.

Apps are an emerging avenue for potential security breaches. Apple and Google now offer over 5 million apps collectively. Apple claims that it examines each and every app to ensure that it plays by Apple's App Store rules, but risks remain. In 2014, malware known as WireLurker attacked iPhone and iPad users in China via the Mac OS X operating system, representing the first attack on iPhones that were not jailbroken. Apple quickly moved to remove affected apps, but the attack was a warning sign that the iOS system is not likely to be a malware-

free environment going forward. In March 2016, new malware called AceDeceiver that infected non-jailbroken Apple devices circulated widely, scanning the App Store for other corrupted apps and automatically downloading them. That these corrupted apps were initially accepted by the App Store staff of reviewers suggests Apple cannot effectively review new apps prior to their use. This problem was further highlighted by a barrage of fake retail and product apps, primarily from developers in China, that also apparently slipped through Apple's review process and began appearing in the App Store preceding the 2016 holiday shopping season. Updates to the iOS operating system in 2016 exposed a series of vulnerabilities, collectively known as Trident, which allow attackers to take complete control of a phone remotely, without any indication that something has gone awry. Though Apple quickly scrambled to fix the vulnerability, releasing an operating system update in ten days, Trident showed that the iOS operating system is not as impervious to malware as many users believe. Any problems Apple has, it will have to fix by itself: third parties are not able to develop services to protect Apple devices as easily as they may be able to with Android because of Apple's "walled garden" approach. Overall, more malware affected iOS devices in 2015 than in the previous five years combined.

Android's security future appears just as murky. The amount of malware on the Android platform has skyrocketed over the past few years, with the number of spyware apps more than quadrupling from just a few years ago and doubling from 2015 to 2016. According to the Pulse Secure Mobile Threat Center, 97% of all mobile malware in 2015 targeted Android devices, and according to Nokia, more than 9 million Android

apps are vulnerable to remote attacks. In part this is due to the fact that security on the Android platform is much less under the control of Google because it employs an “open” app model compared to Apple’s, which makes security flaws easier to detect. In 2016, security firm Check Point reported that malware known as Hummingbad, which installs fraudulent apps and generates unwanted advertising, has infected approximately 10 million Android devices.

Android apps can use any personal information found on a phone but they must also inform the user what each app is capable of doing, and what personal data it requires. Google uses a universal scanning system that checks apps for malicious code and removes any apps that break its rules against malicious activity. Google can also perform a remote wipe of offending apps from all Droid phones without user intervention. In one incident, Google pulled down dozens of mobile banking apps made by a developer called 09Droid. The apps claimed to give users access to their accounts at many banks throughout the world. In fact, the apps were unable to connect users to any bank, and were removed before they could do much harm. Google does take preventive steps to reduce malware apps such as requiring developers to register and be approved by Google before they can distribute apps through Google Play.

Beyond the threat of rogue apps, smartphones of all stripes are susceptible to browser-

based malware that takes advantage of vulnerabilities in all browsers. In addition, most smartphones, including the iPhone, permit the manufacturers to remotely download configuration files to update operating systems and security protections. Unfortunately, flaws in the public key encryption procedures that permit remote server access to iPhones have been discovered, raising further questions about the security of such operations. Attackers have also developed methods of hijacking phones using weaknesses in SIM cards. There are at least 500 million vulnerable SIM cards in use today, and the defects allow hackers to obtain the encryption key that guards users’ personal information, granting them nearly complete access over the phone in the process. Many users don’t even take advantage of the security features they have available to them, such as the use of a lock screen, which only one-third of Android users have enabled.

In 2015, documents obtained by Edward Snowden indicated that the United States and Great Britain had hacked into Gemalto, a manufacturer of SIM cards, and obtained encryption keys that allowed them to surveil mobile phone users across the globe. The investigation is still ongoing, but after these revelations and a turbulent year of security breaches on both iOS and Android, our smartphones and tablets don’t seem quite as safe anymore.

SOURCES: “Beware, iPhone Users: Fake Retail Apps Are Surging Before Holidays,” by Vindu Goel, *New York Times*, November 6, 2016; “Microsoft: ‘Apple Can No More Secure Your iPhone Than Google Can Secure Android,’” by Zdnet.com, October 14, 2016; “Top 10 Ways to Secure Your Mobile Phone,” by Wendy Zamora, *Blog.malwarebytes.com*, September 21, 2016; “Smartphone Infections Double, Hotspots Are Also a Trouble Area,” by Patrick Nelson, *Networkworld.com*, September 7, 2016; “iPhone Malware That Steals Your Data Proves No Platform is Truly Secure,” by Liam Tung and Raymond Wong, *Mashable.com*, August 26, 2016; “This App Can Tell If an iPhone Was Hacked With Latest Pegasus Spy Malware,” by Janko Roettgers, *Variety.com*, August 26, 2016; “iPhone Users Urged to Update Software After Security Flaws Are Found,” by Nicole Perlroth, *New York Times*, August 25, 2016; “Hummingbad Malware Infects 10 Million Devices: How to Check If Your Phone or Tablet Is Among Them,” by Aaron Mamiit, *Tehtimes.com*, July 6, 2016; “This Nasty New Malware Can Infect Your Apple iPhone or iPad,” by Jonathan Vanian, *Fortune*, March 16, 2016; “Mobile Malware on Smartphones and Tablets: The Inconvenient Truth,” by Shaked Vax, *Securityintelligence.com*, February 15, 2016; “Android Accounts for 97 Percent of All Mobile Malware,” by Carly Page, *Theinquirer.net*, June 25, 2015; “Digital-Security Firm Gemalto Probes Alleged U.S., U.K. Hack,” by Amir Mizroch and Lisa Fleisher, *Wall Street Journal*, February 20, 2015; “US and UK Accused of Hacking SIM Card Firm to Steal Codes,” *Bbc.com*, February 20, 2015; “XAgent iPhone Malware Attack Steals Data Without Jailbreaking,” by Jeff Gamet, *Macobserver.com*, February 5, 2015; “Apple Blocks Apps Infected with WireLurker Malware Targeting iPhones and iPads,” by Carly Page, *Theinquirer.net*, November 6, 2014; “NSA Secretly Broke Smartphone Security,” by Cory Doctorow, *Boingboing.com*, September 8, 2013; “Obama Administration Had Restrictions on NSA Reversed in 2011,” by Ellen Nakashima, September 7, 2013; “How Google Just Quietly Made Your Android Phone More Secure,” by JR Raphael, *Computerworld*, July 26, 2013.

CLOUD SECURITY ISSUES

The move of so many Internet services into the cloud also raises security risks. From an infrastructure standpoint, DDoS attacks threaten the availability of cloud services on which more and more companies are relying. For instance, as previously noted, the DDoS attack on Dyn in 2016 caused a major disruption to cloud services across the United States. According to Alert Logic, which analyzed 1 billion security events in the IT environments of more than 3,000 enterprise customers, attacks against cloud-based services and applications increased by 45%. Alert Logic also found a 36% increase in suspicious activity in cloud environment, such as attempts to scan the infrastructure (Alert Logic, 2015). Safeguarding data being maintained in a public cloud environment is also a major concern (Cloud Security Alliance, 2016). For example, researchers identified several ways data could be accessed without authorization on Dropbox, which offers a popular cloud file-sharing service. In 2014, compromising photos of as many as 100 celebrities such as Jennifer Lawrence were posted online, reportedly stolen from Apple's iCloud. Although initially it was thought that the breach was made possible by a vulnerability in Apple's Find My iPhone API, it instead apparently resulted from lower-tech phishing attacks that yielded passwords that could be used to connect to iCloud. A similar hack into writer Mat Honan's Apple iCloud account using social engineering tactics in 2012 allowed the hackers to wipe everything from his Mac computer, iPhone, and iPad, which were linked to the cloud service, as well as take over his Twitter and Gmail accounts (Honan, 2012). These incidents highlight the risks involved as devices, identities, and data become more and more interconnected in the cloud. A 2016 Ponemon Insititute study of 3,400 IT executives found that the majority of IT and IT security practitioners surveyed felt that the likelihood of a data breach increases due to the cloud, in part due to the fact that many organizations do not thoroughly examine cloud security before deploying cloud services. The study also found that only one-third of sensitive data in cloud-based applications was encrypted, and that half of the firms involved do not have a proactive approach to cloud security, relying instead on the cloud providers to ensure security (Loten, 2016; Gemalto and Ponemon, 2016).

INTERNET OF THINGS SECURITY ISSUES

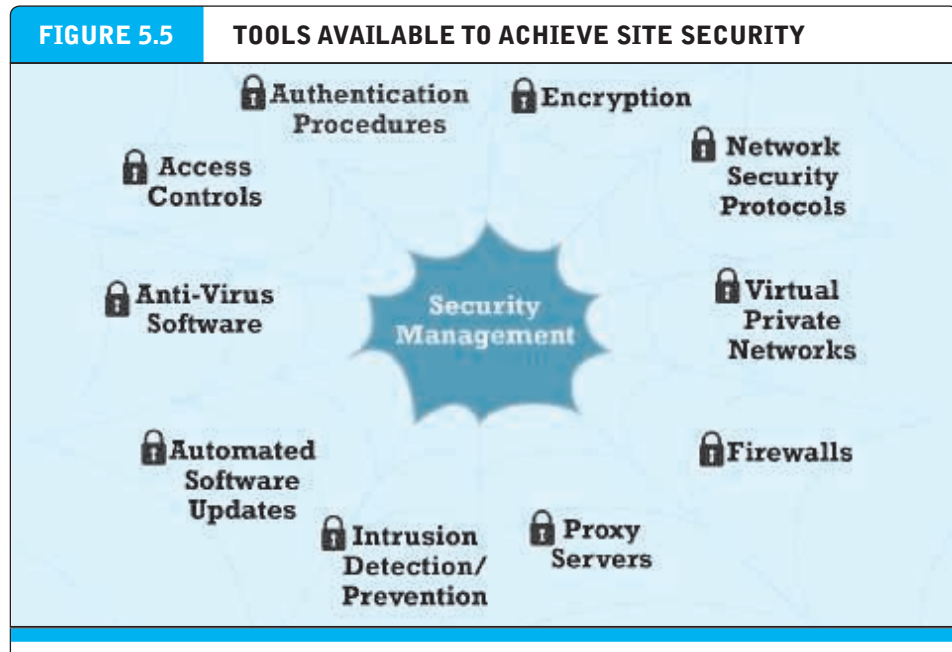
As you learned in Chapter 3, the Internet of Things (IoT) involves the use of the Internet to connect a wide variety of sensors, devices, and machines, and is powering the development of a multitude of smart connected things, such as home electronics (smart TVs, thermostats, home security systems, and more), connected cars, medical devices, and industrial equipment that supports manufacturing, energy, transportation, and other industrial sectors. IoT raises a host of security issues that are in some ways similar to existing security issues, but even more challenging, given the need to deal with a wider range of devices, operating in a less controlled, global environment, and with an expanded range of attack. In a world of connected things, the devices, the data produced and used by the devices, and the systems and applications supported by those devices, can all potentially be attacked (IBM, 2015). **Table 5.5** takes a closer look at some of the unique security challenges posed by IoT identified

TABLE 5.5 **INTERNET OF THINGS SECURITY CHALLENGES**

CHALLENGE	POSSIBLE IMPLICATIONS
Many IoT devices, such as sensors, are intended to be deployed on a much greater scale than traditional Internet-connected devices, creating a vast quantity of interconnected links that can be exploited.	Existing tools, methods, and strategies need to be developed to deal with this unprecedented scale.
Many instances of IoT consist of collections of identical devices that all have the same characteristics.	Magnifies the potential impact of a security vulnerability.
Many IoT devices are anticipated to have a much longer service life than typical equipment.	Devices may “outlive” manufacturer, leaving them without long-term support that creates persistent vulnerabilities.
Many IoT devices are intentionally designed without the ability to be upgraded, or the upgrade process is difficult.	Raises the possibility that vulnerable devices cannot or will not be fixed, leaving them perpetually vulnerable.
Many IoT devices do not provide the user with visibility into the workings of the device or the data being produced, nor alert the user when a security problem arises.	Users may believe an IoT device is functioning as intended when in fact, it may be performing in a malicious manner.
Some IoT devices, such as sensors, are unobtrusively embedded in the environment such that a user may not even be aware of the device.	Security breach might persist for a long time before being noticed.

by the Internet Society (ISOC), a consortium of corporations, government agencies, and nonprofit organizations that monitors Internet policies and practices (Internet Society, 2016, 2015).

Already, alarming reports of hacked IoT devices are starting to pop up in the popular press. For example, in July 2015, researchers demonstrated the ability to hack into a Jeep Cherokee through its entertainment system, sending commands to the dashboard, steering, brakes, and transmission system from a remote laptop that turned the steering wheel, disabled the brakes, and shut down the engine (Greenberg, 2015). Fiat Chrysler Automobiles immediately issued a recall notice to fix the software vulnerability involved, but it is almost certain that such incidents will continue to occur, as auto manufacturers add more and more wireless “connected car” features to automobiles. Other reports have surfaced of wireless baby monitors being hacked, as well as medical devices such as hospital lab blood gas analyzers, radiology picture archive and communication systems, drug infusion pumps, and hospital x-ray systems (Storm, 2015a, 2015b). The previously mentioned DDoS 2016 attack on Dyn relied in part on millions of Internet-connected security cameras (Sanger and Perlroth, 2016).



There are a number of tools available to achieve site security.

5.3 TECHNOLOGY SOLUTIONS

At first glance, it might seem like there is not much that can be done about the onslaught of security breaches on the Internet. Reviewing the security threats in the previous section, it is clear that the threats to e-commerce are very real, widespread, global, potentially devastating for individuals, businesses, and entire nations, and likely to be increasing in intensity along with the growth in e-commerce and the continued expansion of the Internet. But in fact a great deal of progress has been made by private security firms, corporate and home users, network administrators, technology firms, and government agencies. There are two lines of defense: technology solutions and policy solutions. In this section, we consider some technology solutions, and in the following section, we look at some policy solutions that work.

The first line of defense against the wide variety of security threats to an e-commerce site is a set of tools that can make it difficult for outsiders to invade or destroy a site. **Figure 5.5** illustrates the major tools available to achieve site security.

PROTECTING INTERNET COMMUNICATIONS

Because e-commerce transactions must flow over the public Internet, and therefore involve thousands of routers and servers through which the transaction packets flow, security experts believe the greatest security threats occur at the level of Internet communications. This is very different from a private network where a dedicated communication line is established between two parties. A number of tools are available to protect the security of Internet communications, the most basic of which is message encryption.

ENCRYPTION

Encryption is the process of transforming plain text or data into **cipher text** that cannot be read by anyone other than the sender and the receiver. The purpose of encryption is (a) to secure stored information and (b) to secure information transmission. Encryption can provide four of the six key dimensions of e-commerce security referred to in Table 5.3 on page 260:

- *Message integrity*—provides assurance that the message has not been altered.
- *Nonrepudiation*—prevents the user from denying he or she sent the message.
- *Authentication*—provides verification of the identity of the person (or computer) sending the message.
- *Confidentiality*—gives assurance that the message was not read by others.

This transformation of plain text to cipher text is accomplished by using a key or cipher. A **key** (or **cipher**) is any method for transforming plain text to cipher text.

Encryption has been practiced since the earliest forms of writing and commercial transactions. Ancient Egyptian and Phoenician commercial records were encrypted using substitution and transposition ciphers. In a **substitution cipher**, every occurrence of a given letter is replaced systematically by another letter. For instance, if we used the cipher “letter plus two”—meaning replace every letter in a word with a new letter two places forward—then the word “Hello” in plain text would be transformed into the following cipher text: “JGNNQ.” In a **transposition cipher**, the ordering of the letters in each word is changed in some systematic way. Leonardo Da Vinci recorded his shop notes in reverse order, making them readable only with a mirror. The word “Hello” can be written backwards as “OLLEH.” A more complicated cipher would (a) break all words into two words and (b) spell the first word with every other letter beginning with the first letter, and then spell the second word with all the remaining letters. In this cipher, “HELLO” would be written as “HLO EL.”

Symmetric Key Cryptography

In order to decipher (decrypt) these messages, the receiver would have to know the secret cipher that was used to encrypt the plain text. This is called **symmetric key cryptography** or **secret key cryptography**. In symmetric key cryptography, both the sender and the receiver use the same key to encrypt and decrypt the message. How do the sender and the receiver have the same key? They have to send it over some communication media or exchange the key in person. Symmetric key cryptography was used extensively throughout World War II and is still a part of Internet cryptography.

The possibilities for simple substitution and transposition ciphers are endless, but they all suffer from common flaws. First, in the digital age, computers are so powerful and fast that these ancient means of encryption can be broken quickly. Second, symmetric key cryptography requires that both parties share the same key. In order to share the same key, they must send the key over a presumably *insecure* medium where it could be stolen and used to decipher messages. If the secret key is lost or stolen, the entire encryption system fails. Third, in commercial use, where we are not all part of the same team, you would need a secret key for each of the parties with whom you transacted, that is, one key for the bank, another for the department store,

encryption

the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the receiver. The purpose of encryption is (a) to secure stored information and (b) to secure information transmission

cipher text

text that has been encrypted and thus cannot be read by anyone other than the sender and the receiver

key (cipher)

any method for transforming plain text to cipher text

substitution cipher

every occurrence of a given letter is replaced systematically by another letter

transposition cipher

the ordering of the letters in each word is changed in some systematic way

symmetric key cryptography (secret key cryptography)

both the sender and the receiver use the same key to encrypt and decrypt the message

and another for the government. In a large population of users, this could result in as many as $n^{(n-1)}$ keys. In a population of millions of Internet users, thousands of millions of keys would be needed to accommodate all e-commerce customers (estimated at about 177 million in the United States). Potentially, 177^2 million different keys would be needed. Clearly this situation would be too unwieldy to work in practice.

Modern encryption systems are digital. The ciphers or keys used to transform plain text into cipher text are digital strings. Computers store text or other data as binary strings composed of 0s and 1s. For instance, the binary representation of the capital letter “A” in ASCII computer code is accomplished with eight binary digits (bits): 01000001. One way in which digital strings can be transformed into cipher text is by multiplying each letter by another binary number, say, an eight-bit key number 0101 0101. If we multiplied every digital character in our text messages by this eight-bit key and sent the encrypted message to a friend along with the secret eight-bit key, the friend could decode the message easily.

The strength of modern security protection is measured in terms of the length of the binary key used to encrypt the data. In the preceding example, the eight-bit key is easily deciphered because there are only 2^8 or 256 possibilities. If the intruder knows you are using an eight-bit key, then he or she could decode the message in a few seconds using a modern desktop PC just by using the brute force method of checking each of the 256 possible keys. For this reason, modern digital encryption systems use keys with 56, 128, 256, or 512 binary digits. With encryption keys of 512 digits, there are 2^{512} possibilities to check out. It is estimated that all the computers in the world would need to work for 10 years before stumbling upon the answer.

The **Data Encryption Standard (DES)** was developed by the National Security Agency (NSA) and IBM in the 1970s. DES uses a 56-bit encryption key. To cope with much faster computers, it has been improved by the *Triple DES Encryption Algorithm (TDEA)*—essentially encrypting the message three times, each with a separate key. Today, the most widely used symmetric key algorithm is **Advanced Encryption Standard (AES)**, which offers key sizes of 128, 192, and 256 bits. AES had been considered to be relatively secure, but in 2011, researchers from Microsoft and a Belgian university announced that they had discovered a way to break the algorithm, and with this work, the “safety margin” of AES continues to erode. There are also many other symmetric key systems that are currently less widely used, with keys up to 2,048 bits.¹

Public Key Cryptography

In 1976, a new way of encrypting messages called **public key cryptography** was invented by Whitfield Diffie and Martin Hellman. Public key cryptography (also referred to as *asymmetric cryptography*) solves the problem of exchanging keys. In this method, two mathematically related digital keys are used: a public key and a private key. The private key is kept secret by the owner, and the public key is widely disseminated. Both keys can be used to encrypt and decrypt a message. However, once the keys are used

Data Encryption Standard (DES)

developed by the National Security Agency (NSA) and IBM. Uses a 56-bit encryption key

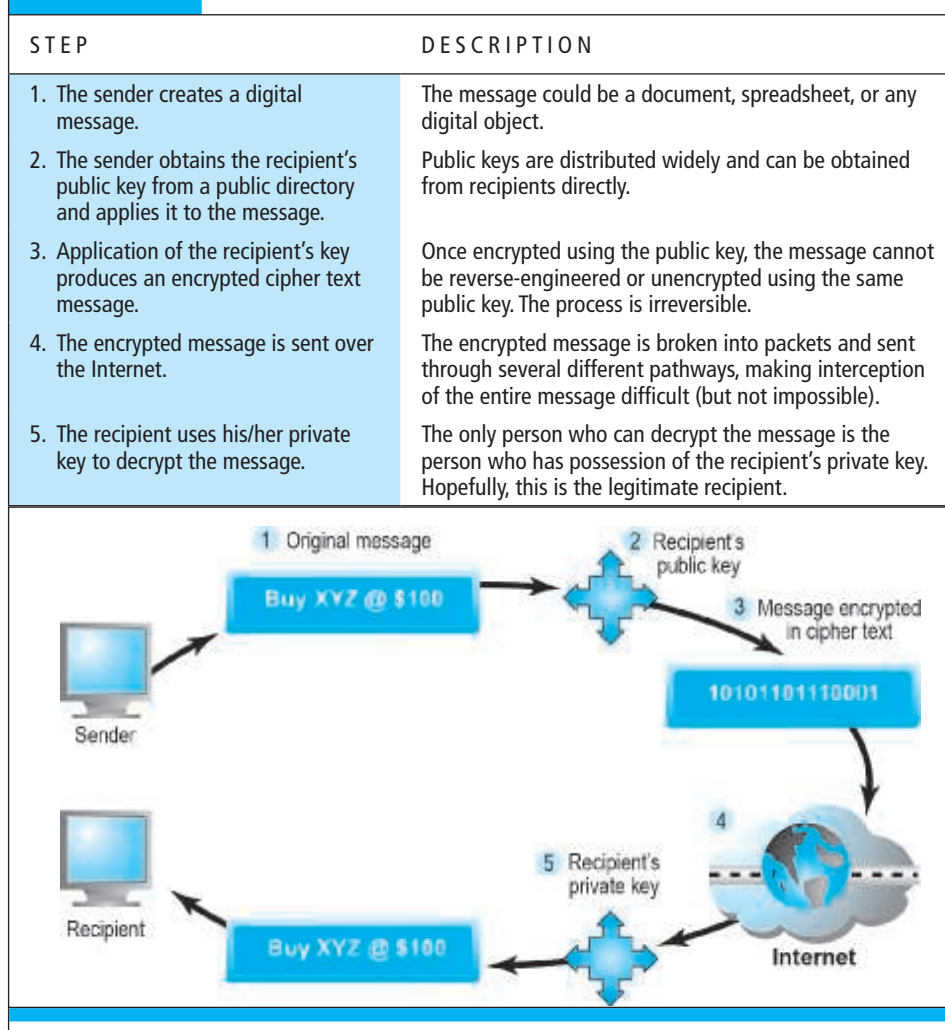
Advanced Encryption Standard (AES)

the most widely used symmetric key algorithm, offering 128-, 192-, and 256-bit keys

public key cryptography

two mathematically related digital keys are used: a public key and a private key. The private key is kept secret by the owner, and the public key is widely disseminated. Both keys can be used to encrypt and decrypt a message. However, once the keys are used to encrypt a message, that same key cannot be used to unencrypt the message

¹ For instance: DESX, GDES, and RDES with 168-bit keys; the RC Series: RC2, RC4, and RC5 with keys up to 2,048 bits; and the IDEA algorithm, the basis of PGP, e-mail public key encryption software described later in this chapter, which uses 128-bit keys.

FIGURE 5.6 PUBLIC KEY CRYPTOGRAPHY—A SIMPLE CASE

In the simplest use of public key cryptography, the sender encrypts a message using the recipient's public key, and then sends it over the Internet. The only person who can decrypt this message is the recipient, using his or her private key. However, this simple case does not ensure integrity or an authentic message.

to encrypt a message, the same key cannot be used to unencrypt the message. The mathematical algorithms used to produce the keys are one-way functions. A *one-way irreversible mathematical function* is one in which, once the algorithm is applied, the input cannot be subsequently derived from the output. Most food recipes are like this. For instance, it is easy to make scrambled eggs, but impossible to retrieve whole eggs from the scrambled eggs. Public key cryptography is based on the idea of irreversible mathematical functions. The keys are sufficiently long (128, 256, and 512 bits) that it would take enormous computing power to derive one key from the other using the largest and fastest computers available. **Figure 5.6** illustrates a simple use of public key cryptography and takes you through the important steps in using public and private keys.

Public Key Cryptography Using Digital Signatures and Hash Digests

In public key cryptography, some elements of security are missing. Although we can be quite sure the message was not understood or read by a third party (message confidentiality), there is no guarantee the sender really is the sender; that is, there is no authentication of the sender. This means the sender could deny ever sending the message (repudiation). And there is no assurance the message was not altered somehow in transit. For example, the message “Buy Cisco @ \$16” could have been accidentally or intentionally altered to read “Sell Cisco @ \$16.” This suggests a potential lack of integrity in the system.

A more sophisticated use of public key cryptography can achieve authentication, nonrepudiation, and integrity. **Figure 5.7** illustrates this more powerful approach.

hash function

an algorithm that produces a fixed-length number called a hash or message digest

To check the integrity of a message and ensure it has not been altered in transit, a hash function is used first to create a digest of the message. A **hash function** is an algorithm that produces a fixed-length number called a *hash* or *message digest*. A hash function can be simple, and count the number of digital 1s in a message, or it can be more complex, and produce a 128-bit number that reflects the number of 0s and 1s, the number of 00s and 11s, and so on. Standard hash functions are available (MD4 and MD5 produce 128- and 160-bit hashes) (Stein, 1998). These more complex hash functions produce hashes or hash results that are unique to every message. The results of applying the hash function are sent by the sender to the recipient. Upon receipt, the recipient applies the hash function to the received message and checks to verify the same result is produced. If so, the message has not been altered. The sender then encrypts both the hash result and the original message using the recipient's public key (as in Figure 5.6 on page 289), producing a single block of cipher text.

digital signature (e-signature)

“signed” cipher text that can be sent over the Internet

One more step is required. To ensure the authenticity of the message and to ensure nonrepudiation, the sender encrypts the entire block of cipher text one more time using the sender's private key. This produces a **digital signature** (also called an *e-signature*) or “signed” cipher text that can be sent over the Internet.

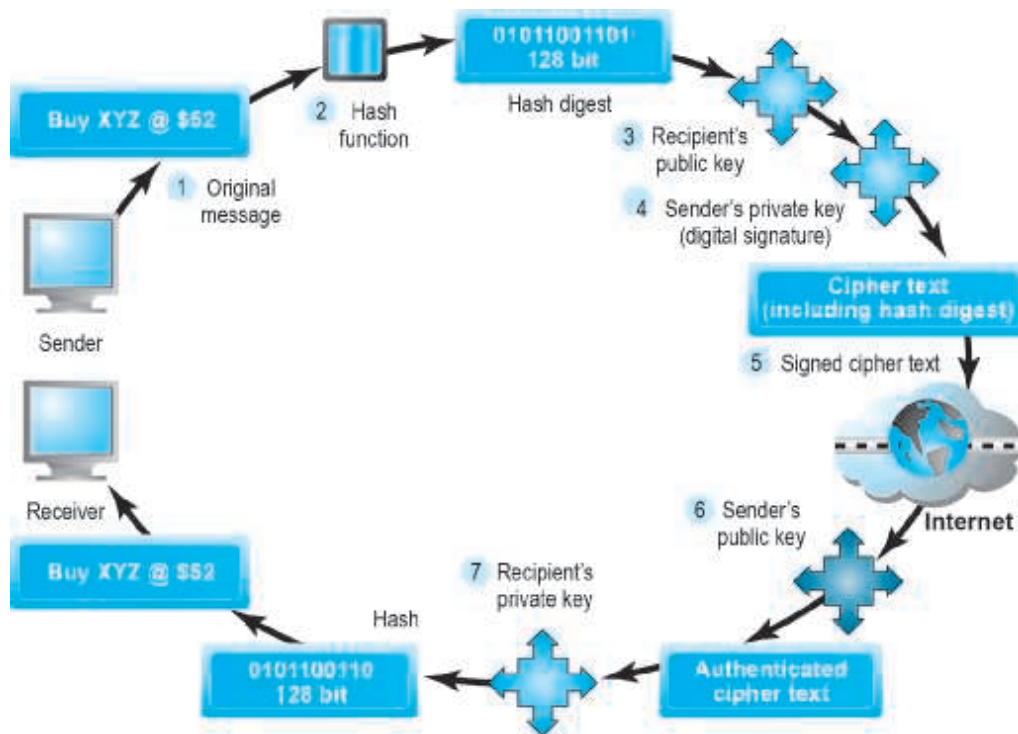
A digital signature is a close parallel to a handwritten signature. Like a handwritten signature, a digital signature is unique—only one person presumably possesses the private key. When used with a hash function, the digital signature is even more unique than a handwritten signature. In addition to being exclusive to a particular individual, when used to sign a hashed document, the digital signature is also unique to the document, and changes for every document.

The recipient of this signed cipher text first uses the sender's public key to authenticate the message. Once authenticated, the recipient uses his or her private key to obtain the hash result and original message. As a final step, the recipient applies the same hash function to the original text, and compares the result with the result sent by the sender. If the results are the same, the recipient now knows the message has not been changed during transmission. The message has integrity.

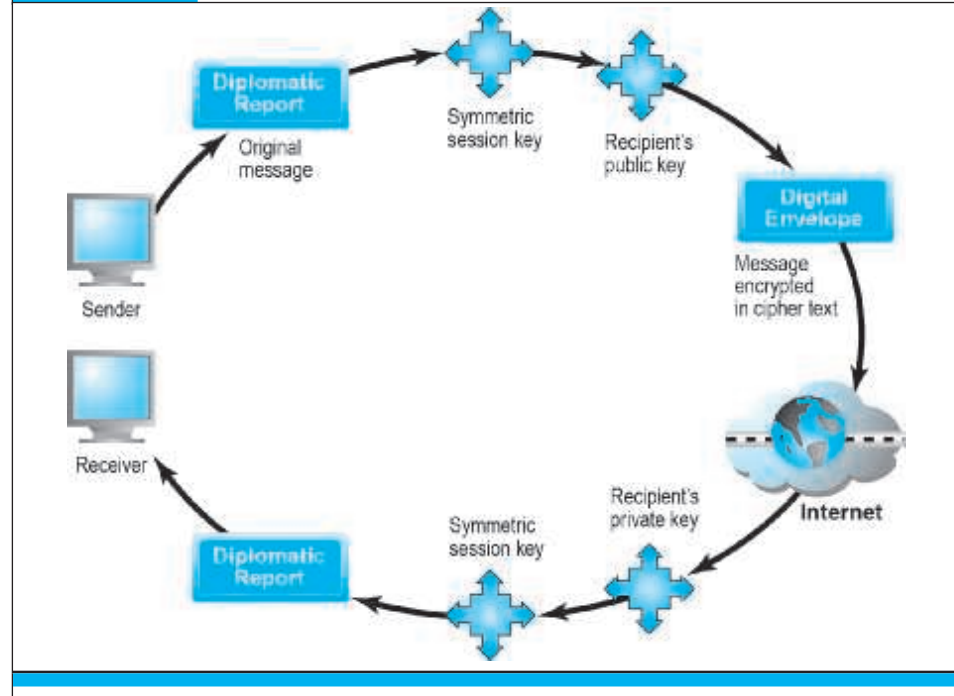
Early digital signature programs required the user to have a digital certificate, and were far too difficult for an individual to use. Newer programs are Internet-based and do not require users to install software, or understand digital certificate technology. DocuSign, Adobe eSign, and Sertifi are among a number of companies offering online

FIGURE 5.7 PUBLIC KEY CRYPTOGRAPHY WITH DIGITAL SIGNATURES

STEP	DESCRIPTION
1. The sender creates an original message.	The message can be any digital file.
2. The sender applies a hash function, producing a 128-bit hash result.	Hash functions create a unique digest of the message based on the message contents.
3. The sender encrypts the message and hash result using the recipient's public key.	This irreversible process creates a cipher text that can be read only by the recipient using his or her private key.
4. The sender encrypts the result, again using his or her private key.	The sender's private key is a digital signature. There is only one person who can create this digital mark.
5. The result of this double encryption is sent over the Internet.	The message traverses the Internet as a series of independent packets.
6. The receiver uses the sender's public key to authenticate the message.	Only one person can send this message, namely, the sender.
7. The receiver uses his or her private key to decrypt the hash function and the original message. The receiver checks to ensure the original message and the hash function results conform to one another.	The hash function is used here to check the original message. This ensures the message was not changed in transit.



A more realistic use of public key cryptography uses hash functions and digital signatures to both ensure the confidentiality of the message and authenticate the sender. The only person who could have sent the above message is the owner or the sender using his/her private key. This authenticates the message. The hash function ensures the message was not altered in transit. As before, the only person who can decipher the message is the recipient, using his/her private key.

FIGURE 5.8 PUBLIC KEY CRYPTOGRAPHY: CREATING A DIGITAL ENVELOPE

A digital envelope can be created to transmit a symmetric key that will permit the recipient to decrypt the message and be assured the message was not intercepted in transit.

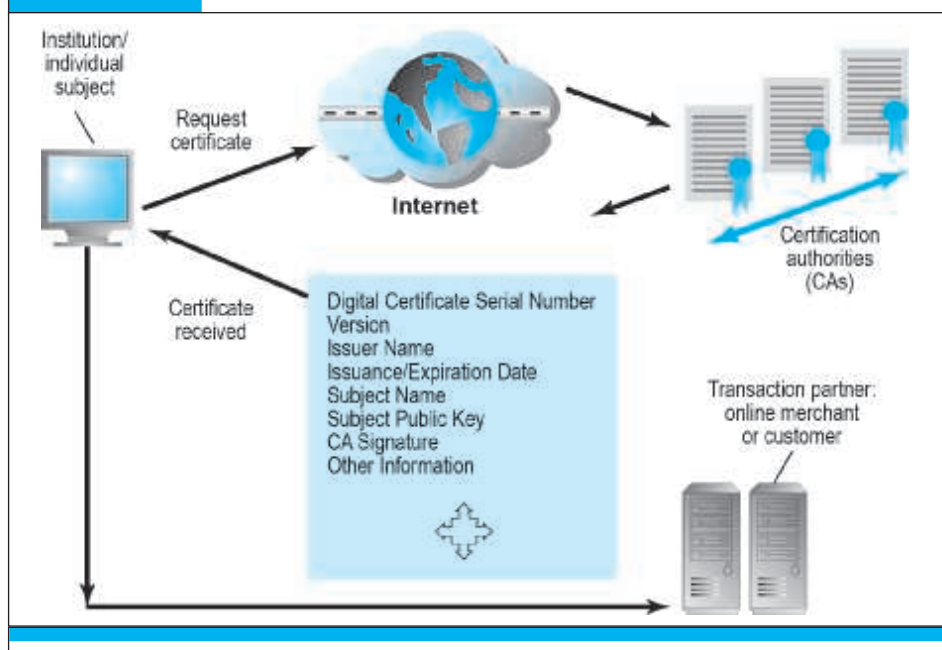
digital signature solutions. Many insurance, finance, and surety companies now permit customers to electronically sign documents.

Digital Envelopes

Public key cryptography is computationally slow. If one used 128- or 256-bit keys to encode large documents—such as this chapter or the entire book—significant declines in transmission speeds and increases in processing time would occur. Symmetric key cryptography is computationally faster, but as we pointed out previously, it has a weakness—namely, the symmetric key must be sent to the recipient over insecure transmission lines. One solution is to use the more efficient symmetric encryption and decryption for large documents, but public key cryptography to encrypt and send the symmetric key. This technique is called using a **digital envelope**. See **Figure 5.8** for an illustration of how a digital envelope works.

In **Figure 5.8**, a diplomatic document is encrypted using a symmetric key. The symmetric key—which the recipient will require to decrypt the document—is itself encrypted, using the recipient's public key. So we have a “key within a key” (a *digital envelope*). The encrypted report and the digital envelope are sent across the Web. The recipient first uses his/her private key to decrypt the symmetric key, and then

digital envelope
a technique that uses symmetric encryption for large documents, but public key cryptography to encrypt and send the symmetric key

FIGURE 5.9 DIGITAL CERTIFICATES AND CERTIFICATION AUTHORITIES

The PKI includes certification authorities that issue, verify, and guarantee digital certificates that are used in e-commerce to assure the identity of transaction partners.

the recipient uses the symmetric key to decrypt the report. This method saves time because both encryption and decryption are faster with symmetric keys.

Digital Certificates and Public Key Infrastructure (PKI)

There are still some deficiencies in the message security regime described previously. How do we know that people and institutions are who they claim to be? Anyone can make up a private and public key combination and claim to be someone they are not. Before you place an order with an online merchant such as Amazon, you want to be sure it really is Amazon you have on the screen and not a spoofer masquerading as Amazon. In the physical world, if someone asks who you are and you show a social security number, they may well ask to see a picture ID or a second form of certifiable or acceptable identification. If they really doubt who you are, they may ask for references to other authorities and actually interview these other authorities. Similarly, in the digital world, we need a way to know who people and institutions really are.

Digital certificates, and the supporting public key infrastructure, are an attempt to solve this problem of digital identity. A **digital certificate** is a digital document issued by a trusted third-party institution known as a **certification authority (CA)** that contains the name of the subject or company, the subject's public key, a digital certificate serial number, an expiration date, an issuance date, the digital signature of the certification authority (the name of the CA encrypted using the CA's private key), and other identifying information (see **Figure 5.9**).

digital certificate

a digital document issued by a certification authority that contains a variety of identifying information

certification authority (CA)

a trusted third party that issues digital certificates

**public key
infrastructure (PKI)**

CAs and digital certificate
procedures that are
accepted by all parties

In the United States, private corporations such as VeriSign, browser manufacturers, security firms, and government agencies such as the U.S. Postal Service and the Federal Reserve issue CAs. Worldwide, thousands of organizations issue CAs. A hierarchy of CAs has emerged with less-well-known CAs being certified by larger and better-known CAs, creating a community of mutually verifying institutions. **Public key infrastructure (PKI)** refers to the CAs and digital certificate procedures that are accepted by all parties. When you sign into a “secure” site, the URL will begin with “https” and a closed lock icon will appear on your browser. This means the site has a digital certificate issued by a trusted CA. It is not, presumably, a spoof site.

To create a digital certificate, the user generates a public/private key pair and sends a request for certification to a CA along with the user's public key. The CA verifies the information (how this is accomplished differs from CA to CA). The CA issues a certificate containing the user's public key and other related information. Finally, the CA creates a message digest from the certificate itself (just like a hash digest) and signs it with the CA's private key. This signed digest is called the *signed certificate*. We end up with a totally unique cipher text document—there can be only one signed certificate like this in the world.

There are several ways the certificates are used in commerce. Before initiating a transaction, the customer can request the signed digital certificate of the merchant and decrypt it using the merchant's public key to obtain both the message digest and the certificate as issued. If the message digest matches the certificate, then the merchant and the public key are authenticated. The merchant may in return request certification of the user, in which case the user would send the merchant his or her individual certificate. There are many types of certificates: personal, institutional, web server, software publisher, and CAs themselves.

PKI and CAs can also be used to secure software code and content for applications that are directly downloaded to mobile devices from the Internet. Using a technique referred to as code signing, mobile application developers use their private key to encrypt a digital signature. When end users decrypt the signature with the corresponding public key, it confirms the developer's identity and the integrity of the code.

You can easily obtain a public and private key for personal, noncommercial use at the International PGP Home Page website, Pgpi.org. **Pretty Good Privacy (PGP)** was invented in 1991 by Phil Zimmerman, and has become one of the most widely used e-mail public key encryption software tools in the world. Using PGP software installed on your computer, you can compress and encrypt your messages as well as authenticate both yourself and the recipient. There are also a number of Firefox, Chrome, Internet Explorer, and Safari add-ons, extensions, or plug-ins that enable you to encrypt your e-mail.

**Pretty Good Privacy
(PGP)**

a widely used e-mail public
key encryption software
program

Limitations of PKI

PKI is a powerful technological solution to security issues, but it has many limitations, especially concerning CAs. PKI applies mainly to protecting messages in transit on the Internet and is not effective against insiders—employees—who have legitimate access to corporate systems including customer information. Most e-commerce sites

do not store customer information in encrypted form. Other limitations are apparent. For one, how is your private key to be protected? Most private keys will be stored on insecure desktop or laptop computers.

There is no guarantee the person using your computer—and your private key—is really you. For instance, you may lose your laptop or smartphone, and therefore lose the private key. Likewise, there is no assurance that someone else in the world cannot use your personal ID papers, such as a social security card, to obtain a PKI authenticated online ID in your name. If there's no real world identification system, there can be no truly secure Internet identification system. Under many digital signature laws, you are responsible for whatever your private key does even if you were not the person using the key. This is very different from mail-order or telephone order credit card rules, where you have a right to dispute the credit card charge. Second, there is no guarantee the verifying computer of the merchant is secure. Third, CAs are self-selected organizations seeking to gain access to the business of authorization. They may not be authorities on the corporations or individuals they certify. For instance, how can a CA know about all the corporations within an industry to determine who is or is not legitimate? A related question concerns the method used by the CA to identify the certificate holder. Was this an e-mail transaction verified only by claims of the applicants who filled out an online form? For instance, VeriSign acknowledged in one case that it had mistakenly issued two digital certificates to someone fraudulently claiming to represent Microsoft. Digital certificates have been hijacked by hackers, tricking consumers into giving up personal information. For example, in 2014, India's National Informatics Centre, an intermediate CA that was trusted by the Indian Controller of Certifying Authorities, whose certificates were included in the Microsoft Root Store and thus trusted by the vast majority of programs running on Windows, including Internet Explorer and Chrome, was hacked and a number of unauthorized digital certificates were issued for domains operated by Google and Yahoo (Datta, 2014). Last, what are the policies for revoking or renewing certificates? The expected life of a digital certificate or private key is a function of the frequency of use and the vulnerability of systems that use the certificate. Yet most CAs have no policy or just an annual policy for reissuing certificates. If Microsoft, Apple, or Cisco ever rescinded a number of CAs, millions of users would not be able to access sites. The CA system is difficult and costly to police.

SECURING CHANNELS OF COMMUNICATION

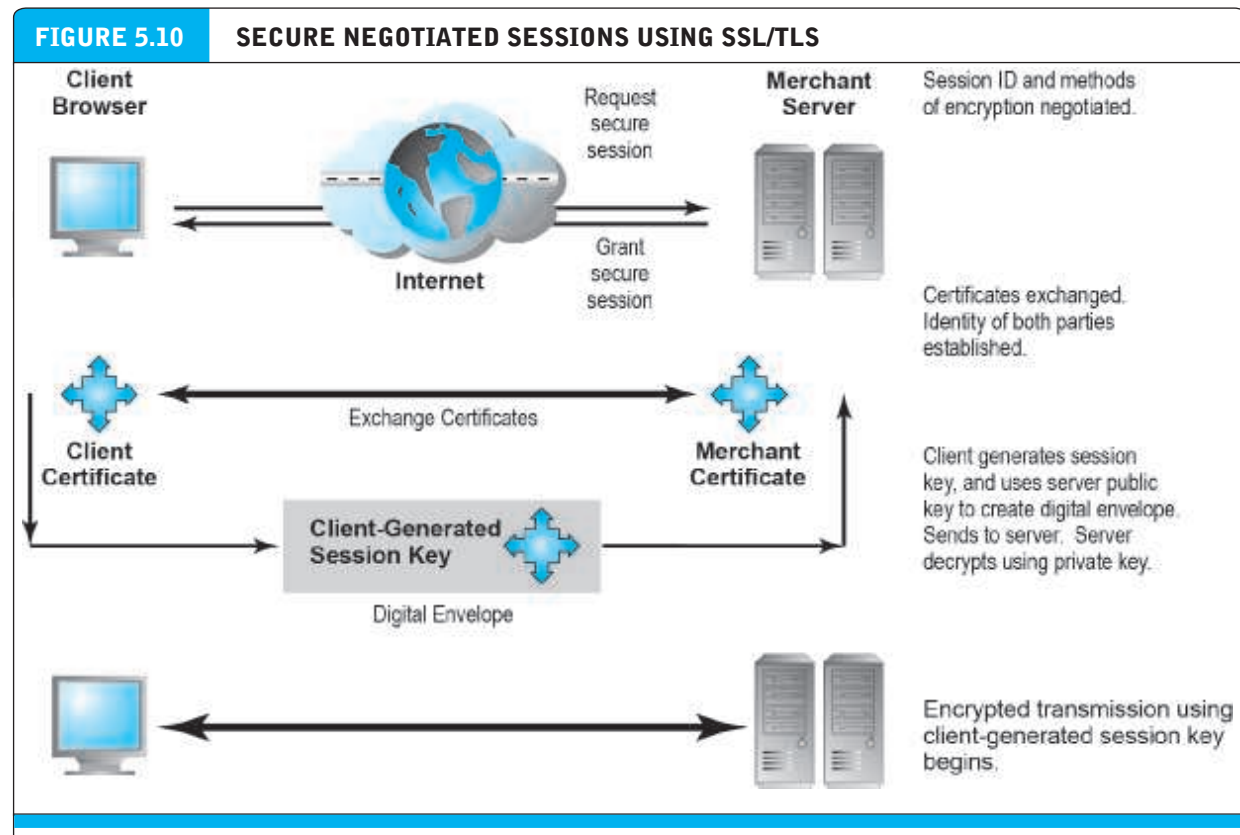
The concepts of public key cryptography are used routinely for securing channels of communication.

Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

The most common form of securing channels is through the *Secure Sockets Layer (SSL)* and *Transport Layer Security (TLS)* protocols. When you receive a message from a server on the Web with which you will be communicating through a secure channel, this means you will be using SSL/TLS to establish a secure negotiated session. (Notice that the URL changes from HTTP to HTTPS.) A **secure negotiated session** is a client-

secure negotiated session

a client-server session in which the URL of the requested document, along with the contents, contents of forms, and the cookies exchanged, are encrypted



Certificates play a key role in using SSL/TLS to establish a secure communications channel.

session key

a unique symmetric encryption key chosen for a single secure session

server session in which the URL of the requested document, along with the contents, contents of forms, and the cookies exchanged, are encrypted (see **Figure 5.10**). For instance, your credit card number that you entered into a form would be encrypted. Through a series of handshakes and communications, the browser and the server establish one another's identity by exchanging digital certificates, decide on the strongest shared form of encryption, and then proceed to communicate using an agreed-upon session key. A **session key** is a unique symmetric encryption key chosen just for this single secure session. Once used, it is gone forever. Figure 5.10 shows how this works.

In practice, most private individuals do not have a digital certificate. In this case, the merchant server will not request a certificate, but the client browser will request the merchant certificate once a secure session is called for by the server.

SSL/TLS provides data encryption, server authentication, optional client authentication, and message integrity for TCP/IP connections. SSL/TLS addresses the issue of authenticity by allowing users to verify another user's identity or the identity of a server. It also protects the integrity of the messages exchanged. However, once the merchant receives the encrypted credit and order information, that information is typi-

cally stored in unencrypted format on the merchant's servers. While SSL/TLS provides secure transactions between merchant and consumer, it only guarantees server-side authentication. Client authentication is optional.

In addition, SSL/TLS cannot provide irrefutability—consumers can order goods or download information products, and then claim the transaction never occurred. Recently, social network sites such as Facebook and Twitter have begun to use SSL/TLS for a variety of reasons, including the ability to thwart account hijacking using Firesheep over wireless networks. Firesheep, an add-on for Firefox, can be used by hackers to grab unencrypted cookies used to “remember” a user and allow the hacker to immediately log on to a website as that user. SSL/TLS can thwart such an attack because it encrypts the cookie. In June 2015, the White House's Office of Management and Budget issued a memorandum requiring that all publicly accessible federal websites and web services use HTTPS by December 31, 2016. HTTPS encrypts user requests to website servers. It is implemented by the server adopting the HTTP Strict Transport Security (HSTS) feature that forces browsers to only access the server using HTTPS (CIO.gov, 2016).

Virtual Private Networks (VPNs)

A **virtual private network (VPN)** allows remote users to securely access a corporation's local area network via the Internet, using a variety of VPN protocols. VPNs use both authentication and encryption to secure information from unauthorized persons (providing confidentiality and integrity). Authentication prevents spoofing and misrepresentation of identities. A remote user can connect to a remote private local network using a local ISP. The VPN protocols will establish the link from the client to the corporate network as if the user had dialed into the corporate network directly. The process of connecting one protocol through another (IP) is called *tunneling*, because the VPN creates a private connection by adding an invisible wrapper around a message to hide its content. As the message travels through the Internet between the ISP and the corporate network, it is shielded from prying eyes by an encrypted wrapper.

A VPN is “virtual” in the sense that it appears to users as a dedicated secure line when in fact it is a temporary secure line. The primary use of VPNs is to establish secure communications among business partners—larger suppliers or customers, and employees working remotely. A dedicated connection to a business partner can be very expensive. Using the Internet and VPN as the connection method significantly reduces the cost of secure communications.

Wireless (Wi-Fi) Networks

Accessing the Internet via a wireless (Wi-Fi) network has its own particular security issues. Early Wi-Fi networks used a security standard called Wired Equivalent Privacy (WEP) to encrypt information. WEP was very weak, and easy for hackers to crack. A new standard, Wi-Fi Protected Access (WPA), was developed that provided a higher standard of protection, but this too soon became vulnerable to intrusion. Today, the current standard is **WPA2**, which uses the AES algorithm for encryption and CCMP, a more advanced authentication code protocol.

virtual private network (VPN)

allows remote users to securely access internal networks via the Internet, using the Point-to-Point Tunneling Protocol (PPTP)

WPA2

wireless security standard that uses the AES algorithm for encryption and CCMP, a more advanced authentication code protocol

PROTECTING NETWORKS

Once you have protected communications as well as possible, the next set of tools to consider are those that can protect your networks, as well as the servers and clients on those networks.

Firewalls

Firewalls and proxy servers are intended to build a wall around your network and the attached servers and clients, just like physical-world firewalls protect you from fires for a limited period of time. Firewalls and proxy servers share some similar functions, but they are quite different.

firewall

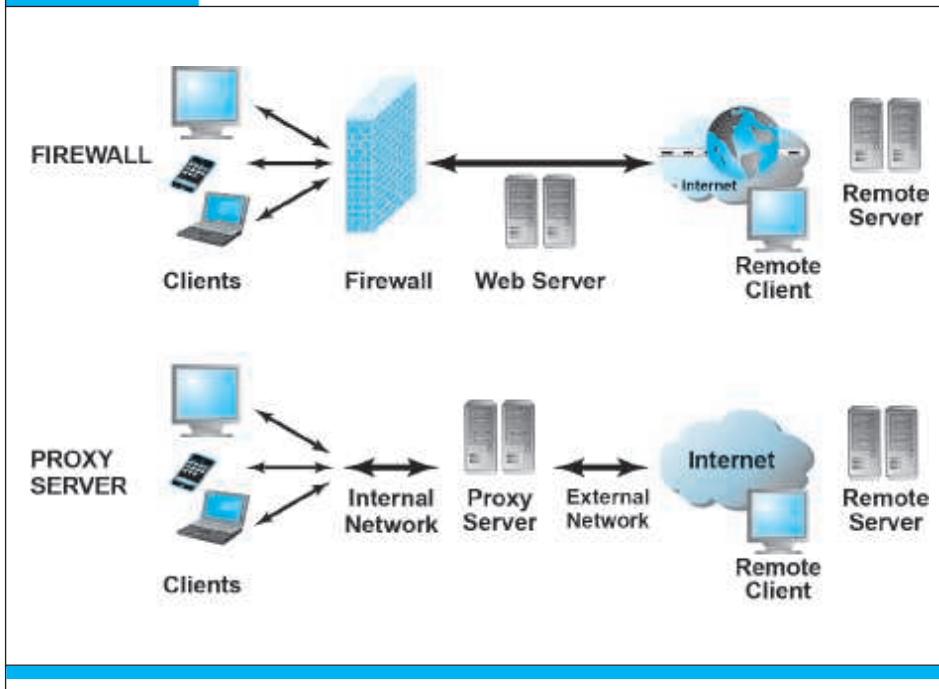
refers to either hardware or software that filters communication packets and prevents some packets from entering the network based on a security policy

A **firewall** refers to either hardware or software that filters communication packets and prevents some packets from entering or exiting the network based on a security policy. The firewall controls traffic to and from servers and clients, forbidding communications from untrustworthy sources, and allowing other communications from trusted sources to proceed. Every message that is to be sent or received from the network is processed by the firewall, which determines if the message meets security guidelines established by the business. If it does, it is permitted to be distributed, and if it doesn't, the message is blocked. Firewalls can filter traffic based on packet attributes such as source IP address, destination port or IP address, type of service (such as WWW or HTTP), the domain name of the source, and many other dimensions. Most hardware firewalls that protect local area networks connected to the Internet have default settings that require little if any administrator intervention and employ simple but effective rules that deny incoming packets from a connection that does not originate from an internal request—the firewall only allows connections from servers that you requested service from. A common default setting on hardware firewalls (DSL and cable modem routers) simply ignores efforts to communicate with TCP port 445, the most commonly attacked port. The increasing use of firewalls by home and business Internet users has greatly reduced the effectiveness of attacks, and forced hackers to focus more on e-mail attachments to distribute worms and viruses.

There are two major methods firewalls use to validate traffic: packet filters and application gateways. *Packet filters* examine data packets to determine whether they are destined for a prohibited port or originate from a prohibited IP address (as specified by the security administrator). The filter specifically looks at the source and destination information, as well as the port and packet type, when determining whether the information may be transmitted. One downside of the packet filtering method is that it is susceptible to spoofing, because authentication is not one of its roles.

Application gateways are a type of firewall that filters communications based on the application being requested, rather than the source or destination of the message. Such firewalls also process requests at the application level, farther away from the client computer than packet filters. By providing a central filtering point, application gateways provide greater security than packet filters but can compromise system performance.

Next-generation firewalls use an application-centric approach to firewall control. They are able to identify applications regardless of the port, protocol, or security evasion tools used; identify users regardless of device or IP address; decrypt outbound SSL; and protect in real-time against threats embedded in applications.

FIGURE 5.11 FIREWALLS AND PROXY SERVERS

The primary function of a firewall is to deny access by remote client computers to local computers. The primary purpose of a proxy server is to provide controlled access from local computers to remote computers.

Proxy Servers

Proxy servers (proxies) are software servers (often a dedicated computer) that handle all communications originating from or being sent to the Internet by local clients, acting as a spokesperson or bodyguard for the organization. Proxies act primarily to limit access of internal clients to external Internet servers, although some proxy servers act as firewalls as well. Proxy servers are sometimes called *dual-home systems* because they have two network interfaces. To internal computers, a proxy server is known as the *gateway*, while to external computers it is known as a *mail server* or *numeric address*.

When a user on an internal network requests a web page, the request is routed first to the proxy server. The proxy server validates the user and the nature of the request, and then sends the request onto the Internet. A web page sent by an external Internet server first passes to the proxy server. If acceptable, the web page passes onto the internal network web server and then to the client desktop. By prohibiting users from communicating directly with the Internet, companies can restrict access to certain types of sites, such as pornographic, auction, or stock-trading sites. Proxy servers also improve web performance by storing frequently requested web pages locally, reducing upload times, and hiding the internal network's address, thus making it more difficult for hackers to monitor. **Figure 5.11** illustrates how firewalls and proxy servers protect a local area network from Internet intruders and prevent internal clients from reaching prohibited web servers.

proxy server (proxy) software server that handles all communications originating from or being sent to the Internet, acting as a spokesperson or bodyguard for the organization

intrusion detection system (IDS)

examines network traffic, watching to see if it matches certain patterns or preconfigured rules indicative of an attack

intrusion prevention system (IPS)

has all the functionality of an IDS, with the additional ability to take steps to prevent and block suspicious activities

Intrusion Detection and Prevention Systems

In addition to a firewall and proxy server, an intrusion detection and/or prevention system can be installed. An **intrusion detection system (IDS)** examines network traffic, watching to see if it matches certain patterns or preconfigured rules indicative of an attack. If it detects suspicious activity, the IDS will set off an alarm alerting administrators and log the event in a database. An IDS is useful for detecting malicious activity that a firewall might miss. An **intrusion prevention system (IPS)** has all the functionality of an IDS, with the additional ability to take steps to prevent and block suspicious activities. For instance, an IPS can terminate a session and reset a connection, block traffic from a suspicious IP address, or reconfigure firewall or router security controls.

PROTECTING SERVERS AND CLIENTS

Operating system features and anti-virus software can help further protect servers and clients from certain types of attacks.

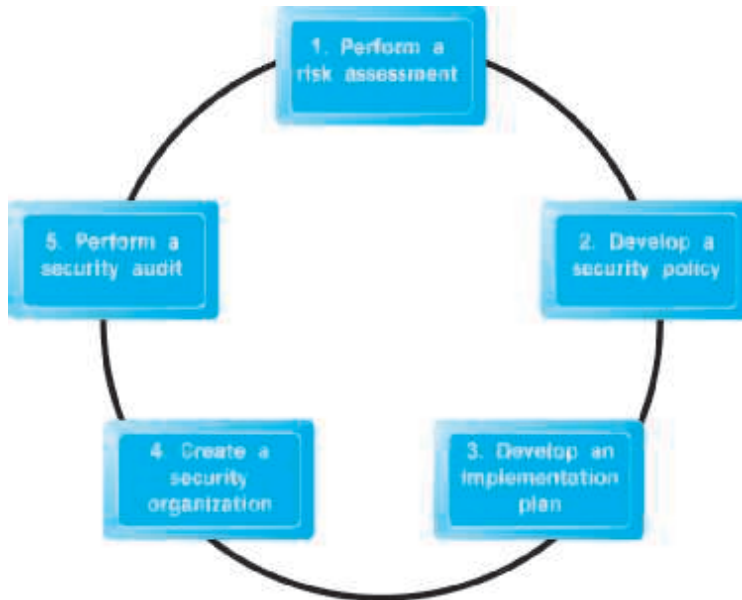
Operating System Security Enhancements

The most obvious way to protect servers and clients is to take advantage of automatic computer security upgrades. The Microsoft, Apple, and Linux/Unix operating systems are continuously updated to patch vulnerabilities discovered by hackers. These patches are autonomic; that is, when using these operating systems on the Internet, you are prompted and informed that operating system enhancements are available. Users can easily download these security patches for free. The most common known worms and viruses can be prevented by simply keeping your server and client operating systems and applications up to date. In April 2014, Microsoft ended security support and updates for its Windows XP operating system. Despite this, many organizations continue to use XP-based systems, and as a result, many security experts anticipate a wave of strikes against such systems. Application vulnerabilities are fixed in the same manner. For instance, most popular Internet browsers are updated automatically with little user intervention.

Anti-Virus Software

The easiest and least-expensive way to prevent threats to system integrity is to install anti-virus software. Programs by Malwarebytes, McAfee, Symantec (Norton AntiVirus), and many others provide inexpensive tools to identify and eradicate the most common types of malicious code as they enter a computer, as well as destroy those already lurking on a hard drive. Anti-virus programs can be set up so that e-mail attachments are inspected before you click on them, and the attachments are eliminated if they contain a known virus or worm. It is not enough, however, to simply install the software once. Because new viruses are developed and released every day, daily routine updates are needed in order to prevent new threats from being loaded. Some premium-level anti-virus software is updated hourly.

Anti-virus suite packages and stand-alone programs are available to eliminate intruders such as bot programs, adware, and other security risks. Such programs work much like anti-virus software in that they look for recognized hacker tools or signature actions of known intruders.

FIGURE 5.12 **DEVELOPING AN E-COMMERCE SECURITY PLAN**

There are five steps involved in building an e-commerce security plan.

5.4 MANAGEMENT POLICIES, BUSINESS PROCEDURES, AND PUBLIC LAWS

Worldwide, in 2016, companies are expected to spend over \$81 billion on security hardware, software, and services, up 8% from the previous year (Gartner, 2016). However, most CEOs and CIOs believe that technology is not the sole answer to managing the risk of e-commerce. The technology provides a foundation, but in the absence of intelligent management policies, even the best technology can be easily defeated. Public laws and active enforcement of cybercrime statutes also are required to both raise the costs of illegal behavior on the Internet and guard against corporate abuse of information. Let's consider briefly the development of management policy.

A SECURITY PLAN: MANAGEMENT POLICIES

In order to minimize security threats, e-commerce firms must develop a coherent corporate policy that takes into account the nature of the risks, the information assets that need protecting, and the procedures and technologies required to address the risk, as well as implementation and auditing mechanisms. **Figure 5.12** illustrates the key steps in developing a solid security plan.

risk assessment

an assessment of the risks and points of vulnerability

security policy

a set of statements prioritizing the information risks, identifying acceptable risk targets, and identifying the mechanisms for achieving these targets

implementation plan

the action steps you will take to achieve the security plan goals

security organization

educates and trains users, keeps management aware of security threats and breakdowns, and maintains the tools chosen to implement security

access controls

determine who can gain legitimate access to a network

authentication procedures

include the use of digital signatures, certificates of authority, and public key infrastructure

A security plan begins with **risk assessment**—an assessment of the risks and points of vulnerability. The first step is to inventory the information and knowledge assets of the e-commerce site and company. What information is at risk? Is it customer information, proprietary designs, business activities, secret processes, or other internal information, such as price schedules, executive compensation, or payroll? For each type of information asset, try to estimate the dollar value to the firm if this information were compromised, and then multiply that amount by the probability of the loss occurring. Once you have done so, rank order the results. You now have a list of information assets prioritized by their value to the firm.

Based on your quantified list of risks, you can start to develop a **security policy**—a set of statements prioritizing the information risks, identifying acceptable risk targets, and identifying the mechanisms for achieving these targets. You will obviously want to start with the information assets that you determined to be the highest priority in your risk assessment. Who generates and controls this information in the firm? What existing security policies are in place to protect the information? What enhancements can you recommend to improve security of these most valuable assets? What level of risk are you willing to accept for each of these assets? Are you willing, for instance, to lose customer credit card data once every 10 years? Or will you pursue a 100-year hurricane strategy by building a security edifice for credit card data that can withstand the once-in-100-year disaster? You will need to estimate how much it will cost to achieve this level of acceptable risk. Remember, total and complete security may require extraordinary financial resources. By answering these questions, you will have the beginnings of a security policy.

Next, consider an **implementation plan**—the steps you will take to achieve the security plan goals. Specifically, you must determine how you will translate the levels of acceptable risk into a set of tools, technologies, policies, and procedures. What new technologies will you deploy to achieve the goals, and what new employee procedures will be needed?

To implement your plan, you will need an organizational unit in charge of security, and a security officer—someone who is in charge of security on a daily basis. For a small e-commerce site, the security officer will likely be the person in charge of Internet services or the site manager, whereas for larger firms, there typically is a dedicated team with a supporting budget. The **security organization** educates and trains users, keeps management aware of security threats and breakdowns, and maintains the tools chosen to implement security.

The security organization typically administers access controls, authentication procedures, and authorization policies. **Access controls** determine which outsiders and insiders can gain legitimate access to your networks. Outsider access controls include firewalls and proxy servers, while insider access controls typically consist of login procedures (usernames, passwords, and access codes).

Authentication procedures include the use of digital signatures, certificates of authority, and PKI. Now that e-signatures have been given the same legal weight as an original pen-and-ink version, companies are in the process of devising ways to test and confirm a signer's identity. Companies frequently have signers type their full

name and click on a button indicating their understanding that they have just signed a contract or document.

Biometric devices can also be used to verify physical attributes associated with an individual, such as a fingerprint or retina (eye) scan or speech recognition system. (**Biometrics** is the study of measurable biological, or physical, characteristics.) A company could require, for example, that an individual undergo a fingerprint scan before being allowed access to a website, or before being allowed to pay for merchandise with a credit card. Biometric devices make it even more difficult for hackers to break into sites or facilities, significantly reducing the opportunity for spoofing. Newer Apple iPhones (5S and later) feature a fingerprint sensor called Touch ID built into the iPhone's home button that can unlock the phone and authorize purchases from the iTunes, iBooks, and App Stores without requiring users to enter a PIN or other security code. According to Apple, the system does not store an actual fingerprint, but rather biometric data, which will be encrypted and stored only on a chip within the iPhone, and will not be made available to third parties.

Security tokens are physical devices or software that generate an identifier that can be used in addition to or in place of a password. Security tokens are used by millions of corporation and government workers to log on to corporate clients and servers. One example is RSA's SecurID token, which continuously generates six-digit passwords.

Authorization policies determine differing levels of access to information assets for differing levels of users. **Authorization management systems** establish where and when a user is permitted to access certain parts of a website. Their primary function is to restrict access to private information within a company's Internet infrastructure. Although there are several authorization management products currently available, most operate in the same way: the system encrypts a user session to function like a passkey that follows the user from page to page, allowing access only to those areas that the user is permitted to enter, based on information set at the system database. By establishing entry rules up front for each user, the authorization management system knows who is permitted to go where at all times.

The last step in developing an e-commerce security plan is performing a security audit. A **security audit** involves the routine review of access logs (identifying how outsiders are using the site as well as how insiders are accessing the site's assets). A monthly report should be produced that establishes the routine and nonroutine accesses to the systems and identifies unusual patterns of activities. As previously noted, tiger teams are often used by large corporate sites to evaluate the strength of existing security procedures. Many small firms have sprung up in the last five years to provide these services to large corporate sites.

THE ROLE OF LAWS AND PUBLIC POLICY

The public policy environment today is very different from the early days of e-commerce. The net result is that the Internet is no longer an ungoverned, unsupervised, self-controlled technology juggernaut. Just as with financial markets in the last 70 years, there is a growing awareness that e-commerce markets work only when a powerful institutional set of laws and enforcement mechanisms are in place. These laws

biometrics

the study of measurable biological or physical characteristics

security token

physical device or software that generates an identifier that can be used in addition to or in place of a password

authorization policies

determine differing levels of access to information assets for differing levels of users

authorization management system

establishes where and when a user is permitted to access certain parts of a website

security audit

involves the routine review of access logs (identifying how outsiders are using the site as well as how insiders are accessing the site's assets)

help ensure orderly, rational, and fair markets. This growing public policy environment is becoming just as global as e-commerce itself. Despite some spectacular internationally based attacks on U.S. e-commerce sites, the sources and persons involved in major harmful attacks have almost always been uncovered and, where possible, prosecuted.

Voluntary and private efforts have played a very large role in identifying criminal hackers and assisting law enforcement. Since 1995, as e-commerce has grown in significance, national and local law enforcement activities have expanded greatly. New laws have been passed that grant local and national authorities new tools and mechanisms for identifying, tracing, and prosecuting cybercriminals. For instance, a majority of states now require companies that maintain personal data on their residents to publicly disclose when a security breach affecting those residents has occurred. **Table 5.6** lists the most significant federal e-commerce security legislation and regulation. In addition, the Federal Trade Commission has asserted that it has authority over corporations' data security practices. The FTC sued the Wyndham hotel chain after hacking attacks in 2008 and 2009 resulted in a data breach that led to fraudulent credit charges of more than \$10 million. According to the FTC, its investigation showed that Wyndham had failed to follow basic data security practices, while at the same time assuring customers that their data was safe. In August 2015, the U.S. Court of Appeals for the Third Circuit ruled that the FTC was within the scope of its authority, opening the door for it to take a greater role, especially in light of the failure of Congress to adopt legislation governing data security. By increasing the punishment for cybercrimes, the U.S. government is attempting to create a deterrent to further hacker actions. And by making such actions federal crimes, the government is able to extradite international hackers and prosecute them within the United States.

After September 11, 2001, Congress passed the USA PATRIOT Act, which broadly expanded law enforcement's investigative and surveillance powers. The act has provisions for monitoring e-mail and Internet use. The Homeland Security Act of 2002 also attempts to fight cyberterrorism and increases the government's ability to compel information disclosure by computer and ISP sources. Recent proposed legislation that focuses on requiring firms to report data breaches to the FTC, protection of the national electric grid, and cybersecurity has all failed to pass. However, in December 2015, the Cybersecurity Information Sharing Act (CISA) was signed into law by President Obama. The Act, which creates a system that lets companies share evidence about attacks without the risk of being sued, had been opposed by many large technology companies and privacy advocates on the grounds that it did not do enough to protect individual privacy and could lead to increased government surveillance. However, implementation of the CISA is still a work in progress and it remains to be seen how effective it will be (Chew and Newby, 2016; Peterson, 2015).

Private and Private-Public Cooperation Efforts

The good news is that e-commerce sites are not alone in their battle to achieve security on the Internet. Several organizations—some public and some private—are

TABLE 5.6

E-COMMERCE SECURITY LEGISLATION AND REGULATION

LEGISLATION/REGULATION	SIGNIFICANCE
Computer Fraud and Abuse Act (1986)	Primary federal statute used to combat computer crime.
Electronic Communications Privacy Act (1986)	Imposes fines and imprisonment for individuals who access, intercept, or disclose the private e-mail communications of others.
National Information Infrastructure Protection Act (1996)	Makes DoS attacks illegal; creates NIPC in the FBI.
Health Insurance Portability and Accountability Act (1996)	Requires certain health care facilities to report data breaches.
Financial Modernization Act (Gramm-Leach-Bliley Act) (1999)	Requires certain financial institutions to report data breaches.
Cyberspace Electronic Security Act (2000)	Reduces export restrictions.
Computer Security Enhancement Act (2000)	Protects federal government systems from hacking.
Electronic Signatures in Global and National Commerce Act (the "E-Sign Law") (2000)	Authorizes the use of electronic signatures in legal documents.
USA PATRIOT Act (2001)	Authorizes use of computer-based surveillance of suspected terrorists.
Homeland Security Act (2002)	Authorizes establishment of the Department of Homeland Security, which is responsible for developing a comprehensive national plan for security of the key resources and critical infrastructures of the United States; DHS becomes the central coordinator for all cyberspace security efforts.
CAN-SPAM Act (2003)	Although primarily a mechanism for civil and regulatory lawsuits against spammers, the CAN-SPAM Act also creates several new criminal offenses intended to address situations in which the perpetrator has taken steps to hide his or her identity or the source of the spam from recipients, ISPs, or law enforcement agencies. Also contains criminal sanctions for sending sexually explicit e-mail without designating it as such.
U.S. SAFE WEB Act (2006)	Enhances FTC's ability to obtain monetary redress for consumers in cases involving spyware, spam, Internet fraud, and deception; also improves FTC's ability to gather information and coordinate investigations with foreign counterparts.
Improving Critical Infrastructure Cybersecurity Executive Order (2013)	After Congress failed to pass cybersecurity legislation in 2012, this executive order issued by the Obama administration directs federal agencies to share cybersecurity threat intelligence with private sector companies that may be targets, and the development and implementation of a cybersecurity framework for private industry, incorporating best practices and voluntary standards.
Cybersharing Information Sharing Act (2015)	Encourages businesses and the federal government to share cyber threat information in the interests of national security,

US-CERT

division of the U.S. Department of Homeland Security that coordinates cyber incident warnings and responses across government and private sectors

CERT Coordination Center

monitors and tracks online criminal activity reported to it by private corporations and government agencies that seek out its help

devoted to tracking down criminal organizations and individuals engaged in attacks against Internet and e-commerce sites. On the federal level, the Office of Cybersecurity and Communications (CS&C) within the U.S. Department of Homeland Security (DHS) is responsible for overseeing the security, resilience, and reliability of the United States' cyber and communications infrastructure. The National Cybersecurity and Communications Integration Center (NCCIC) acts as a 24/7 cyber monitoring, incident response, and management center. In addition, the DHS also operates the **United States Computer Emergency Readiness Team (US-CERT)**, which coordinates cyber incident warnings and responses across both the government and private sectors. One of the better-known private organizations is the **CERT Coordination Center** (formerly known as the Computer Emergency Response Team) at Carnegie Mellon University. CERT monitors and tracks online criminal activity reported to it by private corporations and government agencies that seek out its help. CERT is composed of full-time and part-time computer experts who can trace the origins of attacks against sites despite the complexity of the Internet. Its staff members also assist organizations in identifying security problems, developing solutions, and communicating with the public about widespread hacker threats. The CERT Coordination Center also provides product assessments, reports, and training in order to improve the public's knowledge and understanding of security threats and solutions.

Government Policies and Controls on Encryption

In the United States, both Congress and the executive branch have sought to regulate the uses of encryption and to restrict availability and export of encryption systems as a means of preventing crime and terrorism. At the international level, four organizations have influenced the international traffic in encryption software: the Organization for Economic Cooperation and Development (OECD), G-7 (the heads of state of the top seven industrialized countries in the world, not including Russia, which was suspended from participation in 2014), the European Council, and the Wassenaar Arrangement (which includes 41 countries that produce sensitive industrial equipment or weapons). Various governments have proposed schemes for controlling encryption software or at least preventing criminals from obtaining strong encryption tools (see **Table 5.7**). The U.S. and U.K. governments are also devoting a large amount of resources to cryptography-related programs that will enable them to break encrypted communications collected on the Internet. Documents leaked by former NSA contractor Edward Snowden indicate that both the NSA and its U.K. counterpart, the GCHQ, may be able to break encryption schemes used by SSL/TLS, VPNs, and on 4G smartphones (Vaughan-Nichols, 2013). In recent years, the fight between the U.S. government and technology companies over encryption has shifted to the mobile platform, with Apple resisting U.S. government efforts to break Apple's iCloud and Apple iPhone encryption systems (see the Chapter 8 *Insight on Society* case, *Apple: Defender of Privacy?*) and concerns over encryption messaging apps such as WhatsApp, Signal, and Telegram, that offer end-to-end encryption for texts, photos, and videos that make it difficult, if not impossible, for authorities to intercept communications using such services (Isaac, 2016).

TABLE 5.7 **GOVERNMENT EFFORTS TO REGULATE AND CONTROL ENCRYPTION**

REGULATORY EFFORT	IMPACT
Restricted export of strong security systems	Supported primarily by the United States. Widespread distribution of encryption schemes weakens this policy. The policy is changing to permit exports except to pariah countries.
Key escrow/key recovery schemes	France, the United Kingdom, and the United States supported this effort in the late 1990s but now have largely abandoned it. There are few trusted third parties.
Lawful access and forced disclosure	Growing support in U.S. legislation and in OECD countries.
Official hacking	All countries are rapidly expanding budgets and training for law enforcement “technical centers” aimed at monitoring and cracking computer-based encryption activities of suspected criminals.

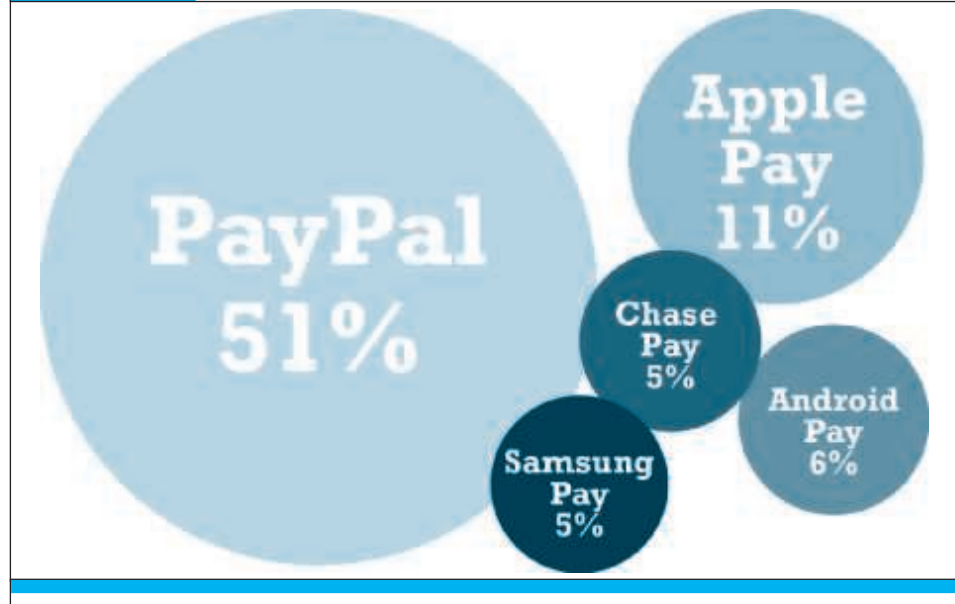
5.5 E-COMMERCE PAYMENT SYSTEMS

For the most part, existing payment mechanisms such as cash, credit cards, debit cards, checking accounts, and stored value accounts have been able to be adapted to the online environment, albeit with some significant limitations that have led to efforts to develop alternatives. In addition, new types of purchasing relationships, such as between individuals online, and new technologies, such as the development of the mobile platform, have also created both a need and an opportunity for the development of new payment systems. In this section, we provide an overview of the major e-commerce payment systems in use today. **Table 5.8** lists some of the major trends in e-commerce payments in 2016–2017.

U.S. online payments represent a market of almost \$600 billion in 2016, and are expected to grow an additional \$332 billion to around \$932 billion by 2020. Institutions and business firms that can handle this volume of transactions (mostly the large

TABLE 5.8 **MAJOR TRENDS IN E-COMMERCE PAYMENTS 2016–2017**

- Payment by credit and/or debit card remains the dominant form of online payment.
- Mobile retail payment volume skyrockets.
- PayPal remains the most popular alternative payment method online.
- Apple, Google, Samsung, and PayPal extend their reach in mobile payment apps.
- Large banks enter the mobile wallet and P2P payments market.
- Square gains further traction with a smartphone app, credit card reader, and credit card processing service that permits anyone to accept credit card payments.
- Google refocuses Google Wallet, which had met with tepid response, solely on sending and receiving money.
- Mobile P2P payment systems such as Venmo take off.

FIGURE 5.13**ALTERNATIVE PAYMENT METHODS USED BY U.S. CONSUMERS**

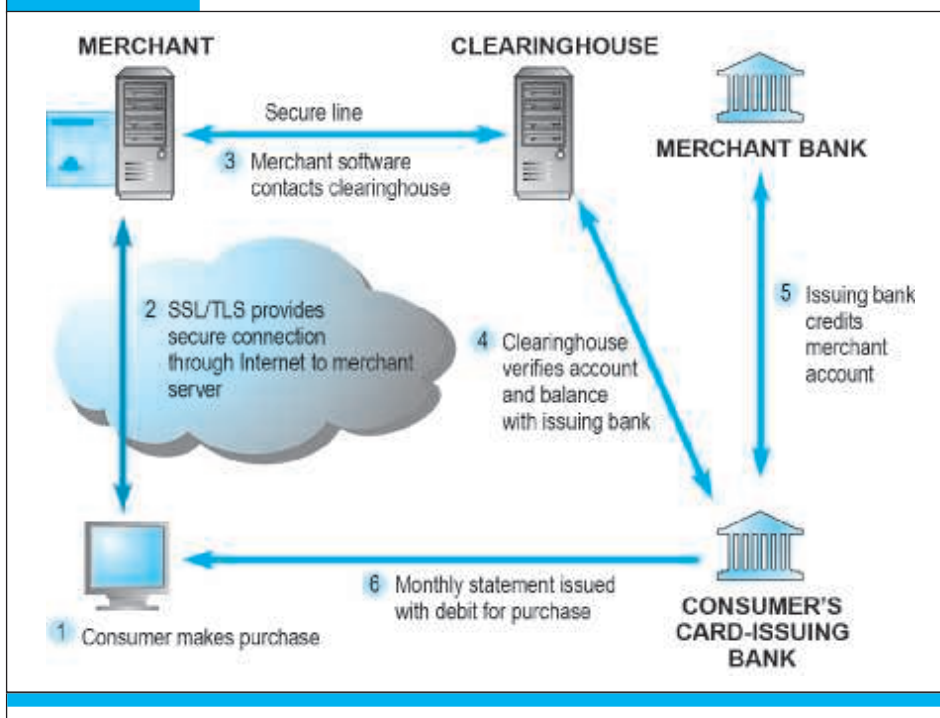
PayPal is still, by far, the most popular alternative payment method.

SOURCE: Based on data from eMarketer, 2016a.

banking and credit firms) generally extract 2%–3% of the transactions in the form of fees, or about \$18 billion a year in revenue. Given the size of the market, competition for online payments is spirited. New forms of online payment are expected to attract a substantial part of this growth.

In the United States, the primary form of online payment is still the existing credit and debit card system. Alternative payment methods such as PayPal continue to make inroads into traditional payment methods. Mobile payments are also expected to grow significantly. **Figure 5.13** illustrates the percentage of consumers that use various alternative payment methods in 2016. However, none of these alternative payment methods have become substitutes for the bank and credit cards, but instead provide consumers with alternative methods of accessing their existing bank and credit accounts.

In other parts of the world, e-commerce payments can be very different depending on traditions and infrastructure. Credit cards are not nearly as dominant a form of online payment as they are in the United States. If you plan on operating an e-commerce site in Europe, Asia, or Latin America, you will need to develop different payment systems for each region. For instance, in Denmark, Norway, and Finland payment is primarily with debit or credit cards, while in Sweden, payment after being tendered an invoice and by bank transfer are very popular in addition to credit/debit cards. In the Netherlands, the online payments service iDEAL is the most popular retail e-commerce payment method. In Italy, consumers rely heavily on both credit

FIGURE 5.14 HOW AN ONLINE CREDIT CARD TRANSACTION WORKS

cards and PayPal. In Japan, although credit card is the primary payment method, many consumers still pick up and pay for goods using cash at local convenience stores (konbini) (eMarketer, Inc., 2015).

ONLINE CREDIT CARD TRANSACTIONS

Because credit and debit cards are the dominant form of online payment, it is important to understand how they work and to recognize the strengths and weaknesses of this payment system. Online credit card transactions are processed in much the same way that in-store purchases are, with the major differences being that online merchants never see the actual card being used, no card impression is taken, and no signature is available. Online credit card transactions most closely resemble Mail Order-Telephone Order (MOTO) transactions. These types of purchases are also called Cardholder Not Present (CNP) transactions and are the major reason that charges can be disputed later by consumers. Because the merchant never sees the credit card, nor receives a hand-signed agreement to pay from the customer, when disputes arise, the merchant faces the risk that the transaction may be disallowed and reversed, even though he has already shipped the goods or the user has downloaded a digital product.

Figure 5.14 illustrates the online credit card purchasing cycle. There are five parties involved in an online credit card purchase: consumer, merchant, clearinghouse, merchant bank (sometimes called the “acquiring bank”), and the consumer’s card-issuing bank. In order to accept payments by credit card, online merchants must have

merchant account

a bank account that allows companies to process credit card payments and receive funds from those transactions

a merchant account established with a bank or financial institution. A **merchant account** is simply a bank account that allows companies to process credit card payments and receive funds from those transactions.

As shown in Figure 5.14, an online credit card transaction begins with a purchase (1). When a consumer wants to make a purchase, he or she adds the item to the merchant's shopping cart. When the consumer wants to pay for the items in the shopping cart, a secure tunnel through the Internet is created using SSL/TLS. Using encryption, SSL/TLS secures the session during which credit card information will be sent to the merchant and protects the information from interlopers on the Internet (2). SSL does not authenticate either the merchant or the consumer. The transacting parties have to trust one another.

Once the consumer credit card information is received by the merchant, the merchant software contacts a clearinghouse (3). As previously noted, a clearinghouse is a financial intermediary that authenticates credit cards and verifies account balances. The clearinghouse contacts the issuing bank to verify the account information (4). Once verified, the issuing bank credits the account of the merchant at the merchant's bank (usually this occurs at night in a batch process) (5). The debit to the consumer account is transmitted to the consumer in a monthly statement (6).

Credit Card E-commerce Enablers

Companies that have a merchant account still need to buy or build a means of handling the online transaction; securing the merchant account is only step one in a two-part process. Today, Internet payment service providers (sometimes referred to as payment gateways) can provide both a merchant account and the software tools needed to process credit card purchases online.

For instance, Authorize.net is an Internet payment service provider. The company helps a merchant secure an account with one of its merchant account provider partners and then provides payment processing software for installation on the merchant's server. The software collects the transaction information from the merchant's site and then routes it via the Authorize.net "payment gateway" to the appropriate bank, ensuring that customers are authorized to make their purchases. The funds for the transaction are then transferred to the merchant's merchant account. CyberSource is another well-known Internet payment service provider.

PCI-DSS Compliance

The **PCI-DSS (Payment Card Industry-Data Security Standard)** is a data security standard instituted by the five major credit card companies (Visa, MasterCard, American Express, Discover, and JCB). PCI-DSS is not a law or governmental regulation, but an industry-mandated standard. Every online merchant must comply with the appropriate level of PCI-DSS in order to accept credit card payments. Those that fail to comply and are involved in a credit card breach may ultimately be subjected to fines and other expenses. PCI-DSS has various levels, related to the number of credit and/or debit cards processed by the merchant each year. Level 1, the strictest level, applies to very large merchants that process more than 6 million transactions a year, while Level 2 applies to those who process between 1 million and 6 million. Level 3

PCI-DSS (Payment Card Industry-Data Security Standards)

data security standards instituted by the five major credit card companies

applies to organizations that process between 20,000 and 1 million transactions, while Level 4 applies to smaller merchants that process less than 20,000 transactions. PCI-DSS has six major control objectives. It requires the merchant to (a) build and maintain a secure network, (b) protect cardholder data, (c) maintain a vulnerability management program, (d) implement strong access control measures, (e) regularly test and monitor networks, and (f) maintain an information security policy. Each of these six broad control objectives has further specific requirements that must be met. The most current version of PCI-DSS is Version 3.1, which went into effect as of April 2015 (PCI Security Standards Council, 2015).

Limitations of Online Credit Card Payment Systems

There are a number of limitations to the existing credit card payment system. The most important limitations involve security, merchant risk, administrative and transaction costs, and social equity.

The existing system offers poor security. Neither the merchant nor the consumer can be fully authenticated. The merchant could be a criminal organization designed to collect credit card numbers, and the consumer could be a thief using stolen or fraudulent cards. The risk facing merchants is high: consumers can repudiate charges even though the goods have been shipped or the product downloaded. The banking industry attempted to develop a secure electronic transaction (SET) protocol, but this effort failed because it was too complex for consumers and merchants alike. The rate of online credit card fraud is expected to reach \$4 billion in 2016, up from \$2 billion in 2011. As banks switch to EMV cards with computer chips, offline credit card fraud becomes more difficult, encouraging criminals to focus on online fraud (Sidel, 2016).

The administrative costs of setting up an online credit card system and becoming authorized to accept credit cards are high. Transaction costs for merchants also are significant—roughly 3% of the purchase plus a transaction fee of 20–35 cents per transaction, plus other setup fees.

Credit cards are not very democratic, even though they seem ubiquitous. Millions of young adults do not have credit cards, along with almost 100 million other adult Americans who cannot afford cards or who are considered poor risks because of low incomes.

ALTERNATIVE ONLINE PAYMENT SYSTEMS

The limitations of the online credit card system have opened the way for the development of a number of alternative online payment systems. Chief among them is PayPal. PayPal (purchased by eBay in 2002 and then spun-off as an independent company again in 2015) enables individuals and businesses with e-mail accounts to make and receive payments up to a specified limit. PayPal is an example of an **online stored value payment system**, which permits consumers to make online payments to merchants and other individuals using their bank account or credit/debit cards. It is available in 202 countries and 25 currencies around the world. PayPal builds on the existing financial infrastructure of the countries in which it operates. You establish a PayPal account by specifying a credit, debit, or checking account you wish to have charged or paid when conducting online transactions. When you make a payment

online stored value payment system

permits consumers to make instant, online payments to merchants and other individuals based on value stored in an online account

using PayPal, you e-mail the payment to the merchant's PayPal account. PayPal transfers the amount from your credit or checking account to the merchant's bank account. The beauty of PayPal is that no personal credit information has to be shared among the users, and the service can be used by individuals to pay one another even in small amounts. However, one issue with PayPal is its relatively high cost. For example, when using a credit card as the source of funds, to send or request money, the cost ranges from 2.9% to 5.99% of the amount (depending on the type of transaction) plus a small fixed fee (typically \$0.30) per transaction. PayPal is discussed in further depth in the case study at the end of the chapter.

Although PayPal is by far the most well-known and commonly used online credit/debit card alternative, there are a number of other alternatives as well. Pay with Amazon is aimed at consumers who have concerns about entrusting their credit card information to unfamiliar online retailers. Consumers can purchase goods and services at non-Amazon websites using the payment methods stored in their Amazon accounts, without having to reenter their payment information at the merchant's site. Amazon provides the payment processing. Visa Checkout (formerly V.me) and MasterCard's MasterPass substitute a user name and password for an actual payment card number during online checkout. Both MasterPass and Visa Checkout are supported by a number of large payment processors and online retailers. However, they have not yet achieved the usage of PayPal.

Bill Me Later (owned by PayPal as well) also appeals to consumers who do not wish to enter their credit card information online. Bill Me Later describes itself as an open-ended credit account. Users select the Bill Me Later option at checkout and are asked to provide their birth date and the last four digits of their social security number. They are then billed for the purchase by Bill Me Later within 10 to 14 days. Bill Me Later is currently offered by more than 1,000 online merchants.

WU Pay (formerly eBillme, and now operated by Western Union) offers a similar service. WU Pay customers who select the WU Pay option at firms such as Sears, Kmart, and other retailers do not have to provide any credit card information. Instead they are e-mailed a bill, which they can pay via their bank's online bill payment service, or in person at any Western Union location. Dwolla is a similar cash-based payment network for both individuals and merchants. It bypasses the credit card network and instead connects directly into a bank account. In 2015, Dwolla eliminated its transaction and processing fees, changing its focus from consumer-to-consumer payments to larger businesses. Dwolla has its own network that bypasses the Automated Clearing House (ACH), the traditional system for processing financial transactions in the United States, and in 2015, signed up major U.S. bank BBVA Compass. Earlier in the year, the U.S. Treasury had selected Dwolla (along with PayPal) to process payments to federal agencies, and in October 2015, the Chicago Mercantile Exchange chose Dwolla to replace ACH. Dwolla now processes nearly \$2 billion a year and has over 1 million accounts (Pendell, 2016; Patane, 2015; Leising, 2015).

Like Dwolla, Stripe is another company that is attempting to provide an alternative to the traditional online credit card system. Stripe focuses on the merchant side of the process. It provides simple software code that enables companies to bypass much of the administrative costs involved in setting up an online credit card system,

and instead lets companies begin accepting credit card payments almost immediately without the need to obtain a merchant account or use a gateway provider. Stripe recently introduced merchant apps that can accept NFC payments. Unlike PayPal, the customer doesn't need a Stripe account to pay, and all payments are made directly to the company rather than being routed through a third party.

MOBILE PAYMENT SYSTEMS: YOUR SMARTPHONE WALLET

The use of mobile devices as payment mechanisms is already well established in Europe and Asia and is now exploding in the United States, where the infrastructure to support mobile payment is finally being put in place.

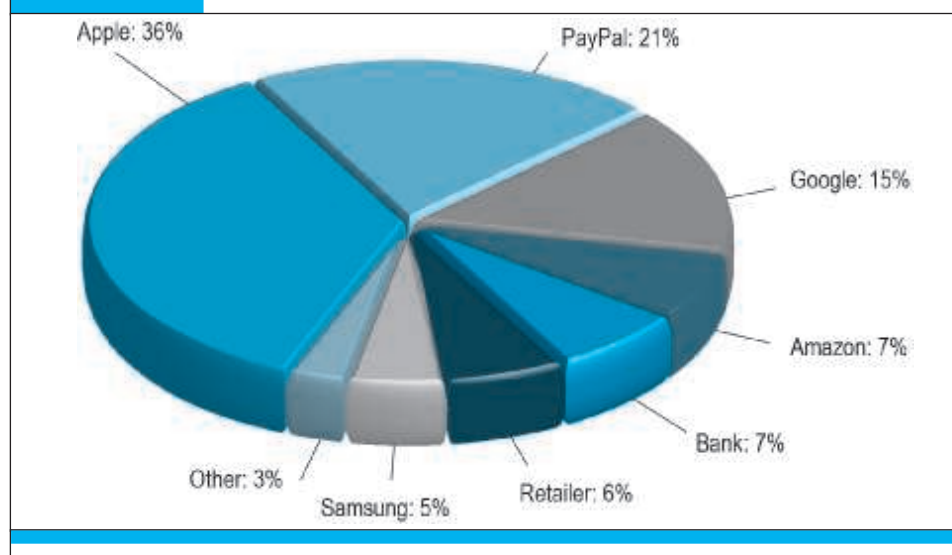
Near field communication (NFC) is the primary enabling technology for mobile payment systems. **Near field communication (NFC)** is a set of short-range wireless technologies used to share information among devices within about 2 inches of each other (50 mm). NFC devices are either powered or passive. A connection requires one powered device (the initiator, such as a smartphone), and one target device, such as a merchant NFC reader, that can respond to requests from the initiator. NFC targets can be very simple forms such as tags, stickers, key fobs, or readers. NFC peer-to-peer communication is possible where both devices are powered. Consumers can swipe their NFC-equipped phone near a merchant's reader to pay for purchases. In September 2014, Apple introduced the iPhone 6, which is equipped with NFC chips designed to work with Apple's mobile payments platform, Apple Pay. Building on Apple Passbook and Touch ID biometric fingerprint scanning and encryption that Apple previously introduced in September 2012, Apple Pay is able to be used for mobile payments at the point-of-sale at a physical store as well as online purchases using an iPhone. Other competitors in NFC-enabled mobile payments include Android Pay, Samsung Pay, PayPal, and Square. Surveys reveal that about 20%–30% of smartphone users have downloaded mobile wallet apps, but that only about 20% of these adopters have made a payment in the last month using these apps. **Figure 5.15** shows that Apple and PayPal are the most widely used mobile payment apps among adopters of mobile wallets. The promise of riches beyond description to a firm that is able to dominate the mobile payments marketplace has set off what one commentator has called a goat rodeo surrounding the development of new technologies and methods of mobile payment. The end-of-chapter case study, *Mobile Payment Marketplace: Goat Rodeo*, provides a further look at the future of online and mobile payment in the United States, including the efforts of Apple, Google, Samsung, Square, PayPal, and major financial institutions.

near field communication (NFC)

a set of short-range wireless technologies used to share information among devices

SOCIAL/MOBILE PEER-TO-PEER PAYMENT SYSTEMS

In addition to using a mobile device as a vehicle for e-commerce and as a payment method at physical point-of-sale, another type of mobile payment transaction is becoming increasingly popular: social/mobile peer-to-peer payments. Services such as Venmo, Square Cash, Snapcash, the newly refocused Google Wallet, and the new Facebook Messenger Payment service all enable users to send another person money through a mobile application or website, funded by a bank debit card. There is no charge for this service. Currently, these services are the most popular among Millennials, which is the key demographic driving their growth. Venmo, owned by PayPal,

FIGURE 5.15 MOBILE WALLET ADOPTION

Apple Pay and PayPal's mobile wallet are the most widely used methods of mobile payment.

SOURCE: Based on data from eMarketer, Inc., 2016b.

is particularly popular, with its success in part due to its integration with Facebook and its social network newsfeed, which lets users see when friends are paying other friends or paying for products and services. In 2015, Venmo processed an estimated \$8 billion in transactions and is growing at over 200% annually. In 2016, Facebook and PayPal announced that Facebook subscribers could use PayPal to purchase goods and services, with notifications coming through Facebook Messenger. Analysts forecast that mobile P2P will grow to \$174 billion, worth 30% of total P2P payment volume, by 2020. That's up from \$5.6 billion, or just 1%, in 2014 (BI Intelligence, 2016).

REGULATION OF MOBILE WALLETS AND RECHARGEABLE CARDS

In October 2016, the Bureau of Consumer Financial Protection (BCFP), a federal regulatory agency, issued the first regulations on what it called General Purpose Reloadable (GPR) cards. The regulations apply to some mobile digital wallets and to physical cards that can be loaded with prepaid funds, as well as cards that can be purchased at retail locations or recharged with funds at a bank ATM or merchant point-of-sale terminal (but not to gift cards purchased at retail locations). Previously, GPR cards were not subject to existing federal consumer banking regulations that provide protection from unauthorized transfers and require disclosure with respect to their terms and error resolution procedures. The BCFP estimates that GPR transactions grew from \$1 billion in 2003 to \$65 billion in 2012, with a projected growth to \$117 billion in 2019 (BCFP, 2016). Physical GPR cards are generally sold to people who do not have a bank or credit account, and who use them as a substitute for a checking account and cash for mobile payments. Mobile digital wallets, in comparison, are typically used by people who already have these banking credentials. Venmo and similar peer-to-peer payment

services, as well as Android Pay and Samsung Pay, are subject to these regulations because they allow for the storage of prepaid funds. Apple Pay and similar wallets are not subject to these regulations because they do not store prepaid funds and simply act as an intermediary between the banks and consumers using existing bank credentials.

The new regulations require disclosure of financial terms to consumers prior to and after acquisition of a prepaid account, access to periodical statements, a means for consumers to correct errors in payments, consumer opt-in for over-draft and credit features, and a 21-day minimum repayment period. The regulations prohibit requiring customers to set up preauthorized electronic fund transfers to repay credit extended through an overdraft service or credit feature. These requirements are extensions of the existing Electronic Funds Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z) that apply to products of bank and credit institutions such as credit and debit cards.

DIGITAL CASH AND VIRTUAL CURRENCIES

Although the terms digital cash and virtual currencies are often used synonymously, they actually refer to two separate types of alternative payment systems. **Digital cash** typically is based on an algorithm that generates unique authenticated tokens representing cash value that can be used “in the real world.” Bitcoin is the best known example of digital cash. Bitcoins are encrypted numbers (sometimes referred to as cryptocurrency) that are generated by a complex algorithm using a peer-to-peer network in a process referred to as “mining” that requires extensive computing power. Like real currency, Bitcoins have a fluctuating value tied to open-market trading. Like cash, Bitcoins are anonymous—they are exchanged via a 34-character alphanumeric address that the user has, and do not require any other identifying information. Bitcoins have recently attracted a lot of attention as a potential money laundering tool for cyber-criminals and illicit drug markets like Silk Road, and have also been plagued by security issues, with some high-profile heists. Nonetheless, there are companies now using Bitcoins as a legitimate alternative payment system. Read the *Insight on Business* case, *Bitcoin*, for a further look at Bitcoin and some of the issues surrounding it.

Virtual currencies, on the other hand, typically circulate primarily within an internal virtual world community, such as Linden Dollars, created by Linden Lab for use in its virtual world, Second Life. Virtual currencies are typically used for purchasing virtual goods.

digital cash

an alternative payment system in which unique, authenticated tokens represent cash value

virtual currency

typically circulates within an internal virtual world community or is issued by a specific corporate entity, and used to purchase virtual goods

5.6 ELECTRONIC BILLING PRESENTMENT AND PAYMENT

In 2007, for the first time, the number of bill payments made online exceeded the number of physical checks written (Fiserv, 2007). In the \$19 trillion U.S. economy with a \$13.3 trillion consumer sector for goods and services, there are billions of bills to pay. According to the U.S. Postal Service, U.S. households received about 21 billion bills in 2015 via the mail. No one knows for sure, but some experts believe the life-cycle cost of a paper bill for a business, from point of issuance to point of payment, ranges from \$3 to \$7. This calculation does not include the value of time to consumers, who must open bills, read them, write checks, address envelopes, stamp, and then mail remit-

INSIGHT ON BUSINESS

BITCOIN



In recent years, a number of countries around the world have experienced banking crises, eroding trust in the system. Enter Bitcoin, a form of electronic currency that can be transferred from one person to another via peer-to-peer networks, without the need for a bank or other financial institution as intermediary. This ability to operate outside the banking system has made Bitcoin a favorite of hackers and buyers and sellers of illicit goods and services; but more recently, it has made Bitcoin a darling among many in the technological elite who believe that Bitcoin and the technology behind it could be the next big thing in the payments industry.

Bitcoin has many unique attributes that differentiate it from traditional currencies. Bitcoins are not physically minted, but are generated by computer software at a predetermined rate beginning in 2009. A finite amount of coins are “built into the software,” such that in the year 2140, all of the coins will be mined and present in the market. The program that is used to generate Bitcoins runs on a peer-to-peer network and requires powerful computer systems to operate. “Mining” a Bitcoin is the result of these powerful computers solving cryptographic problems in tandem with other similar computers—the computer that hits upon the solution is awarded the coin, and a record of all of the involved computers’ attempts at mining the coin is logged. Bitcoins derive some of their initial value because of the time and computational effort required to mine them.

There are, however, many reasons to be skeptical of Bitcoin. Although law enforcement has improved its ability to apprehend criminals using Bitcoin, including the founder of the online black market Silk Road in 2015, governments are justifiably concerned about the emergence of a new currency without any tangible form whose purpose

is to avoid regulation. Bitcoin has also been lauded for its democratic structure, under which anyone running the underlying software has a say in making future changes. However, in 2016, Bitcoin is embroiled in a bitter civil war. As the currency continues to gain in popularity, limits on the Bitcoin transactions that can be processed each second, originally imposed as a safeguard, have begun to create backlogs and cripple transaction speed. Some of Bitcoin’s long-time supporters want to raise these limits to bring Bitcoin processing speed in line with services like PayPal; others argue that doing so could abandon the decentralized nature of the currency and place Bitcoin in the control of the few companies with the computing power to handle such a significant load, and out of the hands of the people. In 2016, there are now competing versions of Bitcoin, one which has removed transaction limits, and the other which remains faithful to the currency’s original vision, poor processing speed notwithstanding. Because of Bitcoin’s uncertainties and legal quandaries, the governments of many countries, including China, Denmark, Russia, and Israel, have taken a firm stand against digital cash.

Each of these developments has put downward pressure on Bitcoin’s value and slowed its growth, although Chinese exchanges accounted for 42% of all Bitcoin transactions in 2016, suggesting that China’s attempts to limit Bitcoin’s usage have been unsuccessful. A 2015 analysis of Bitcoin usage suggested that Bitcoins are still used primarily for gambling, illicit goods, and hoarding by speculators. Security concerns have also ravaged the largest Bitcoin exchanges to date, including Mt. Gox and Flexcoin. Hackers stole \$425 million and \$600,000 in Bitcoins from the two exchanges, respectively, and in 2016 the identity of the thieves and location of the Bitcoins stolen from Mt. Gox is still shrouded in mystery. These regulatory pressures and security concerns have driven Bitcoin’s dizzying volatility.

In 2012, Bitcoin's value was \$6; in 2013, it rose to \$1,200; and in 2016, it has surged back to \$650 after plummeting to nearly \$200 in 2015.

Despite all of these drawbacks, Bitcoin continues to move forward, and more banks and regulators are recognizing that the underlying technology may be here to stay. In 2015, Goldman Sachs invested heavily in Circle Internet Financial, a Bitcoin peer-to-peer payment platform, noting that Bitcoin could gain international acceptance over time. In September 2015, New York issued the first license to operate a virtual currency business, called a BitLicense, to Circle Internet, giving it the right to operate in the state, while subjecting it to strict capital, consumer protection, and anti-money laundering requirements. Many large U.S. banks, the New York Stock Exchange, Japanese telecom giant DoCoMo, the Bank of Tokyo, and other companies have invested in Coinbase, an intermediary for Bitcoin transactions. The first Bitcoin bank and the first Bitcoin investment fund launched in 2015 and the IRS began taxing Bitcoin earnings, further legitimizing it in the eyes of regulators. The EU, Japan, and a host of other countries proposed rules for the regulation, use, and trading of virtual currencies in 2016.

Companies like Circle Internet Financial hope to harness Bitcoin's decentralized network of computers to enable frictionless and inexpensive movement of currencies across international borders. Bitcoins and Bitcoin transactions are all logged on a public ledger known as the block-

chain, which is updated and maintained by all of the members of the network. Contrast this with a bank, which is a central hub where all currency and financial information resides. With the blockchain, there isn't a single point of failure or vulnerability the way there may be with a bank, and no single entity must update and maintain the ledger. For Bitcoin to truly gain acceptance, regular people will need to begin using it for everyday transactions. In countries where the banking system is less developed than in the United States, this has already begun to happen. In Argentina, the Philippines, Kenya, and other similar countries, banking regulations have made Bitcoin a more appealing alternative for ordinary people making normal commercial transactions.

A number of high-profile online businesses accept Bitcoin, such as Dell, Microsoft Expedia, and Newegg, as well as reportedly over 80,000 other merchants around the world. Bitcoin trading volume is still down significantly from its peak in 2014, but by July 2016, volume had spiked up again. Industry analysts predict that the number of active Bitcoin users will grow to 4.7 million in 2019, up from roughly 1.3 million today. Analysts also believe that the number of transactions per day will grow to 200,000 per day in 2016, with a value of more than \$92 billion, up from \$27 billion in 2015. For Bitcoin to continue to grow, however, it must become more than just a trading commodity and prove itself to be a useful tool to actually purchase goods and services.

SOURCES: "Coinbase Eyes Japan Expansion After Landing Investment from Bank of Tokyo," by Jon Russell, Techcrunch.com, July 8, 2016; "EU Proposes Stricter Rules on Bitcoin, Prepaid Cards, Terrorism Fight," by Foo Yun Chee, Reuters.com, July 5, 2016; "How China Took Center Stage in Bitcoin's Civil War," by Nathaniel Popper, *New York Times*, June 29, 2016; "Bitcoin Transactions Values to Triple This Year, Reaching Over \$92BN," by Juniper Research, June 4, 2016; "Bitcoin Is on the Verge of Splitting in Two," by Ben Popper, Theverge.com, February 9, 2016; "Mt. Gox Creditors Seek Trillions Where There Are Only Millions," by Nathaniel Popper, *New York Times*, May 25, 2016; "We Must Regulate Bitcoin. Problem Is, We Don't Understand It," by Primavera De Filippi, Wired.com, March 1, 2016; "A Bitcoin Believer's Crisis of Faith," by Nathaniel Popper, *New York Times*, January 14, 2016; "Bitcoin's Big Challenge in 2016: Reaching 100 Million Users," by Michael Jackson, Coindesk.com, January 1, 2016; "Circle Gets First 'BitLicense,' Releases Circle Pay, New Service," by Paul Vigna, *Wall Street Journal*, September 22, 2015; "Goldman and IDG Put \$50 Million to Work in a Bitcoin Company," by Nathaniel Popper, *New York Times*, April 30, 2015; "Bitcoin Behemoth Coinbase launches in the UK," by Alex Hern, *The Guardian*, April 29, 2015; "The World's First Proper Bitcoin Exchange Will Go Live in a Month," by Kieren McCarthy, *The Register*, April 29, 2015; "Final New York Bitcoin Regulation Released: BitLicense," by P.H. Madore, Cryptocoin-news.com, April 6, 2015; "Bitcoin's Golden Moment: BIT Gets FINRA Approval," by Brian Kelly, Cnbc.com, March 4, 2015; "Tokyo Court: Bitcoin Exchange Mt. Gox Will Liquidate," by Donna Leinwand, *USA Today*, April 16, 2014; "China Cracks Down on Bitcoin," by Chao Deng and Lingling Wei, *Wall Street Journal*, April 1, 2014; "The Mt. Gox Bitcoin Scandal Is the Best Thing to Happen to Bitcoin In Years," by Heidi Moore, Theguardian.com, February 26, 2014; "Israel's Central Bank Warns on Potential Fraud With Bitcoin," by Calev Ben-David, Bloomberg.com, February 19, 2014; "Russian Authorities Say Bitcoin Illegal," by Gabriela Baczynska, Reuters.com, February 9, 2014; "Bitcoin Pitchman Busted for 'Selling \$1M in Currency to Silk Road,'" by Kaja Whitehouse and Rich Calder, *New York Post*, January 27, 2014; "Following the Bitcoin Trail," Economist.com, August 28, 2013.

electronic billing presentment and payment (EBPP) system

form of online payment
system for monthly bills

tances. The billing market represents an extraordinary opportunity for using the Internet as an electronic billing and payment system that potentially could greatly reduce both the cost of paying bills and the time consumers spend paying them. Estimates vary, but online payments are believed to cost between only 20 to 30 cents to process.

Electronic billing presentment and payment (EBPP) systems are systems that enable the online delivery and payment of monthly bills. EBPP services allow consumers to view bills electronically using either their desktop PC or mobile device and pay them through electronic funds transfers from bank or credit card accounts. More and more companies are choosing to issue statements and bills electronically, rather than mailing out paper versions, especially for recurring bills such as utilities, insurance, and subscriptions.

MARKET SIZE AND GROWTH

In 2002, 61% of bill payments were made by check, and only 12% by online bill payments. In 2015, in contrast, online bill payments accounted for more than 55% of all bill payments, while paper checks now account for less than 20%. Among online households, almost three-quarters pay at least one bill online each month, and almost half receive at least one bill electronically each month. Mobile bill payments are surging, with 33% U.S. households in 2015 paying at least one bill on a mobile device. Most consumers cited the convenience and time saved by using mobile bill payment (Fiserv, 2016).

One major reason for the surge in EBPP usage is that companies are starting to realize how much money they can save through online billing. Not only is there the savings in postage and processing, but payments can be received more quickly (3 to 12 days faster, compared to paper bills sent via regular mail), thereby improving cash flow. Online bill payment options can also reduce the number of phone calls to a company's customer service line. In order to realize these savings, many companies are becoming more aggressive in encouraging their customers to move to EBPP by instituting a charge for the privilege of continuing to receive a paper bill.

Financials don't tell the whole story, however. Companies are discovering that a bill is both a sales opportunity and a customer retention opportunity, and that the electronic medium provides many more options when it comes to marketing and promotion. Rebates, savings offers, cross-selling, and upselling are all possible in the digital realm, and much less expensive than mailed envelopes stuffed with offers.

EBPP BUSINESS MODELS

There are four EBPP business models: online banking, biller-direct, mobile, and consolidator.

The online banking model is the most widely used today. Consumers share their banking or credit card credentials with the merchant and authorize the merchant to charge the consumer's bank account. This model has the advantage of convenience for the consumer because the payments are deducted automatically, usually with a notice from the bank or the merchant that their account has been debited.

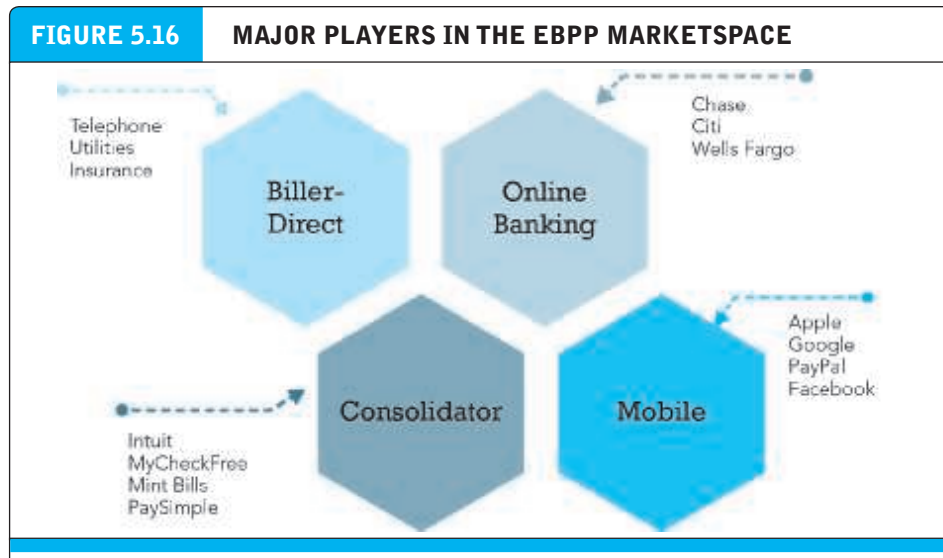
In the biller-direct model, consumers are sent bills by e-mail notification, and go to the merchant's website to make payments using their banking credentials. This

model has the advantage of allowing the merchant to engage with the consumer by sending coupons or rewards. The biller-direct model is a two-step process, and less convenient for consumers.

The mobile model allows consumers to make payments using mobile apps, once again relying on their bank credentials as the source of funds. Consumers are notified of a bill by text message and authorize the payment. An extension of this is the social-mobile model, where social networks like Facebook integrate payment into their messaging services. The mobile model has several advantages, not least of which is the convenience for consumers of paying bills while using their phones, but also the speed with which bills can be paid in a single step. This is the fastest growing form of EBPP. In 2016, Facebook and PayPal announced a deal in which Facebook users can pay for purchases on Facebook using PayPal (Demos, 2016). Consumers will not have to leave Facebook in order to purchase and pay for products.

In the consolidator model, a third party, such as a financial institution or a focused portal such as Intuit's Paytrust, Fiserv's MyCheckFree, Mint Bills, and others, aggregates all bills for consumers and permits one-stop bill payment. This model has the advantage of allowing consumers to see all their bills at one website or app. However, because bills come due at different times, consumers need to check their portals often. The consolidator model faces several challenges. For billers, using the consolidator model means an increased time lag between billing and payment, and also inserts an intermediary between the company and its customer.

Supporting these primary business models are infrastructure providers such as Fiserv, Yodlee, FIS Global, ACI Worldwide, MasterCard RPPS (Remote Payment and Presentment Service), and others that provide the software to create the EBPP system or handle billing and payment collection for the biller. **Figure 5.16** categorizes the major players in the EBPP marketplace.



The main business models in the EBPP marketplace are biller-direct, online banking, consolidator, and mobile. Infrastructure providers support all of these competing models.

5.7

CASE STUDY

The Mobile Payment Marketplace:

Goat Rodeo

Nearly every day, it seems, a new mobile payment system is announced by giant tech companies, startups, merchants, and banks. The mobile payment marketplace is experiencing an explosion of innovative ideas, plans, and announcements, which one commentator has likened to a goat rodeo, a chaotic situation in which powerful players with different agendas compete with one another for public acceptance, and above all, huge potential revenues. The mobile payment market is expected to generate somewhere between \$27 billion and \$75 billion in transaction volume in 2016, more than doubling the 2015 number. This wide-range estimate indicates how little is really known about the size of mobile payments, except that they are rapidly growing, especially among Millennials who have stopped using checks, and unlike their parents, are comfortable handling their financial trans-



actions and banking using a smartphone. Times are changing: for the first time, more people are using mobile banking on their phones and laptops than going to a bank branch.

American consumers spent over \$5.1 trillion on credit and debit card transactions in 2015, and mobile payments are still just a tiny percentage of the existing credit and debit card system. But even if a small percentage of the \$5 trillion credit card transactions move from plastic to mobile, the potential revenue is very large. On the other hand, moving consumers away from over 800 million credit and debit cards, which can be swiped at millions of merchants and used online with ease and safety, is proving to be a difficult task. The rosy future of mobile payments painted by tech companies may be a long time coming.

The mobile payment market is a battle among the titans of online payment and retailing: PayPal, credit card companies like Visa and MasterCard, Google, Apple, Samsung, and startup tech companies like Venmo and Square. The startups are backed by millions in venture capital. Even large retailers like Walmart, Best Buy, and Target are getting into the game by developing their own mobile payment apps. Major banks are in the line of fire: who needs a checking account when you can pay with a mobile phone? Rising to this challenge, the banks are slowly building their own mobile payment systems, and investing in startups to lead the charge.

There are, by one count, already about 8,000 startups in the mobile payment market. The most recent startups focus on peer-to-peer mobile payments. Venmo is a good example. Venmo is a social-mobile payment app that lets users transfer money to one another. It can also be used to pay at a small number of participating merchants. Founded in 2010 by two college students who wanted to send cash to one another for sharing restaurant tabs and paying small debts without the hassle of cash or writing checks, Venmo was purchased by PayPal in 2013. Users sign up for a Venmo account and link their account to a bank account, a debit card, or credit card. Users can also create a Venmo balance by sending money to their Venmo account, and then charge payments against that balance. There is no charge for the service when users have a Venmo balance or use a debit card, and a 3% charge for using a credit card as the source of funds. There is a social aspect of Venmo that allows users to share their purchase events (but with amount paid stripped from the notification). Users have the option to keep all transactions private as well. When they want to make a payment to another person, they enter the person's e-mail and the funds are transferred when the recipient, who must also have a Venmo account, accepts the payment. Venmo relies on NFC technology to make in-person payments to individuals by tapping their phones. Venmo's popularity has skyrocketed, especially among Millennials, and in January 2016 it processed \$1 billion in transactions, a 250% increase over the previous year. The company does not release information on its subscriber base, and because it is largely a free service, it does not contribute significantly to PayPal's gross revenues. PayPal has begun to monetize its investment in Venmo by expanding beyond peer-to-peer small payments, and extending its use to merchants who accept PayPal payments, a much larger user base, which includes large retailers like Home Depot, Target, Sears, and OfficeMax.

Startups like Venmo are small fry compared to the three other giants in the mobile payment market. First in terms of subscribers are the technology companies like

Apple, Google, Samsung, PayPal, and Square, all of which have major hardware and software mobile payment initiatives. Apple, Google, and Samsung own and license the hardware and software platform of the ubiquitous smartphone, while PayPal and Square operate large-scale payment processing platforms. Second, the large national merchants are developing their own mobile payment systems in an effort, in part, to sidestep the credit card companies (Visa, MasterCard, Discover, and American Express), which charge them a 3% transaction fee that gets passed along to the consumer as 3% higher prices, and in part to maintain control over the point-of-sale consumer moment at the cash register. These firms have tens of millions of loyal customers. Banks like JPMorgan Chase, Wells Fargo, Citi, and other money center banks, and of course, the credit card companies Visa, MasterCard, and others, are the third major player. These firms have the advantage of owning and operating the global banking and credit card systems, with hundreds of millions of loyal banking and credit card customers, and the expertise to provide security and financial stability for their products. They are, however, very slow movers and are just now entering the mobile payment marketplace.

Let's take a look at the technology companies first, all of whom offer variations on contactless payments, often referred to as digital or mobile wallets. Apple Pay is an app that comes with iPhone 6 phones and later. It uses built-in NFC technology. Users set up an account, and enter their banking credentials, using either their credit/debit card account information, or their checking or savings account, as the source of funds.

When a customer wants to make a payment, he or she presses the iPhone Touch ID button, which reads the customer's fingerprint and ensures the phone does indeed belong to the person. On the Apple Watch, there's a special button just for Apple Pay transactions. Next, the consumer swipes the device near a merchant's NFC point-of-sale terminal, which begins the transaction process. The iPhone 6 and later comes with a hardware-defined secure area on a chip that contains a unique device number and the ability to generate a one-time 16-digit code. Together they form a digital token. The token information is encrypted and sent to Apple servers to verify the authenticity of the device and the person. Apple sends the payment request to the credit card issuer. Credit card issuers verify the account owner and available credit. In about one second, the transaction is approved or denied. Credit card information is not shared with the merchant and not transmitted from the iPhone. The 800 million credit cards stored on Apple's servers are also encrypted. If hackers intercept the NFC communication at the point-of-sale, or intercept the stream of data moving over the cellular network, it would be useless, and incapable of supporting additional transactions because the message is encrypted, and involves a one-time-only digital token.

Apple Pay is free to consumers, and the credit card companies charge their usual fee of 3% for each transaction. Apple collects .15% from the credit companies and banks, and in return, guarantees the transaction is valid. Apple Pay does not store any user funds and is solely a technology-based intermediary between consumers and banks, and, unlike Venmo, is not subject to federal banking regulations. Merchants' point-of-sale terminals need to be NFC-enabled, and merchants need to install Apple software to accept payments. Apple Pay can be used by any consumer that has a credit card from a major issuer bank.

Apple has developed relationships with many of the key players in the payment ecosystem, including credit giants Visa, MasterCard, American Express, and Discover, as well as 11 large bank credit card issuers including JPMorgan Chase, Bank of America, Citigroup, and Wells Fargo, which together account for 83% of U.S. credit card payment volume. Apple has also signed up national merchants such as Walgreens, Duane Reade, McDonald's, Disney, Macy's, Bloomingdale's, Staples, and Whole Foods. Groupon and Uber have integrated Apple Pay into their systems.

Android Pay is a Google app that provides an NFC-based payment system much like Apple Pay. Android is the most widely used smartphone operating system in the world. Launched in 2015, Android Pay replaces Google Wallet, which has been repurposed as a peer-to-peer payment service that allows users to pay friends using only their e-mail address, similar to PayPal and Venmo. Users sign up for an Android Pay account by entering their existing bank credit or debit card account information, or by depositing a prepaid balance of funds in their Android Pay account. Google is for some users a prepaid digital card where users transfer funds to their Android Pay account, and therefore is subject to federal regulations. To use Android Pay, customers hold their phone near the merchant's NFC terminal at checkout. Users are asked to enter their PIN and then choose to pay with either the credit or debit card on file with Android Pay or with their cash balance. If the user chooses to pay with a bank card, the app creates a unique digital token and sends this as an encrypted message to Android servers, which then communicate with the issuing bank, for approval. Approval messages are sent to the merchant's point-of-sale terminal. No card information is transmitted from the point of purchase. Android Pay is free for subscribers except when they use their credit card, which entails a 3% credit card transaction fee charged by the credit card companies. However, Google may offer consumers rewards, and in the future, display ads. Because Android Pay can store user funds, it is subject to federal banking regulations.

Samsung Pay was introduced by Samsung in the United States in September 2015, after an earlier roll-out in Samsung's home country, South Korea. Samsung smartphones are the most widely used smartphones in the world. As with Apple Pay and Android Pay, users create an account, and submit their bank credit or debit card information. Samsung Pay prioritizes the use of NFC technology when merchants have the appropriate terminal, but when that is not available, switches to a technology called Magnetic Secure Transmission that sends the card data stored on the user's device to traditional magnetic stripe terminals. This means that Samsung Pay can be used by the millions of existing point-of-sale card swiping terminals without upgrading to NFC terminals or installing any apps. Samsung Pay also stores coupons and reward cards, but does not store user funds and is not a prepaid card. Therefore, it most likely will not be subject to U.S. federal regulations. Like the other mobile wallets, it is essentially a place where users can store all their credit cards.

Currently, the most popular mobile payment systems are offered by PayPal and Square, some of which do not use NFC. While claiming to be financial services firms, both PayPal and Square are financial service software platform firms, technology companies in disguise. PayPal was late to the mobile payment market, beaten to the punch by Square. Square started in 2009 with Square Reader, a square plastic device

that plugged into an iPhone or iPad, and allowed users to easily set up a merchant license to accept credit cards, and then swipe the cards locally on the Square Reader device. Using the Square app, it allows merchants to easily accept credit card payments from customers on the go. Square also developed Square Register (now called Point of Sale), which is a software app that turns a tablet into a point-of-sale terminal and cash register. Square has morphed into a small business services company, serving coffee shops, newsstands, small retailers, and farmers' market merchants, as well as piano teachers, baby sitters, and taxi drivers, allowing them to easily accept credit card payments. Square generated \$1 billion in revenue in 2015, and showed a loss of \$174 million.

PayPal is currently the most successful and profitable non-traditional online payment system, used mostly on desktops and tablets, but rapidly becoming a mobile payment force. PayPal is currently the largest alternative (non-credit card) online payment service, processing \$282 billion in transactions in 2015, and has 188 million subscribers. PayPal processed \$66 billion in mobile payments in 2015, up from \$27 billion in 2013. PayPal is growing payment volume at around 20% annually.

PayPal currently enables mobile payments in three ways. First, PayPal sells a device that allows merchants (mostly small businesses) to swipe credit cards using a smartphone or tablet, just like the Square device. Second, the most common PayPal mobile payment occurs when customers use their mobile device browser on a tablet or smartphone to make a purchase or payment at a website. This is not very helpful for merchants like Starbucks, Macys, or local restaurants, who would like customers to be able to purchase goods in their stores and outlets on the fly without keying in information to a smartphone. A third method is PayPal's updated app for iOS and Android devices. On entering a merchant's store that accepts PayPal app payments, the app establishes a link using Bluetooth with the merchant's app that is also running on an iOS or Android device. This step authenticates the user's PayPal account. On checkout, the customer tells the merchant he or she will pay with PayPal. The merchant app charges the customer's PayPal account. After the payment is authorized, a message is sent to the customer's phone. No credit card information is being transmitted or shared with the merchant. Users do not have to enter a pin code or swipe their phone at a special merchant device, so merchants are not required to purchase an expensive NFC point-of-sale device, but they must have the PayPal merchant app stored on a PC which is really acting like a digital cash register. In 2012, PayPal launched PayPal Here, a device that will both read credit cards equipped with computer chips, as well as accept payments from Android Pay and Apple Pay. The service includes a card reader that plugs into a tablet or smartphone, and a stand-alone contactless device that can accept NFC payments, as well as swipe credit cards. In 2015, PayPal launched the PayPal.me app, a peer-to-peer payment service that allows users to make and receive payments from friends. Users share their PayPal.me link with friends and can transfer money to their PayPal accounts. The service is free and is a direct competitor with Venmo and other P2P payment services. Venmo, which PayPal also owns, only works with U.S. banks, credit and debit cards, while PayPal.me is targeted at PayPal's global user base. In 2016 PayPal launched NFC payments for locations that accept VISA's contactless payments.

SOURCES: "Consumer Bill Payments Shifts & Strategies," by Jim Gilligan and Kellie Thomas, Payments.com, 2016; "PayPal Gets Friendlier With Facebook," by Telis Demos, *New York Times*, October 24, 2016; "Apple Pay at Two Years: Not Much to Celebrate (Yet)," by Mark Hamblen, Computerworld.com, October 20, 2016; "How Millennials Became Spooked by Credit Cards," by Nathaniel Popper,

While mobile payment systems developed by technology companies are experiencing rapid growth, mobile wallets developed by large national merchants have sputtered. Large national merchants have had a contentious relationship with credit card firms because of the 3% fees charged by credit card companies, which raise prices to consumers by the same amount. Merchants would much prefer customers pay with store credit cards that are linked to the customer's bank account, or debit accounts, where banks do not charge a fee, or customer-supplied prepayment funds. Some merchants also offer their own store credit cards and have developed their own transaction processing systems, circumventing the bank credit card system entirely. Merchants also want to control the point-of-sale moment, where they can offer coupons, loyalty rewards, and special discounts, rather than rely on mobile wallets provided by the technology companies, which do not offer these capabilities.

In 2012, a joint venture of the 15 largest merchants announced the Merchant Customer Exchange (MCX). MCX was backed by Walmart, Target, Sears, 7-Eleven, Sunoco, and 10 other national pharmacies, supermarkets, and restaurant chains. The backers of this effort have annual sales of more than \$1 trillion dollars. That was enough to make everyone involved in mobile payments stand up and listen, even Google and Apple. Their initial effort was coined CurrentC, and was piloted in 2014. CurrentC was an app that allowed customers to pay using their bank accounts, bank debit cards, or store-issued credit cards, but not traditional bank credit cards. The idea was to circumvent the bank credit system entirely, and avoid paying the credit companies their typical 3% fee. CurrentC was withdrawn in 2016, and the MCX joint venture has ended due to squabbles among the partners, and an excessively long development time for the app. In 2016, Walmart introduced its own Walmart Pay app for both iOS and Android phones. Using QR recognition technology, not NFC, Walmart Pay now accepts all bank credit and debit cards, as well as Walmart store credit cards. It can also read coupons and offer rewards to loyal customers. Walmart Pay can only be used at Walmart stores, but given that Walmart has 140 million customers a week in the United States, that's not a terrible disadvantage. As of October 2016, 22 million customers are using the Walmart Pay app every month. The advantage to Walmart is that it owns the customer transaction, and information, without the intervention of the tech giants. Walmart, and the other large national merchants, will have to live with the credit card companies and their 3% fees for now.

The third entrant to the mobile payment market is composed of the large national banks and credit card companies. Banks and credit card firms have been very slow moving into the mobile payment space, in part because the existing credit system works so well and their cards are widely accepted by consumers and merchants. Mobile payment systems from tech companies and merchants are competitors for the loyalty of bank customers who deposit billions of dollars in bank checking, savings, and debit cards, where banks can charge fees, and use the deposits essentially free of cost, given the low or non-existent interest rates on these accounts. JP Morgan Chase has launched Retail Checkout, a card reader that accepts tap card and mobile wallet NFC payments, and the Chase Mobile app for smartphones and tablets, which allows bank customers to perform a wide variety of banking functions like peer-to-peer payments by e-mail (QuickPay), pay bills, deposit checks, check balances, and even apply for

New York Times, August 14, 2016; "Under Pressure, Big Banks Vie for Instant Payment Market," by Michael Corkery, *New York Times*, August 1, 2016; "PayPal to Roll Out NFC Mobile Payments Across the US Through Visa Deal," by Rian Boden, *NFCworld.com*, July 25, 2016; "Walmart Pay vs. Apple Pay: Hardware Age Dictates All," by Evan Shuman, *Computerworld.com*, July 8, 2016; "In Mobile Payments War, Big Banks Strike Back," by Aaron Black, *Wall Street Journal*, July 8, 2016; "The Mobile Payments Report," by Evan Baker, *Businessinsider.com*, June 3, 2016; "Reasons that US Smartphone Users Don't Use Mobile Payments," eMarketer, Inc., June 2016; "Why Apple Pay and Other Mobile Wallets Beat Chip Cards," by Brian Chen, *New York Times*, May 4, 2016; "Apple Pay's Big Drop," *Pymnts.com*, March 18, 2016; "Latest Mobile-Banking Research Shows Laptops Still Reign," by Robin Sidel, *Wall Street Journal*, January 27, 2016; "As More Pay by Smartphone, Banks Scramble to Keep Up," by Steve Lohr, *New York Times*, January 18, 2016; "For the First Time, More Are Mobile-Banking Than Going to a Branch," by Telis Demos, *Wall Street Journal*, January 12, 2016; "US Mobile Payments Forecast," by Bryan Yeager, eMarketer, Inc., November 2015; "Bold Bet That Banking Industry Is Poised for Serious Disruption," by Michael Casey, *Wall Street Journal*, June 5, 2015; "'Pretty Useless': Consumer Frustrations Grow Over New Credit Card Chip," by Alexandra Zaslow, *Todaymoney.com*, October 16, 2015; "Square's IPO Filing: It's Complicated," *Recode.net*, by Jason Del Rey, October 14, 2015; "PayPal Here Launches a Mobile Card Reader That Accepts Android Pay and Apple Pay," by Ruth Reader, *Venturebeat.com*, September 28, 2015; "Samsung Pay: What You Need to Know (FAQ)," by Lexy Savvides, *Cnet.com*, September 28, 2015; "Revamped Google Wallet Arrives on iOS," by Stephanie Mlot, *Pcmagazine.com*, September 22, 2015; "Apple Pay Competitor CurrentC May Not Launch Until Next Year," by Jason Del Rey, *Recode.net*, August 12, 2015;

"PayPal Returns to Market with \$52 Billion Valuation," by Devika Krishna Kumar and Mari Saito, Reuters.com, July 20, 2015; "There Are No Transaction Fees for Android Pay, Which Is Good for Us, Bad for Google," by Robert Nazarian, Digitaltrends.com, June 8, 2015; "The State of Mobile Payments in 2015," by James A. Martin, CIO.com, April 22, 2015; "Apple Sees Mobile-Payment Service Gaining in Challenge to PayPal," by Olga Kharif, Bloomberg.com, January 27, 2015; "What Apple Pay Means for Retailers," by Abby Callard, Internetretailer.com, September 12, 2014; "Apple Pay: No Charge for Merchants, But Transaction-Security Fees for Issuers," by Jim Daly, Digitaltransaction.net, September 11, 2014.

mortgages. Citi has launched Citi Mobile with similar functionality. Banks so far have not introduced apps for making NFC payments for consumer purchases, but these will surely be introduced shortly. The large banks are investing heavily in payment startups to acquire these capabilities.

The future for smartphone mobile wallets is assured given the size of the players involved, the potential rewards for successful players, and the demands of consumers for a payment system that does not involve swiping plastic cards, dealing with slips of paper receipts, and digging for cash in their pockets and purses.

But the transition is going much slower than pundits initially thought, with millions of consumers trying the new methods once, and then not using them again because not enough merchants accept them, lack of familiarity, and concerns about security and privacy. One recent study found there are now 11 million contactless mobile payment users in the United States, but just 2.3 million who are active users. It is unlikely that all the mobile payment systems described above will survive, and also quite likely that consumers will remain confused by all their payment options for some time yet to come. A full transition to mobile payments will be a long time coming.

Case Study Questions

1. Who are the three major players in the mobile payment market?
2. Why is Venmo considered a social-mobile payment system?
3. How does Apple Pay differ from Android Pay and Samsung Pay?
4. How does PayPal enable mobile payments?

5.8 REVIEW

KEY CONCEPTS

- Understand the scope of e-commerce crime and security problems, the key dimensions of e-commerce security, and the tension between security and other values.
- While the overall size of cybercrime is unclear, cybercrime against e-commerce sites is growing rapidly, the amount of losses is growing, and the management of e-commerce sites must prepare for a variety of criminal assaults.
- There are six key dimensions to e-commerce security: integrity, nonrepudiation, authenticity, confidentiality, privacy, and availability.
- Although computer security is considered necessary to protect e-commerce activities, it is not without a downside. Two major areas where there are tensions between security and website operations are:
 - *Ease of use*—The more security measures that are added to an e-commerce site, the more difficult it is to use and the slower the site becomes, hampering ease of use. Security is purchased at the price

of slowing down processors and adding significantly to data storage demands. Too much security can harm profitability, while not enough can potentially put a company out of business.

- *Public safety*—There is a tension between the claims of individuals to act anonymously and the needs of public officials to maintain public safety that can be threatened by criminals or terrorists.

■ Identify the key security threats in the e-commerce environment

- The most common and most damaging forms of security threats to e-commerce sites include:
 - *Malicious code*—viruses, worms, Trojan horses, ransomware, and bot networks are a threat to a system's integrity and continued operation, often changing how a system functions or altering documents created on the system.
 - *Potentially unwanted programs (adware, spyware, etc.)*—a kind of security threat that arises when programs are surreptitiously installed on your computer or computer network without your consent.
 - *Phishing*—any deceptive, online attempt by a third party to obtain confidential information for financial gain.
 - *Hacking and cybervandalism*—intentionally disrupting, defacing, or even destroying a site.
 - *Credit card fraud/theft*—one of the most-feared occurrences and one of the main reasons more consumers do not participate in e-commerce. The most common cause of credit card fraud is a lost or stolen card that is used by someone else, followed by employee theft of customer numbers and stolen identities (criminals applying for credit cards using false identities).
 - *Identity fraud*—involves the unauthorized use of another person's personal data, such as social security, driver's license, and/or credit card numbers, as well as user names and passwords, for illegal financial benefit.
 - *Spoofing*—occurs when hackers attempt to hide their true identities or misrepresent themselves by using fake e-mail addresses or masquerading as someone else.
 - *Pharming*—involves redirecting a web link to an address different from the intended one, with the site masquerading as the intended destination.
 - *Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks*—hackers flood a website with useless traffic to inundate and overwhelm the network, frequently causing it to shut down and damaging a site's reputation and customer relationships.
 - *Sniffing*—a type of eavesdropping program that monitors information traveling over a network, enabling hackers to steal proprietary information from anywhere on a network, including e-mail messages, company files, and confidential reports. The threat of sniffing is that confidential or personal information will be made public.
 - *Insider jobs*—although the bulk of Internet security efforts are focused on keeping outsiders out, the biggest threat is from employees who have access to sensitive information and procedures.
 - *Poorly designed server and client software*—the increase in complexity and size of software programs has contributed to an increase in software flaws or vulnerabilities that hackers can exploit.
 - *Social network security issues*—malicious code, PUPs, phishing, data breaches, identity fraud, and other e-commerce security threats have all infiltrated social networks.
 - *Mobile platform security issues*—the mobile platform presents an alluring target for hackers and cybercriminals, and faces all the same risks as other Internet devices, as well as new risks associated with wireless network security.
 - *Cloud security issues*—as devices, identities, and data become more and more intertwined in the cloud, safeguarding data in the cloud becomes a major concern.

■ Describe how technology helps secure Internet communications channels and protect networks, servers, and clients.

- Encryption is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the receiver. Encryption can provide four of the six key dimensions of e-commerce security: message integrity, nonrepudiation, authentication, and confidentiality.

- There are a variety of different forms of encryption technology currently in use. They include:
 - *Symmetric key cryptography*—Both the sender and the receiver use the same key to encrypt and decrypt a message.
 - *Public key cryptography*—Two mathematically related digital keys are used: a public key and a private key. The private key is kept secret by the owner, and the public key is widely disseminated. Both keys can be used to encrypt and decrypt a message. Once the keys are used to encrypt a message, the same keys cannot be used to unencrypt the message.
 - *Public key cryptography using digital signatures and hash digests*—This method uses a mathematical algorithm called a hash function to produce a fixed-length number called a hash digest. The results of applying the hash function are sent by the sender to the recipient. Upon receipt, the recipient applies the hash function to the received message and checks to verify that the same result is produced. The sender then encrypts both the hash result and the original message using the recipient's public key, producing a single block of cipher text. To ensure both the authenticity of the message and nonrepudiation, the sender encrypts the entire block of cipher text one more time using the sender's private key. This produces a digital signature or "signed" cipher text that can be sent over the Internet to ensure the confidentiality of the message and authenticate the sender.
 - *Digital envelope*—This method uses symmetric cryptography to encrypt and decrypt the document, but public key cryptography to encrypt and send the symmetric key.
 - *Digital certificates and public key infrastructure*—This method relies on certification authorities who issue, verify, and guarantee digital certificates (a digital document that contains the name of the subject or company, the subject's public key, a digital certificate serial number, an expiration date, an issuance date, the digital signature of the certification authority, and other identifying information).
 - In addition to encryption, there are several other tools that are used to secure Internet channels of communication, including: Secure Sockets Layer (SSL)/Transport Layer Security (TLS), virtual private networks (VPNs), and wireless security standards such as WPA2.
 - After communications channels are secured, tools to protect networks, the servers, and clients should be implemented. These include: firewalls, proxies, intrusion detection and prevention systems (IDS/IDP), operating system controls, and anti-virus software.
- **Appreciate the importance of policies, procedures, and laws in creating security.**
- In order to minimize security threats, e-commerce firms must develop a coherent corporate policy that takes into account the nature of the risks, the information assets that need protecting, and the procedures and technologies required to address the risk, as well as implementation and auditing mechanisms.
 - Public laws and active enforcement of cybercrime statutes also are required to both raise the costs of illegal behavior on the Internet and guard against corporate abuse of information.
 - The key steps in developing a security plan are:
 - *Perform a risk assessment*—an assessment of the risks and points of vulnerability.
 - *Develop a security policy*—a set of statements prioritizing the information risks, identifying acceptable risk targets, and identifying the mechanisms for achieving these targets.
 - *Create an implementation plan*—a plan that determines how you will translate the levels of acceptable risk into a set of tools, technologies, policies, and procedures.
 - *Create a security team*—the individuals who will be responsible for ongoing maintenance, audits, and improvements.
 - *Perform periodic security audits*—routine reviews of access logs and any unusual patterns of activity.
- **Identify the major e-commerce payment systems in use today.**
- The major types of e-commerce payment systems in use today include:

- *Online credit card transactions*, which are the primary form of online payment system. There are five parties involved in an online credit card purchase: consumer, merchant, clearinghouse, merchant bank (sometimes called the “acquiring bank”), and the consumer’s card-issuing bank. However, the online credit card system has a number of limitations involving security, merchant risk, cost, and social equity.
 - *PayPal*, which is an example of an alternative payment system that permits consumers to make instant, online payments to merchants and other individuals based on value stored in an online account. Other examples include Pay with Amazon, Visa Checkout, MasterPass, Bill Me Later, and WU Pay.
 - *Mobile payment systems*, which use either credit card readers attached to a smartphone (Square, PayPal Here) or near field communication (NFC) chips, which enable mobile payment at point-of-sale (Apple Pay, Android Pay, and Samsung Pay).
 - *Digital cash*, such as Bitcoin and virtual currencies. Digital cash is growing in importance and can be used to hide payments from authorities, as well as support the legitimate exchange of value.
- Describe the features and functionality of electronic billing presentment and payment systems.
- Electronic billing presentment and payment (EBPP) systems are a form of online payment systems for monthly bills. EBPP services allow consumers to view bills electronically and pay them through electronic funds transfers from bank or credit card accounts.
 - Major players in the EBPP marketplace include: online banking, biller-direct systems, mobile payment systems, and consolidators.

QUESTIONS

1. Why is it less risky to steal online? Explain some of the ways criminals deceive consumers and merchants.
2. Explain why an e-commerce site might not want to report being the target of cybercriminals.
3. Give an example of security breaches as they relate to each of the six dimensions of e-commerce security. For instance, what would be a privacy incident?
4. How would you protect your firm against a Denial of Service attack?
5. Name the major points of vulnerability in a typical online transaction.
6. How does spoofing threaten a website’s operations?
7. Why is adware or spyware considered to be a security threat?
8. What are some of the steps a company can take to curtail cybercriminal activity from within a business?
9. Explain some of the modern-day flaws associated with encryption. Why is encryption not as secure today as it was earlier in the century?
10. Briefly explain how public key cryptography works.
11. Compare and contrast firewalls and proxy servers and their security functions.
12. Is a computer with anti-virus software protected from viruses? Why or why not?
13. Identify and discuss the five steps in developing an e-commerce security plan.
14. How do biometric devices help improve security? What particular type of security breach do they reduce?
15. Briefly discuss the disadvantages of credit cards as the standard for online payments. How does requiring a credit card for payment discriminate against some consumers?
16. Describe the major steps involved in an online credit card transaction.
17. Why is Bitcoin so controversial?
18. What is NFC and how does it work?
19. Discuss why EBPP systems are becoming increasingly popular.
20. How are the main types of EBPP systems both alike and different from each other?