CHAPTER 5
Security and Encryption
Created by, David Zolzer, Northwestern State University—Louisiana

Learning Objectives

- Understand the scope of e-commerce crime and security problems
- Describe the key dimensions of e-commerce security
- Understand the tension between security and other values
- Identify the key security threats in the e-commerce environment

Learning Objectives

- Describe how various forms of encryption technology help protect the security of messages sent over the Internet
- Identify the tools used to establish secure Internet communications channels
- Identify the tools used to protect networks, servers, and clients
- Appreciate the importance of policies, procedures, and laws in creating security

The E-commerce Security Environment

- Recent survey of 538 security practitioners in U.S. corporations and government agencies reported:
  - 85% detected breaches of computer security within the last 12 months
  - 64% acknowledged financial loss as a result
  - 35% quantified their financial loss to total $337 million in aggregate

The E-commerce Security Environment

- Most serious losses involved theft of proprietary information or financial fraud
- 40% reported attacks from outside the organization
- 38% experienced denial of service attacks
- 94% detected virus attacks
Internet Fraud Complaints Reported to the IFCC

Page 232, Figure 5.1

The E-commerce Security Environment

Page 234, Figure 5.2

Dimensions of E-commerce Security

- Integrity refers to the ability to ensure that information being displayed on a Web site or transmitted or received over the Internet, has not been altered in any way by an unauthorized party
- Nonrepudiation refers to the ability to ensure that e-commerce participants do not deny (i.e., repudiate) their online actions

Dimensions of E-commerce Security

- Authenticity refers to the ability to identify the identity of a person or entity with whom you are dealing on the Internet
- Confidentiality refers to the ability to ensure that messages and data are available only to those who are authorized to view them

Dimensions of E-commerce Security

- Privacy refers to the ability to ensure the use of information about oneself
- Availability refers to the ability to ensure that an e-commerce site continues to function as intended

Dimensions of E-commerce Security

<table>
<thead>
<tr>
<th>DIMENSIONS</th>
<th>CUSTOMER'S PERSPECTIVE</th>
<th>MERCHANT'S PERSPECTIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>How information transmitted or received?</td>
<td>How does this site handle without unauthorized access?</td>
</tr>
<tr>
<td>Nonrepudiation</td>
<td>Can a party in an action who has denied the action.</td>
<td>If a customer deny ordering products?</td>
</tr>
<tr>
<td>Authenticity</td>
<td>Can a merchant identify itself?</td>
<td>What is the real identity of the customer?</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Can a merchant identify messages?</td>
<td>No message or confidential data are produced in response to the unauthorized one.</td>
</tr>
<tr>
<td>Privacy</td>
<td>Can the user control the use of information?</td>
<td>Are orders accepted in a commercial environment?</td>
</tr>
<tr>
<td>Availability</td>
<td>Can the site access the site?</td>
<td>Is the site operational?</td>
</tr>
</tbody>
</table>
The Tension Between Security and Other Values

- **Ease of use**
  - The more security measures that are added to an e-commerce site, the more difficult it is to use and the slower the site becomes, hampering ease of use. Security is purchased at the price of slowing down processors and adding significantly to data storage demands. Too much security can harm profitability, while not enough can potentially put a business out of business.

- **Public Safety and the Criminal Uses of Security**
  - There is tension between the claims of individuals to act anonymously and the needs of the public officials to maintain public safety that can be threatened by criminals or terrorists.

Security Threats in the E-commerce Environment

- Three key points of vulnerability
  - the client
  - the server
  - communications pipeline

A Typical E-commerce Transaction

Vulnerable Points in an E-commerce Environment

Seven Security Threats to E-commerce Sites

- **Malicious code**
  - Includes a variety of threats such as viruses, worms, Trojan horses, and “bad applets”
  - Virus is a computer program that has the ability to replicate or make copies of itself, and spread to other files
  - Worm is designed to spread from computer to computer
  - Trojan horse appears to be benign, but then does something other than expected
Examples of Malicious Code

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>MBO</td>
<td>malware</td>
</tr>
<tr>
<td>SPOOKS</td>
<td>spyware</td>
</tr>
<tr>
<td>CRYSTAL</td>
<td>trojan</td>
</tr>
<tr>
<td>CYBERDUkie</td>
<td>trojan</td>
</tr>
<tr>
<td>ONIOMALL</td>
<td>fire-stuffing</td>
</tr>
<tr>
<td>BANANA</td>
<td>trojan</td>
</tr>
</tbody>
</table>

Seven Security Threats to E-commerce Sites

- Hacking and cybervandalism
  - hacker is an individual who intends to gain unauthorized access to a computer system
  - cracker is the term typically used within the hacking community to demote a hacker with criminal intent
  - cybervandalism is intentionally disrupting, defacing, or even destroying a site

- Credit card fraud
  - Different from traditional commerce
  - Hackers target files on merchant server
  - Spoofing
    - Misrepresenting oneself by using fake email addresses or masquerading as someone else

- Denial of Service Attacks
  - Flooding a Web site with useless traffic to inundate and overwhelm the network
  - Distributed Denial of Service attack uses numerous computers to attack the target network from numerous launch points

- Sniffing
  - A type of eavesdropping program that monitors information traveling over a network

- Insider Jobs
  - Employees with access to sensitive information
  - Sloppy internal security procedures
  - Able to roam throughout an organization’s system without leaving a trace
Tools Available to Achieve Site Security

Encryption

- The process of transforming plain text or data into cipher text that cannot be read by anyone outside of the sender and the receiver. The purpose of encryption is (a) to secure stored information and (b) to secure information transmission.
- Cipher text is text that has been encrypted and thus cannot be read by anyone besides the sender and the receiver.

Encryption

- Key or cipher is any method for transforming plain text to cipher text
- Substitution cipher is where every occurrence of a given letter is systematically replaced by another letter
- Transposition cipher changes the ordering of the letters in each word in some systematic way

Encryption

- Symmetric key encryption (secret key encryption) the sender and the receiver use the same key to encrypt and decrypt the message
- Data Encryption Standard (DES) is the most widely used symmetric key encryption, developed by the National Security Agency (NSA) and IBM. Uses a 56-bit encryption key

Public Key Cryptography - A Simple Case

- Public key cryptography uses two mathematically related digital keys are used: a public key and a private key.
- The private key is kept secret by the owner, and the public key is widely disseminated.
- Both keys can be used to encrypt and decrypt a message.
- However, once the keys are used to encrypt a message, the same key cannot be used to unencrypt the message.
Public Key Cryptography with Digital Signatures

Encryption

- Digital signature is a “signed” cipher text that can be sent over the Internet
- Hash function uses an algorithm that produces a fixed-length number called a hash or message digest
- Digital envelop is a technique that uses symmetric encryption for large documents, but public key encryption to encrypt and send the symmetric key

Public Key Cryptography: Creating a Digital Envelope

Digital Certificates and Public Key Infrastructure

Encryption

- Digital certificate is a digital document issued by a certification authority that contains the name of the subject or company, the subject’s public key, a digital certificate serial number, an expiration date, the digital signature of the certification authority, and other identifying information
- Certification Authority (CS) is a trusted third party that issues digital certificates

Encryption

- Public Key Infrastructure (PKI) are certification authorities and digital certificate procedures that are accepted by all parties
- Pretty Good Privacy (PGP) is a widely used email public key encryption software program
Securing Channels of Communications

- Secure Sockets Layer (SSL) is the most common form of securing channels
- Secure negotiated session is a client-server session in which the URL of the requested document, along with the contents, the contents of forms, and the cookies exchanged, are encrypted.
- Session key is a unique symmetric encryption key chosen for a single secure session

Secure Negotiated Sessions Using SSL

- Secure Hypertext Transfer Protocol (S-HTTP) is a secure message-oriented communications protocol designed for use in conjunction with HTTP. Cannot be used to secure non-HTTP messages
- Virtual Private Networks (VPN) allow remote users to securely access internal networks via the Internet, using Point-to-Point Tunneling Protocol (PPTP)
- PPTP is an encoding mechanism that allows one local network to connect to another using the Internet as a conduit

Protecting Networks

- Firewalls are software applications that act as a filter between a company’s private network and the Internet itself
- Proxy server is a software server that handles all communications originating from or being sent to the Internet, acting as a spokesperson or bodyguard for the organization

Firewalls and Proxy Servers

- Operating system controls allow for the authentication of the user and access controls to files, directories, and network paths
- Anti-virus software is the easiest and least expensive way to prevent threats to system integrity
Policies, Procedures, and Laws

- Developing an e-commerce security plan
  - perform a risk assessment
  - develop a security policy
  - develop an implementation plan
  - create a security organization
  - perform a security audit

A Security Plan: Management Policies

- Risk assessment is the assessment of risks and points of vulnerability
- Security policy is a set of statements prioritizing the information risks, identifying acceptable risk targets, and identifying the mechanisms for achieving these targets
- Implementation plan is the action steps you will take to achieve the security plan goals

Developing an E-commerce Security Plan

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

A Security Plan: Management Policies

- Security organization educations and trains users, keeps management aware of security threats and breakdowns, and maintains the tools chosen to implement security
- Access controls determine who can gain legitimate access to a network
- Authentication procedures include the use of digital signatures, certificates of authority, and public key infrastructure

A Security Plan: Management Policies

- Biometrics is the study of measurable biological or physical characteristics that can be used for access controls
- Authorization policies determine differing levels of access to information assets for differing levels of users
- Authorization management system establishes where and when a user is permitted to access certain parts of a Web site

A Security Plan: Management Policies

- Security audit involves the routine review of access logs identifying how outsiders are using the site as well as how insiders are accessing the site’s assets
- Tiger team is a group whose sole job activity is attempting to break into a site
- CERT Coordination Center monitors and tracks criminal activity reported to it by private corporations and government agencies that seek out its help
Role of Laws and Public Policy

- National Infrastructure Protection Center is a unit within the FBI whose sole mission is to identify and combat threats against the United States’ technology and telecommunications infrastructure.
- DCS100 (Carnivore) an email sniffing software program developed by the FBI that can copy and filter all data sent from a user’s computer to a local ISP.

E-commerce Security Legislation

<table>
<thead>
<tr>
<th>LEGISLATION</th>
<th>SIGNIFICANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Fraud and Abuse Act (1996)</td>
<td>Primary federal statute used to combat computer crime.</td>
</tr>
<tr>
<td>Electronic Communications Privacy Act</td>
<td>Improves fines and imprisonment for individuals who access, intercept or disclose private e-mail communications of others.</td>
</tr>
<tr>
<td>(1996)</td>
<td>Malware Dell attacks Illegal. Creates MPC in the FBI.</td>
</tr>
<tr>
<td>National Information Infrastructure</td>
<td>Reduces export restrictions.</td>
</tr>
<tr>
<td>Protection Act (1996)</td>
<td></td>
</tr>
<tr>
<td>Computer Security Act (1989)</td>
<td></td>
</tr>
</tbody>
</table>

Government Efforts to Regulate and Control Encryption

<table>
<thead>
<tr>
<th>REGULATORY EFFORT</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrict export of strong encryption</td>
<td>Export restrictions on strong encryption supported primarily by the United States, Ukraine, and Russia. The policy is changing to permit exports to several countries.</td>
</tr>
<tr>
<td>Key recovery statements</td>
<td>For the United Kingdom and the United States approved Enigma in 1939. This led to breaking Enigma communications to the third parties.</td>
</tr>
<tr>
<td>Lawful access and denied disclosure</td>
<td>There is growing support in several EU legislation and in E.C.B countries.</td>
</tr>
<tr>
<td>Official breaking</td>
<td>All countries are rapidly expanding budgets and new laws. The National Security Agency (NSA) installed a monitoring and a filtering computer-based network security in 1991, in accordance with the U.S. Computer Fraud and Abuse Act. The FBI OFED system is commonly in use.</td>
</tr>
</tbody>
</table>