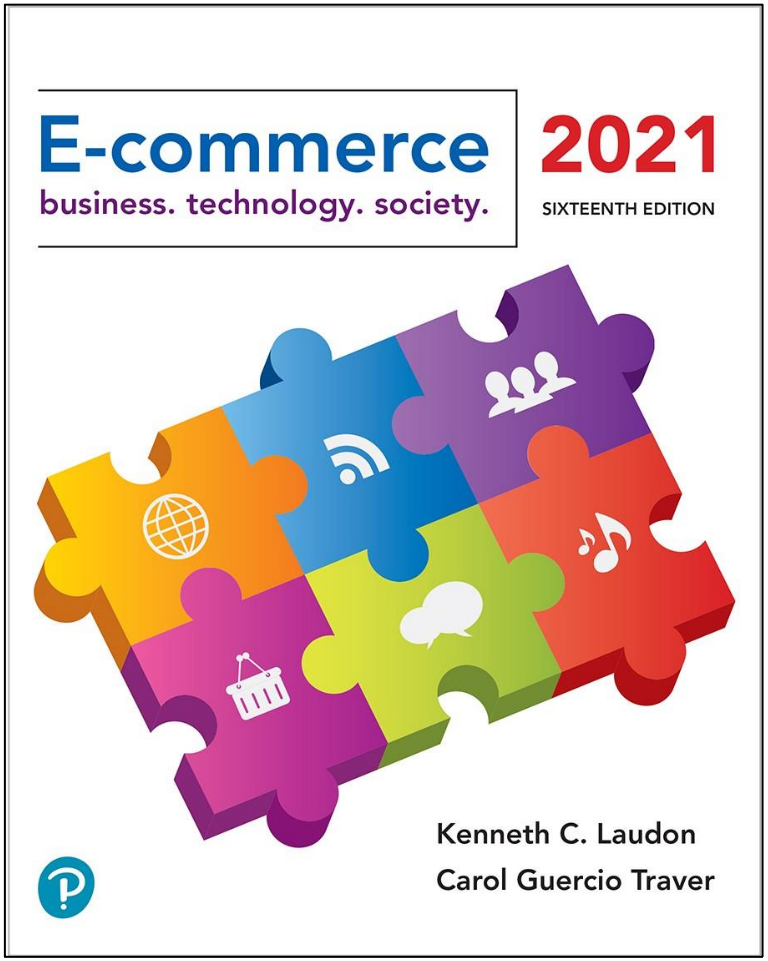
E-commerce 2021: Business. Technology. Society.

Sixteenth Edition



Chapter 5

E-commerce Security and Payment Systems

Learning Objectives

5.1 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.

5.2 Identify the key security threats in the e-commerce environment.

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

5.4 Appreciate the importance of policies, procedures, and laws in creating security.

5.5 Identify the major e-commerce payment systems in use today.

5.6 Describe the features and functionality of electronic billing presentment and payment systems.

Cyberwar: MAD 2.0

electricty grid

- Class Discussion
  - What is the difference between cyberwar against hard targets versus cyberwar versus soft targets?
  - Why has cyberwar become potentially more devastating in the past decade?
  - What damage can be done by attacks against hard targets?
  - What steps can nations take to prevent the escalation of cyberwar?

The E-commerce Security Environment

- Scope of the problem
  - Overall size of and losses due to cybercrime unclear
  - McAfee/Center for Strategic and International Studies study: Global economic impact of cybercrime and cyberespionage between $455 billion to $600 billion
  - Reports by security product providers indicate increasing cybercrime
  - Online credit card fraud one of the most high-profile forms
- Underground economy marketplaces sell stolen information, malware and more

What Is Good E-commerce Security?

- To achieve highest degree of security
  - New technologies
  - Organizational policies and procedures
  - Industry standards and government laws
- Other factors
  - Time value of money
  - Cost of security vs potential loss
  - Security often breaks at weakest link

Figure 5.1 The E-commerce Security Environment

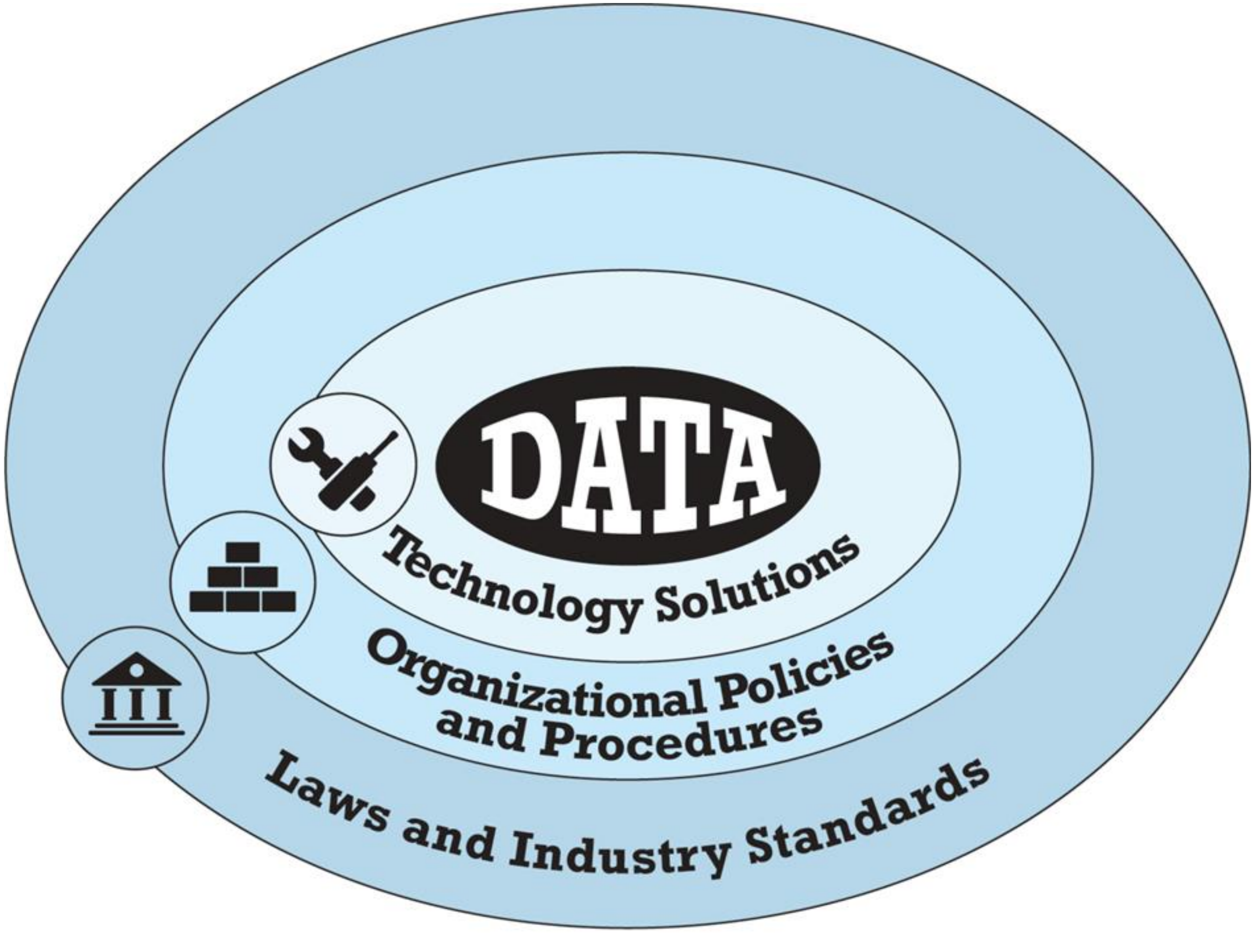

DATA
Technology Solutions
Organizational Policies and Procedures
Laws and Industry Standards

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?

The Tension Between Security and Other Values

- Ease of use
  - The more security measures added, the more difficult a site is to use, and the slower it becomes
- Public safety and the criminal uses of the Internet
  - Use of technology by criminals to plan crimes or threaten nation-state

Security Threats in the E-commerce Environment

- Three key points of vulnerability in e-commerce environment:
  - Client
  - Server
  - Communications pipeline (Internet communications channels)

Figure 5.2 A Typical E-commerce Transaction

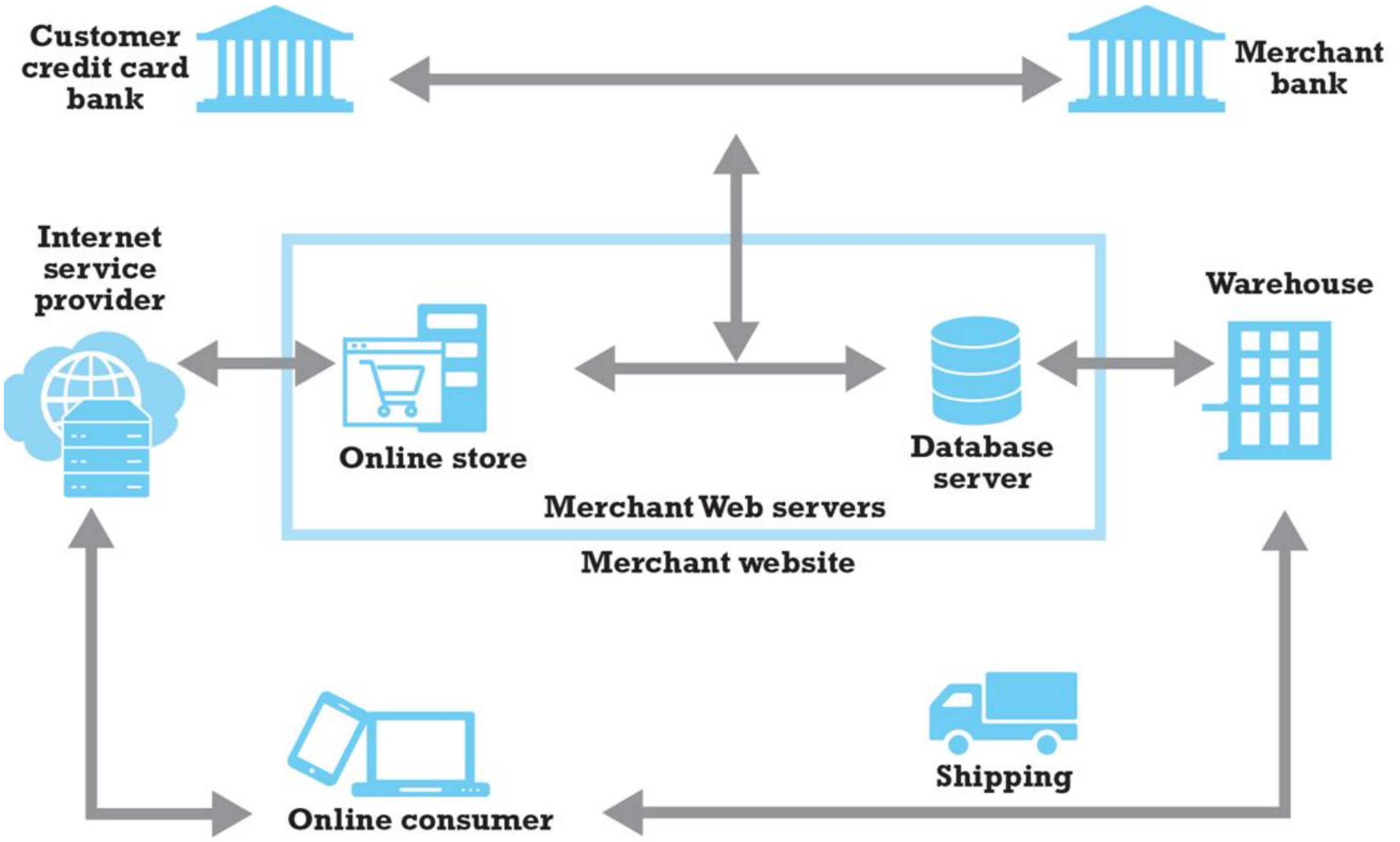
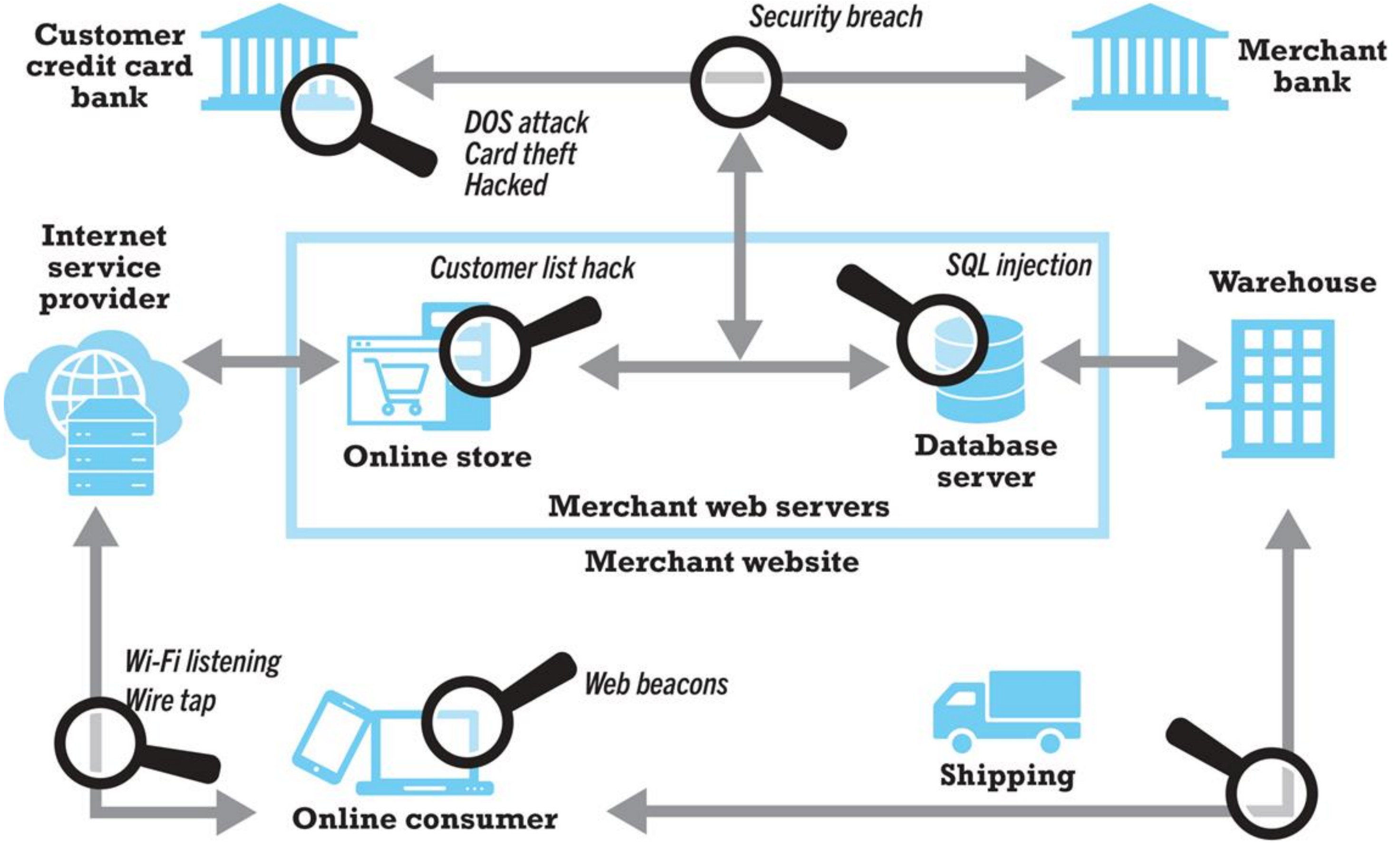


Figure 5.3 Vulnerable Points in an E-commerce Transaction



Malicious Code

- Exploits and exploit kits
- Malvertising
- Drive-by downloads
- Viruses
- Worms
- Ransomware
- Trojan horses
- Backdoors
- Bots, botnets

Potentially Unwanted Programs

- Browser parasites
  - Monitor and change user’s browser
- Adware
  - Used to call pop-up ads
- Spyware
  - Tracks users’ keystrokes, e-mails, IMs, etc.

Phishing

- Any deceptive, online attempt by a third party to obtain confidential information for financial gain
- Tactics
  - Social engineering
  - E-mail scams and BEC phishing
  - Spear phishing
- Used for identity fraud and theft

Hacking, Cybervandalism, and Hacktivism

- Hacking
  - Hackers vs crackers
  - Goals: cybervandalism, data breaches
- Cybervandalism:
  - Disrupting, defacing, destroying Web site
- Tiger teams and bug bounty hunters
- Hacktivism

Data Breaches

- Organization loses control over corporate information to outsiders
- Over 1,470 breaches in 2019, 17% increase over 2018
- Data breaches an enabler for credential stuffing attacks
- Yahoo and Equifax two of the most notorious
- Leading causes
  - Hacking
  - Unauthorized access
  - Employee error/negligence

Insight on Society: Equifax: Really Big Data Hacked

- Class Discussion
  - What organizational and technological failures led to the data breach at Equifax?
  - What technical solutions are available to combat data breaches?
  - Have you or anyone you know experienced a data breach?

Credit Card Fraud/Theft

- One of most feared occurrences, despite federal law limits on liability
- Hacking and looting of corporate servers is primary cause
- Central security issue: establishing customer identity
  - E-signatures
  - Multi-factor authentication
  - Fingerprint identification

Identity Fraud/Theft

- Unauthorized use of another person’s personal data for illegal financial benefit
  - Social security number
  - Driver’s license
  - Credit card numbers
  - Usernames/passwords
- 2019: Almost 13 million U.S. consumers suffered identity fraud

Spoofing, Pharming, and Spam (Junk) Websites

- Spoofing
  - Attempting to hide one’s true identity by using someone else’s e-mail or IP address
- Pharming
  - Automatically redirecting a URL to a different address, to benefit the hacker
- Spam (junk) websites
  - Offer collection of advertisements for other sites, which may contain malicious code

Sniffing and Man-in-The-Middle Attacks

- Sniffer
  - Eavesdropping program monitoring networks
  - Can identify network trouble spots
  - Can be used by criminals to steal proprietary information
- E-mail wiretaps
  - Recording e-mails at the mail server level
- Man-in-the-middle attack
  - Attacker intercepts and changes communication between two parties who believe they are communicating directly

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

- Denial of service (DoS) attack
  - Flooding website with pings and page request
  - Overwhelm and can shut down site’s web servers
  - Often accompanied by blackmail attempts
  - Botnets
- Distributed Denial of Service (DDoS) attack
  - Uses hundreds or thousands of computers to attack target network
  - Can use devices from Internet of Things, mobile devices
- DDoS smokescreening

Insider Attacks

- Biggest financial threat to businesses comes from insider embezzlement
- Employee access to privileged information
- Poor security procedures
- Insiders more likely to be source of cyberattacks than outsiders

Poorly Designed Software

- Increase in complexity of and demand for software has led to increase in flaws and vulnerabilities
- SQL injection attacks
- Zero-day vulnerabilities
- Heartbleed bug; Shellshock (BashBug); FREAK

Social Network Security Issues

- Social networks an environment for:
  - Viruses, site takeovers, identity fraud, malware-loaded apps, click hijacking, phishing, spam
- 2020 Twitter hack used social engineering to take control of dozens of prominent accounts and post Bitcoin scam
- Manual sharing scams
  - Sharing of files that link to malicious sites
- Fake offerings, fake Like buttons, and fake apps

Mobile Platform Security Issues

- Little public awareness of mobile device vulnerabilities
- 2018: Symantec blocked over 10,500 mobile apps per day
- Vishing
- Smishing
- SMS spoofing
- Madware

Insight on Technology: Think Your Smartphone Is Secure?

- Class Discussion
  - What types of threats do smartphones face?
  - Are there any vulnerabilities specific to mobile devices?
  - What qualities of apps make them a vulnerable security point in smartphone use?
  - Are apps more or less likely to be subject to threats than traditional PC software programs?

Cloud Security Issues

- DDoS attacks
- Infrastructure scanning
- Lower-tech phishing attacks yield passwords and access
- Use of cloud storage to connect linked accounts
- Lack of encryption and strong security procedures

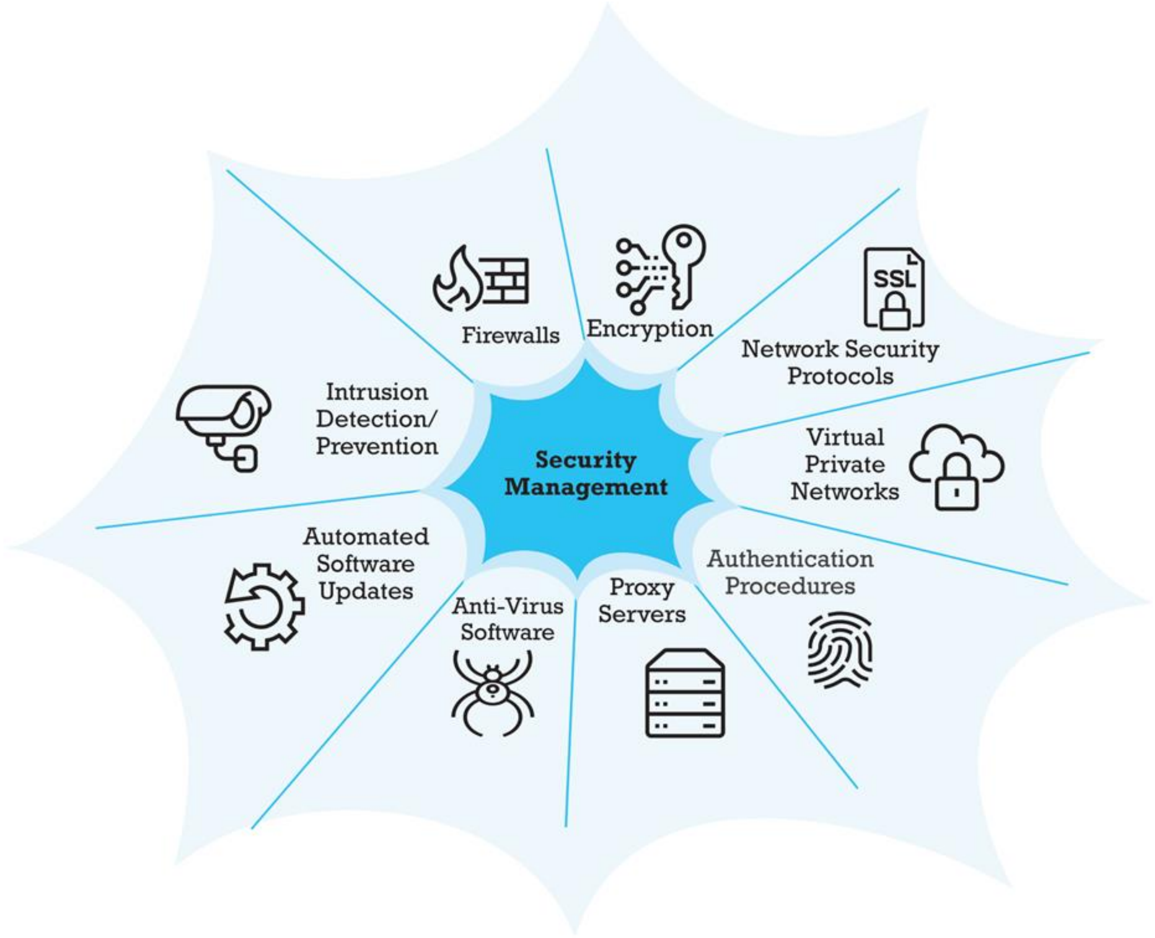
Internet of Things Security Issues

- Challenging environment to protect
- Vast quantity of interconnected links
- Near identical devices with long service lives
- Many devices have no upgrade features
- Little visibility into workings, data, or security

Technology Solutions

- Protecting Internet communications
  - Encryption
- Securing channels of communication
  - SSL, TLS, VPNs, Wi-Fi
- Protecting networks
  - Firewalls, proxy servers, IDS, IPS
- Protecting servers and clients
  - OS security, anti-virus software

Figure 5.5 Tools Available to Achieve E-commerce Security


Security Management
Firewalls
Encryption
SSL
Network Security Protocols
Virtual Private Networks
Authentication Procedures
Proxy Servers
Anti-Virus Software
Automated Software Updates
Intrusion Detection/ Prevention

Encryption

- Encryption
  - Transforms data into cipher text readable only by sender and receiver
  - Secures stored information and information transmission
  - Provides 4 of 6 key dimensions of e-commerce security:
    - Message integrity
    - Nonrepudiation
    - Authentication
    - Confidentiality

Pearson

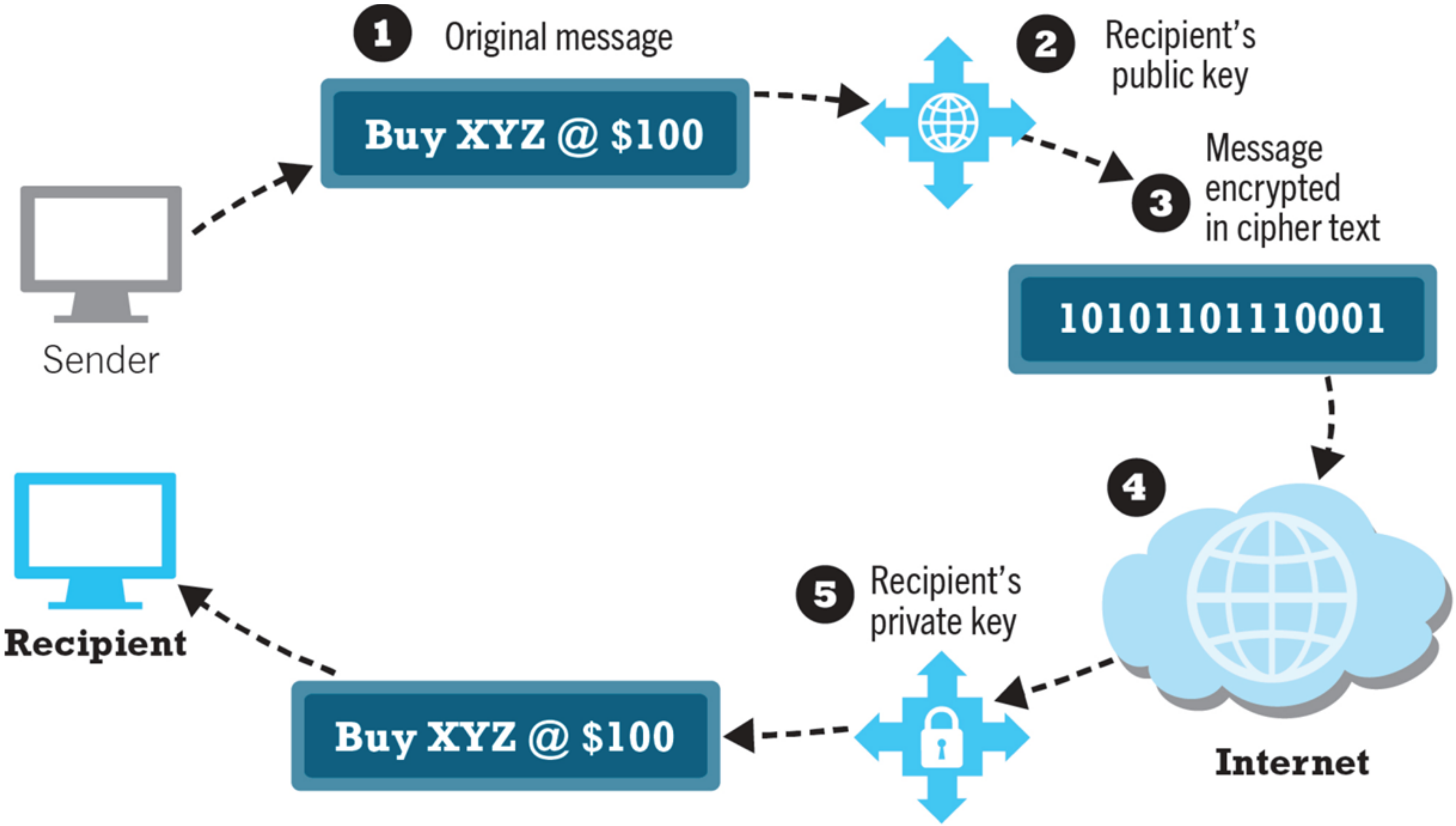
Symmetric Key Cryptography

- Sender and receiver use same digital key to encrypt and decrypt message
- Requires different set of keys for each transaction
- Strength of encryption: Length of binary key
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- Other standards use keys with up to 2,048 bits

Public Key Cryptography

- Uses two mathematically related digital keys
  - Public key (widely disseminated)
  - Private key (kept secret by owner)
- Both keys used to encrypt and decrypt message
- Once key used to encrypt message, same key cannot be used to decrypt message
- Sender uses recipient’s public key to encrypt message; recipient uses private key to decrypt it

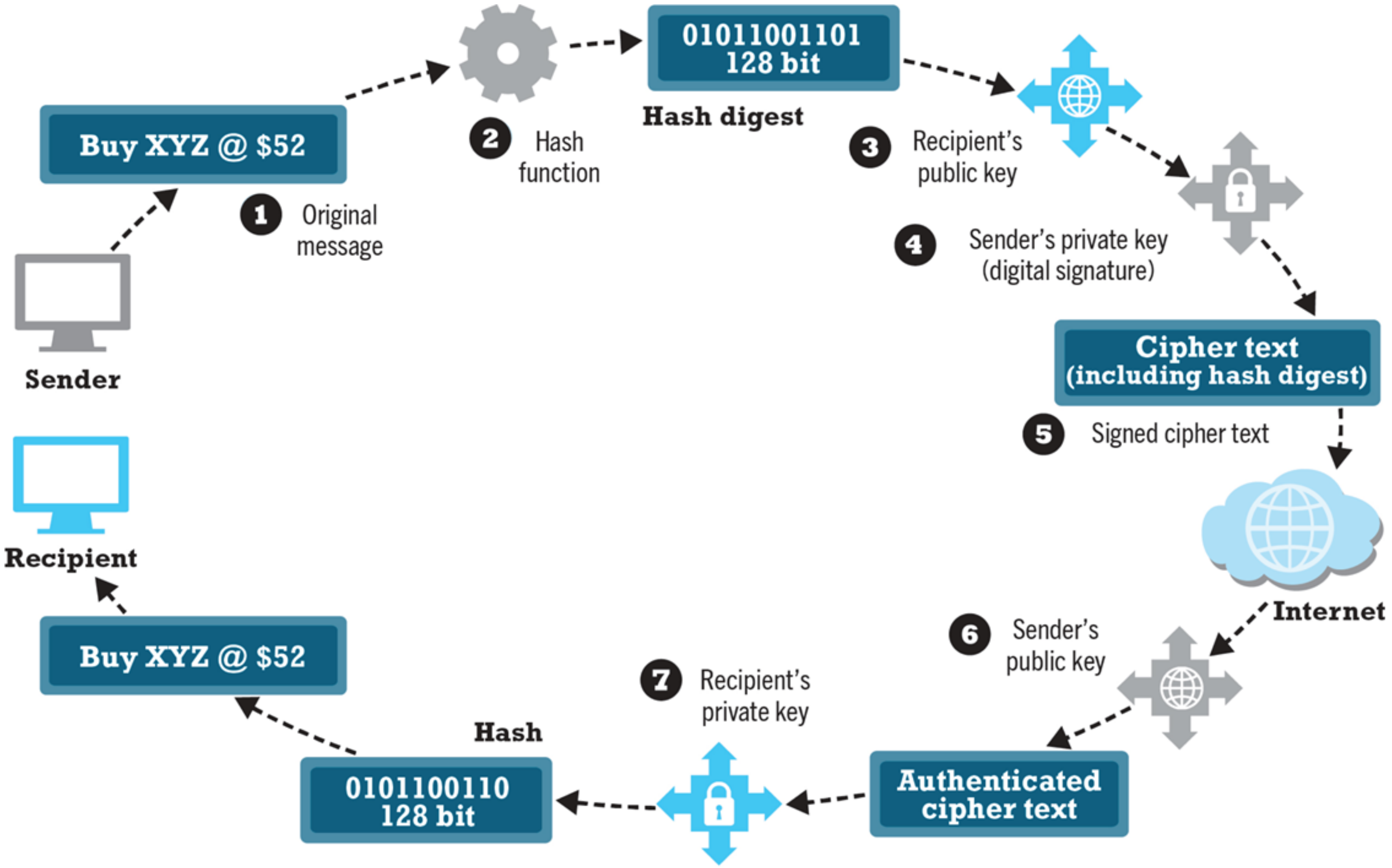
Figure 5.6 Public Key Cryptography: A Simple Case



Public Key Cryptography Using Digital Signatures and Hash Digests

- Sender applies a mathematical algorithm (hash function) to a message and then encrypts the message and hash result with recipient’s public key
- Sender then encrypts the message and hash result with sender’s private key-creating digital signature-for authenticity, nonrepudiation
- Recipient first uses sender’s public key to authenticate message and then the recipient’s private key to decrypt the hash result and message

Figure 5.7 Public Key Cryptography With Digital Signatures

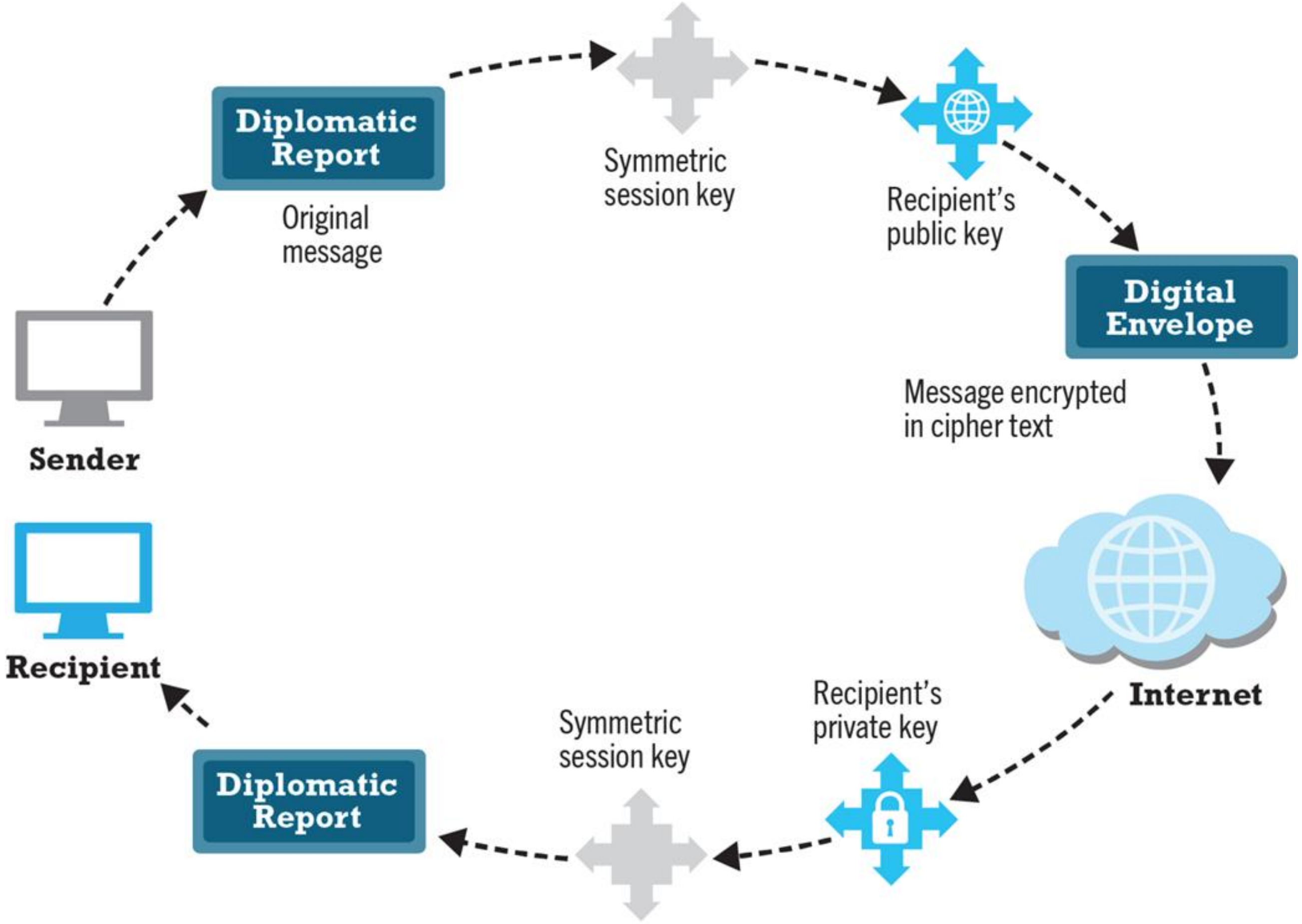


Digital Envelopes

- Address weaknesses of:
  - Public key cryptography
    - Computationally slow, decreased transmission speed, increased processing time
  - Symmetric key cryptography
    - Insecure transmission lines
- Uses symmetric key cryptography to encrypt document
- Uses public key cryptography to encrypt and send symmetric key

Pearson

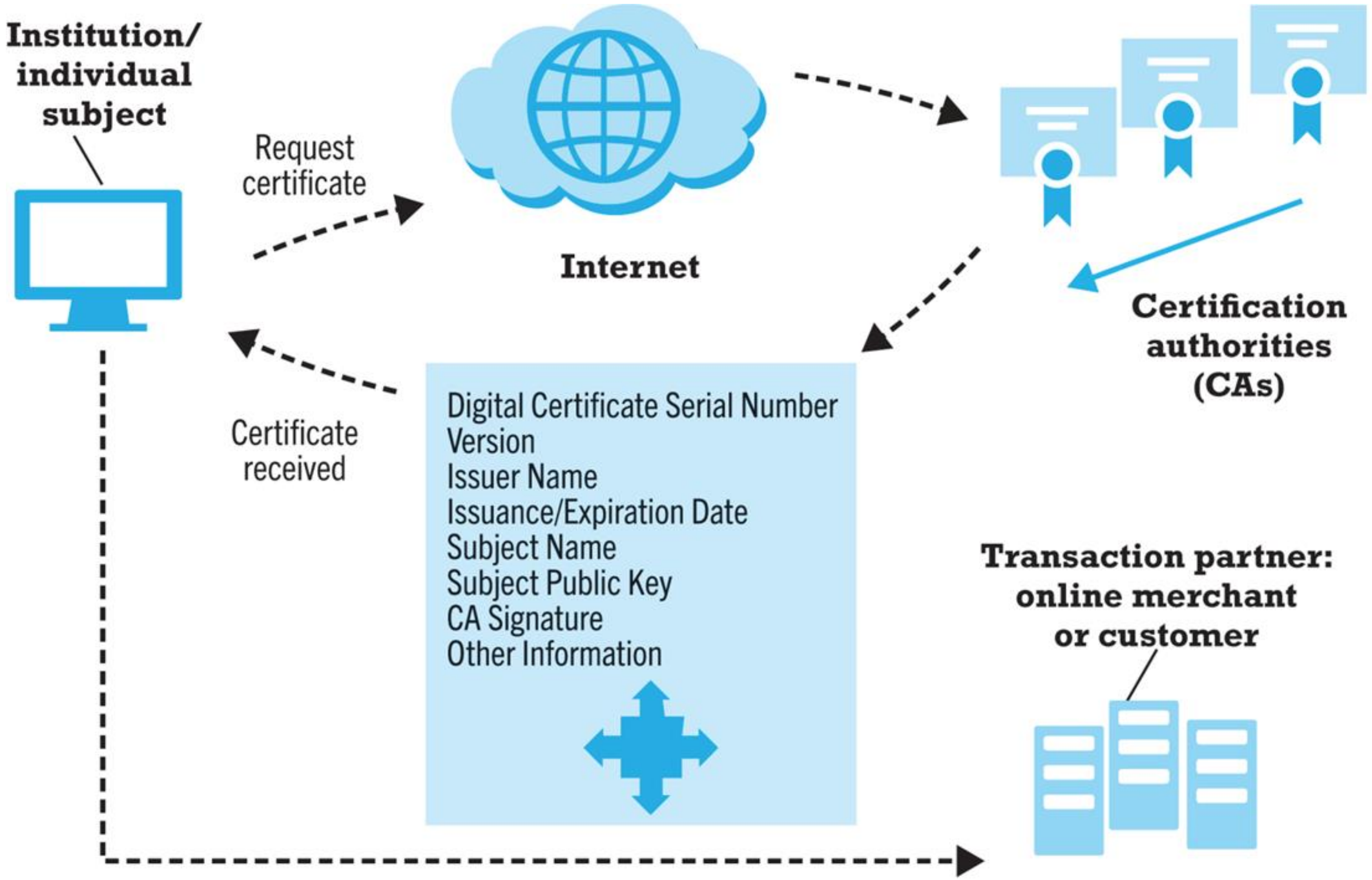
Figure 5.8 Public Key Cryptography: Creating a Digital Envelope



Digital Certificates and Public Key Infrastructure (PKI)

- Digital certificate includes:
  - Name of subject/company
  - Subject’s public key
  - Digital certificate serial number
  - Expiration date, issuance date
  - Digital signature of CA
- Public Key Infrastructure (PKI):
  - CAs and digital certificate procedures
  - PGP

Figure 5.9 Digital Certificates and Certification Authorities



Digital Certificate Serial Number
Version
Issuer Name
Issuance/Expiration Date
Subject Name
Subject Public Key
CA Signature
Other Information

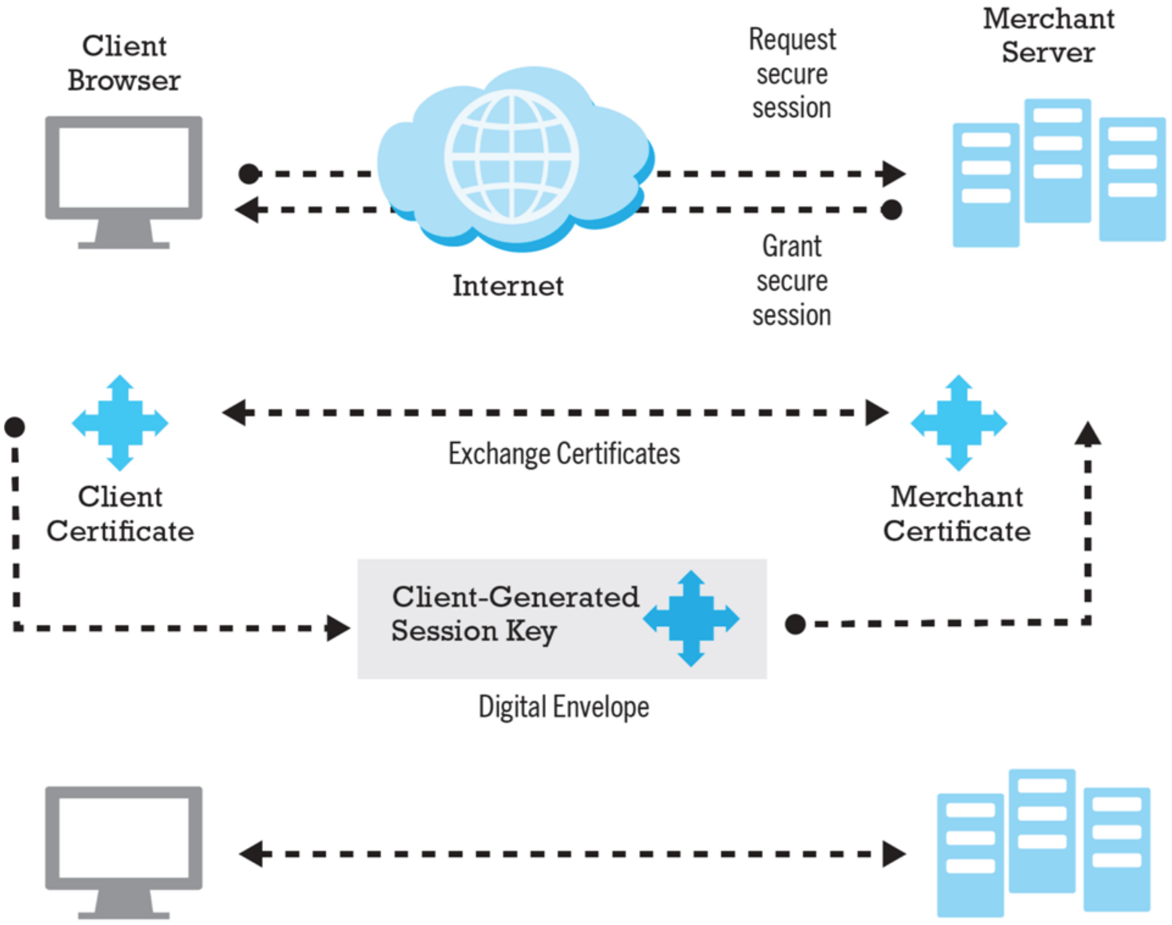
Limitations of PKI

- Doesn’t protect storage of private key
  - PKI not effective against insiders, employees
  - Protection of private keys by individuals may be haphazard
- No guarantee that verifying computer of merchant is secure
- CAs are unregulated, self-selecting organizations

Securing Channels of Communication

- Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
  - Establishes secure, negotiated client-server session
- Virtual Private Network (VPN)
  - Allows remote users to securely access internal network via the Internet
- Wireless (Wi-Fi) networks
  - WPA2
  - WPA3

Figure 5.10 Secure Negotiated Sessions Using TLS



Session ID and methods of encryption negotiated.

Certificates exchanged. Identity of both parties established.

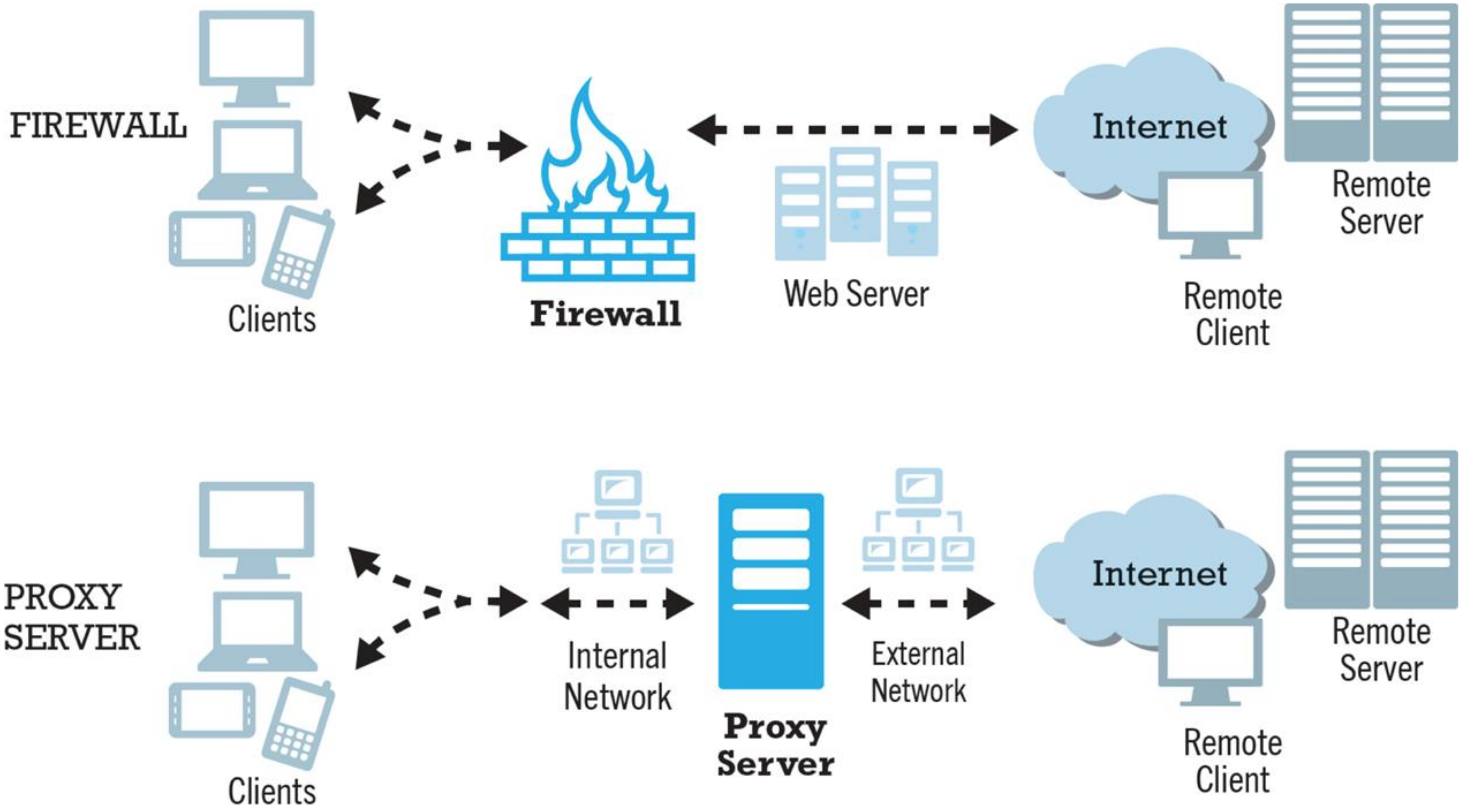
Client generates session key, and uses server public key to create digital envelope. Sends to server. Server decrypts using private key.

Encrypted transmission using client-generated session key begins.

Protecting Networks

- Firewall
  - Hardware or software that uses security policy to filter packets
    - Packet filters
    - Application gateways
  - Next-generation firewalls
- Proxy servers (proxies)
  - Software servers that handle all communications from or sent to the Internet
- Intrusion detection systems
- Intrusion prevention systems

Figure 5.11 Firewalls and Proxy Servers



Protecting Servers and Clients

- Operating system and application software security enhancements
  - Upgrades, patches
- Anti-virus software
  - Easiest and least expensive way to prevent threats to system integrity
  - Requires daily updates

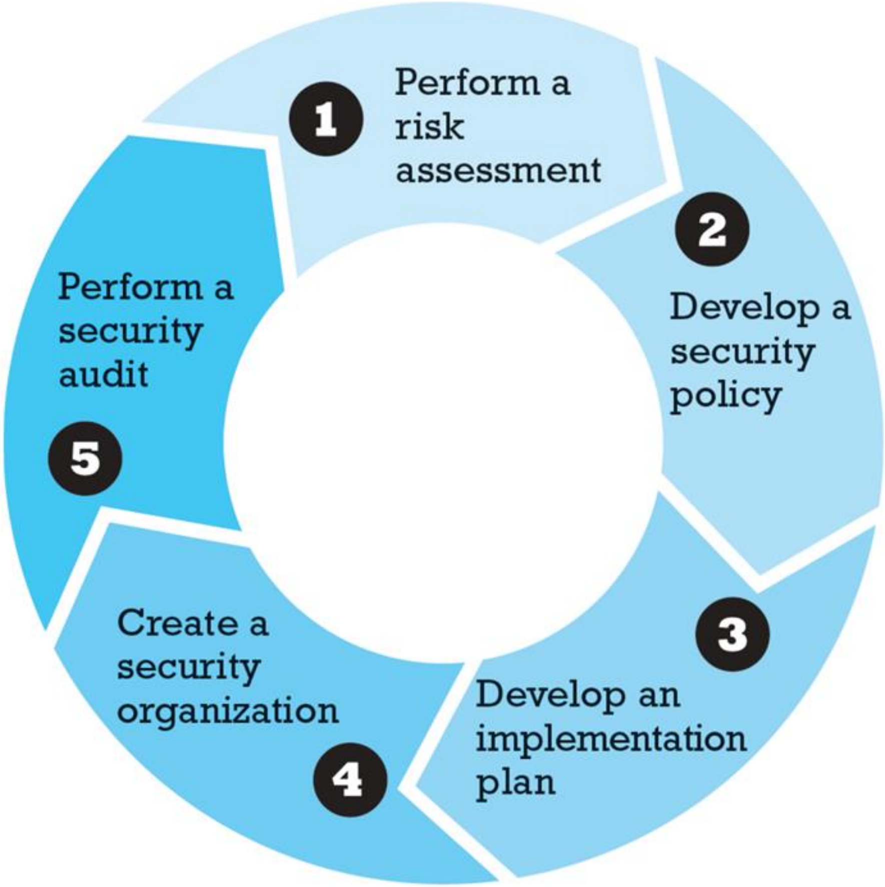
Management Policies, Business Procedures, and Public Laws

- Worldwide, companies spend more than $124 billion on security hardware, software, services
- Managing risk includes:
  - Technology
  - Effective management policies
  - Public laws and active enforcement

A Security Plan: Management Policies

- Risk assessment
- Security policy
- Implementation plan
  - Security organization
  - Access controls
  - Authentication procedures, including biometrics
  - Authorization policies, authorization management systems
- Security audit

Figure 5.12 Developing an E-commerce Security Plan


1
Perform a risk assessment
2
Develop a security policy
3
Develop an implementation plan
4
Create a security organization
5
Perform a security audit

Insight on Business: Are Biometrics the Solution for E-commerce Security?

- Class Discussion
  - What are biometrics?
  - How can the use of biometrics make e-commerce more secure?
  - What are some of the potential dangers in using biometrics?

The Role of Laws and Public Policy

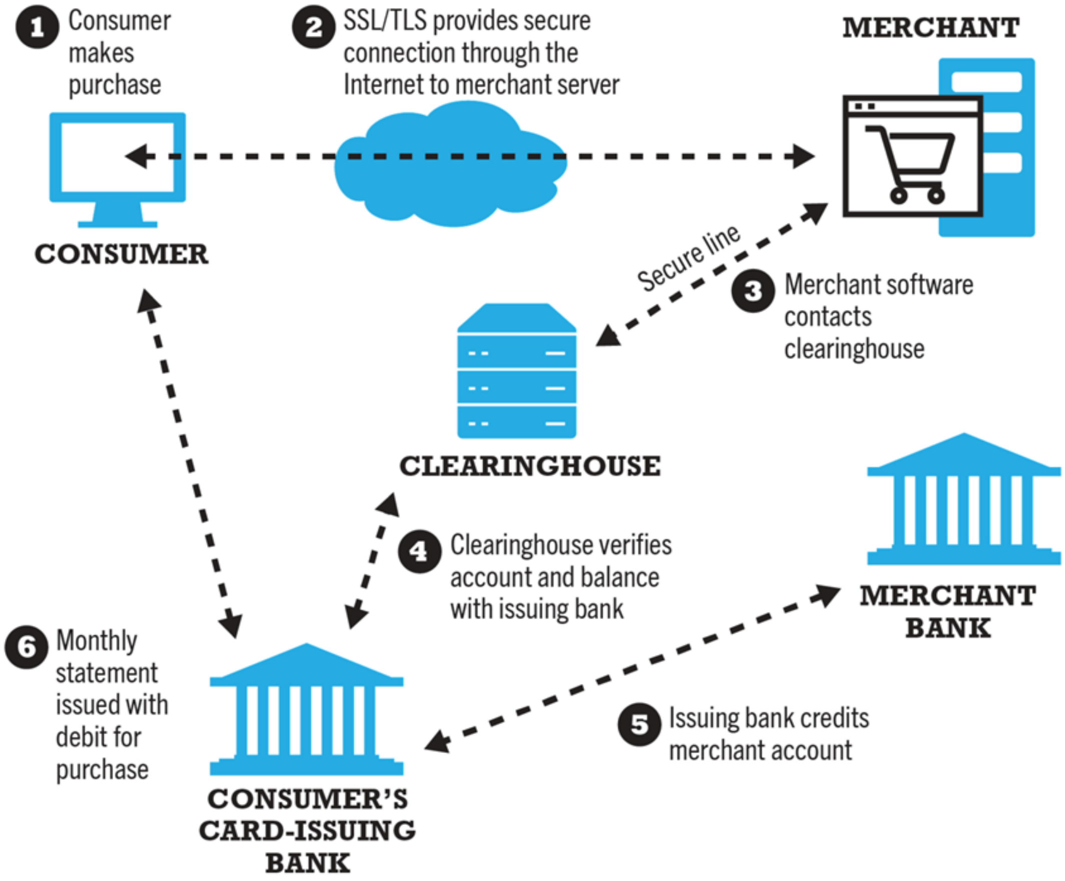
- Laws that give authorities tools for identifying, tracing, prosecuting cybercriminals:
  - USA Patriot Act
  - Homeland Security Act
- Private and private-public cooperation
  - US-CERT
  - CERT Coordination Center
- Government policies and controls on encryption software
  - Organization for Economic Cooperation and Development (OECD), G7, European Council, Wassenar Arrangement

E-commerce Payment Systems

- In U.S., credit and debit cards are primary online payment methods
  - Other countries have different systems
- Online credit card purchasing cycle
- Credit card e-commerce enablers
- Limitations of online credit card payment
  - Security, merchant risk
  - Cost
  - Social equity

Pearson

Figure 5.13 How an Online Credit Card Transaction Works


1 Consumer makes purchase
2 SSL/TLS provides secure connection through the Internet to merchant server
MERCHANT
CONSUMER
Secure line
3 Merchant software contacts clearinghouse
CLEARINGHOUSE
4 Clearinghouse verifies account and balance with issuing bank
MERCHANT BANK
6 Monthly statement issued with debit for purchase
5 Issuing bank credits merchant account
CONSUMER'S CARD-ISSUING BANK

Pearson

Alternative Online Payment Systems

- Online stored value systems:
  - Based on value stored in a consumer’s bank, checking, or credit card account
  - Example: PayPal
- Other alternatives:
  - Amazon Pay
  - Facebook Pay
  - Visa Checkout, Mastercard’s MasterPass

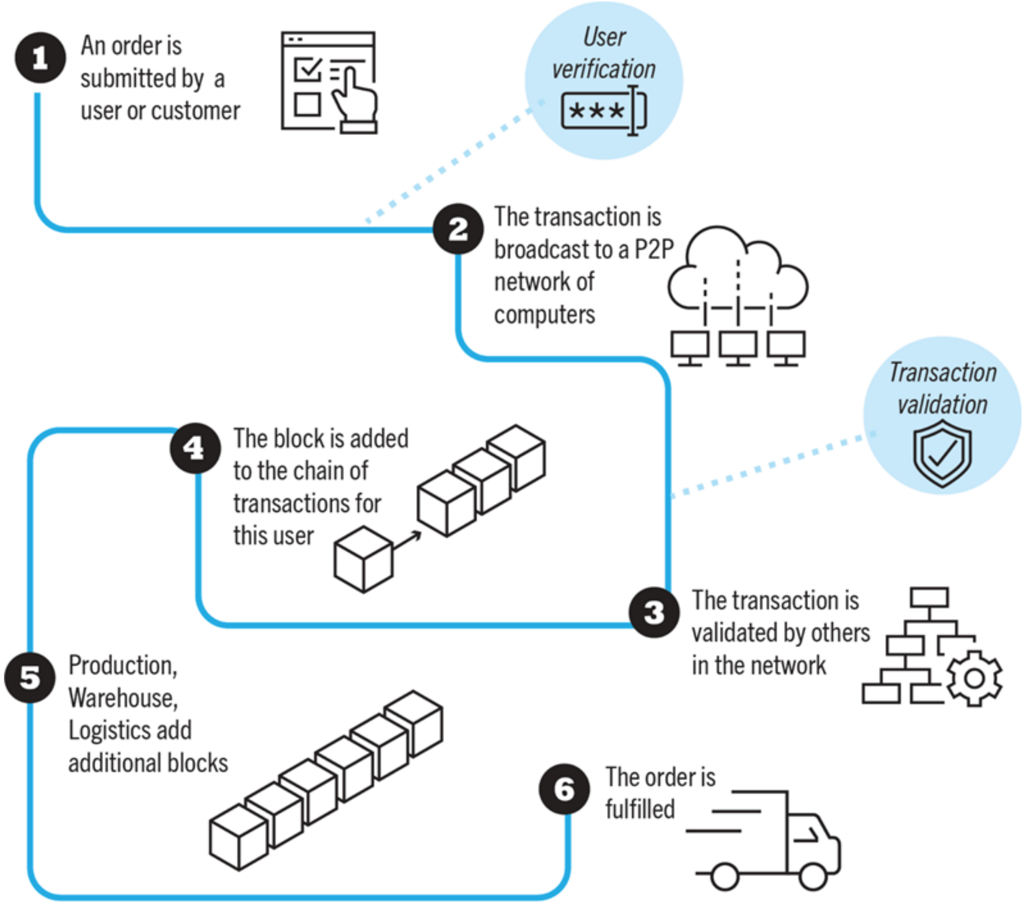
Mobile Payment Systems

- Use of mobile phones as payment devices
  - Established in Europe and Asia
  - Expanding in United States
- Near field communication (NFC) and QR codes
- Different types of mobile wallets
  - Universal proximity mobile wallet apps, such as Apple Pay, Google Pay, Samsung Pay
  - Branded store proximity wallet apps, offered by Walmart, Target, Starbucks, others
  - P2P mobile payment apps, such as Zelle, Venmo, Square Cash

Blockchain

- Blockchain
  - Enables organizations to create and verify transactions nearly instantaneously using a distributed P2P database (distributed ledger)
- Benefits:
  - Reduces costs of verifying users, validating transactions, and risks of storing and processing transaction information
  - Transactions cannot be altered retroactively and therefore are more secure
- Foundation technology for cryptocurrencies and supply chain management, as well as potential applications in financial services and healthcare industries

Figure 5.15 How Blockchain Works


1
An order is submitted by a user or customer
User verification
***
2
The transaction is broadcast to a P2P network of computers
Transaction validation
3
The transaction is validated by others in the network
4
The block is added to the chain of transactions for this user
5
Production, Warehouse, Logistics add additional blocks
6
The order is fulfilled

Cryptocurrencies

- Use blockchain technology and cryptography to create a purely digital medium of exchange
- Bitcoin the most prominent example
  - Value of Bitcoins have widely fluctuated
  - Major issues with theft and fraud
  - Some governments have banned Bitcoin, although it is gaining acceptance in the U.S.
- Other cryptocurrencies (altcoins) include Ethereum/Ether, Ripple, Litecoin and Monero
- Initial coin offerings (ICOs) being used by some startups to raise capital

Electronic Billing Presentment and Payment (EBPP)

- Online payment systems for monthly bills
- Four EBPP business models:
  - Online banking model (most widely used)
  - Biller-direct
  - Mobile
  - Consolidator
- All models are supported by EBPP infrastructure providers

Careers in E-commerce

- Position: Cybersecurity Threat Management Team Trainee
- Qualification/Skills
- Preparing for the Interview
- Possible Interview Questions

Copyright