

Chapter 11

E-Commerce Security

© 2008 Pearson Prentice Hall, Electronic Commerce 2008, Efrain Turban, et al.

Learning Objectives

1. Explain EC-related crimes and why they cannot be stopped.
2. Describe an EC security strategy and why a life cycle approach is needed.
3. Describe the information assurance security principles.
4. Describe EC security issues from the perspective of customers and e-businesses.

11-2

Learning Objectives

5. Identify the major EC security threats, vulnerabilities, and risk.
6. Identify and describe common EC threats and attacks.
7. Identify and assess major technologies and methods for securing EC communications.
8. Identify and assess major technologies for information assurance and protection of EC networks.

11-3

Stopping E-Commerce Crimes

- **Information assurance (IA)**

The protection of information systems against unauthorized access to or modification of information whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats

- **human firewalls**

Methods that filter or limit people's access to critical business documents

11-4

Stopping E-Commerce Crimes

- **zombies**

Computers infected with malware that are under the control of a spammer, hacker, or other criminal

- **application firewalls**

Specialized tools designed to increase the security of Web applications

- **common (security) vulnerabilities and exposures (CVE)**

Publicly known computer security risks, which are collected, listed, and shared by a board of security-related organizations (cve.mitre.org)

11-5

Stopping E-Commerce Crimes

- **vulnerability**

Weakness in software or other mechanism that threatens the confidentiality, integrity, or availability of an asset (recall the CIA model). It can be directly used by a hacker to gain access to a system or network

- **risk**

The probability that a vulnerability will be known and used

11-6

Stopping E-Commerce Crimes

- **exposure**

The estimated cost, loss, or damage that can result if a threat exploits a vulnerability

- **standard of due care**

Care that a company is reasonably expected to take based on the risks affecting its EC business and online transactions

11-7

Stopping E-Commerce Crimes

- **CSI/FBI Computer Crime and Security Survey**

Annual security survey of U.S. corporations, government agencies, financial and medical institutions, and universities conducted jointly by the FBI and the Computer Security Institute

11-8

Stopping E-Commerce Crimes

- **Highlights from CSI/FBI Computer Crime and Security Survey:**

- Total financial losses from attacks have declined dramatically
- Attacks on computer systems or (detected) misuse of these systems have been slowly but steadily decreasing in all areas
- Defacements of Internet Web sites have increased dramatically
- "Inside jobs" occur about as often as external attacks
- Organizations largely defend their systems through firewalls, antivirus software, intrusion detection systems, and server-based access control lists
- Organizations largely defend their systems through firewalls, antivirus software, intrusion detection systems, and server-based access control lists
- Computer security investments per employee vary widely

11-9

E-Commerce Security Strategy and Life Cycle Approach

- **The Internet's Vulnerable Design**
 - **domain name system (DNS)**
Translates (converts) domain names to their numeric IP addresses
 - **IP address**
An address that uniquely identifies each computer connected to a network or the Internet

11-10

E-Commerce Security Strategy and Life Cycle Approach

- **The Shift to Profit-Motivated Crimes**
- **Treating EC Security as a Project**
 - **EC security program**
Set of controls over security processes to protect organizational assets
 - Four high-level stages in the life cycle of an EC security program:
 1. Planning and organizing
 2. Implementation
 3. Operations and maintenance
 4. Monitoring and evaluating

11-11

E-Commerce Security Strategy and Life Cycle Approach

- Organizations that do not follow such a life cycle approach usually:
 - Do not have policies and procedures that are linked to or supported by security activities
 - Suffer disconnect, confusion, and gaps in responsibilities for protecting assets
 - Lack methods to fully identify, understand, and improve deficiencies in the security program
 - Lack methods to verify compliance to regulations, laws, or policies
 - Have to rely on *patches*, *hotfixes*, and *service packs* because they lack a holistic EC security approach

11-12

E-Commerce Security Strategy and Life Cycle Approach

- **patch**
Program that makes needed changes to software that is already installed on a computer. Software companies issue patches to fix bugs in their programs, to address security problems, or to add functionality
- **hotfix**
Microsoft's name for a patch. Microsoft bundles hotfixes into service packs for easier installation
- **service pack**
The means by which product updates are distributed. Service packs may contain updates for system reliability, program compatibility, security, and more

11-13

E-Commerce Security Strategy and Life Cycle Approach

- **Ignoring EC Security Best Practices**
 - **Computing Technology Industry Association (CompTIA)**
Nonprofit trade group providing information security research and best practices
 - Despite the known role of human behavior in information security breaches, only 29% of the 574 government, IT, financial, and educational organizations surveyed worldwide had mandatory security training. Only 36% offered end-user security awareness training

11-14

Information Assurance

- **CIA security triad (CIA triad)**
Three security concepts important to information on the Internet: confidentiality, integrity, and availability

EXHIBIT 11.2 CIA Security Triad



11-15

Information Assurance

- **confidentiality**

Assurance of data privacy and accuracy. Keeping private or sensitive information from being disclosed to unauthorized individuals, entities, or processes

- **integrity**

Assurance that stored data has not been modified without authorization; and a message that was sent is the same message that was received

- **availability**

Assurance that access to data, the Web site, or other EC data service is timely, available, reliable, and restricted to authorized users

11-16

Information Assurance

- **authentication**

Process to verify (assure) the real identity of an individual, computer, computer program, or EC Web site

- **authorization**

Process of determining what the authenticated entity is allowed to access and what operations it is allowed to perform

11-17

Information Assurance

- **nonrepudiation**

Assurance that online customers or trading partners cannot falsely deny (repudiate) their purchase or transaction

- **digital signature or digital certificate**

Validates the sender and time stamp of a transaction so it cannot be later claimed that the transaction was unauthorized or invalid

11-18

Enterprisewide E-Commerce Security and Privacy Model

- **Senior Management Commitment and Support**
- **EC Security Policies and Training**
 - To avoid violating privacy legislation when collecting confidential data, policies need to specify that customers:
 - Know they are being collected
 - Give permission, or "opt in," for them to be collected
 - Have some control over how the information is used
 - Know they will be used in a reasonable and ethical manner

11-22

Enterprisewide E-Commerce Security and Privacy Model

- **acceptable use policy (AUP)**

Policy that informs users of their responsibilities when using company networks, wireless devices, customer data, and so forth

11-23

Enterprisewide E-Commerce Security and Privacy Model

- **EC Security Procedures and Enforcement**
 - **business impact analysis (BIA)**

An exercise that determines the impact of losing the support of an EC resource to an organization and establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and supporting systems
 - **Security Tools: Hardware and Software**

11-24

Basic E-Commerce Security Issues and Perspectives

- Some of the major technology defenses to address these security issues that can occur in EC:
 - Authentication
 - Authorization
 - **auditing**
Process of recording information about what Web site, data, file, or network was accessed, when, and by whom or what
 - Confidentiality (privacy) and integrity (trust)
 - Availability
 - Nonrepudiation

11-25

Threats and Attacks

- **nontechnical attack**
An attack that uses chicanery to trick people into revealing sensitive information or performing actions that compromise the security of a network
- **social engineering**
A type of nontechnical attack that uses some ruse to trick users into revealing information or performing an action that compromises a computer or network

11-26

Threats and Attacks

- **technical attack**
An attack perpetrated using software and systems knowledge or expertise
- **time-to-exploitation**
The elapsed time between when a vulnerability is discovered and the time it is exploited
- **SpywareGuide**
A public reference site for spyware

11-27

Threats and Attacks

- **zero-day incidents**

Attacks through previously unknown weaknesses in their computer networks

- **denial of service (DOS) attack**

An attack on a Web site in which an attacker uses specialized software to send a flood of data packets to the target computer with the aim of overloading its resources

11-28

Threats and Attacks

- Web server and Web page hijacking

- **botnet**

A huge number (e.g., hundreds of thousands) of hijacked Internet computers that have been set up to forward traffic, including spam and viruses, to other computers on the Internet

- **malware**

A generic term for malicious software

- **virus**

A piece of software code that inserts itself into a host, including the operating systems, in order to propagate; it requires that its host program be run to activate it

11-29

Threats and Attacks

- **worm**

A software program that runs independently, consuming the resources of its host in order to maintain itself, that is capable of propagating a complete working version of itself onto another machine

- **macro virus (macro worm)**

A virus or worm that executes when the application object that contains the macro is opened or a particular procedure is executed

- **Trojan horse**

A program that appears to have a useful function but that contains a hidden function that presents a security risk

11-30

Threats and Attacks

- **Trojan-Phisher-Rebery**
A new variant of a Trojan program that stole tens of thousands of stolen identities from 125 countries that the victims believed were collected by a legitimate company
- **banking Trojan**
A Trojan that comes to life when computer owners visit one of a number of online banking or e-commerce sites
- **rootkit**
A special Trojan horse program that modifies existing operating system software so that an intruder can hide the presence of the Trojan program

11-31

Securing E-Commerce Communications

- **access control**
Mechanism that determines who can legitimately use a network resource
- **passive token**
Storage device (e.g., magnetic strip) that contains a secret code used in a two-factor authentication system
- **active token**
Small, stand-alone electronic device that generates one-time passwords used in a two-factor authentication system

11-32

Securing E-Commerce Communications

- **biometric systems**
Authentication systems that identify a person by measurement of a biological characteristic, such as fingerprints, iris (eye) patterns, facial features, or voice
- **public key infrastructure (PKI)**
A scheme for securing e-payments using public key encryption and various technical components

11-33

Securing E-Commerce Communications

- **encryption**
The process of scrambling (encrypting) a message in such a way that it is difficult, expensive, or time-consuming for an unauthorized person to unscramble (decrypt) it
- **plaintext**
An unencrypted message in human-readable form
- **ciphertext**
A plaintext message after it has been encrypted into a machine-readable form

11-34

Securing E-Commerce Communications

- **encryption algorithm**
The mathematical formula used to encrypt the plaintext into the ciphertext, and vice versa
- **key (key value)**
The secret code used to encrypt and decrypt a message
- **key space**
The large number of possible key values (keys) created by the algorithm to use when transforming the message

11-35

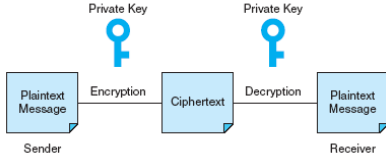
Securing E-Commerce Communications

- **symmetric (private) key system**
An encryption system that uses the same key to encrypt and decrypt the message
- **Data Encryption Standard (DES)**
The standard symmetric encryption algorithm supported by the NIST and used by U.S. government agencies until October 2000
- **Rijndael**
An advanced encryption standard (AES) used to secure U.S. government communications since October 2, 2000

11-36

Securing E-Commerce Communications

EXHIBIT 11.8 Symmetric (Private) Key Encryption



11-37

Securing E-Commerce Communications

- **public (asymmetric) key encryption**
Method of encryption that uses a pair of matched keys—a public key to encrypt a message and a private key to decrypt it, or vice versa
- **public key**
Encryption code that is publicly available to anyone
- **private key**
Encryption code that is known only to its owner
- **RSA**
The most common public key encryption algorithm; uses keys ranging in length from 512 bits to 1,024 bits

11-38

Securing E-Commerce Communications

- **hash**
A mathematical computation that is applied to a message, using a private key, to encrypt the message
- **message digest (MD)**
A summary of a message, converted into a string of digits after the hash has been applied
- **digital envelope**
The combination of the encrypted original message and the digital signature, using the recipient's public key
- **certificate authorities (CAs)**
Third parties that issue digital certificates

11-39

Securing E-Commerce Communications

- **Secure Socket Layer (SSL)**

Protocol that utilizes standard certificates for authentication and data encryption to ensure privacy or confidentiality

- **Transport Layer Security (TLS)**

As of 1996, another name for the SSL protocol

11-40

Securing E-Commerce Networks

- The selection and operation of technologies that ensure network security should be based on:

- Defense in depth
- Need-to-access basis
 - **policy of least privilege (POLP)**
Policy of blocking access to network resources unless access is required to conduct business
- Role-specific security
- Monitoring
- Patch management
- Incident response team (IRT)

11-41

Securing E-Commerce Networks

- **FIREWALLS**

- **firewall**

A single point between two or more networks where all traffic must pass (choke point); the device authenticates, controls, and logs all traffic

- **packet**

Segment of data sent from one computer to another on a network

11-42

Securing E-Commerce Networks

- Firewalls can be designed to protect against:
 - Remote login
 - Application backdoors
 - SMTP session hijacking
 - Macros
 - Viruses
 - Spam

11-43

Securing E-Commerce Networks

- **packet-filtering routers**
Firewalls that filter data and requests moving from the public Internet to a private network based on the network addresses of the computer sending or receiving the request
- **packet filters**
Rules that can accept or reject incoming packets based on source and destination addresses and the other identifying information

11-44

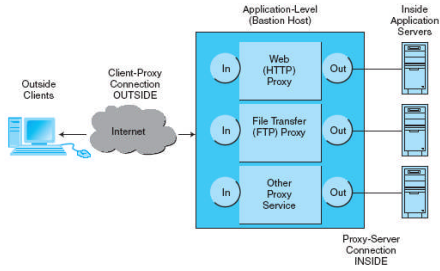
Securing E-Commerce Networks

- **application-level proxy**
A firewall that permits requests for Web pages to move from the public Internet to the private network
- **bastion gateway**
A special hardware server that utilizes application-level proxy software to limit the types of requests that can be passed to an organization's internal networks from the public Internet

11-45

Securing E-Commerce Networks

EXHIBIT 11.10 Application-Level Proxy (Bastion Gateway Host)



11-46

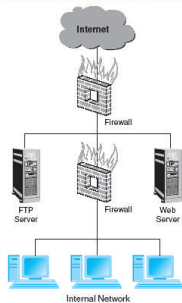
Securing E-Commerce Networks

- **proxies**
Special software programs that run on the gateway server and pass repackaged packets from one network to the other
- **demilitarized zone (DMZ)**
Network area that sits between an organization's internal network and an external network (Internet), providing physical isolation between the two networks that is controlled by rules enforced by a firewall

11-47

Securing E-Commerce Networks

EXHIBIT 11.11 Demilitarized Zone (DMZ)



11-48

Securing E-Commerce Networks

- **personal firewall**
A network node designed to protect an individual user's desktop system from the public network by monitoring all the traffic that passes through the computer's network interface card
- **virtual private network (VPN)**
A network that uses the public Internet to carry information but remains private by using encryption to scramble the communications, authentication to ensure that information has not been tampered with, and access control to verify the identity of anyone using the network
- **protocol tunneling**
Method used to ensure confidentiality and integrity of data transmitted over the Internet, by encrypting data packets, sending them in packets across the Internet, and decrypting them at the destination address

11-49

Securing E-Commerce Networks

- **intrusion detection systems (IDSs)**
A special category of software that can monitor activity across a network or on a host computer, watch for suspicious activity, and take automated action based on what it sees
- **honeynet**
A network of honeypots
- **honeypot**
Production system (e.g., firewalls, routers, Web servers, database servers) that looks like it does real work, but which acts as a decoy and is watched to study how network intrusions occur

11-50

Managerial Issues

1. Why should managers learn about EC security?
2. Why is an EC security strategy and life cycle approach needed?
3. How should managers view EC security issues?
4. What is the key to establishing strong e-commerce security?
5. What steps should businesses follow in establishing a security plan?
6. Should organizations be concerned with internal security threats?

11-51
