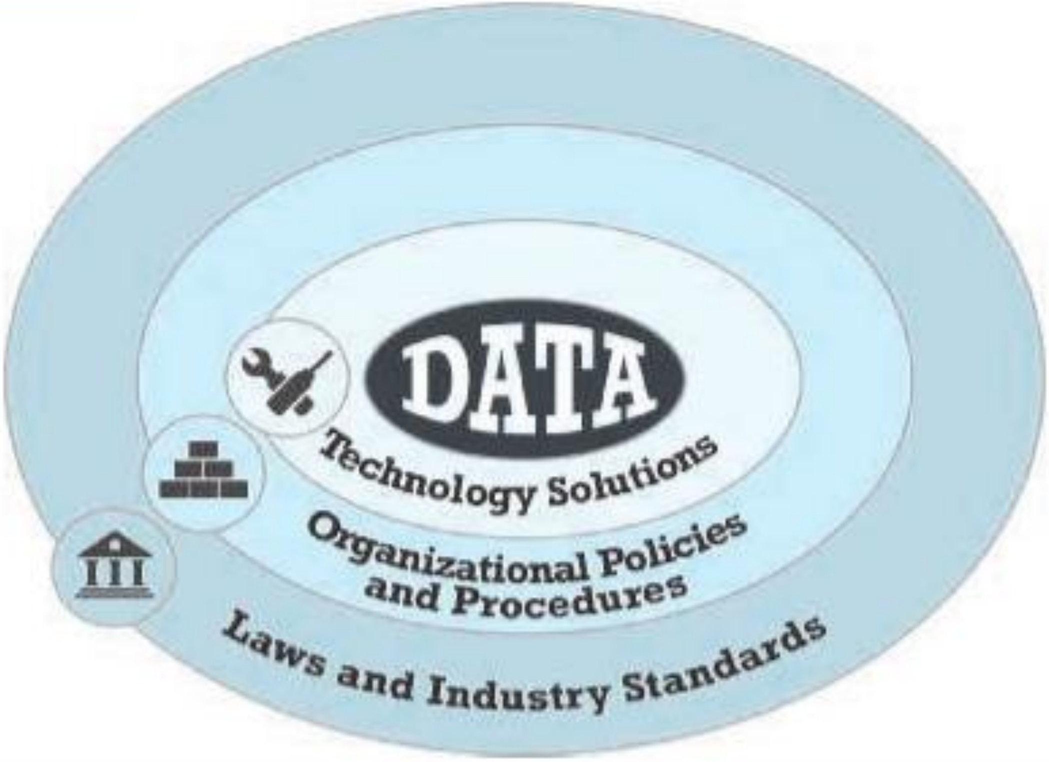
Unit 5: Security in E-Commerce (7 Hrs.)

WHAT IS GOOD E-COMMERCE SECURITY?

- 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 on next slide illustrates** the multi-layered nature of e-commerce security.

E-COMMERCE SECURITY ENVIRONMENT

FIGURE 5.1 **THE E-COMMERCE SECURITY ENVIRONMENT**


DATA
Technology Solutions
Organizational Policies and Procedures
Laws and Industry Standards

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

DIMENSIONS OF E-COMMERCE SECURITY: 6

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

Integrity

- It 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wire transfer into a different account, the integrity of the message has been compromised because the communication no longer represents what the original sender intended.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

- It 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

- **It 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 and Privacy

- **It 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.

Availability

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

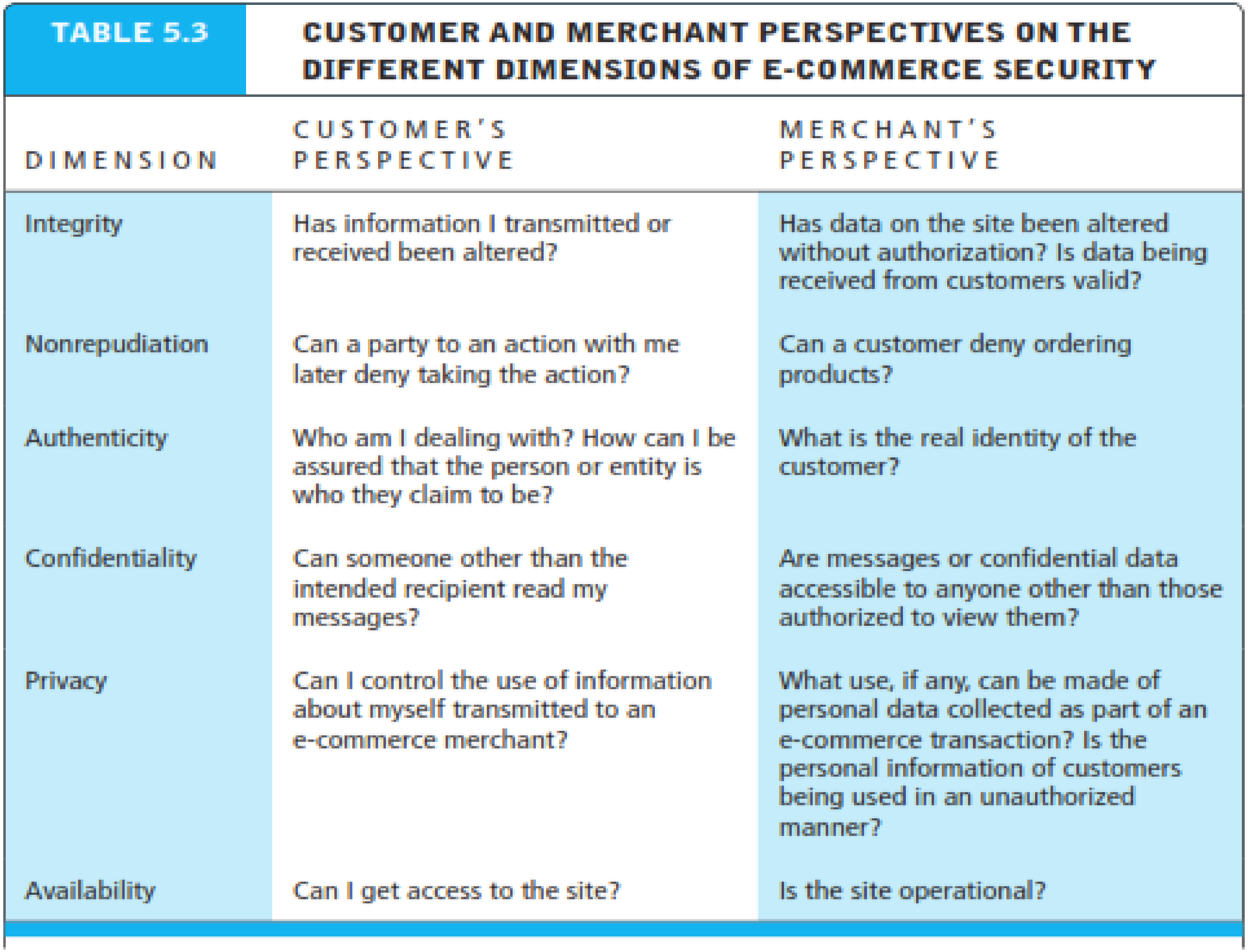
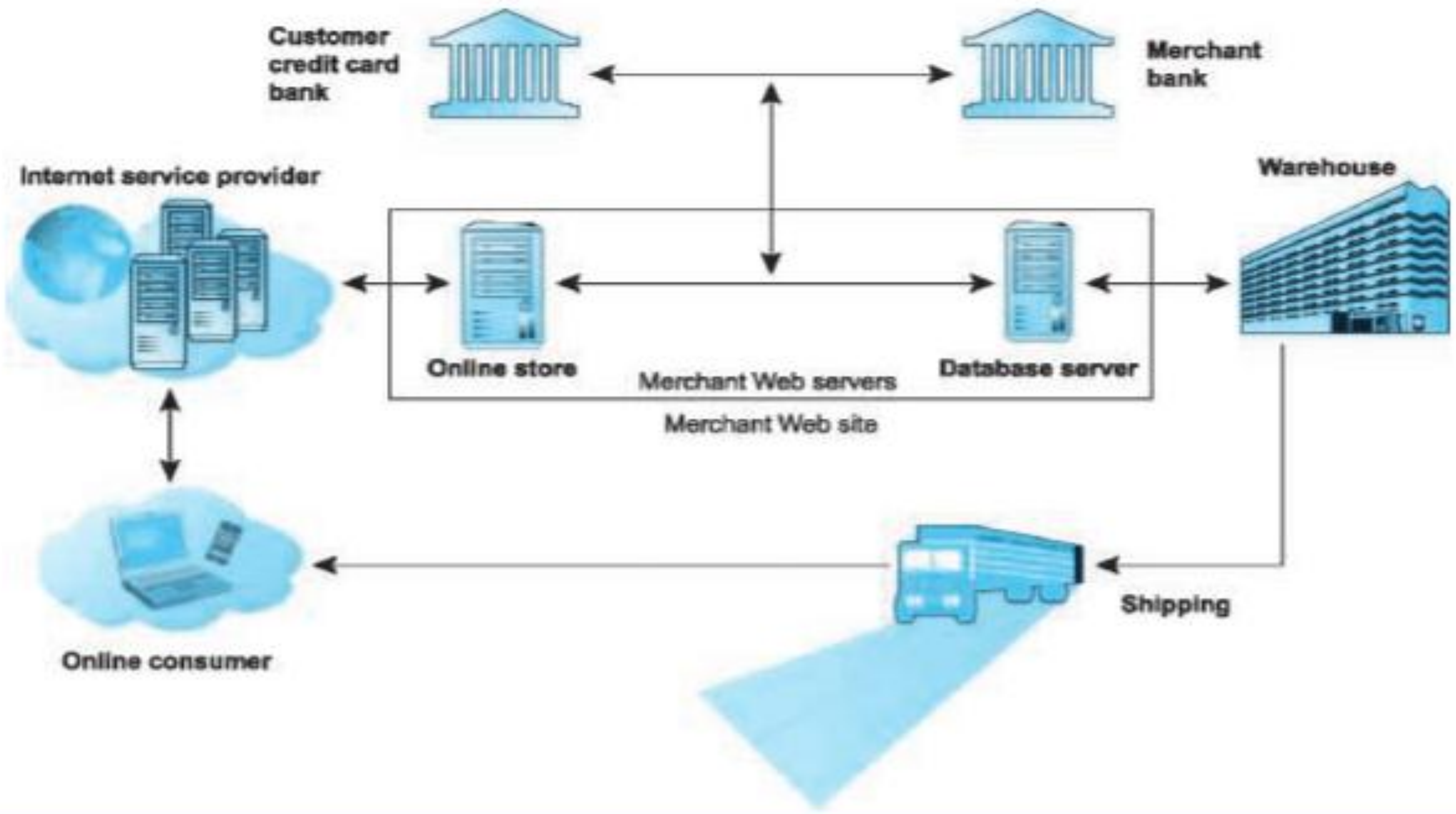


TABLE 5.3 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

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?

SECURITY THREATS IN THE E-COMMERCE ENVIRONMENT

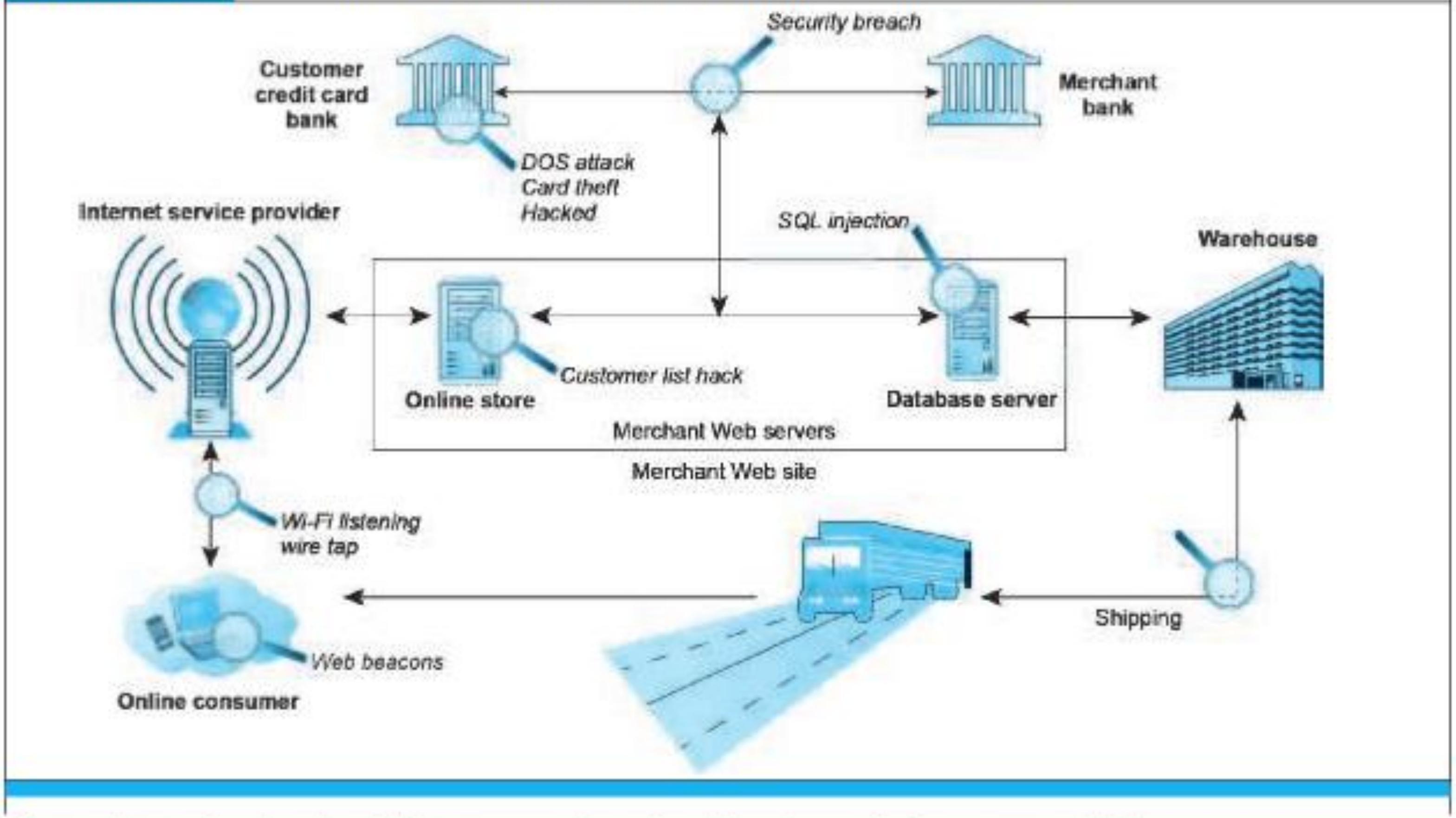
FIGURE 5.2 A TYPICAL E-COMMERCE TRANSACTION



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

Vulnerable Points in E Commerce

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.

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 novicesto become cybercriminals.
- Exploit kits typically target software that is widely deployed, such as Microsoft Windows, Internet Explorer, Adobe Flash and Reader, and Oracle Java.

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.

Adware and Spyware

- **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.
- **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).

Social Engineering and 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.

- **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 a million dollars.
- This type of e-mail scam is popularly known as a "Nigerian letter" scam

- 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.

HACKING

- **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
- **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

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.
- Incidences of stolen credit card information are actually much lower than users think, around 0.8% of all online card transactions.
- 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 other 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.
- 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.
- 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.

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.
- 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.

- **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 travelling 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.
- 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.

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.

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.
- By sneaking in among our friends, hackers can masquerade as friends and dupe users into scams.

PROTECTING INTERNET COMMUNICATION

- 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:
  - ***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) n*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 which 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.
- 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.
- 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, and another for the government.

- The **Data Encryption Standard (DES) was developed by the National Security Agency (NSA)** and **IBM** in the 1950s.
- 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.

Public Key Cryptography

- **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 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.
- 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.

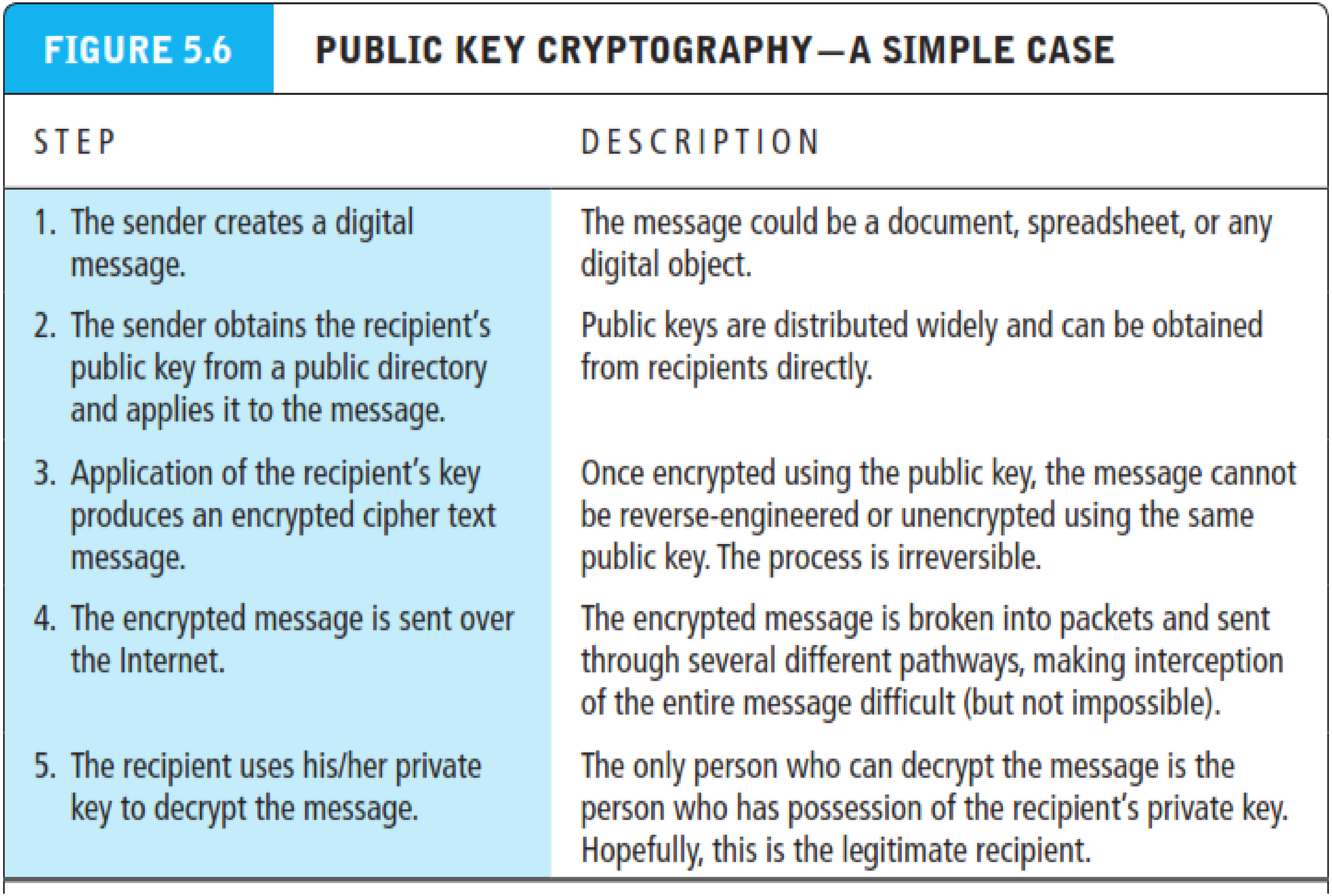


FIGURE 5.6 PUBLIC KEY CRYPTOGRAPHY—A SIMPLE CASE

STEP	DESCRIPTION
1. The sender creates a digital message.	The message could be a document, spreadsheet, or any digital object.
2. The sender obtains the recipient's public key from a public directory and applies it to the message.	Public keys are distributed widely and can be obtained from recipients directly.
3. Application of the recipient's key produces an encrypted cipher text message.	Once encrypted using the public key, the message cannot be reverse-engineered or unencrypted using the same public key. The process is irreversible.
4. The encrypted message is sent over the Internet.	The encrypted message is broken into packets and sent through several different pathways, making interception of the entire message difficult (but not impossible).
5. The recipient uses his/her private key to decrypt the message.	The only person who can decrypt the message is the person who has possession of the recipient's private key. Hopefully, this is the legitimate recipient.

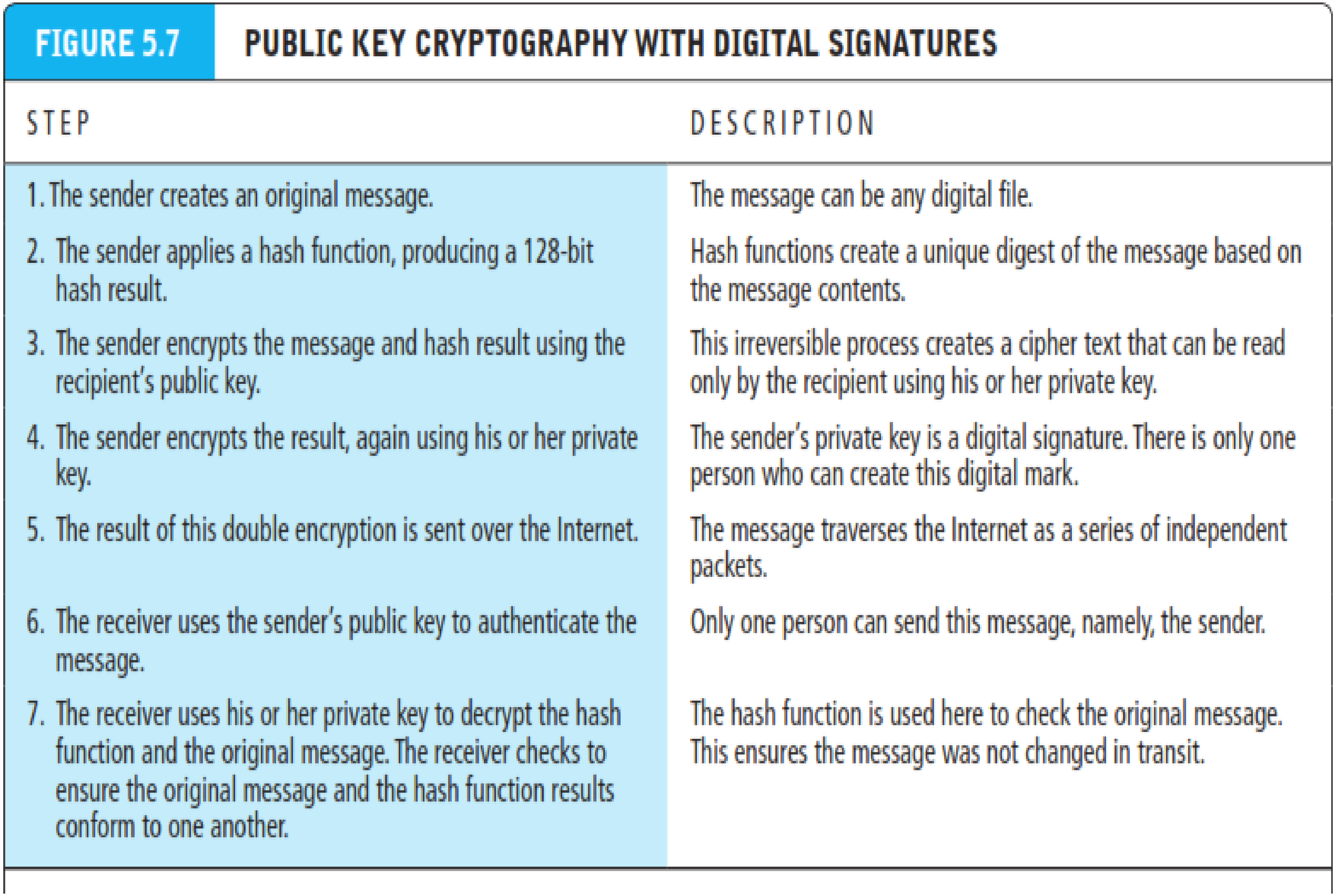
Public Key Cryptography Using Digital Signatures and Hash Digests

- 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.

- 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 producing a single block of cipher text.

- 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.

FIGURE 5.7 PUBLIC KEY CRYPTOGRAPHY WITH DIGITAL SIGNATURES



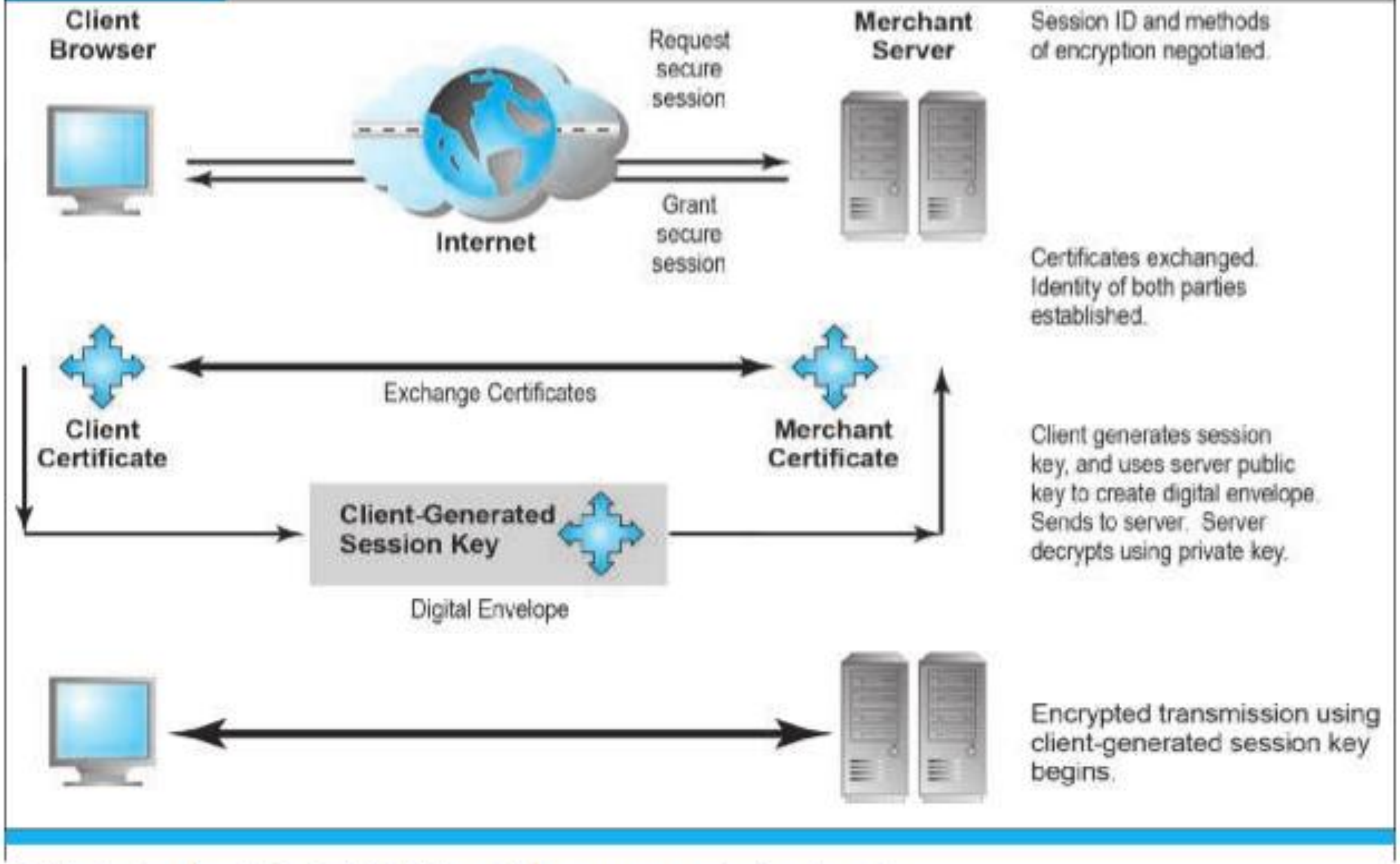
STEP	DESCRIPTION
1. The sender creates an original message.	The message can be any digital file.
2. The sender applies a hash function, producing a 128-bit hash result.	Hash functions create a unique digest of the message based on the message contents.
3. The sender encrypts the message and hash result 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.

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 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 SECURE NEGOTIATED SESSIONS USING SSL/TLS


Client Browser
Internet
Request secure session
Grant secure session
Merchant Server
Session ID and methods of encryption negotiated.
Certificates exchanged. Identity of both parties established.
Exchange Certificates
Client Certificate
Merchant Certificate
Client-Generated Session Key
Digital Envelope
Client generates session key, and uses server public key to create digital envelope. Sends to server. Server decrypts using private key.
Encrypted transmission using client-generated session key begins.

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

Digital Certificates and Public Key Infrastructure (PKI)

- 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.
- **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.

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.

Home Assignment: 5

PROTECTING SERVERS AND CLIENTS

- Operating System Security Enhancements
- Anti-Virus Software
- Firewalls
- Proxy Servers