Key Points

• This chapter summarizes the security threats and solutions that managers of e-commerce sites need to be aware of when they build and operate commercial Web sites.
• E-commerce sites—just like physical stores and markets—are open to malicious behavior by individuals and organizations with criminal intent.
• But because they exist in the digital environment of the Web, e-commerce sites face some unique problems.

Key Points

• Security is a complex, multi-layered phenomenon that involves a diverse set of risks, and a balanced approach that requires special technology, organizational rules and procedures, and ultimately laws and industry standards.
• Figure 5.2 illustrates the interaction and supportive nature of these three elements.
• No single "magic bullet" solution exists for Internet security, anymore than for general societal security.

Key Points

• Credit card fraud on the Web is about 3-5 times larger than credit card fraud in the general economy but still represents only 3-5% of all Web transactions.
• Moreover, the merchant—not the consumer—faces the greatest risks given the nature of banking laws and regulations.
• The opening case summarizes a number of credit card fraud situations that underscore the risks to merchants.

The E-commerce Security Environment: The Scope of the Problem

• Overall size of cybercrime unclear; amount of losses significant but stable; individuals face new risks of fraud that may involve substantial uninsured losses.
  - Symantec: Over 50 overall attacks a day against business firms between July 2004–June 2005

- 2005 Computer Security Institute survey
  - 56% of respondents had detected breaches of computer security within last 12 months and 91% of these suffered financial loss as a result
  - Over 35% experienced denial of service attacks
  - Over 75% detected virus attacks
The E-commerce Security Environment

Figure 5.4, Page 253

Dimensions of E-commerce Security

- **Integrity**: ability to ensure that information being displayed on a Web site or transmitted/received over the Internet has not been altered in any way by an unauthorized party
- **Nonrepudiation**: ability to ensure that e-commerce participants do not deny (repudiate) online actions
- **Authenticity**: ability to identify the identity of a person or entity with whom you are dealing on the Internet
- **Confidentiality**: ability to ensure that messages and data are available only to those authorized to view them
- **Privacy**: ability to control use of information a customer provides about himself or herself to merchant
- **Availability**: ability to ensure that an e-commerce site continues to function as intended

Customer and Merchant Perspectives on the Different Dimensions of E-commerce Security

Table 5.1, Page 254

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Customer’s Perspective</th>
<th>Merchant’s Perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>Has information transmitted or received been altered?</td>
<td>Has data on the site been altered without authorization? Is data being monitored from customers?</td>
</tr>
<tr>
<td>Nonrepudiation</td>
<td>Can a party to an action with respect to data taking the action?</td>
<td>Can a customer deny ordering products?</td>
</tr>
<tr>
<td>Authenticity</td>
<td>Can a person or entity be assured that the person or entity is who they claim to be?</td>
<td>Can a recipient deny sending products?</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Can someone other than the intended recipient read my messages?</td>
<td>Are messages or confidential data accessible to anyone other than the intended recipient?</td>
</tr>
<tr>
<td>Privacy</td>
<td>Can I control the use of information about myself transmitted to an e-commerce merchant?</td>
<td>What sort of data can be made available to customers willing to share it and not part of an e-commerce transaction?</td>
</tr>
<tr>
<td>Availability</td>
<td>Can I get access to the site?</td>
<td>Is the site operational?</td>
</tr>
</tbody>
</table>

The Tension Between Security and Other Values

- **Security vs. ease of use**: the more security measures that are added, the more difficult a site is to use, and the slower it becomes
- **Security vs. desire of individuals to act anonymously**

Security Threats in the E-commerce Environment

- Three key points of vulnerability:
  - **Client**
  - **Server**
  - **Communications channel**

Security Threats in the E-commerce Environment (cont’d)

- Most common threats:
  - Malicious code
  - Phishing
  - Hacking and cybervandalism
  - Credit card fraud/theft
  - Spoofing (pharming)
  - Denial of service attacks
  - Sniffing
  - Insider jobs
  - Poorly designed server and client software
The Ten Most Critical Cyber Security Threats

Prinya Hom-anek
CISPP, CISA, CISM, SANS GIAC GCFW, (ISC)2® Asian Advisory Board, ISACA Thailand Committee
ACIS Professional Center Co., Ltd., Thailand

1. Malware attack with Social Engineering Tactics
2. SPAM
3. DoS and DDoS attack
4. Phishing and Pharming (Identity Theft)
5. Botnets
6. IM and P2P attack
7. Mobile and Wireless attack (Wi-Fi and Bluetooth)
8. Rootkits
9. Web Application Hacking (OWASP)
10. Hacking with Google

The Ten Most Advanced Critical Cyber Security Threats

1. Zero Day Attack
2. Web 2.0 Attack
3. RFID Attack
4. VoIP Attack
5. Web Services Attack
6. SOA Attack
7. Removable Storage Data Leakage (USB Attack)
8. Virtualized Exploit/Trojan/RAT Attack (MOSVM virtual machine)
9. IP Storage Security Vulnerabilities (iSCSI Attack)
10. Completely Anonymity: TOR (The Onion Router)

A Typical E-commerce Transaction

Vulnerable Points in an E-commerce Environment

Malicious Code

- **Viruses**: computer program that has ability to replicate and spread to other files; most also deliver a “payload” of some sort (may be destructive or benign); include macro viruses, file-infecting viruses, and script viruses
- **Worms**: designed to spread from computer to computer
- **Trojan horse**: appears to be benign, but then does something other than expected
- **Bots**: can be covertly installed on computer; responds to external commands sent by the attacker
Phishing

- Any deceptive, online attempt by a third party to obtain confidential information for financial gain
  - Most popular type: e-mail scam letter
  - One of fastest growing forms of e-commerce crime

Hacking and Cybervandalism

- Hacker: Individual who intends to gain unauthorized access to computer systems
- Cracker: Used to denote hacker with criminal intent (two terms often used interchangeably)
- Cybervandalism: Intentionally disrupting, defacing or destroying a Web site
- Types of hackers include:
  - White hats
  - Black hats
  - Grey hats

Credit Card Fraud

- Fear that credit card information will be stolen deters online purchases
- Hackers target credit card files and other customer information files on merchant servers; use stolen data to establish credit under false identity
- One solution: New identity verification mechanisms

Spoofing (Pharming)

- Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
- Threatens integrity of site; authenticity

DoS and dDoS Attacks

- Denial of service (DoS) attack: Hackers flood Web site with useless traffic to inundate and overwhelm network
- Distributed denial of service (dDoS) attack: Hackers use numerous computers to attack target network from numerous launch points

Other Security Threats

- Sniffing: Type of eavesdropping program that monitors information traveling over a network; enables hackers to steal proprietary information from anywhere on a network
- Insider jobs: Single largest financial threat
- Poorly designed server and client software: Increase in complexity of software programs has contributed to an increase in vulnerabilities that hackers can exploit
Technology Solutions

- Protecting Internet communications (encryption)
- Securing channels of communication (SSL, S-HTTP, VPNs)
- Protecting networks (firewalls)
- Protecting servers and clients

Tools Available to Achieve Site Security

- Encryption
- Firewalls
- Security Tools
- Network Security Protocols
- Security Management
- Access Controls
- Authentication
- Virtual Private Networks
- Proxy/Agent Systems
- Intrusion Detection
- Tunneling

Protecting Internet Communications: Encryption

- **Encryption**: The process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and receiver
- **Purpose**: Secure stored information and information transmission
- Provides:
  - Message integrity
  - Nonrepudiation
  - Authentication
  - Confidentiality

Symmetric Key Encryption

- Also known as *secret key encryption*
- Both the sender and receiver use the same digital key to encrypt and decrypt message
- Requires a different set of keys for each transaction
- **Data Encryption Standard (DES)**: Most widely used symmetric key encryption today; uses 56-bit encryption key; other types use 128-bit keys up through 2048 bits

Public Key Encryption

- Public key cryptography solves symmetric key encryption problem of having to exchange secret key.
- Uses two mathematically related digital keys – **public key** (widely disseminated) and **private key** (kept secret by owner)
- Both keys are used to encrypt and decrypt message
- Once key is used to encrypt message, same key cannot be used to decrypt message
- For example, sender uses recipient’s public key to encrypt message; recipient uses his/her private key to decrypt it

Public Key Cryptography – A Simple Case

1. Original message
2. Recipient’s public key
3. Message encrypted using AES
4. Recipient’s private key
5. Original message decrypted

1. Original message
2. Recipient’s public key
3. Message encrypted
4. Recipient’s private key
5. Original message decrypted
**Public Key Encryption using Digital Signatures and Hash Digests**

- Application of hash function (mathematical algorithm) by sender prior to encryption produces hash digest that recipient can use to verify integrity of data
- Double encryption with sender’s private key (digital signature) helps ensure authenticity and nonrepudiation

A **hash function** is a reproducible method of turning some kind of data into a (relatively) small number that may serve as a digital "fingerprint" of the data. The algorithm "chops and mixes" (i.e., substitutes or transposes) the data to create such fingerprints, called **hash values**. These are commonly used as indices into hash tables or hash files. Cryptographic hash functions are used for various purposes in information security applications.

**Digital Envelopes**

- Addresses weaknesses of public key encryption (computationally slow, decreases transmission speed, increases processing time) and symmetric key encryption (faster, but more secure)
- Uses symmetric key encryption to encrypt document but public key encryption to encrypt and send symmetric key
Digital Certificates and Public Key Infrastructure (PKI)

- **Digital certificate**: Digital document that includes:
  - Name of subject or company
  - Subject's public key
  - Digital certificate serial number
  - Expiration date
  - Issuance date
  - Digital signature of certification authority (trusted third party institution) that issues certificate
  - Other identifying information

- **Public Key Infrastructure (PKI)**: refers to the CAs and digital certificate procedures that are accepted by all parties

Limits to Encryption Solutions

- PKI applies mainly to protecting messages in transit
- PKI is not effective against insiders
- Protection of private keys by individuals may be haphazard
- No guarantee that verifying computer of merchant is secure
- CAs are unregulated, self-selecting organizations

Insight on Technology: Advances in Quantum Cryptography May Lead to the Unbreakable Key

- Why are existing encryption systems over time more vulnerable?
- What is quantum encryption?
- What is the weakness of a symmetric key system (even one based on quantum techniques)?
- Would quantum-encrypted messages be immune to the growth in computing power?

Securing Channels of Communication

- **Secure Sockets Layer (SSL)**: Most common form of securing channels of communication; used to establish a secure negotiated session (client-server session in which URL of requested document, along with contents, is encrypted)
- **S-HTTP**: Alternative method; provides a secure message-oriented communications protocol designed for use in conjunction with HTTP
- **Virtual Private Networks (VPNs)**: Allow remote users to securely access internal networks via the Internet, using Point-to-Point Tunneling Protocol (PPTP)

Secure Negotiated Sessions Using SSL
Protecting Networks: Firewalls and Proxy Servers

- **Firewall**: Hardware or software filters communications packets and prevents some packets from entering the network based on a security policy.
- **Firewall methods include**: Packet filters, Application gateways.
- **Proxy servers**: Software servers that handle all communications originating from or being sent to the Internet.

A Security Plan: Management Policies

- **Steps in developing a security plan**
  - **Perform risk assessment**: assessment of risks and points of vulnerability
  - **Develop security policy**: set of statements prioritizing information risks, identifying acceptable risk targets, and identifying mechanisms for achieving targets
  - **Develop implementation plan**: action steps needed to achieve security plan goals
  - **Create security organization**: in charge of security; educates and trains users, keeps management aware of security issues; administers access controls, authentication procedures and authorization policies
  - **Perform security audit**: review of security practices and procedures

Developing an E-commerce Security Plan

- 1. Perform a risk assessment
- 2. Develop a security plan
- 3. Create a security organization
- 4. Implement plan
- 5. Perform a security audit

Insight on Business: Hiring Hackers to Locate Threats: Penetration Testing

- Why would firms hire outsiders to crash its systems?
- What are “grey” and “black” hats and why do firms avoid them as security testers?
- Are penetration specialists like Johnny Long performing a public service or just making the situation worse?
The Role of Laws and Public Policy

- New laws have granted local and national authorities new tools and mechanisms for identifying, tracing and prosecuting cybercriminals
  - National Infrastructure Protection Center – unit within National Cyber Security Division of Department of Homeland Security whose mission is to identify and combat threats against U.S. technology and telecommunications infrastructure
  - USA Patriot Act
  - Homeland Security Act
- Government policies and controls on encryption software

OECD Guidelines

- 2002 Organization for Economic Cooperation and Development (OECD) Guidelines for the Security of Information Systems and Networks has nine principles:
  - Awareness
  - Responsibility
  - Response
  - Ethics
  - Democracy
  - Risk assessment
  - Security design and implementation
  - Security management
  - Reassessment

ISO/IEC 17799:2005

- establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.
- The objectives outlined provide general guidance on the commonly accepted goals of information security management.
- ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:
  - security policy;
  - organization of information security;
  - asset management;
  - human resources security;
  - physical and environmental security;
  - communications and operations management;
  - access control;
  - information systems acquisition, development and maintenance;
  - information security incident management;
  - business continuity management;
  - compliance.

Ref: http://www.computersecuritynow.com/presentation/
**WHY? OBJECTIVES?**

- “It is intended to serve as a single reference point for identifying a range of controls needed for most situations where information systems are used in industry and commerce”

- Essentially the facilitation of trading in a trusted environment

**HISTORY 1**

- First published as DTI Code of Practice in UK
- Re-hashed and published as Version 1 of BS7799
- Published in Feb 1995
- NOT widely embraced – for various reasons, including:
  - not flexible enough
  - simplistic “key control” approach
  - other more pressing issues (e.g. Y2K, EMU, etc)

**HISTORY 2**

- A major revision of BS7799 undertaken… Version TWO
  - Published in May 1999
- Formal certification and accreditation schemes are launched in the same year
- Supporting tools start to appear
- Fast track ISO initiative accelerated, first published as an ISO standard in Dec 2000

**WHAT IS HAPPENING NOW?**

- Burst of activity in terms of uptake...
  - many organisations quote intent
  - same well on route to certification
  - some organisations already certified
  - significant positive take-up
  - massive increase in interest in general the issue itself
  - established as 1st major standard for information security

**WHY THE CHANGE?**

- E-business… organizations seek security assurance in the new environment
- Major Consultancies… have invested very heavily… in the training of certified auditors/assessors. Potential major income generator if successful.
- They may then join the others in making certification a mark of differentiation. Obvious scenario of, for instance, a corporate customer choosing between two similar services (maybe e-business services) for which security is a concern...

**THE MARKET RISKS?**

- What if your competitors are more advanced than you… consider what will happen if they become certified?
- They may then join the others in making certification a mark of differentiation. Obvious scenario of, for instance, a corporate customer choosing between two similar services (maybe e-business services) for which security is a concern...

*Paraphrased: “We are ISO 9000 certified, but not you…”*

*Fear minimization: “Well, we have our own policy, etc… and… etc.”*
ISO/IEC 27000 Series

• ISO has reserved the ISO/IEC 27000-series numbering for a range of information security management standards in similar fashion to the very successful ISO 9000-series quality assurance standards.

ISO 27000
- vocabulary and definitions (terminology for all of these standards)

ISO 27001
- the main Information Security Management System requirements standard (specification) against which organizations are formally certified
- ISO 27002 (currently known as ISO 17799 and formerly known as BS 7799 part 1) - this is the Code of Practice describing a comprehensive set of information security control objectives and a menu of best-practice security controls

ISO 27003 - will be an implementation guide

ISO 27004 - will be a new Information Security Management Metrics and Measurement standard to help measure the effectiveness of information security management system implementations.

ISO 27005 - will be a new Information Security Risk Management standard (will replace the recently issued BS 7799 Part 3)

ISO 27006 - will probably be a new standard: “Guidelines for information and communications technology disaster recovery services”

Key Points

• This chapter summarizes the great variety of payment systems on the Web.
• The challenge is to avoid confusing all the different Web payment schemes.
• Most people are unaware of existing payment systems, let alone the great variety of Web payment systems.
• One way to start is to realise the five basic types of payment systems: cash, checks, credit cards, stored value, and accumulating balance.
• The main point for students to take away from this chapter is that the Web has not created any totally new methods of payment although it has greatly changed how these methods of payment are implemented, namely, electronically over the Web.
• Web consumers in the U.S. predominantly use credit cards for purchases and efforts to wean consumers away from their credit card have generally failed.
• The one exception is P2P payment systems such as PayPal which nevertheless rely on the stored value provided by credit cards or checking accounts.

Topic 5

• Source: .ppt slides from instructor resources
  – Ch 6: E-commerce Payment Systems
Key Points

- **Types of Payment Systems.** There are five generic types of payment systems, each with different characteristics.
- Table 6.1 provides a good illustration of the benefits and costs of each type of payment system.
- Figure 6.3 and supporting text describe the five different types of online payment systems, and illustrate both current e-commerce payment behavior and online merchants' preferred means of payment.

Key Points

- **E-commerce Digital Payment Systems.** This section describes major types of digital payment methods on the Web: digital wallets, digital cash, stored value, accumulating balance, digital credit card, and digital checking.
- The Insight on Business box that describes Micropayments—A Market Worth Dominating provides a good starting point for this discussion. A brief mention is made of wireless payment systems, which in the U.S. have not played a large role but in Japan and Europe are more common.
- The Insight on Technology Wireless Payments Follow Wi-Fi and Cellular Growth builds on this discussion. It describes emerging wireless payment systems and why wireless payment systems have not prospered in the U.S., but do better in Japan and Europe.

Key Points

- **B2B Payment Systems.** B2B payments are much larger than the B2C payments described in the first part of this chapter, both in terms of the overall size of the B2B payment market and also the size of the average payment.
- Table 6.8 describes the unique requirements of B2B payment systems.
- A variety of firms have emerged that provide digital means of B2B payments such as Actrade, which pays foreign sellers immediately for goods shipped and collects from domestic buyers later.

PayPal: The Money's in the E-mail Class Discussion

- Why was it difficult for individuals to accept credit card payments prior to PayPal?
- Why is PayPal called a "peer-to-peer" payment system?
- Who is the main consumer of PayPal services?
- Why did PayPal purchase a merchant services company from VeriSign?
- Who are PayPal's competitors?
Types of Payment Systems

- Cash
- Checking Transfer
- Credit Card
- Stored Value
- Accumulating Balance

Cash
- Legal tender defined by a national authority to represent value
- Most common form of payment in terms of number of transactions
- Instantly convertible into other forms of value without intermediation of any kind
- Portable, requires no authentication, and provides instant purchasing power
- "Free" (no transaction fee), anonymous, low cognitive demands
- Limitations: easily stolen, limited to smaller transaction, does not provide any float

Checking Transfer
- Funds transferred directly via a signed draft or check from a consumer's checking account to a merchant or other individual
- Most common form of payment in terms of amount spent
- Can be used for both small and large transactions
- Some float
- Not anonymous, require third-party intervention (banks)
- Introduce security risks for merchants (forgeries, stopped payments), so authentication typically required

Most Common Payment Systems, Based on Number Of Transactions

![Pie chart showing payment methods]

- Source: Based on data from U.S. Census Bureau, 2005

Most Common Payment Systems, Based on Dollar Amount

![Pie chart showing payment methods]

- Source: Based on data from U.S. Census Bureau, 2005

Credit Card
- Represents an account that extends credit to consumers, permitting consumers to purchase items while deferring payment, and allows consumers to make payments to multiple vendors at one time
- Credit card associations: Nonprofit associations (Visa, MasterCard) that set standards for issuing banks
- Issuing banks: Issue cards and process transactions
- Processing centers (clearinghouses): Handle verification of accounts and balances
Stored Value

• Accounts created by **depositing funds into an account** and from which funds are paid out or withdrawn as needed
  - Examples: Debit cards, gift certificates, prepaid cards, smart cards
  - **Debit cards**: Immediately debit a checking or other demand-deposit account
  - **Peer-to-peer payment** systems such as PayPal

Accumulating Balance

• Accounts that accumulate expenditures and to which consumers make periodic payments
  - Examples: utility, phone, American Express accounts

Dimensions of Payment Systems

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Cash</th>
<th>Personal Check</th>
<th>Credit Card</th>
<th>Stored Value (Debit Card)</th>
<th>Accumulating Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediate availability</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td>No immediate availability</td>
<td>n</td>
<td>n</td>
<td>n</td>
<td>n</td>
<td>n</td>
</tr>
<tr>
<td>Electronic payment</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td>No electronic payment</td>
<td>n</td>
<td>n</td>
<td>n</td>
<td>n</td>
<td>n</td>
</tr>
</tbody>
</table>

Current Online Payment Systems

• Credit cards are dominant form of online payment, accounting for around 80% of online payments in 2005
• New forms of electronic payment include:
  - Digital cash
  - Online stored value systems
  - Digital accumulating balance payment systems
  - Digital credit accounts
  - Digital checking

Various Payment Methods Offered or Planned to be Offered by Online Merchants

<table>
<thead>
<tr>
<th>Payment Method Offered</th>
<th>3%</th>
<th>10%</th>
<th>20%</th>
<th>30%</th>
<th>40%</th>
<th>50%</th>
<th>60%</th>
<th>70%</th>
<th>80%</th>
<th>90%</th>
<th>100%</th>
<th>% of Merchants Offering/Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit cards</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>E-checks</td>
<td>7%</td>
<td>14%</td>
<td>21%</td>
<td>28%</td>
<td>35%</td>
<td>42%</td>
<td>49%</td>
<td>56%</td>
<td>63%</td>
<td>70%</td>
<td>77%</td>
<td>100</td>
</tr>
<tr>
<td>Pre/Partial payment</td>
<td>4%</td>
<td>8%</td>
<td>12%</td>
<td>16%</td>
<td>20%</td>
<td>24%</td>
<td>28%</td>
<td>32%</td>
<td>36%</td>
<td>40%</td>
<td>44%</td>
<td>100</td>
</tr>
<tr>
<td>Instant payment</td>
<td>3%</td>
<td>6%</td>
<td>9%</td>
<td>12%</td>
<td>15%</td>
<td>18%</td>
<td>21%</td>
<td>24%</td>
<td>27%</td>
<td>30%</td>
<td>33%</td>
<td>100</td>
</tr>
<tr>
<td>Bank transfer</td>
<td>1%</td>
<td>2%</td>
<td>3%</td>
<td>4%</td>
<td>5%</td>
<td>6%</td>
<td>7%</td>
<td>8%</td>
<td>9%</td>
<td>10%</td>
<td>11%</td>
<td>100</td>
</tr>
<tr>
<td>Direct debit</td>
<td>1%</td>
<td>2%</td>
<td>3%</td>
<td>4%</td>
<td>5%</td>
<td>6%</td>
<td>7%</td>
<td>8%</td>
<td>9%</td>
<td>10%</td>
<td>11%</td>
<td>100</td>
</tr>
</tbody>
</table>

How an Online Credit Card Transaction Works

• Processed in much the same way that in-store purchases are
• Major difference is that online merchants do not see or take impression of card, and **no signature is available** (CNP – Cardholder Not Present, transactions)
• Participants include **consumer, merchant, clearinghouse, merchant bank (acquiring bank)** and consumer’s card issuing bank
Limitations of Online Credit Card Payment Systems

- **Security**: neither merchant nor consumer can be fully authenticated
- **Cost**: for merchants, around 3.5% of purchase price plus transaction fee of 20 – 30 cents per transaction
- **Social equity**: many people do not have access to credit cards (young adults, plus almost 100 million other adult Americans who cannot afford cards or are considered poor risk)

Insight on Society: The Right to Shop

Class Discussion

- What is the “Digital Divide”
- Is the digital divide becoming a larger problem than in the past?
- Why is access to computers and the Internet becoming less of a problem?
- Why are digital payments a problem for millions of Americans?

The SET (Secure Electronic Transaction) Protocol

- Authenticates cardholder and merchant identity through use of digital certificates
- An open standard developed by MasterCard and Visa
- Transaction process similar to standard online credit card transaction, with more identity verification
- Thus far, has not caught on much, due to costs involved in integrating SET into existing systems, and lack of interest among consumers

Digital Wallets

- Concept of digital wallet relevant to many of the new digital payment systems
- Seeks to emulate the functionality of traditional wallet
- Most important functions:
  - Authenticate consumer through use of digital certificates or other encryption methods
  - Store and transfer value
  - Secure payment process from consumer to merchant
- Most common types are client-based software applications: Gator eWallet.com, MasterCard Wallet
Digital Cash
• One of the first forms of alternative payment systems
• Not really “cash”: rather, are forms of value storage and value exchange that have limited convertibility into other forms of value, and require intermediaries to convert
• Many of early examples have disappeared; concepts survive as part of P2P payment systems

Online Stored Value Systems
• Permit consumers to make instant, online payments to merchants and other individuals based on value stored in an online account
• Rely on value stored in a consumer’s bank, checking, or credit card account

Smart Cards as Stored Value Systems
• Another kind of stored value system based on credit-card sized plastic cards that have embedded chips that store personal information
• Two types:
  • Contact
  • Contactless
• Examples: Mondex, Octopus

Digicash: How First Generation Digital Cash Worked

How Ecount.com Works: A Stored Value System
Digital Accumulating Balance Payment Systems

- Allows users to make micropayments and purchases on the Web, accumulating a debit balance for which they are billed at the end of the month
- Examples: Qpass, Valista, Clickshare, Click & Buy, Peppercoin

Insight on Business: Micropayments – A Market Worth Dominating?
Class Discussion

- What are micropayments? Give some offline and online examples. Why are they increasingly important online?
- Why do micropayments pose a problem for online merchants?
- How can Apple’s iTunes make money selling songs for .99 cents?
- Explain Peppercoin’s “single-merchant aggregation model”. Why is this a solution?
- Explain BitPass’s online stored value system. Why is this a solution and for whom?

Digital Credit Card Payment Systems

- Extend the functionality of existing credit cards for use as online shopping payment tools
- Focus specifically on making use of credit cards safer and more convenient for online merchants and consumers
- Example: eCharge

How a Digital Credit Card Payment System Works: eCharge

Digital Checking Payment Systems

- Extend the functionality of existing checking accounts for use as online shopping payment tools
- Examples: PayByCheck, Western Union MoneyZap
Digital Payment Systems and the Wireless Web

- **Mobile payment** (m-payments) systems not very well established yet in U.S, but with growth in Wi-Fi and 3G cellular phone systems, this is beginning to change
- Juniper Research predicts global m-commerce will total at least $88 billion by 2009, majority of transactions will be micro-m-payments

Insight on Technology: Wireless Payments Follow Wi-Fi and Cellular Growth

- Class Discussion
  - What are “wireless payment” systems?
  - How will the development of Wi-Fi and Bluetooth drive growth of wireless payment in the United States?
  - What are the important factors in the growth of wireless payment systems?
  - Why did Simpay fail in Europe?
  - Why would cell phone carriers be ideal “bankers” for wireless payment systems?

Electronic Billing Presentment and Payment (EBPP)

- Online payment systems for monthly bills
- EBPP expected to grow rapidly, to an estimated 40% of all households by 2007
- Main business models in EBPP market include:
  - Biller-direct
  - Consolidator
- Above are supported by EBPP infrastructure providers

Growth of the EBPP Market

![Graph showing growth of the EBPP market from 2001 to 2009](image)

**Source:** Based on data from eMarketer, Inc., 2004b; Forrester Research, 2005; authors' estimates.

Major Players in the EBPP Marketspace

![Diagram showing major players in the EBPP marketspace](image)

B2B Payment Systems

- More complex than B2C
- Major types:
  - Systems that replace traditional banks (example: TradeCard, Orbian)
  - Financial institutions hoping to extend to the B2B marketplace
  - Credit card companies
### Key Features of B2B Payment Systems

**Table 6.8, Page 343**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit verification and guarantors</td>
<td>Provides an assessment of creditworthiness and payment guarantees.</td>
</tr>
<tr>
<td>Custom service</td>
<td>Helps ensure that both parties will perform their obligations.</td>
</tr>
<tr>
<td>Non-revocation</td>
<td>Ensures that purchases are not reversible, allowing both parties to trade with one another more confidently.</td>
</tr>
<tr>
<td>Funds collection for seller</td>
<td>Handles funds transfers, transmittal, and storage.</td>
</tr>
<tr>
<td>Financing</td>
<td>Provides “float” on available payment delays to buyers in return for a fee.</td>
</tr>
<tr>
<td>Integration with other business documents</td>
<td>Integrates purchase orders, invoices, shipping documents, and payments.</td>
</tr>
<tr>
<td>Fraud detection</td>
<td>Helps sellers trade more securely.</td>
</tr>
<tr>
<td>Accounting</td>
<td>Provides account summary and invoice details.</td>
</tr>
<tr>
<td>Dispute handling</td>
<td>Provides a method for adjudicating disputes.</td>
</tr>
<tr>
<td>Integration to back-end corporate systems</td>
<td>Links payment systems with shipping, accounting, and other corporate systems.</td>
</tr>
<tr>
<td>Online bill presentation</td>
<td>Has the ability to generate and present electronic bills.</td>
</tr>
<tr>
<td>Multiple payment options</td>
<td>Ensure that buyers may pay with credit card, debit card, ACH check, electronic funds transfer, or other means.</td>
</tr>
</tbody>
</table>