Chapter 12
E-Commerce Security

Learning Objectives

Upon completion of this chapter, you will be able to:

1. Document the rapid rise in computer and network security attacks.
2. Describe the common security practices of businesses of all sizes.
3. Understand the basic elements of EC security.
4. Explain the basic types of network security attacks.
5. Describe common mistakes that organizations make in managing security.
6. Discuss some of the major technologies for securing EC communications.
7. Detail some of the major technologies for securing EC networks components.

Content

Answers to Pause/Break Section Review Questions

Section 12.1 Review Questions

1. *What evidence exists that cyber attacks and crime are on the rise?*

Industry surveys indicate the increase.

2. *What units does the FBI have for combating cyber attacks?*

The FBI has created the National Infrastructure Protection Center (NIPC).

3. *What is CERT and what services does it provide?*

A group of three teams at Carnegie Mellon University that monitor incidence of cyber attacks, analyze vunerablities, and provide guidence on protecting against attacks.

Section 12.2 Review Questions

1. Based on the ISM survey results, what are some of the major differences in security issues facing small, medium, large, and very large organizations?

Small – lack of organizational resources
Medium – lower staff, less budget, low knowledge
Large – inadequate staffing, low budget per employee
Very Large - low budget per employee, complex systems

2. Does the amount of money that an organization spends on security have an impact on the chance of an organization suffering loss or damage due to cyber attacks? Explain.

Student responses will vary. This is all dependent on the use of the funds and the visibility of the firm.

Section 12.3 Review Questions

1. If a customer purchases an item from an online store, what are some of the security concerns that might arise?

- Legitimate company?
- Malicious code on the Web site?
- Privacy?
- Secure network?
- Secure communications?

2. What are the major security issues facing EC sites?

- Authentication
- Authorization
- Auditing
- Privacy
- Integrity
- Availability
- Nonrepudiation

Section 12.4 Review Questions

1. Describe the difference between a nontechnical and a technical cyber attack?

A technical attack uses IT technology, whereas a nontechnical attack uses (or attacks) standard security measures.

2. What is a CVE?

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

3. How are DDoS attacks perpetrated?

A denial of service attack in which the attacker gains illegal administration access to as many computers on the Internet as possible and uses these multiple computers to send a flood of data packets to the target computer.

4. What are the major forms of malicious code?

- Viruses
- Worms
- Macro viruses and worms
- Trojan horses

Section 12.5 Review Questions

1. What are some common mistakes that EC sites make in managing their security?

- Undervalued information
- Narrow security boundaries
- Reactive security management
- Dated processes
- Lack of communication

2. Describe the basic steps in security risk management.

- Assessment
- Planning
- Implementation
- Monitoring

Section 12.6 Review Questions

1. What are the basic elements of an authentication system?

- A group or person to be authenticated
- A distinguishing characteristic

- A system proprietor
- Authentication mechanism
- Access control mechanism

2. *What is a passive token? An active token?*

A passive token is a storage device used in two-factor authentication systems that contain a secret code. An active token is a small, stand-alone electronic device in a two-factor authentication system that generates one-time passwords.

3. *Describe the basic components of encryption.*

The process of scrambling a message in such a way that it is difficult, expensive, or time-consuming for an unauthorized person to unscramble it.

4. *What are the key elements of PKI?*

The 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.

5. *What are the basic differences between symmetric and asymmetric encryption?*

Symmetric systems use the same key for encryption and decryption whereas asymmetric systems use a combination of public and private keys.

6. *Describe how a digital signature is created.*

See Figure 12.6.

7. *What is a digital certificate? What role does a certificate authority play?*

It is a verification that the holder of a public or private key is who they claim to be. These certificates are issued by certificate authorities.

8. *What is the SSL protocol? The SET protocol?*

SSL – protocol that utilizes standard certificates for authentication and data encryption to ensure privacy or confidentiality
SET – protocol designed to provide secure online credit card transactions for both customers and merchants

Section 12.7 Review Questions

1. *List the basic types of firewalls and briefly describe each.*

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 and receiving the request.
Application-level proxies – firewall that permits requests for Web pages to move from the public Internet to the private network.

2. *What is a 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.

3. *How does a VPN work?*

A VPN is 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.

4. *Briefly describe the major types of IDSs.*

Audit logs – show attempted logins and system use
Host-based IDS – watches for unauthorized file changes
Network-based ICS – examines network traffic

<u>Answers to EC Application Case Questions</u>

EC Application Case 12.1: Social Engineering

1. *Describe the different types of social engineering.*

Human-based – relies on traditional communication methods
Computer-based – relies on IT and Internet communication methods

2. *Who is Kevin Mitnick?*

A hacker who illegally accessed computers and networks.

3. *What types of people are most likely to be targeted by social engineering?*

Inexperienced or overly-trusting users are generally the targets.

EC Application Case 12.2: Honeynets Attract Hackers

1. *What is a honeynet? A honeypot?*

Honeynet – a way to evaluate vulnerabilities of an organization by studying the types of attacks to which a site is subjected, using a network of systems called honeypots.
Honeypots – production systems designed to do real work but to be watched and studied as network intrusions occur.

2. *What are the main goals of the Honeynet Project?*

To evaluate the ways systems are attacked and to help solve vulnerabilities.

3. *How can a honeypot be used in a production system?*

It can help mitigate risk, since early warning signs usually come before a major attack.

EC Application Case 12.3: Biometrics Authentication at Thriftway

1. *Explain how a fingerprint-scanning system works.*

The system matches a pre-scanned fingerprint to the customer's in addition to a passcode to determine identity.

2. *Why would Thriftyway have chosen a verification system rather than an identification system?*

The system is less expensive in terms of interchange fees. It also speeds checkout.

3. *What are some of the complications that might arise in using a fingerprint-scanning system to verify a person's identify?*

The user may have a cut, broken finger or oily/dirty hands.

Answers to Discussion Questions

1. *Cyber attacks are on the rise. What are some of the reasons for the increase? Do you expect the situation to get worse or better? Explain.*

EC systems are built from a number of complex components and applications. Many of these components and applications are supplied by third-party vendors, some of whom treat security as an afterthought and, even when they find security holes in their systems, expend little effort to correct them. At many sites, the people responsible for building and administering the sites have little training in network security. Even when they are trained, they often opt for minimal security settings because this makes it easier (for consumers and partners alike) to do business with the site. Unfortunately, all it takes is a vulnerability in one component or application to compromise the security of the whole system. Automated tools make it possible for hackers—of practically any skill level—to discover and exploit these vulnerabilities in relatively short order. Even if they can't find a vulnerability at a particular site of interest, they can always perform a flanking maneuver. Because of the interconnectedness of the Internet, its always possible to use a vulnerable site to launch an attack against a secure site.

2. A homeowner has just installed a cable modem. The homeowner feels that there is no need to worry about security because no one will ever know about their home computer. Why should the homeowner be worried about attacks by hackers? What are some of the steps the homeowner should take to secure their home computer?

A cable modem is an always-on connection to the Internet making it easier for hackers to find the computer. In addition, some cable modem companies provide their customers with a static IP address. This makes it even easier for hackers to find the computer. Cable modem users can use firewall software (such as ZoneAlarm or BlackICE) to protect their computer. They can also purchase firewall hardware. In addition, cable modem users should set their operating system security to a high level.

3. A large number of B2C EC sites have experienced DDoS attacks. Why are these attacks so hard to safeguard against? What are some of the things a site can do to mitigate such attacks?

DDoS attacks come from many computers (zombies) at the same time. It is therefore difficult to isolate just the attacker's IP address and shut off traffic from it. Use of a firewall may help mitigate these attacks.

4. All EC sites share common security threats and vulnerabilities. Discuss these threats and vulnerabilities and some of the security policies that can be implemented to mitigate them. Do you think that B2C Web sites face different threats and vulnerabilities than B2B sites? Explain.

EC sites are vulnerable to the following major types of security attacks: operating system holes, Web server holes, database server holes, problems with storefront and shopping cart software, DoS attacks, input validation attacks, eavesdropping attacks, malicious code attacks, and malicious mobile code attacks. Simple policies that can help mitigate risks are: restrict access to the system, implement technologies such as firewalls and antivirus software, be sure that security patches are up-to-date, and monitor the network.

5. What type of security attack is most prevalent on the Internet? Discuss some of the major reasons for its prevalence.

Computer viruses are the most prevalent attack. The ability of computer viruses to spread via e-mail has increased their prevalence.

6. All EC sites employ one or more security safeguards. Yet, B2C and B2B sites differ in the safeguards they use. Discuss the similarities and differences between the two types of sites.

Both types of sites employ the same main security technologies. However, B2B sites tend to use a more layered approach – overlapping various technologies.

7. A business wants to establish and run its own Web site for advertising and marketing. Some of the marketing materials will come from databases located on its LAN. What types of security components could be used to ensure that outsiders do not have direct access to those databases? What type of network configuration (e.g., bastion gateway server) will provide the most security?

Firewalls and intrusion detection systems could be used to ensure outsiders don't gain access to the database.

8. Two businesses want to use the Internet to handle purchase orders, payments, and deliveries. They are afraid that hackers will eavesdrop on the Internet communications between them. What type of security technology could they use to safeguard against this threat?

A virtual private network (VPN) would ensure their communication remains private.

9.*You are responsible for the security at a B2C EC site and need to do an audit of your network's vulnerabilities. What type of software tool should you use to conduct the audit? What types of information will the tool provide? Once you've identified various vulnerabilities and corrected them, how can you be sure your site is safe? Explain.*

You could use SAINT which would provide information about the network's topology, hardware and software used on the network, and an assessment of potential vulnerabilities.

<u>Internet Exercises</u>

(Note: URLs may change over time; please check the Internet Exercises on the Turban Web site for possible updates: www.prenhall.com/turban.)

*1.The Computer Vulnerabilities and Exposures Board (**cve.mitre.org**) maintains a list of common network security vulnerabilities. Review the list. How many vulnerabilities are there? Based on that list, which system components appear to be most vulnerable to attack? What impact do these vulnerable components have on EC?*

The site is located at www.cve.mitre.org. Many of the vulnerabilities appear to be buffer overflows.

2.A number of B2C sites rely on hidden fields in their Web forms to pass information back and forth between a consumer's browser and their Web servers. Go to Google

*(**google.com**) and search for the following string: <INPUT TYPE=hidden NAME="price." What types of EC forms use this type of hidden field? Give some examples. What sort of security threat does a hidden field of this sort represent?*

Hidden tags are used by a variety of EC sites in order to pass data to the server. Theoretically, any form can lead to some type of input validation attack.

*3. Your B2C site has just been hacked. You would like to report the incident to the Computer Emergency Response Team (**cert.org**) at Carnegie Mellon University so they can alert other sites. How do you do this, and what types of information do you have to provide?*

Fill out the CERT incident report form (available at http://www.cert.org/reporting/incident_form.txt) and e-mail it to cert@cert.org.

*4. Go to McAfee virus library (**vil.nai.com/vil/default.asp**). What are the general characteristics of a virus? What tips does McAfee (**mcafeeb2b.com**) give for avoiding or minimizing the impact of viruses?*

A virus is a computer program that executes when the infected program is executed. A virus makes copies of itself and attempts to infect other systems with the copies. Virus risks are assessed on three criteria: prevalence, danger, and commonality of infection vehicle.

5. The World Wide Web consortium maintains a security FAQ (list of frequently asked questions). Based on this FAQ (w3.org/Security/Faq/www-security-faq.html#contents), what sorts of general precautions should be taken to secure a Web site?

According to the FAQ, "CGI scripts are a major source of security holes. Although the CGI (Common Gateway Interface) protocol is not inherently insecure, CGI scripts must be written with just as much care as the server itself. Unfortunately some scripts fall short of this standard and trusting Web administrators install them at their sites without realizing the problems."

*6. SecurityDogs.com (**securitydogs.com**) provides access to a number of third-party reviews of commercial firewall products. Select three of the products and compare their features. Based on your comparison, which product would you select?*

Student reports will vary.

7. You have just installed a DSL line in your home so you will have faster Internet access. You have heard that this makes your computer susceptible to DDoS attacks and you want to install a personal firewall to guard against this threat. What sorts of commercial products are available? Which one would you choose?

The two main types of firewall products available for home use are firewall software and personal firewall hardware. The software is loaded onto the computer and serves as a firewall. Popular software includes ZoneAlarm, BlackICE, and Norton's Internet Security. Personal firewall hardware may be a better choice for the home user who is sharing the DSL line over a home network.

Team Assignments and Role Playing

1. *Script kiddies, white hats, black hats, hacktivists, and cyberterrorists are some of the terms used to describe different types of hackers. Divide the class up into teams. Using the Web as a primary data source , have each team explore one of these types. The team should provide a general description of the hackers within this type and the methods they employ to compromise Web sites. For each type, explain how a site can detect and defend against these attacks.*
Student reports will vary.

2. *There are several personal firewall products on the market. A list of these products can be found at* ***firewallguide.com/software.htm****. Assign each team three products from the list. Each team should prepare a detailed review and comparison of each of the products they have been assigned.*

Student reports will vary.

3. *Assign each team member a different B2C or B2B Web site. Have each team prepare a report summarizing the site's security assets, threats, and vulnerabilities. Prepare a brief security risk management plan for the site.*
Student reports will vary.

Answers to End-of-Chapter Real-World Case Questions:: Is It a Question of Common Sense?

1. *How do the results of the ISAlliance survey compare with the results of the CSI/FBI survey reported in Section 12.1? Explain the similarities and differences.*

Both indicate a rise in attacks and the understanding of the importance of security. The ISAlliance goes on to list recommended standards.

2. *Most of the ISAlliance recommendations seem like common sense. Why do you think that common-sense advice is required? What types of businesses do you think these standards are aimed at? Based on what you know about information security, what other recommendations would you make?*

Student answers will vary.

3. *Given the breadth of known vulnerabilities, what sort of impact will any set of security standards have on the rise in cyber attacks?*

Given the current lack of standards, any standards should help decrease vulnerability.

4. For any organization, why is the involvement of senior management involvement crucial to the success of their security information practices?

Senior management must support IT's efforts with budgets and manpower.