Chapter 5
Online Security and Payment Systems
Cyberwar Becomes a Reality
Class Discussion

- What is a DDoS attack? Why did it prove to be so effective against Estonia?

- What are botnets? Why are they used in DDoS attacks?

- What percentage of computers belong to botnets? What percentage of spam is sent by botnets?

- Can anything be done to stop DDoS attacks?
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: Cybercrime on the rise from 2007
  - IC3: Processed 200,000+ Internet crime complaints
  - 2007 CSI survey: 46% respondent firms detected security breach in last year
  - Underground economy marketplace that offers sales of stolen information growing
Categories of Internet Crime Complaints Reported to IC3

Figure 5.1, Page 262

<table>
<thead>
<tr>
<th>Type of Fraud</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auction fraud</td>
<td>35.7%</td>
</tr>
<tr>
<td>Non-delivery</td>
<td>24.9%</td>
</tr>
<tr>
<td>Confidence fraud</td>
<td>6.7%</td>
</tr>
<tr>
<td>Credit/debit card fraud</td>
<td>6.3%</td>
</tr>
<tr>
<td>Check fraud</td>
<td>6%</td>
</tr>
</tbody>
</table>
Types of Attacks Against Computer Systems

Figure 5.3, Page 264

- Insider abuse: 59%
- Virus: 52%
- Nigerian letter fraud: 50%
- Laptop/mobile device theft: 26%
- Phishing: 25%
- IM misuse: 25%
- Denial of service: 25%
- Unauthorized access to information: 21%
- Bots: 17%
- Theft of data: 17%
- Abuse of wireless network: 13%
- Financial fraud: 12%
- Password sniffing: 10%
- Web site defacement: 10%
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
The E-commerce Security Environment

Figure 5.4, Page 267
## Customer and Merchant Perspectives on the Different Dimensions of E-commerce Security

### Table 5.2, Page 268

<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 I transmit or receive been altered?</td>
<td>Has data on the site been altered without authorization? Is data being received from customers valid?</td>
</tr>
<tr>
<td>Nonrepudiation</td>
<td>Can a party to an action with me later deny taking the action?</td>
<td>Can a customer deny ordering products?</td>
</tr>
<tr>
<td>Authenticity</td>
<td>Who am I dealing with? How can I be assured that the person or entity is who they claim to be?</td>
<td>What is the real identity of the customer?</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 those authorized to view them?</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 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?</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 added, the more difficult a site is to use, and the slower it becomes.

- Security vs. desire of individuals to act anonymously:
  - Use of technology by criminals to plan crimes or threaten nation-state.
Security Threats in the E-commerce Environment

- Three key points of vulnerability:
  - Client
  - Server
  - Communications pipeline
A Typical E-commerce Transaction

Figure 5.5, Page 270

Vulnerable Points in an E-commerce Environment

Figure 5.6, Page 271

Security Risks
Internet communications
Servers
ISP
Merchant
Banks

Clients
Business
Home

Tapping and sniffing
Alteration of messages
Theft and fraud

DoS attack
Hacking
Malicious code attack
Theft and fraud
Line taps
Vandalism

Malicious code attack
Line taps
Physical loss of computer

Most Common Security Threats in the E-commerce Environment

- Malicious code (viruses, worms, Trojans)
- Unwanted programs (spyware, browser parasites)
- Phishing/identity theft
- Hacking and cybervandalism
- Credit card fraud/theft
- Spoofing (pharming)/spam (junk) Web sites
- DoS and DDoS attacks
- Sniffing
- Insider attacks
- Poorly designed server and client software
Malicious Code

- Viruses:
  - Replicate and spread to other files; most deliver “payload” (destructive or benign)
  - Macro viruses, file-infecting viruses, script viruses

- Worms:
  - Designed to spread from computer to computer

- Trojan horse:
  - Appears benign, but does something other than expected

- Bots:
  - Covertly installed on computer; respond to external commands sent by attacker
Unwanted Programs

- Installed without user’s informed consent
  - Browser parasites
    - Can monitor and change settings of a user’s browser
  - Adware
    - Calls for unwanted pop-up ads
  - Spyware
    - Can be used to obtain information, such as a user’s keystrokes, e-mail, IMs, etc.
Phishing and Identity Theft

- Any deceptive, online attempt by a third party to obtain confidential information for financial gain, e.g.
  - E-mail scam letter – most popular phishing attack
  - Spoofing legitimate financial institution’s Web site

- Use information to commit fraudulent acts (access checking accounts), steal identity

- One of fastest growing forms of e-commerce crime
Hacking and Cybervandalism

- Hacker:
  - Individual who intends to gain unauthorized access to computer systems

- Cracker:
  - Hacker with criminal intent

- Cybervandalism:
  - Intentionally disrupting, defacing, destroying Web site

- Types of hackers
  - White hats
  - Black hats
  - Grey hats
Credit Card Fraud

- Fear of stolen credit card information 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
- Online companies at higher risk than offline
- In development: New identity verification mechanisms
Spoofing (Pharming) and Spam (Junk) Web Sites

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

- Spam (Junk) Web sites
  - Use domain names similar to legitimate one, redirect traffic to spammer-redirection domains
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 multiple computers to attack target network from numerous launch points
Other Security Threats

- **Sniffing:**
  - 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 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

Figure 5.9, Page 284
Protecting Internet Communications: Encryption

- Encryption
  - Transforming plain text, data into cipher text that can’t be read by anyone other than sender and receiver
  - Secures stored information and information transmission

- Provides:
  - Message integrity
  - Nonrepudiation
  - Authentication
  - Confidentiality
Symmetric Key Encryption

- Also known as secret key encryption
- Both sender and receiver use same digital key to encrypt and decrypt message
- Requires different set of keys for each transaction
- 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
Public Key Encryption

- 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 his/her private key to decrypt it
Public Key Cryptography – A Simple Case

Figure 5.10, Page 283

1. Original message
   Buy Cisco @ $25

2. Recipient’s public key
   10101101110001

3. Message encrypted in cipher text

4. Internet

5. Recipient’s private key
   Buy Cisco @ $25
Public Key Encryption using Digital Signatures and Hash Digests

- **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
Digital Envelopes

- Addresses weaknesses of public key encryption (computationally slow, decreases transmission speed, increases processing time) and symmetric key encryption (faster, but less secure)

- Uses symmetric key encryption to encrypt document but public key encryption to encrypt and send symmetric key
Public Key Cryptography: Creating a Digital Envelope

Figure 5.12, Page 290
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 certification authority (trusted third party institution) that issues certificate
  - Other identifying information

- Public Key Infrastructure (PKI): CAs and digital certificate procedures that are accepted by all parties
Digital Certificates and Certification Authorities

Figure 5.13, Page 291
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 Society

In Pursuit of E-mail Privacy
Class Discussion

- What are some of the current risks and problems with using e-mail?
- What are some of the technology solutions that have been developed?
- Are these solutions compatible with modern law?
- Consider the benefits of a thorough business record retention policy. Do you agree that these benefits are worth giving up some control of your e-mail?
Securing Channels of Communication

- **Secure Sockets Layer (SSL):**
  - Establishes a secure, negotiated client-server session in which URL of requested document, along with contents, is encrypted.

- **S-HTTP:**
  - Provides a secure message-oriented communications protocol designed for use in conjunction with HTTP.

- **Virtual Private Network (VPN):**
  - Allows remote users to securely access internal network via the Internet, using Point-to-Point Tunneling Protocol (PPTP).
Secure Negotiated Sessions Using SSL

Figure 5.14, Page 295

- **Client Browser**
  - Request secure session
  - Exchange Certificates

- **Internet**
  - Grant secure session
  - Client-Generated Session Key

- **Merchant Server**
  - 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 filters packets
  - Prevents some packets from entering the network based on security policy
  - Two main methods:
    - Packet filters
    - Application gateways

- **Proxy servers (proxies)**
  - Software servers that handle all communications originating from or being sent to the Internet
Firewalls and Proxy Servers

Figure 5.15, Page 298
Protecting Servers and Clients

- Operating system controls:
  - Authentication and access control mechanisms

- Anti-virus software:
  - Easiest and least expensive way to prevent threats to system integrity
  - Requires daily updates
Management Policies, Business Procedures, and Public Laws

- U.S. firms and organizations spend 10% of IT budget on security hardware, software, services
- Attacks against organizational computers down
- Attacks against Web sites, individual records up
- Technology a foundation of security
- Effective management policies also required
A Security Plan: Management Policies

- Risk assessment
- Security policy
- Implementation plan
  - Security organization
  - Access controls
  - Authentication procedures
    - Biometrics
  - Authorization policies
    - Authorization management systems
- Security audit
Developing an E-commerce Security Plan

Figure 5.16, Page 300

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 Technology

Securing Your Information: Cleversafe Hippie Storage

Class Discussion

- What is LOCKSS? What are the advantages and disadvantages to LOCKSS?
- How is Cleversafe’s storage method different? How does it work?
- Why is it accurate to say that Cleversafe’s method is “green” or “hippie storage”?
The Role of Laws and Public Policy

- New laws have given authorities tools and mechanisms for identifying, tracing, prosecuting cybercriminals
  - National Information Infrastructure Protection Act of 1996: created National Infrastructure Protection Center
  - USA Patriot Act
  - Homeland Security Act
- CERT Coordination Center – private group
- Government policies and controls on encryption software
- OECD guidelines
Types of Payment Systems

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

- Legal tender
- Most common form of payment in terms of number of transactions
- Instantly convertible into other forms of value without intermediation
- Portable, requires no authentication
- “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 signed draft/check from a consumer’s checking account to merchant/other individual
- Most common form of payment in terms of amount spent
- Can be used for small and large transactions
- Some float
- Not anonymous, requires third-party intervention (banks)
- Introduces security risks for merchants (forgeries, stopped payments), so authentication typically required
Credit Card

- Represents account that extends credit to consumers; 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
- Peer-to-peer payment systems
  - Variation on stored value systems
  - e.g. PayPal
Accumulating Balance

- Accounts that accumulate expenditures and to which consumers make period payments
  - Examples: Utility, phone, American Express accounts

- Evaluating payment systems:
  - Different stakeholders (consumers, merchants, financial intermediaries, government regulators) have different priorities in payment system dimensions (refutability, risk, anonymity, etc.)
### Table 5.6: 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>Instantly convertible without</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>intermediation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low transaction cost for small</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>transactions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low transaction cost for large</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>transactions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low fixed costs for merchant</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Refutable (able to be repudiated)</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no (usually)</td>
<td>yes</td>
</tr>
<tr>
<td>Financial risk for consumer</td>
<td>yes</td>
<td>no</td>
<td></td>
<td>up to $50</td>
<td>limited</td>
</tr>
<tr>
<td>Financial risk for merchant</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Anonymous for consumer</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Anonymous for merchant</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Immediately respendable</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Security against unauthorized use</td>
<td>no</td>
<td>some</td>
<td>some</td>
<td>some</td>
<td>some</td>
</tr>
<tr>
<td>Tamper-resistant</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Requires authentication</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Special hardware required</td>
<td>no</td>
<td>no</td>
<td>yes—by</td>
<td>yes—by</td>
<td>yes—by</td>
</tr>
<tr>
<td>merchant</td>
<td></td>
<td></td>
<td>merchant</td>
<td></td>
<td>merchant</td>
</tr>
<tr>
<td>Buyer keeps float</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Account required</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Has immediate monetary value</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>
E-commerce Payment Systems

- Credit cards are dominant form of online payment, accounting for around 60% of online payments in 2008

- Other e-commerce payment systems:
  - Digital wallets
  - Digital cash
  - Online stored value payment systems
  - Digital accumulating balance systems
  - Digital checking
How an Online Credit Transaction Works

1. Consumer makes purchase
2. SSL provides secure connection through Internet to merchant server
3. Merchant software contacts clearinghouse
4. Clearinghouse verifies account and balance with issuing bank
5. Issuing bank credits merchant account
6. Monthly statement issued with debit for purchase
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
Digital Wallets

- 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

- Early efforts to popularize have failed

- Newest effort: Google Checkout
Digital Cash

- One of the first forms of alternative payment systems
- Not really “cash”
  - Form of value storage and value exchange using tokens that has limited convertibility into other forms of value, and requires intermediaries to convert
- Most early examples have disappeared; protocols and practices too complex
Online Stored Value Systems

- Permit consumers to make instant, online payments to merchants and other individuals
- Based on value stored in a consumer’s bank, checking, or credit card account
- PayPal most successful system
- Smart cards
  - Contact smart cards: Require physical reader
    - Mondex
  - Contactless smart cards: Use RFID
    - EZPass
    - Octopus
Digital Accumulating Balance Payment Systems

- Allows users to make micropayments and purchases on the Web
- Users accumulate a debit balance for which they are billed at the end of the month
- Valista’s PaymentsPlus
- Clickshare
Digital Checking Payment Systems

- Extends functionality of existing checking accounts for use as online shopping payment tool

- Example: PayByCheck
Wireless Payment Systems

- Use of mobile handsets as payment devices well-established in Europe, Japan, South Korea
- Japanese mobile payment systems
  - E-money (stored value)
  - Mobile debit cards
  - Mobile credit cards
- Not as well established yet in U.S, but with growth in Wi-Fi and 3G cellular phone systems, this is beginning to change
Insight on Business

Mobile Payment’s Future: Wavepayme, Textpayme

Group Discussion

- What technologies make mobile payment more feasible now than in the past?
- Describe some new experiments that are helping to develop mobile payment systems.
- How has PayPal responded?
- Why haven’t mobile payment systems grown faster? What factors will spur their growth?
Electronic Billing Presentment and Payment (EBPP)

- Online payment systems for monthly bills
- 50% of households in 2008 used some EBPP; expected to grow to 75% by 2012
- Two competing EBPP business models:
  - Biller-direct: Dominant model
  - Consolidator: Third party aggregates consumer’s bills
- Both models are supported by EBPP infrastructure providers