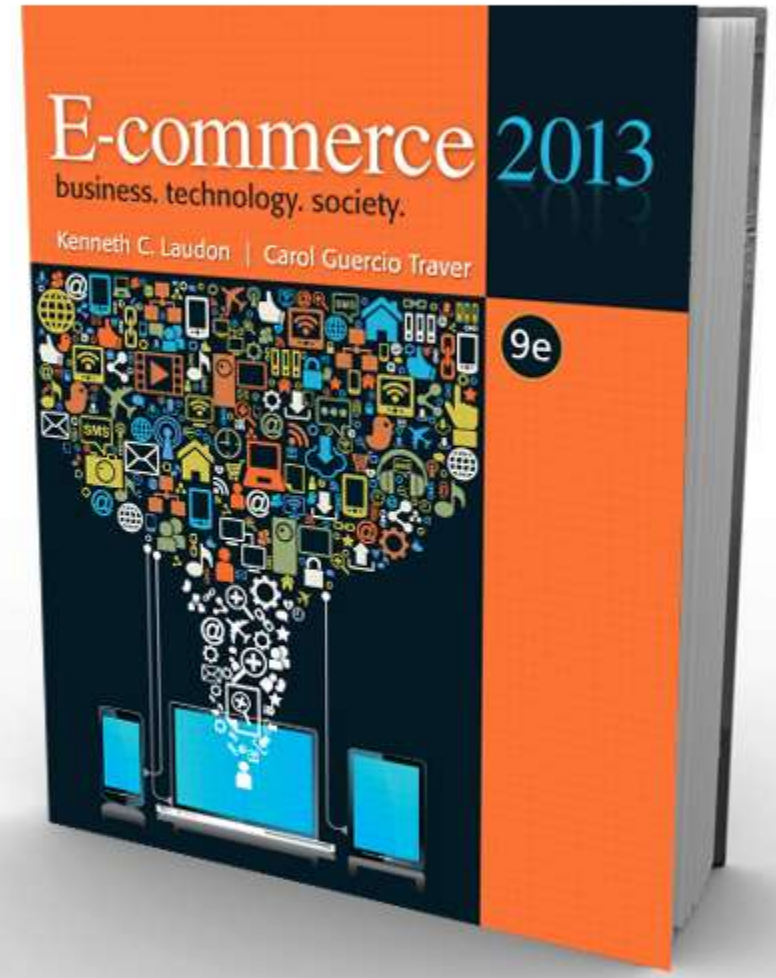

E-commerce 2013

business. technology. society.

ninth edition

Kenneth C. Laudon

Carol Guercio Traver

Copyright © 2013 Pearson Education, Inc.

Chapter 5

E-commerce Security and Payment Systems

أمن التجارة الإلكترونية وأنظمة الدفع

Copyright © 2013 Pearson Education, Inc.

Class Discussion

Cyberwar: MAD 2.0 سيبيروار: ماد 2.0

- **What is the difference between hacking and cyberwar?**
- **Why has cyberwar become more potentially devastating in the past decade?**
- **Why has Google been the target of so many cyberattacks?**
- **Is it possible to find a political solution to MAD 2.0?**

ما هو الفرق بين القرصنة والحرب السيبرانية؟
لماذا أصبح الحرب السيبرانية أكثر مدمرة في العقد الماضي؟
لماذا كانت غوغل هدفا لعدد كبير من الهجمات الإلكترونية؟
هل من الممكن إيجاد حل سياسي ل 2.0 درهم؟

Copyright © 2013 Pearson Education, Inc.

The E-commerce Security Environment
بيئة أمن التجارة الإلكترونية

- **Overall size and losses of cybercrime unclear**
  - Reporting issues
- **2011 CSI survey: 46% of respondent firms detected breach in last year**
- **Underground economy marketplace:**
  - Stolen information stored on underground economy servers

الحجم الكلي للخسائر السيبرانية وخسائرها غير واضحة
الإبلاغ عن المشكلات
2011 مسح كسي: كشفت 46٪ من الشركات المستجيبة عن خرق في العام الماضي
سوق الاقتصاد تحت الأرض:
المعلومات المسروقة المخزنة على خوادم الاقتصاد تحت الأرض

Copyright © 2013 Pearson Education, Inc.

What Is Good E-commerce Security?
ما هو جيد التجارة الإلكترونية الأمن؟

- **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

لتحقيق أعلى درجة من الأمن

التكنولوجيات الجديدة

السياسات والإجراءات التنظيمية

معايير الصناعة والقوانين الحكومية

عوامل اخرى

القيمة الوقتية للمال

تكلفة الأمن مقابل الخسارة المحتملة

الأمن في كثير من الأحيان يكسر في أضعف صلة

Copyright © 2013 Pearson Education, Inc.

The E-commerce Security Environment
بيئة أمن التجارة الإلكترونية

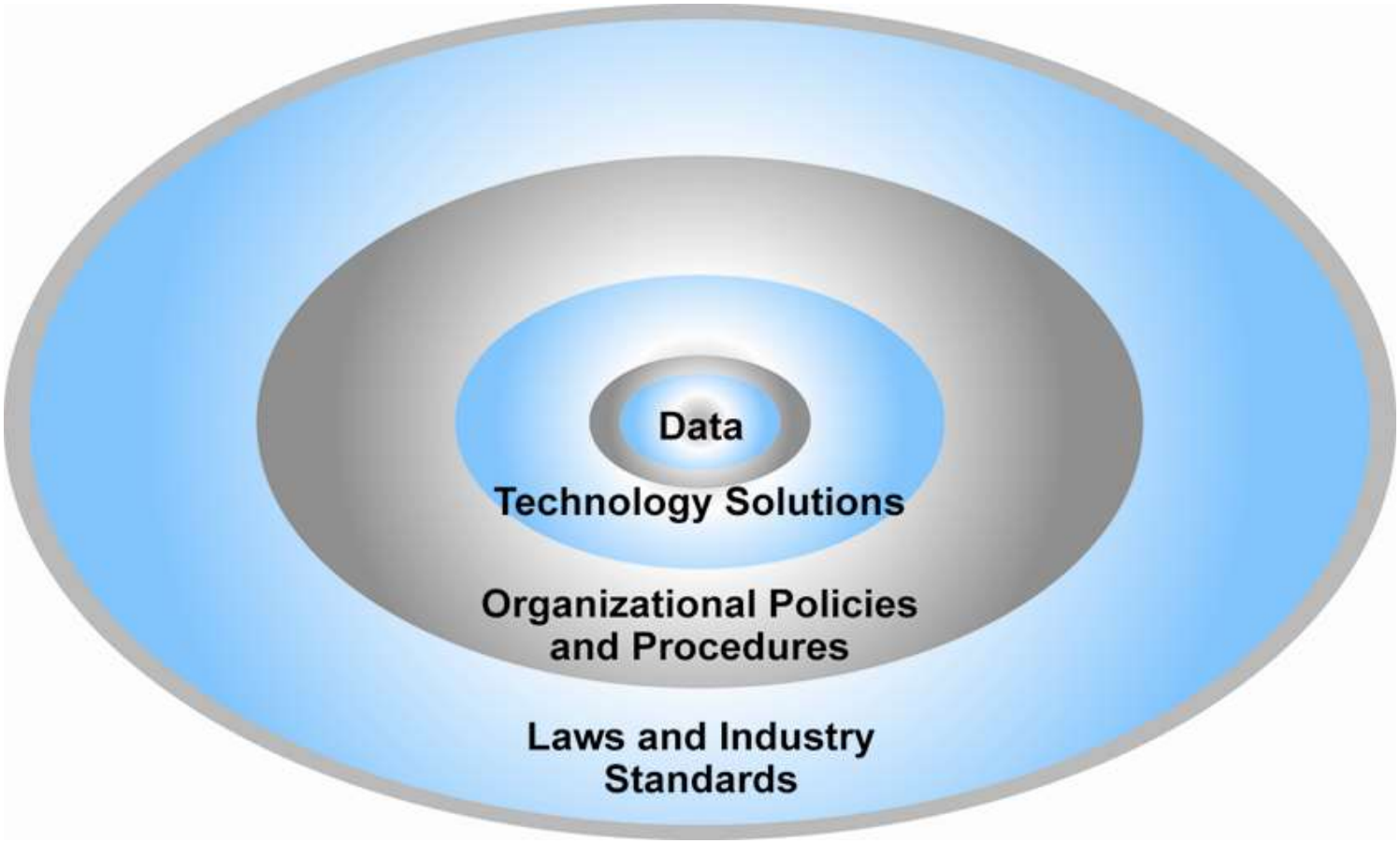

Figure 5.1, Page 266

Copyright © 2013 Pearson Education, Inc.

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?

Table 5.3, Page 267

Copyright © 2013 Pearson Education, Inc.

The Tension Between Security and Other Values
التوتر بين الأمن والقيم الأخرى

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

سهولة الاستعمال
وكلما زادت الإجراءات الأمنية، زاد صعوبة استخدام الموقع، وأبطأ يصبح
السلامة العامة والاستخدامات الإجرامية للإنترنت
استخدام المجرمين للتكنولوجيا في التخطيط للجرائم أو تهديد الدولة القومية

Copyright © 2013 Pearson Education, Inc.

Security Threats in the E-commerce Environment

التهديدات الأمنية في بيئة التجارة الإلكترونية

- **Three key points of vulnerability in e-commerce environment:**

1. Client
2. Server
3. Communications pipeline (Internet communications channels)

ثلاث نقاط رئيسية من الضعف في بيئة التجارة الإلكترونية:

زبون

الخادم

خط أنابيب الاتصالات (قنوات اتصالات الإنترنت)

Copyright © 2013 Pearson Education, Inc.

A Typical E-commerce Transaction
عملية نموذجية للتجارة الإلكترونية

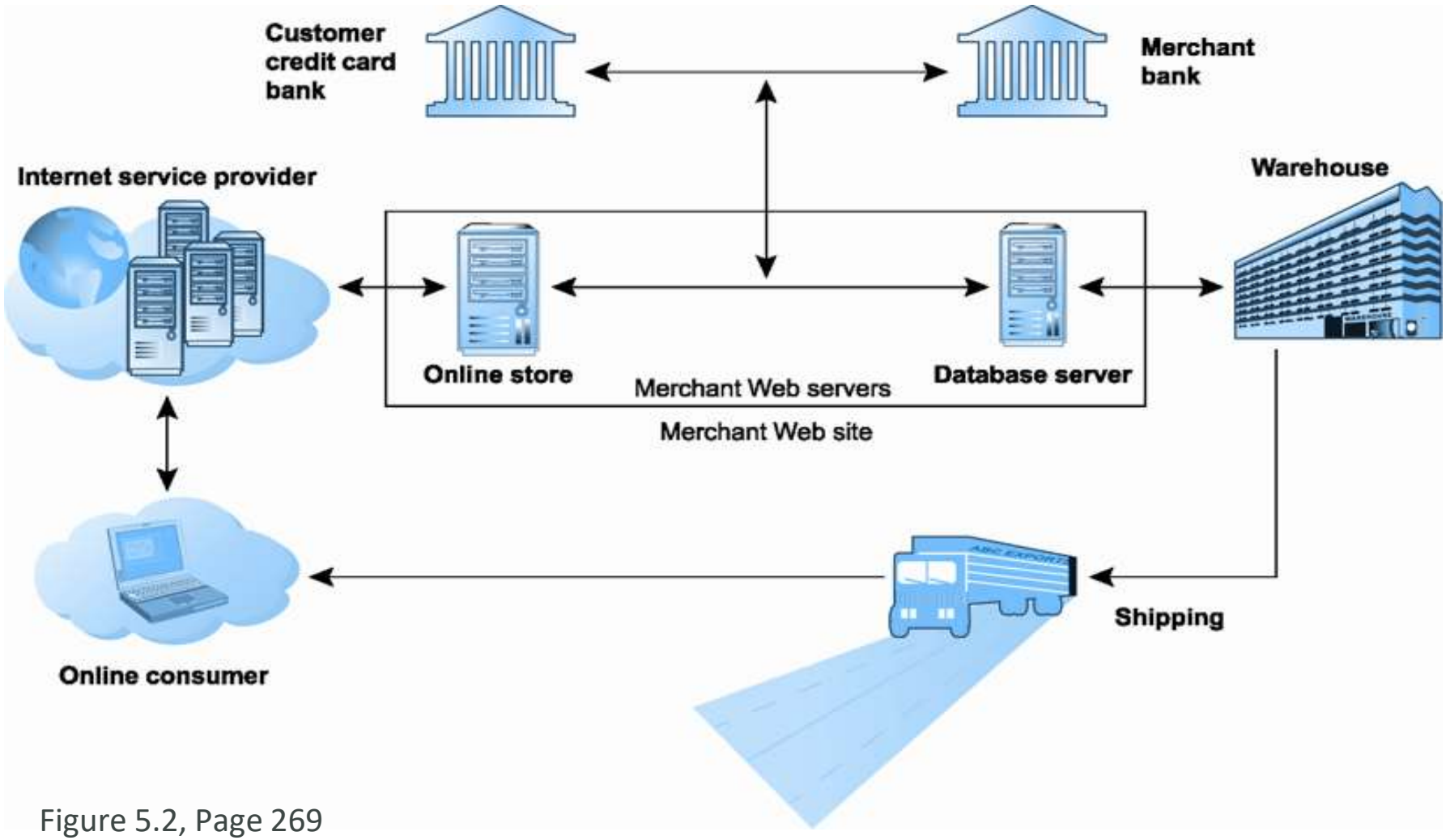

Figure 5.2, Page 269

Copyright © 2013 Pearson Education, Inc.

Vulnerable Points in an E-commerce Transaction
نقاط الضعف في معاملة التجارة الإلكترونية

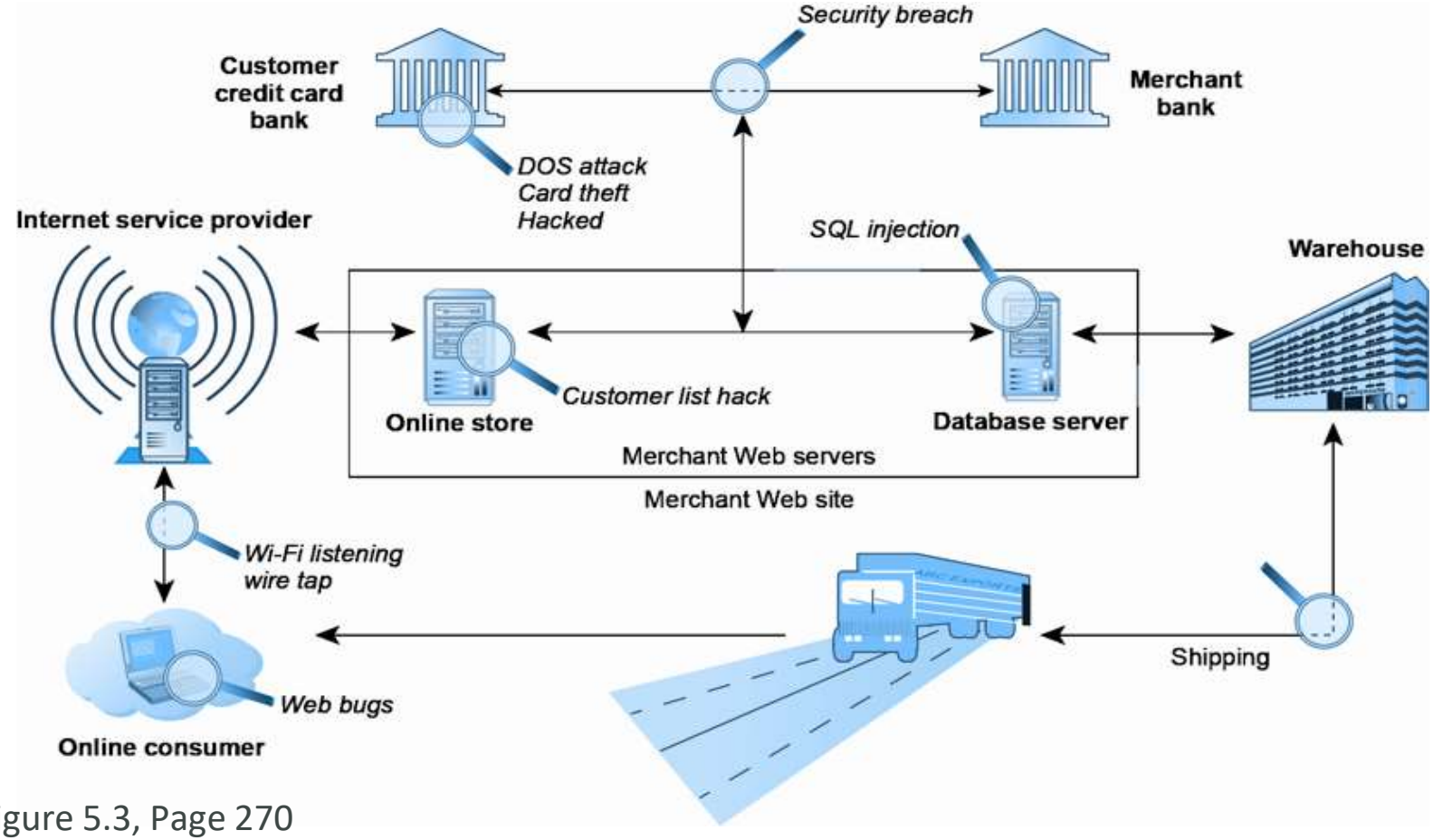

Figure 5.3, Page 270

Copyright © 2013 Pearson Education, Inc.

Most Common Security Threats in the E-commerce Environment

التهديدات الأمنية الأكثر شيوعا في بيئة التجارة الإلكترونية

- **Malicious code**
  - Viruses
  - Worms
  - Trojan horses
  - Drive-by downloads
  - Backdoors
  - Bots, botnets
  - Threats at both client and server levels

شفرة ضارة

الفيروسات

ديدان

أحصنة طروادة

دريف من خلال التنزيلات

خلفي

السير، بوتنيتس

التهديدات على مستوى العميل

والخادم

Copyright © 2013 Pearson Education, Inc.

Most Common Security Threats (cont.)

- **Potentially unwanted programs (PUPs)**
  - Browser parasites
  - Adware
  - Spyware
- **Phishing**
  - E-mail scams
  - Social engineering
  - Identity theft

البرامج غير المرغوب فيها المحتملة (الجراء)

طفيليات المتصفح

ادواري

برامج التجسس

الخداع

البريد الإلكتروني الحيل

هندسة اجتماعية

سرقة الهوية

Copyright © 2013 Pearson Education, Inc.

Most Common Security Threats (cont.)

- **Hacking**
  - Hackers vs. crackers
  - Types of hackers: White, black, grey hats
  - Hacktivism
- **Cybervandalism:**
  - Disrupting, defacing, destroying Web site
- **Data breach**
  - Losing control over corporate information to outsiders

القرصنة

القراصنة مقابل المفرقعات

أنواع القراصنة: أبيض، أسود، القبعات الرمادية

النضال البرمجي

التخريب السيبراني:

تعطيل، تشويه، تدمير موقع ويب

خرق البيانات

فقدان السيطرة على معلومات الشركات إلى الغرباء

Copyright © 2013 Pearson Education, Inc.

Most Common Security Threats (cont.)

- **Credit card fraud/theft**
  - Hackers target merchant servers; use data to establish credit under false identity
- **Spoofing (Pharming)**
- **Spam (junk) Web sites**
- **Denial of service (DoS) attack**
  - Hackers flood site with useless traffic to overwhelm network
- **Distributed denial of service (DDoS) attack**

الاحتيال على بطاقة الائتمان / السرقة

الهاكرز تستهدف خوادم التاجر.

استخدام البيانات لإنشاء الائتمان تحت هوية زائفة

سبوفينغ (فارمينغ)

الرسائل غير المرغوب فيها (غير المرغوب فيه) مواقع ويب

الحرمان من الخدمة (دوس) الهجوم

قراصنة موقع الفيضانات مع حركة المرور عديمة الفائدة لتطغى الشبكة

هجوم رفض الخدمة الموزع (دوس)

Copyright © 2013 Pearson Education, Inc.

Insight on Business: Class Discussion

Sony: Press the Reset Button
سوني: اضغط على زر إعادة الضبط

- **What organization and technical failures led to the April 2011 data breach on the PlayStation Network?**
- **Can Sony be criticized for waiting 3 days to inform the FBI?**
- **Have you or anyone you know experienced data theft?**

ما الفشل التنظيمي والفني أدى إلى خرق البيانات أبريل 2011 على شبكة بلاي ستيشن؟

هل يمكن انتقاد سوني للانتظار 3 أيام لإبلاغ مكتب التحقيقات الفدرالي؟

هل أنت أو أي شخص تعرفه سرقة البيانات من ذوي الخبرة؟

Copyright © 2013 Pearson Education, Inc.

Most Common Security Threats (cont.)

- **Sniffing**
  - Eavesdropping program that monitors information traveling over a network
- **Insider attacks**
- **Poorly designed server and client software**
  - Social network security issues
- **Mobile platform security issues**
  - Same risks as any Internet device
- **Cloud security issues**

استنشاق

برنامج التنصت الذي يراقب المعلومات التي تسافر عبر الشبكة

هجمات من الداخل

تصميم خادم وبرنامج عميل

ضعيف التصميم

مشكلات أمان الشبكة الاجتماعية

القضايا الأمنية منصة المحمول

نفس المخاطر مثل أي جهاز إنترنت

القضايا الأمنية السحابية

Copyright © 2013 Pearson Education, Inc.

Insight on Technology: Class Discussion

Think Your Smartphone Is Secure?
هل تعتقد أن هاتفك الذكي آمن؟

- **What types of threats do smartphones face?**
- **Are there any particular vulnerabilities to this type of device?**
- **What did Nicolas Seriot's "Spyphone" prove?**
- **Are apps more or less likely to be subject to threats than traditional PC software programs?**

ما هي أنواع التهديدات التي تواجهها الهواتف الذكية؟
هل هناك أي نقاط ضعف معينة لهذا النوع من الأجهزة؟
ما الذي أثبته نيكولا سيريوت "سبيفون"؟
هل التطبيقات أكثر أو أقل عرضة للتعرض للتهديدات من برامج الكمبيوتر التقليدية؟

Copyright © 2013 Pearson Education, Inc.

Technology Solutions حلول التكنولوجيا

- **Protecting Internet communications**
  - Encryption
- **Securing channels of communication**
  - SSL, VPNs
- **Protecting networks**
  - Firewalls
- **Protecting servers and clients**

حماية اتصالات الإنترنت

التشفير

تأمين قنوات الاتصال

سل، فين

حماية الشبكات

الجدران النارية

حماية الخوادم والعملاء

Copyright © 2013 Pearson Education, Inc.

Tools Available to Achieve Site Security
الأدوات المتاحة لتحقيق أمن الموقع

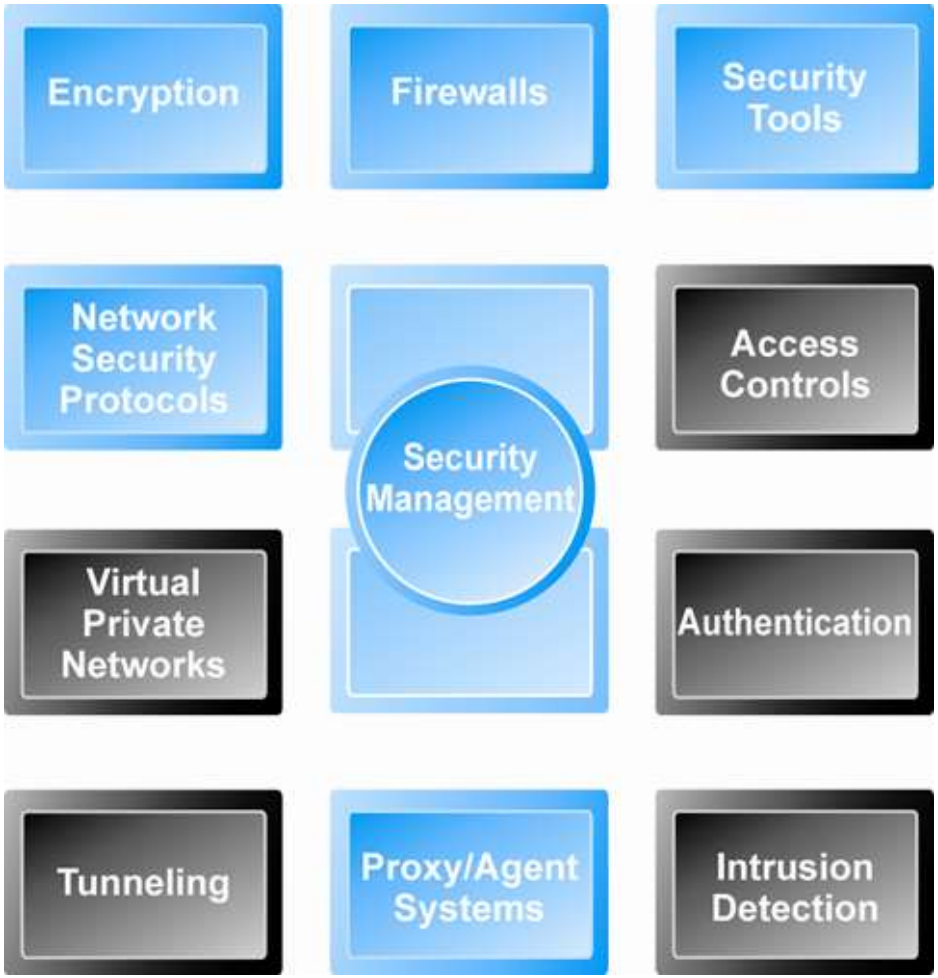

Figure 5.5, Page 288

Copyright © 2013 Pearson Education, Inc.

Encryption التشفير

- **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

التشفير

يحول البيانات إلى نص الشفرات للقراءة فقط من قبل المرسل والمتلقي

يضمن المعلومات المخزنة ونقل المعلومات

يوفر 4 من 6 أبعاد رئيسية للأمن التجارة الإلكترونية:

سلامة الرسالة

عدم التنصل

المصادقة

سرية

Copyright © 2013 Pearson Education, Inc.

Symmetric Key Encryption تشفير مفتاح متماثل

- **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 used to encrypt data
- **Advanced Encryption Standard (AES)**
  - Most widely used symmetric key encryption
  - Uses 128-, 192-, and 256-bit encryption keys
- **Other standards use keys with up to 2,048 bits**

المرسل والمتلقي استخدام نفس المفتاح الرقمي لتشفير وفك تشفير الرسالة
يتطلب مجموعة مختلفة من المفاتيح لكل معاملة
قوة التشفير
طول المفتاح الثنائي المستخدم لتشفير البيانات
معيار التشفير المتقدم (إس)
الأكثر استخداما على نطاق واسع التشفير مفتاح متماثل
يستخدم مفاتيح التشفير 128-، 192-، و 256 بت
معايير أخرى تستخدم مفاتيح مع ما يصل إلى 2،048 بت

Copyright © 2013 Pearson Education, Inc.

Public Key Encryption تشفير المفتاح العمومي

- **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**

يستخدم اثنين من مفاتيح رقمية ذات صلة رياضيا
المفتاح العام (نشر على نطاق واسع)
مفتاح خاص (يبقى سرية من قبل المالك)
كلا المفاتيح المستخدمة لتشفير وفك تشفير الرسالة
مرة واحدة مفتاح تستخدم لتشفير الرسالة، لا يمكن أن تستخدم نفس المفتاح لفك تشفير الرسالة
يستخدم المرسل المفتاح العمومي للمستلم لتشفير الرسالة؛ يستخدم المستلم مفتاح خاص لفك تشفيره

Copyright © 2013 Pearson Education, Inc.

Public Key Cryptography: A Simple Case
تشفير المفتاح العمومي: حالة بسيطة

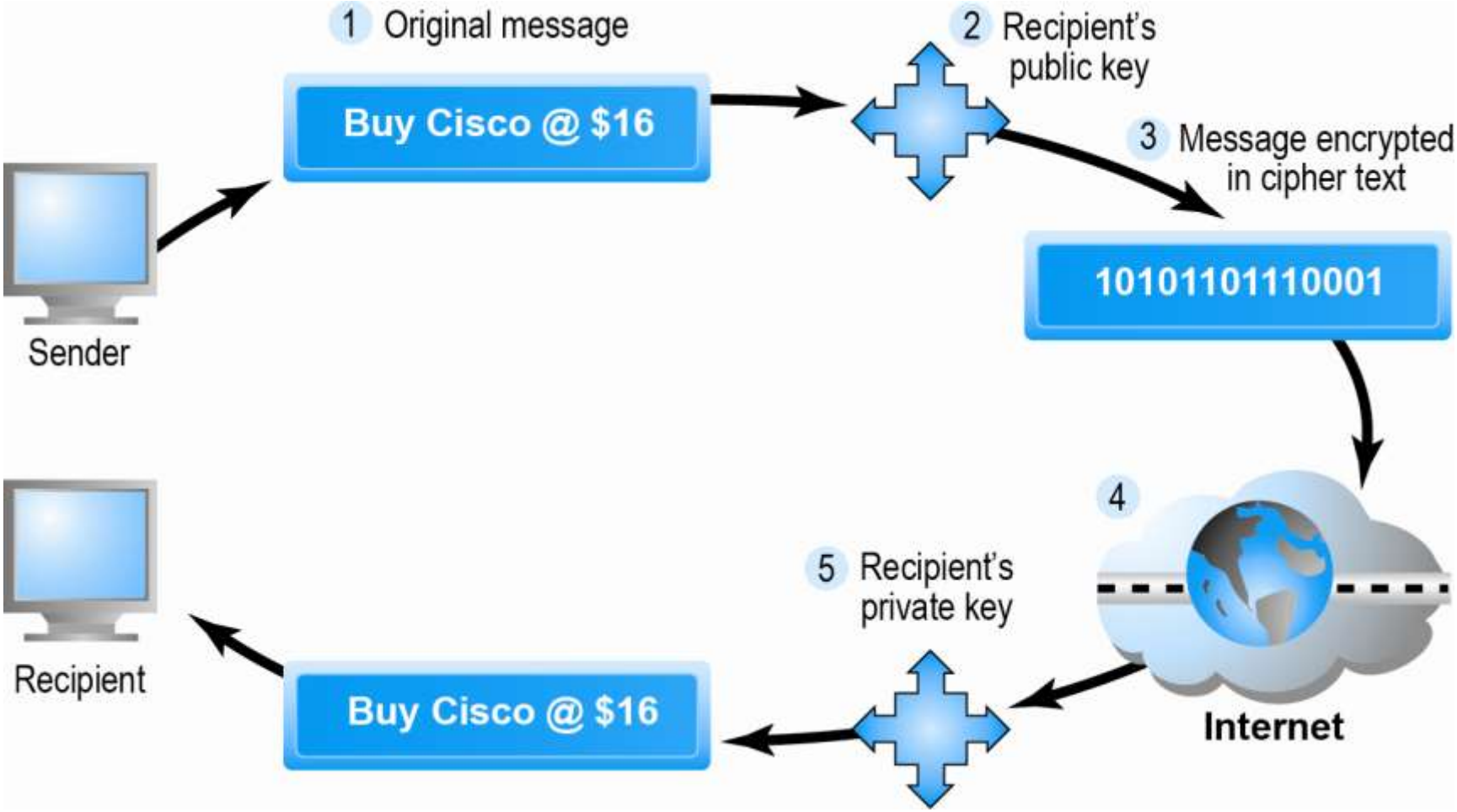

Figure 5.6, Page 291

Copyright © 2013 Pearson Education, Inc.

Public Key Encryption using Digital Signatures and Hash Digests

تشفير المفتاح العمومي باستخدام التوقيعات الرقمية و هاش ديجيستس

- **Hash function:**
  - Mathematical algorithm that produces fixed-length number called message or hash digest
- **Hash digest of message sent to recipient along with message to verify integrity**
- **Hash digest and message encrypted with recipient's public key**
- **Entire cipher text then encrypted with recipient's private key—creating digital signature—for authenticity, nonrepudiation**

دالة تجزئة:
الخوارزمية الرياضية التي تنتج رقم ثابت طول يسمى رسالة أو هضم هاش
تجزئة ملخص الرسالة المرسلة إلى المستلم مع رسالة للتحقق من السلامة
هاش هضم ورسالة مشفرة مع المفتاح العمومي للمستلم
النص الكامل الشفرات ثم مشفرة مع المفتاح الخاص إنشاء التوقيع الرقمي للمستلم - للأصالة، نونريبودياتيون

Copyright © 2013 Pearson Education, Inc.

Public Key Cryptography with Digital Signatures
تشفير المفتاح العمومي مع التوقيعات الرقمية

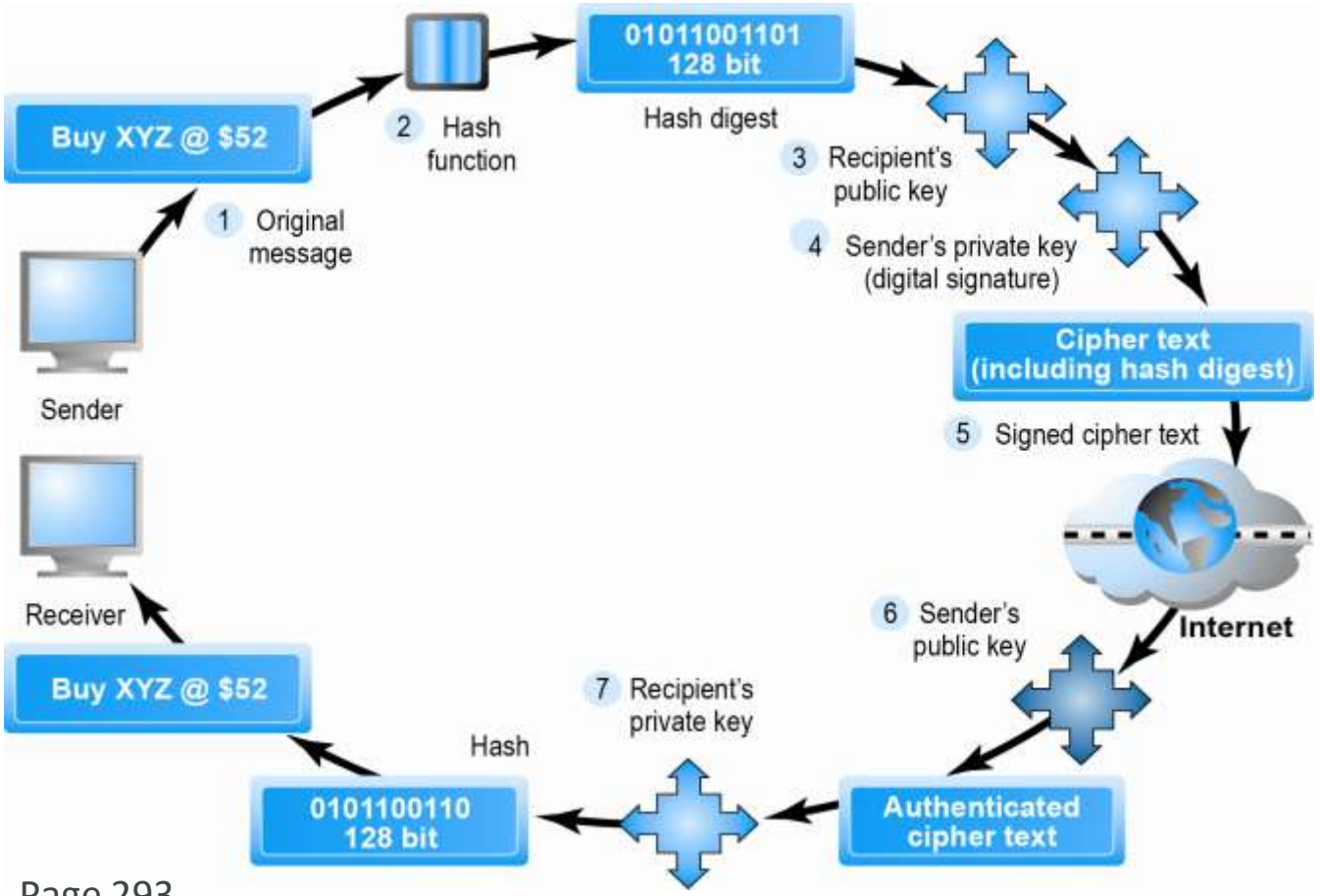

Figure 5.7, Page 293

Copyright © 2013 Pearson Education, Inc.

Digital Envelopes المغلفات الرقمية

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

نقاط ضعف العنوان:

تشفير المفتاح العمومي
بطيئة حسابيا، وانخفاض سرعة انتقال، وزيادة وقت المعالجة

تشفير المفتاح المتماثل
خطوط نقل غير آمنة

يستخدم التشفير مفتاح متماثل لتشفير الوثيقة

يستخدم تشفير المفتاح العمومي لتشفير وإرسال مفتاح متماثل

Copyright © 2013 Pearson Education, Inc.

Creating a Digital Envelope إنشاء مغلف رقمي

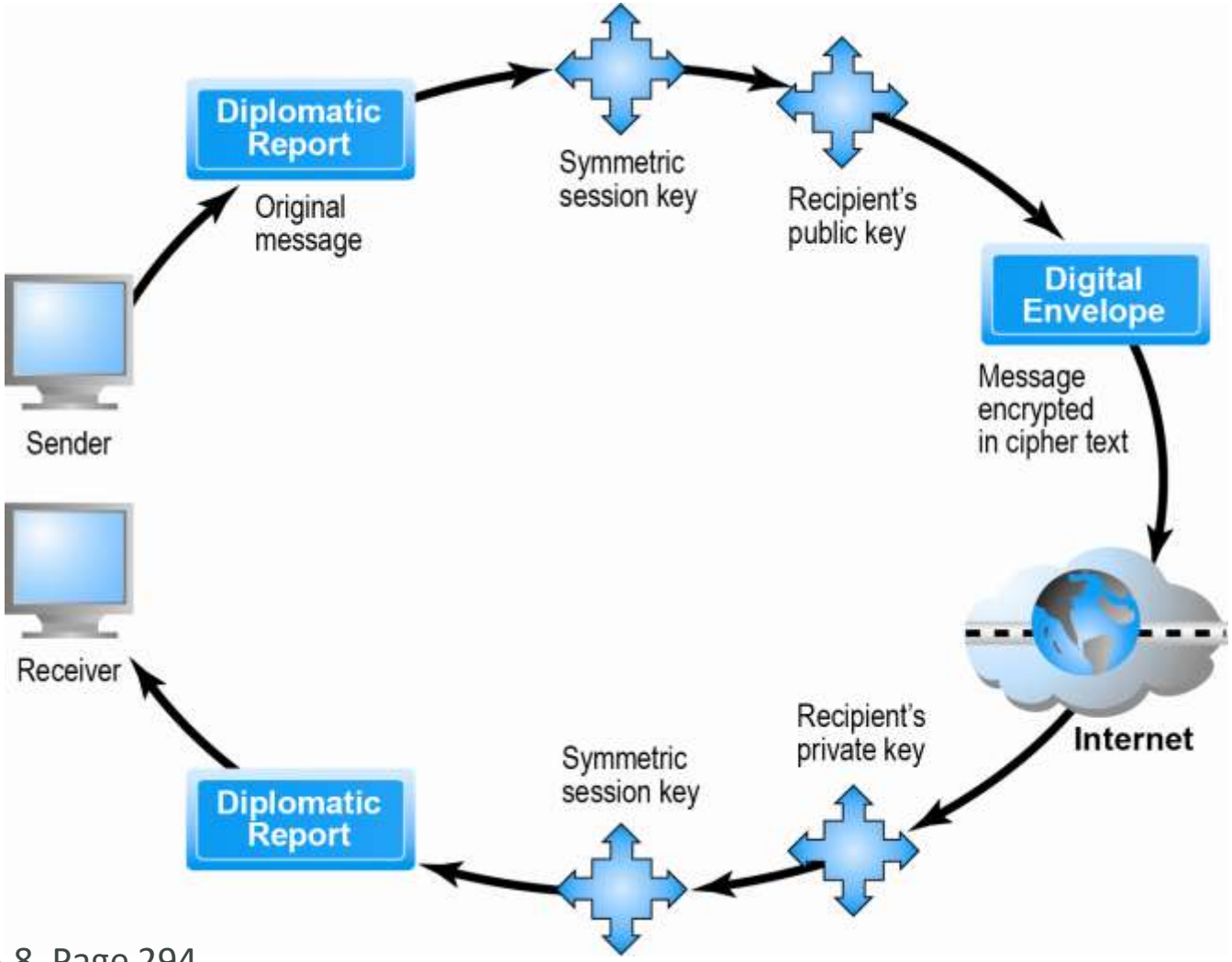

Figure 5.8, Page 294

Copyright © 2013 Pearson Education, Inc.

Digital Certificates and Public Key Infrastructure (PKI)
الشهادات الرقمية والبنية التحتية للمفاتيح العمومية (يكي)

- **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

وتشمل الشهادة الرقمية:

اسم الموضوع / الشركة

المفتاح العام للموضوع

الرقم التسلسلي لشهادة رقمية

تاريخ انتهاء الصلاحية، تاريخ الإصدار

التوقيع الرقمي من كا

البنية التحتية للمفاتيح العمومية (يكي):

كا وإجراءات الشهادة الرقمية

PGP

Copyright © 2013 Pearson Education, Inc.

Digital Certificates and Certification Authorities
الشهادات الرقمية وسلطات التصديق

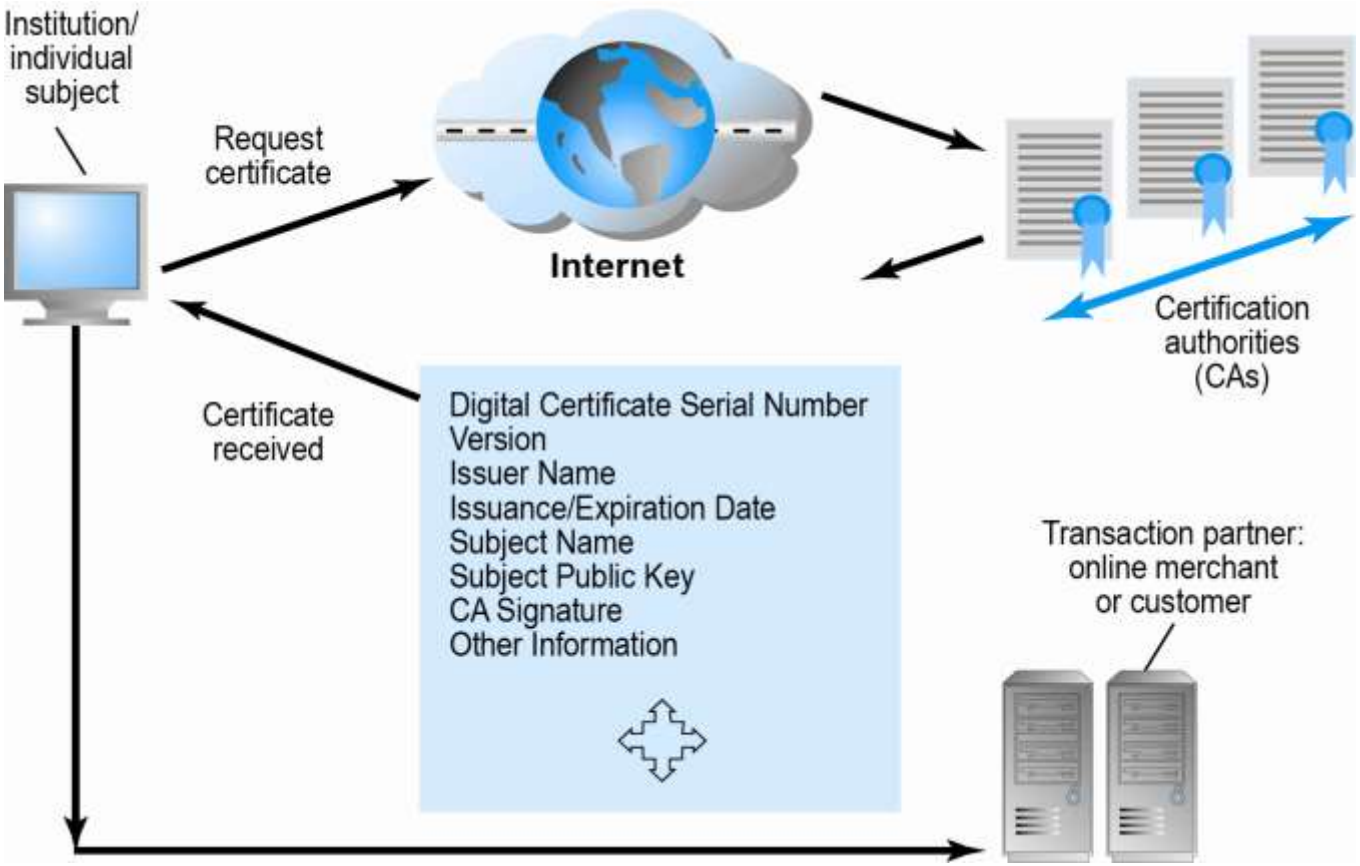

Figure 5.9, Page 295

Copyright © 2013 Pearson Education, Inc.

Limits to Encryption Solutions حدود لحلول التشفير

- **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**

لا يحمي تخزين المفتاح الخاص
يكي غير فعالة ضد المطلعين،
والموظفين
حماية المفاتيح الخاصة من قبل الأفراد
قد تكون عشوائية
لا يضمن أن التحقق من جهاز كمبيوتر التاجر آمن
السلطات الكاثوليكية هي منظمات غير منظمة وذات اختيار ذاتي

Copyright © 2013 Pearson Education, Inc.

Insight on Society: Class Discussion

Web Dogs and Anonymity: Identity 2.0
ويب كلابس آند أنونيمنيتي: إيدنتيتي 2.0

- **What are some of the benefits of continuing the anonymity of the Internet?**
- **What are the disadvantages of an identity system?**
- **Are there advantages to an identity system beyond security?**
- **Who should control a central identity system?**

ما هي بعض فوائد استمرار عدم الكشف عن هوية الإنترنت؟
ما هي عيوب نظام الهوية؟
هل هناك مزايا لنظام هوية يتجاوز الأمن؟
من يجب أن يتحكم في نظام الهوية المركزي؟

Copyright © 2013 Pearson Education, Inc.

Securing Channels of Communication
تأمين قنوات الاتصال

- **Secure Sockets Layer (SSL) and Transport Layer Security (TLS)**
  - Establishes a secure, negotiated client-server session in which URL of requested document, along with contents, is encrypted
- **Virtual Private Network (VPN):**
  - Allows remote users to securely access internal network via the Internet

طبقة المقابس الآمنة (سل) وأمن طبقة النقل (تلس)

إنشاء جلسة عمل عميل متفاوض عليها آمنة يتم فيها تشفير عنوان ورل للوثيقة المطلوبة بالإضافة إلى المحتويات

الشبكة الافتراضية الخاصة (فين):

السماح للمستخدمين عن بعد بالوصول الآمن إلى الشبكة الداخلية عبر الإنترنت

Copyright © 2013 Pearson Education, Inc.

Secure Negotiated Sessions Using SSL/TLS

تأمين جلسات التفاوض باستخدام سل / تلس

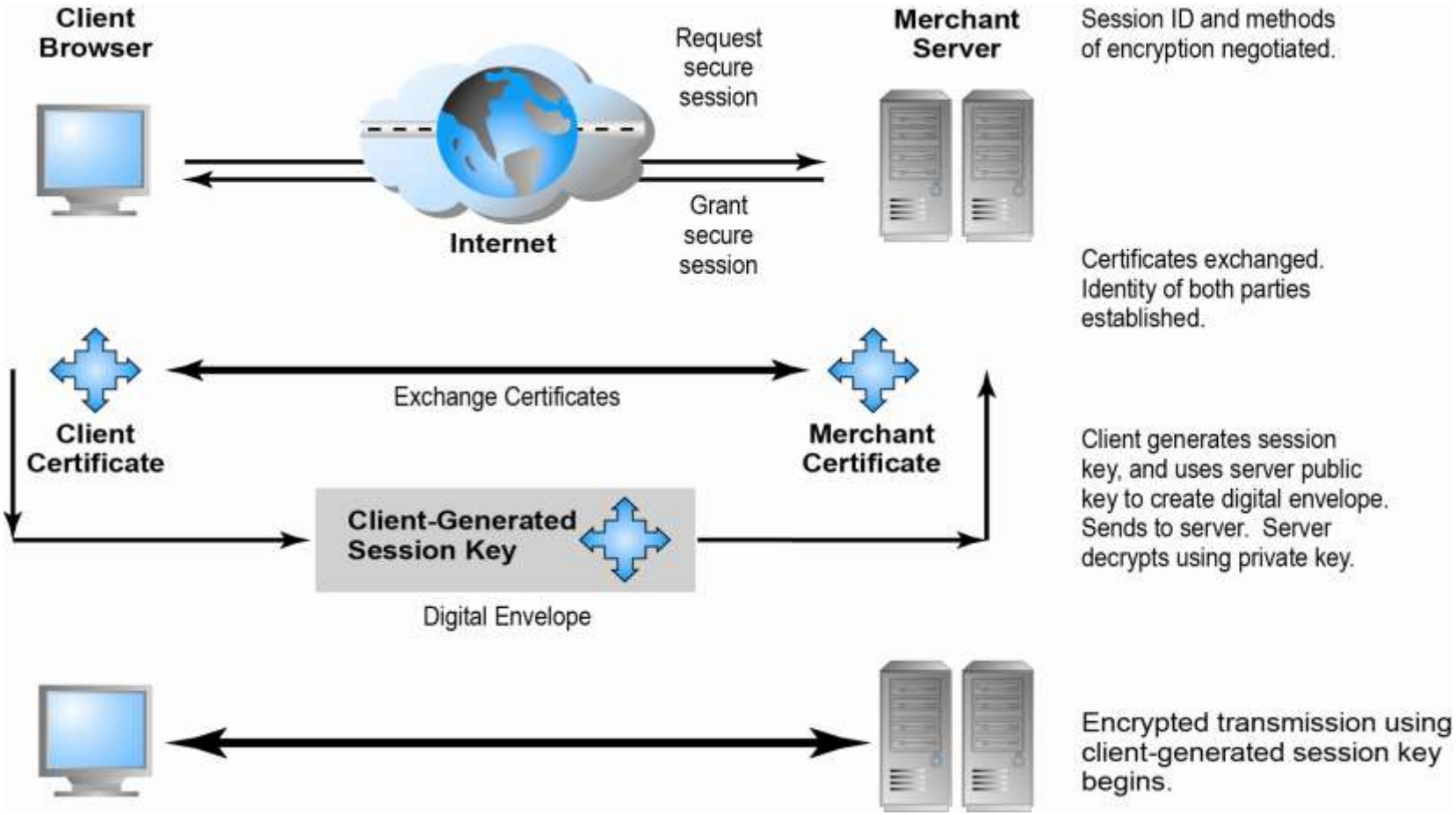

Figure 5.10, Page 300

Copyright © 2013 Pearson Education, Inc.

Protecting Networks حماية الشبكات

- **Firewall**
  - Hardware or software
  - Uses security policy to filter packets
  - Two main methods:
    - Packet filters
    - Application gateways
- **Proxy servers (proxies)**
  - Software servers that handle all communications originating from or being sent to the Internet

جدار الحماية

الأجهزة أو البرامج

يستخدم سياسة الأمان لتصفية الحزم

طريقتان رئيسيتان:

مرشحات الرزم

بوابات التطبيق

خوادم بروكسي (وكلاء)

خوادم البرمجيات التي تتعامل مع جميع الاتصالات الناشئة عن أو يتم إرسالها إلى الإنترنت

Copyright © 2013 Pearson Education, Inc.

Firewalls and Proxy Servers
الجدران النارية وخوادم الوكيل

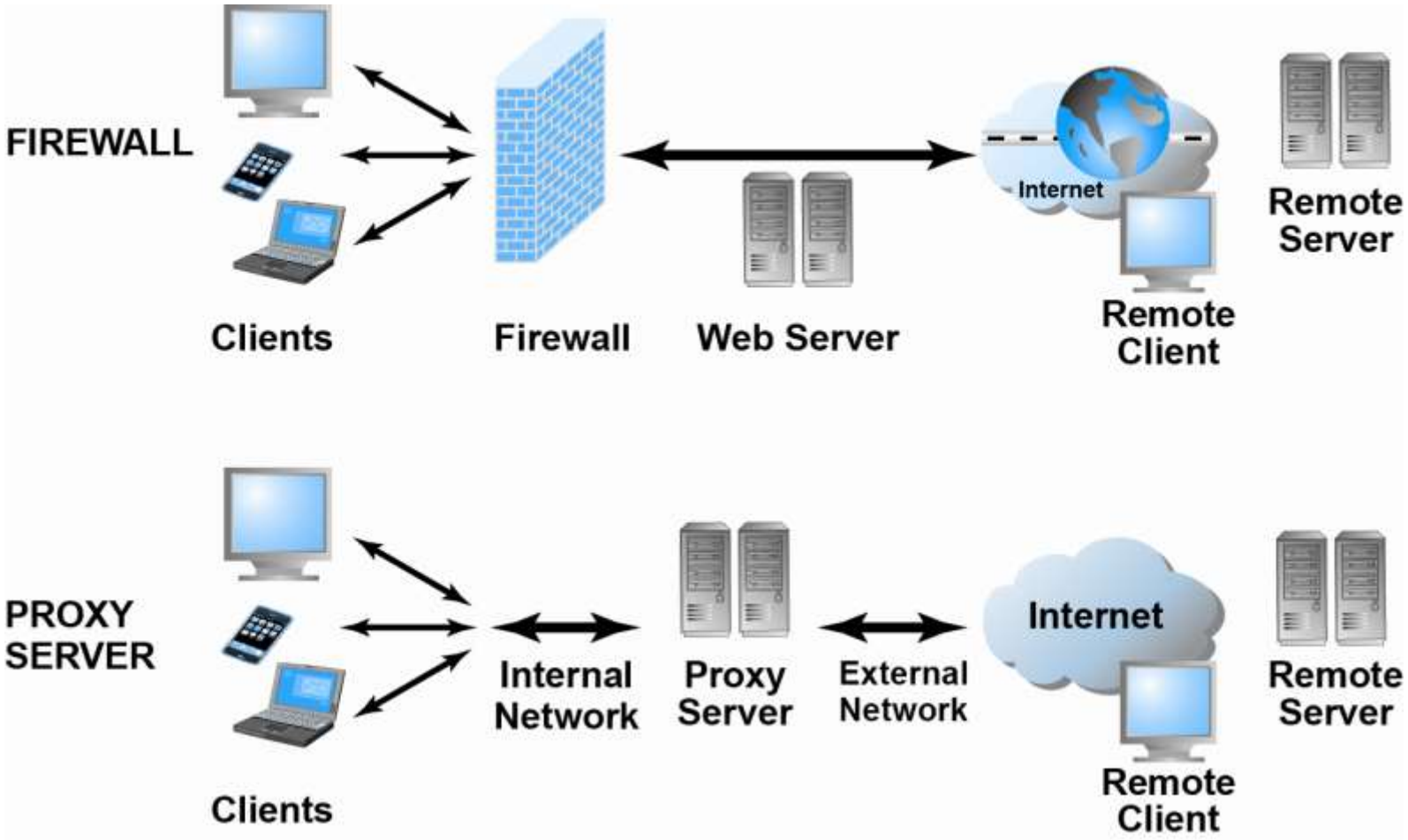

Figure 5.11, Page 303

Copyright © 2013 Pearson Education, Inc.

Protecting Servers and Clients
حماية الخوادم والعملاء

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

تحسينات أمان نظام التشغيل
ترقيات، بقع

برامج مكافحة الفيروسات:
أسهل وأقل تكلفة وسيلة لمنع التهديدات لسلامة النظام
يتطلب التحديثات اليومية

Copyright © 2013 Pearson Education, Inc.

Management Policies, Business Procedures, and Public Laws

سياسات الإدارة، إجراءات الأعمال، والقوانين العامة

- **Worldwide, companies spend $60 billion on security hardware, software, services**
- **Managing risk includes**
  - Technology
  - Effective management policies
  - Public laws and active enforcement

في جميع أنحاء العالم، تنفق الشركات 60 مليار $ على الأجهزة الأمنية والبرمجيات والخدمات

وتشمل إدارة المخاطر

تقنية

سياسات الإدارة الفعالة

القوانين العامة والإنفاذ الفعال

Copyright © 2013 Pearson Education, Inc.

A Security Plan: Management Policies
خطة الأمن: سياسات الإدارة

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

تقييم المخاطر
سياسة الأمن
خطة التنفيذ
منظمة الأمن
ضوابط الوصول
إجراءات المصادقة، بما في ذلك القياسات الحيوية
سياسات التفويض، وأنظمة إدارة التراخيص
التدقيق الأمني

Copyright © 2013 Pearson Education, Inc.

Developing an E-commerce Security Plan
وضع خطة أمن التجارة الإلكترونية

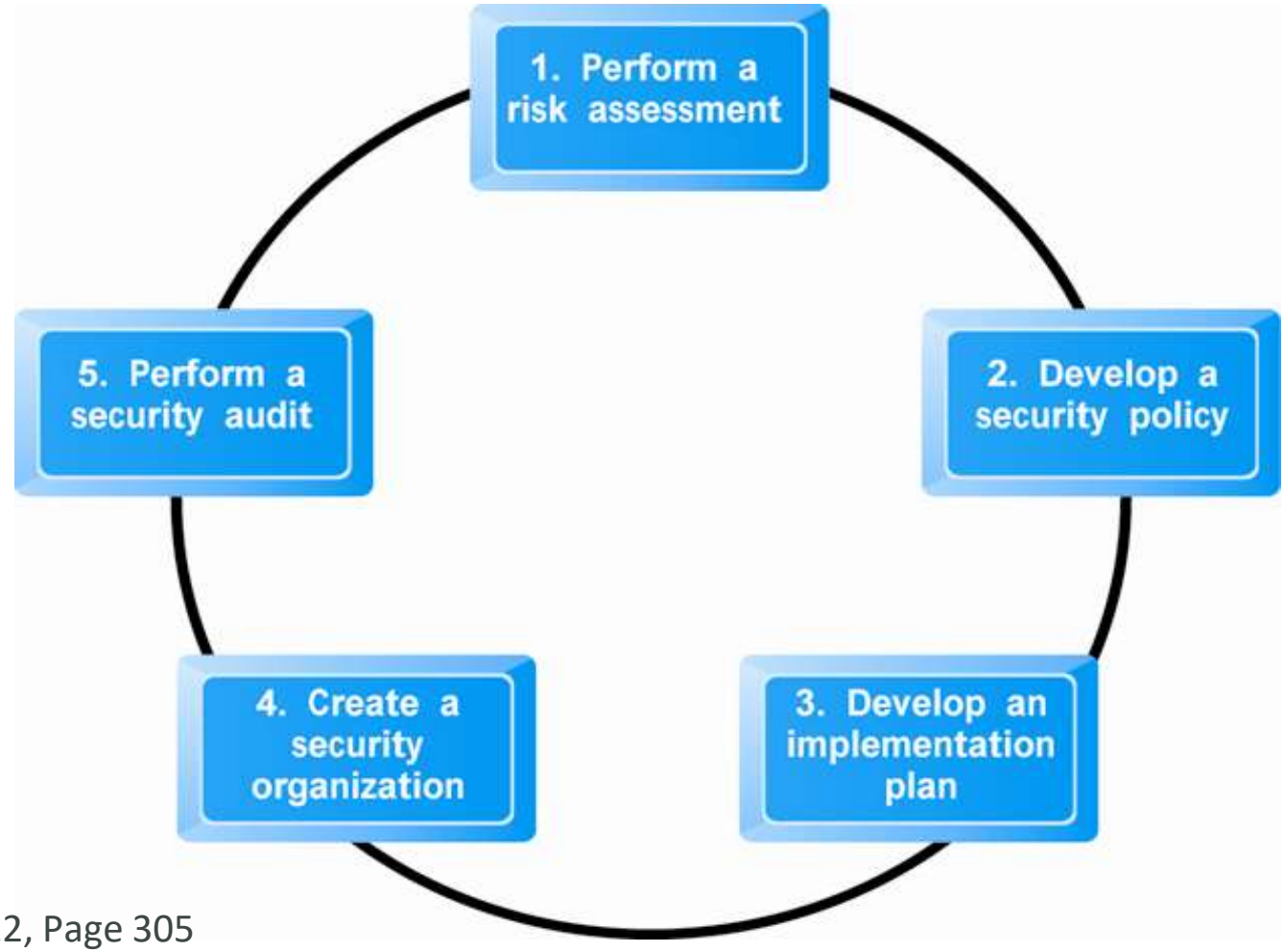

Figure 5.12, Page 305

Copyright © 2013 Pearson Education, Inc.

The Role of Laws and Public Policy
دور القوانين والسياسات العامة

- **Laws that give authorities tools for identifying, tracing, prosecuting cybercriminals:**
  - National Information Infrastructure Protection Act of 1996
  - USA Patriot Act
  - Homeland Security Act
- **Private and private-public cooperation**
  - CERT Coordination Center
  - US-CERT
- **Government policies and controls on encryption software**
  - OECD, G7/G8, Council of Europe, Wassener Arrangement

القوانين التي تعطي السلطات أدوات لتحديد وتعقب ومحاكمة مرتكبي الجرائم الإلكترونية:

قانون حماية البنية التحتية الوطنية للمعلومات لعام 1996

الولايات المتحدة الأمريكية قانون باتريوت

قانون الأمن الداخلي

التعاون بين القطاعين الخاص والعام

مركز تنسيق سيرت CERTالولايات المتحدة-

السياسات والضوابط الحكومية على برامج التشفير

، كونسيل أوف يوروب، G8 / G7أويسد، واسينر أرانجيمنت

Copyright © 2013 Pearson Education, Inc.

Types of Payment Systems
أنواع أنظمة الدفع

- **Cash**
  - Most common form of payment
  - Instantly convertible into other forms of value
  - No float
- **Checking transfer**
  - Second most common payment form in United States
- **Credit card**
  - Credit card associations
  - Issuing banks
  - Processing centers

السيولة النقدية

أكثر طرق الدفع شيوعا

تحويل فوري إلى أشكال أخرى من القيمة

لا تعويم

فحص النقل

نموذج الدفع الثاني الأكثر شيوعا في الولايات المتحدة

بطاقة ائتمان

جمعيات بطاقات الائتمان

البنوك المصدرة

مراكز المعالجة

Copyright © 2013 Pearson Education, Inc.

Types of Payment Systems (cont.)

- **Stored value**
  - Funds deposited into account, from which funds are paid out or withdrawn as needed
  - Debit cards, gift certificates
  - Peer-to-peer payment systems
- **Accumulating balance**
  - Accounts that accumulate expenditures and to which consumers make period payments
  - Utility, phone, American Express accounts

القيمة المخزنة

الأموال المودعة في الاعتبار، والتي يتم دفع الأموال منها أو سحبها حسب الحاجة

بطاقات الخصم، وشهادات الهدايا

نظم الدفع من نظير إلى نظير

تراكم الرصيد

الحسابات التي تتراكم النفقات والتي المستهلكين جعل المدفوعات الفترة

فائدة، هاتف، حسابات أمريكان إكسبريس

Copyright © 2013 Pearson Education, Inc.

Payment System Stakeholders
نظام الدفع أصحاب المصلحة

- **Consumers**
  - Low-risk, low-cost, refutable, convenience, reliability
- **Merchants**
  - Low-risk, low-cost, irrefutable, secure, reliable
- **Financial intermediaries**
  - Secure, low-risk, maximizing profit
- **Government regulators**
  - Security, trust, protecting participants and enforcing reporting

المستهلكين
منخفضة المخاطر، منخفضة التكلفة، قابل للراحة، والراحة، والموثوقية
التجار
منخفضة المخاطر، منخفضة التكلفة، لا دحض، آمنة وموثوق بها
الوسطاء الماليون
آمنة، منخفضة المخاطر، وتعظيم الربح
الجهات التنظيمية الحكومية
الأمن والثقة وحماية المشاركين وإنفاذ التقارير

Copyright © 2013 Pearson Education, Inc.

E-commerce Payment Systems
التجارة الإلكترونية أنظمة الدفع

- **Credit cards**
  - 44% of online payments in 2012 (U.S.)
- **Debit cards**
  - 28% online payments in 2012 (U.S.)
- **Limitations of online credit card payment**
  - Security, merchant risk
  - Cost
  - Social equity

بطاقات الائتمان

44٪ من الدفعات عبر الإنترنت في عام 2012 (الولايات المتحدة)

بطاقات الخصم

28٪ دفعات عبر الإنترنت في عام 2012 (الولايات المتحدة)

قيود دفع بطاقة الائتمان عبر الإنترنت

الأمن، مخاطر التاجر

كلفة

مساواة اجتماعية

Copyright © 2013 Pearson Education, Inc.

How an Online Credit Transaction Works
كيفية عمل معاملات الائتمان عبر الإنترنت

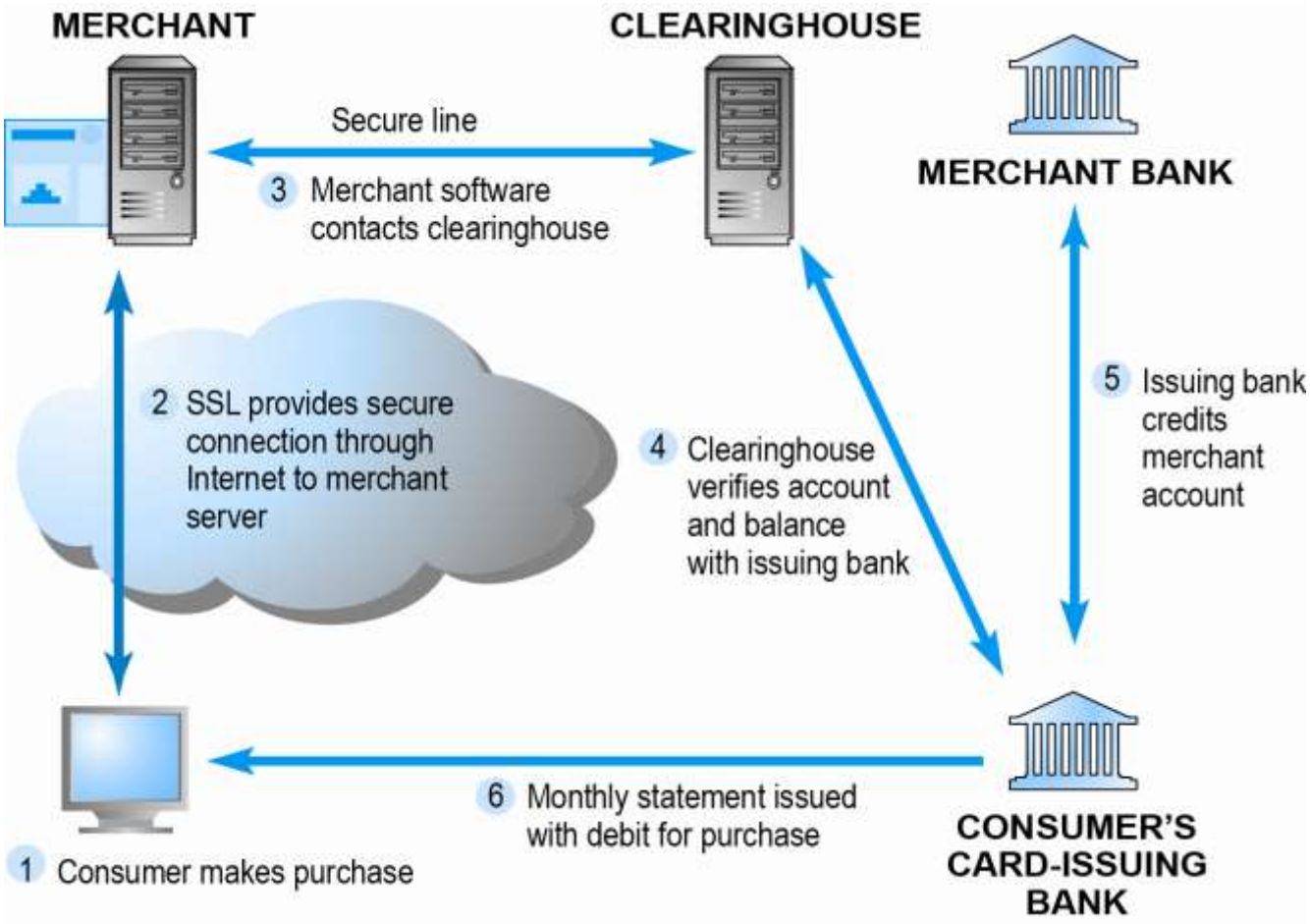

Figure 5.14, Page 315

Copyright © 2013 Pearson Education, Inc.

Alternative Online Payment Systems
أنظمة الدفع البديلة عبر الإنترنت

- **Online stored value systems:**
  - Based on value stored in a consumer's bank, checking, or credit card account
  - e.g., PayPal
- **Other alternatives:**
  - Amazon Payments
  - Google Checkout
  - Bill Me Later
  - WUPay, Dwolla, Stripe

أنظمة القيمة المخزنة عبر الإنترنت:

استنادا إلى القيمة المخزنة في بنك المستهلك، والتحقق، أو حساب بطاقة الائتمان

على سبيل المثال، بايبال

بدائل أخرى:

المدفوعات الأمازون

غوغل تشيكوت

فاتورة لي في وقت لاحق

ووباي، دولا، شريط

Copyright © 2013 Pearson Education, Inc.

Mobile Payment Systems
أنظمة الدفع عبر الهاتف المتحرك

- **Use of mobile phones as payment devices established in Europe, Japan, South Korea**
- **Near field communication (NFC)**
  - Short-range (2”) wireless for sharing data between devices
- **Expanding in United States**
  - Google Wallet
    - Mobile app designed to work with NFC chips
  - PayPal
  - Square

استخدام الهواتف النقالة وأجهزة الدفع التي أنشئت في أوروبا واليابان وكوريا الجنوبية

الاتصالات الميدانية القريبة (نفك)

قصيرة المدى (2 ") اللاسلكية لتبادل البيانات بين الأجهزة

توسيع في الولايات المتحدة

محفظة قوقل

التطبيق المحمول مصممة للعمل مع رقائق نفك

باي بال

ميدان

Copyright © 2013 Pearson Education, Inc.

Digital Cash and Virtual Currencies
النقد الرقمي والعملات الافتراضية

- **Digital cash**
  - Based on algorithm that generates unique tokens that can be used in “real” world
  - e.g., Bitcoin
- **Virtual currencies**
  - Circulate within internal virtual world
  - e.g., Linden Dollars in Second Life, Facebook Credits

النقد الرقمي

استنادا إلى خوارزمية أن يولد الرموز الفريدة التي يمكن استخدامها في العالم "الحقيقي" على سبيل المثال، بيتكوين

العملات الافتراضية

تعميم داخل العالم الظاهري الداخلي

على سبيل المثال، ليندن دولارس إن سيكوند ليف، فاسيبوك كريديتس

Copyright © 2013 Pearson Education, Inc.

Electronic Billing Presentment and Payment (EBPP)
تقديم الفواتير الإلكترونية والدفع (إبب)

- **Online payment systems for monthly bills**
- **50% of all bill payments**
- **Two competing EBPP business models:**
  - Biller-direct (dominant model)
  - Consolidator
- **Both models are supported by EBPP infrastructure providers**

أنظمة الدفع عبر الإنترنت للفواتير الشهرية
50٪ من جميع مدفوعات الفواتير
اثنين من نماذج الأعمال التجارية إبب المتنافسة:
بيلر-ديريكت (نموذج مهيمن)
الموحد
ويدعم كلا النموذجين من قبل مقدمي البنية التحتية إبب

Copyright © 2013 Pearson Education, Inc.

This work is protected by United States copyright laws and is provided solely for the use of instructors in teaching their courses and assessing student learning. Dissemination or sale of any part of this work (including on the World Wide Web) will destroy the integrity of the work and is not permitted. The work and materials from it should never be made available to students except by instructors using the accompanying text in their classes. All recipients of this work are expected to abide by these restrictions and to honor the intended pedagogical purposes and the needs of other instructors who rely on these materials.