BUS 168 – Chapter 5
E-commerce Security and Payment Systems

The E-commerce Security Environment

- 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

What is Good E-commerce Security?

- To achieve highest degree of security
  - New technologies
  - Organizational policies and procedures
  - Industry standards and government laws

Security Threats in the E-commerce Environment

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

Most Common Security Threats in the E-commerce Environment

- Malicious code
  - Viruses
  - Worms
  - Trojan horses
  - Drive-by downloads
  - Backdoors
  - Bots, botnets
  - Threats at both client and server levels
- Potentially unwanted programs (PUPs)
  - Browser parasites
  - Adware
  - Spyware
- Phishing
  - E-mail scams
  - Social engineering
  - Identity theft
- 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

- 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
- 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

Think Your Smartphone Is Secure?

- What types of threats do smartphones face?
- Are there any particular vulnerabilities to this type of device?
- Are apps more or less likely to be subject to threats than traditional PC software programs?

Technology Solutions

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

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

Note - The discussion on Symmetric and Public Key Encryption (page 182-185) is beyond the scope of this course. You are not responsible for this content.

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

Limits to Encryption Solutions

- 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

Securing Channels of Communication

- 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

Protecting Networks

- Firewall
  - Hardware or software
  - Uses security policy to filter packets
- Proxy servers (proxies)
  - Software servers that handle all communications originating from or being sent to the Internet

Protecting Servers and Clients

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

E-commerce Payment Systems

- Credit cards
  - Still the dominant online payment method in United States

- Limitations of online credit card payment systems
  - Security, merchant risk
  - Cost
  - Social equity

Alternative Online Payment Systems

- 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

Mobile Payment Systems

- 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

Digital Cash and Virtual Currencies

- 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

Electronic Billing Presentment and Payment (EBPP)

- 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