Week 8
ECOM13003 Electronic Commerce

Security & Encryption
Chapter 5

Outcomes
after this class you should be able to:
- Describe the key dimensions of e-commerce security
- Identify the key threats in the e-commerce environment
- Describe how various forms of encryption technology help secure internet traffic
- Identify some tools used to secure and protect communication channels and business environments

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

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

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
- Most common threats:

<table>
<thead>
<tr>
<th>Malicious code</th>
<th>Phishing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sniffing</td>
<td>Insider jobs</td>
</tr>
<tr>
<td>Denial of service attacks</td>
<td>Malicious code</td>
</tr>
<tr>
<td>Spoofing (pharming)</td>
<td>Credit card fraud/theft</td>
</tr>
<tr>
<td>Hacking and cybervandalism</td>
<td>Malicious code</td>
</tr>
<tr>
<td>Trojan horse: appears to be benign, but then does something other than expected</td>
<td>Malicious code</td>
</tr>
<tr>
<td>Bots: can be covertly installed on computer; responds to external commands sent by the attacker</td>
<td>Malicious code</td>
</tr>
</tbody>
</table>

A Typical E-commerce Transaction

- Figure 5.5, Page 257

Vulnerable Points in an E-commerce Environment

- Figure 5.6, Page 258

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

Technology Solutions

- Figure 5.7, Page 269
- Protecting Internet communications (encryption)
- Securing channels of communication (SSL, S-HTTP, VPNs)
- Protecting networks (firewalls)
- Protecting servers and clients

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 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

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
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)

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

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

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

Class Discussion

- Case study – page 294
- Question 2 on page 297
Next Week

- E-commerce marketing concepts & communications
- Case study page 488
  - Question 1
- Group Presentation 6