Chapter 12
E-Commerce Security

True-False Questions

1. The Intrusion Detection Center is a new section of the FBI established to protect the nation's infrastructure.

   Answer: F **Reference**: The Accelerating Need for E-Commerce Security

2. The IDC reports that spending on digital security approached $2 billion in 2002
   .
   Answer: F **Reference**: Security Is Everyone's Business

3. Authentication is the process by which both the viewer and the owner of a Web page assure the identity of each other.

   Answer: T **Reference**: Basic Security Issues

4. The authorization process includes determining the identity of the party contacting a Web site.

   Answer: F **Reference**: Basic Security Issues

5. Auditing is a process that prevents data from being altered.

   Answer: F **Reference**: Basic Security Issues

6. Hal claims he did not download a piece of software over the Internet. The merchant who sold him the software proves that the software was downloaded and that the party who downloaded it provided Hal's user name, password, and credit card number. This data is being used for nonrepudiation.

   Answer: F **Reference**: Basic Security Issues

7. A salesperson having computer trouble receives an e-mail from a hacker purporting to be from customer support asking for his username and password. This is an example of a nontechnical attack.

   Answer: T **Reference**: Types of Threats and Attacks

8. Social engineering is a methodical, technical attack on a network by a hacker for the purpose of causing damage to the network.

   Answer: F **Reference**: Types of Threats and Attacks

9. Social engineering attacks are always technical.

   Answer: F **Reference**: Types of Threats and Attacks

10. All technical attacks require the attacker have software and systems expertise.

    Answer: T **Reference**: Types of Threats and Attacks

11. A DoS attack occurs when someone sends a large number of data packets to a server for the purpose of overloading the server's resources.

    Answer: T **Reference**: Types of Threats and Attacks

12. The machines on which DDoS software is loaded are called zombies.

    Answer: T **Reference**: Distributed Denial of Service Attacks

13. A virus is software that can run independently, uses a computer's resources to sustain itself, and can propagate itself in tact to other computers.

    Answer: F **Reference**: Malicious Code: Viruses, Worms, and Trojan Horses

14. Gloria downloads a piece of software that plays a catchy tune to remind her of appointments. Unknown to Gloria, the software also keeps track of every Web site she visits and reports her surfing habits to a remote site once a week. This is an example of a Trojan Horse.

    Answer: T **Reference**: Malicious Code: Viruses, Worms, and Trojan Horses

15. The major difference between a virus and a worm is that a virus propagates between systems while a worm propagates locally.

    Answer: F **Reference**: Malicious Code: Viruses, Worms, and Trojan Horses

16. The payload of a virus is the code that does damage to its host.

    Answer: T **Reference**: Malicious Code: Viruses, Worms, and Trojan Horses

17. The propagation mechanism determines how a virus will behave once it infects a computer.

    Answer: F **Reference**: Malicious Code: Viruses, Worms, and Trojan Horses

18. Many organizations lack a clear understanding of the value of specific information assets.

    Answer: T **Reference**: Managing EC Security

19. A honeynet is a series of network resources that can be monitored as network intrusions occur.

Answer: T **Reference**: Security Risk Management

20. The goal of EC security is to eliminate all threats to a network.

Answer: F **Reference**: Security Risk Management

21. Monitoring is the process of deciding which security measures have succeeded and which have failed.

Answer: T **Reference**: Security Risk Management

22. A successful monitoring program should include regular reviews to identify new assets which need to be protected.

Answer: T **Reference**: Security Risk Management

23. Active tokens are small, stand-alone devices that generate one-time passwords.

Answer: T **Reference**: Authentication

24. The purpose of authentication is to ascertain that the parties to a transaction are legitimate and that the parties have authority to complete the transaction.

Answer: T **Reference**: Authentication

25. Biometric systems determine the identity of a user based on the measurement of a biological attribute.

Answer: T **Reference**: Biometric Systems

26. PKI uses security tokens to assure the identity of users.

Answer: F **Reference**: Private and Public Key Encryption

27. Encrypting prevents a hostile computer from intercepting packets not sent to it.

Answer: F **Reference**: Private and Public Key Encryption

28. The mathematical algorithm used to convert plain text to ciphertext and vice versa is called an encryption algorithm.

Answer: F **Reference**: Private and Public Key Encryption

29. In private key systems, the same key is used to encrypt and decrypt text.

Answer: T **Reference**: Symmetric (Private) Key System

30. In public key systems, the key used to encrypt and decrypt is distributed over the Internet to all users of the secured site.

Answer: F **Reference**: Public (Asymmetric) Key Encryption

31. Digital signatures are based on public keys and can be used to uniquely identify the sender of a Web communication.

Answer: T **Reference**: Digital Signatures

32. Hashing is the application of a mathematical computation to a message using a private key.

Answer: F **Reference**: Digital Signatures

33. The encrypted original message and the digital signature using the recipient's public key are included in a digital envelope.

Answer: T **Reference**: Digital Signatures

34. Digital signatures are issued by certificate authorities.

Answer: F **Reference**: Digital Signatures

35. SSL uses standard certificates for authentication and data encryption.

Answer: T **Reference**: Secure Socket Layer

36. Data on the Internet is split into small pieces called segments.

Answer: F **Reference**: Firewalls

37. Packet filters accept or reject packets of data based on public keys.

Answer: F **Reference**: Firewalls

38. In protocol tunneling, data is encrypted before it is encapsulated in packets for transmission over the Internet.

Answer: T **Reference**: VPNs

39. In a 2002 CSI/FBI survey, 100% of respondents indicated that their systems had experienced unauthorized use.

Answer: F **Reference**: Intrusion Detection Systems

40. The purpose of an IDS is to keep a break in security from occurring.

Answer: F **Reference**: Intrusion Detection Systems

Multiple Choice Questions

41. An attack by a hacker in which the attacker sends a flood of small credit card charges is called:

    a. a virus.
    b. a zombie.
    c. a Trojan horse.
    d. a brute force credit card attack.

    Answer: d **Reference**: Brute Force Credit Card Attack

42. The process that assures a reader of a Web site that the site isn't fraudulent is called:

    a. verification.
    b. approval.
    c. authentication.
    d. security.

    Answer: c **Reference**: Basic Security Issues

43. The process by which one entity knows that another entity is who they claim to be is called:

    a. verification.
    b. auditing.
    c. authentication.
    d. authorization.

    Answer: c **Reference**: Basic Security Issues

44. The process of determining if a user has the right to perform a particular task or view data is called:

    a. verification.
    b. auditing.
    c. authentication.
    d. authorization.

    Answer: d **Reference**: Basic Security Issues

45. The process of collecting information about accessing particular resources, using particular privileges, or performing other security actions (either successfully or unsuccessfully) is known as:

    a. verification.
    b. auditing.
    c. authentication.
    d. security.

    Answer: b **Reference**: Basic Security Issues

46. The idea that information that is private or sensitive should not be disclosed to unauthorized individuals, entities, or computer software processes is called:

    a. confidentiality.
    b. auditing.
    c. authentication.
    d. security.

    Answer: a **Reference**: Basic Security Issues

47. The ongoing process used to determine which measures are successful, which measures are unsuccessful and need modification, whether there are any new types of threats, whether there have been advances or changes in technology, and whether there are any new business assets that need to be secured is called:

    a. monitoring.
    b. auditing.
    c. authentication.
    d. security.

    Answer: a **Reference**: Security Risk Management

48. The ability to protect data from being altered or destroyed in an unauthorized or accidental manner is called:

    a. confidentiality.
    b. auditing.
    c. authentication.
    d. integrity.

    Answer: d **Reference**: Basic Security Issues

49. An online site is available if:

    a. a person or program can gain access to the pages, data, or services provided by the site when they are needed.
    b. the site can be accessed twenty-four hours a day seven days a week.
    c. it can be accessed at least 75% of the time.
    d. data can be downloaded.

    Answer: a **Reference**: Basic Security Issues

50. The ability to limit parties from refuting that a legitimate transaction took place is called:

    a. confidentiality.
    b. nonrepudiation.
    c. authentication.
    d. integrity.

    Answer: b **Reference**: Basic Security Issues

51. An attacker claiming to be from customer service at an ISP sends an instant message demanding the user send his password and username immediately to help the ISP fix a major network problem. This type of attack is called:

    a. social engineering.
    b. a Trojan horse.
    c. a virus.
    d. a distributed denial of service attack.

    Answer: a **Reference**: Types of Threats and Attacks

52. An attack by a hacker in which the attacker sends a flood of data packets to the target computer with the aim of overloading its resources is called:

    a. a virus.
    b. social engineering.
    c. a Trojan horse.
    d. a denial-of-service attack.

    Answer: d **Reference**: Distributed Denial of Service Attacks

53. An attacker creates a virus that sends itself to thousands of e-mail accounts based on the address book of every computer infected. At noon on a given date, every computer infected by this virus sends a search request to Yahoo!, which overloads the Yahoo! servers and causes them to shut down. This is an example of:

    a. a non-technical attack.
    b. social engineering.
    c. a Trojan horse.
    d. a distributed denial-of-service attack.

    Answer: d **Reference**: Distributed Denial of Service Attacks

54. An teenager attaches a program to a picture of Jennifer Lopez and sends it to hundreds of email addresses. The program will cause every computer on which the picture is opened to play the first verse of Jennifer's latest hit every night at 7:00 pm. This is an example of:

    a. a virus.
    b. social engineering.
    c. a nontechnical attack.
    d. a denial-of-service attack.

    Answer: a **Reference**: Malicious Code: Viruses, Worms, and Trojan Horses

55. Elaine downloads free software for photo editing from a bulletin board. The software works beautifully, but it also keeps track of every Web site Elaine visits and reports back to a central server once a week. This is an example of:

    a. a virus.
    b. social engineering.
    c. a Trojan horse.
    d. worm.

    Answer: c **Reference**: Malicious Code: Viruses, Worms, and Trojan Horses

56. When a company follows a reactive security strategy, it:

    a. attempts to identify potential security issues and reacts to prevent attacks.
    b. waits until it is attacked, then takes action.
    c. refuses to use the Internet because there are risks out there.
    d. reacts every time it hears of a potential attack strategy.

    Answer: b **Reference**: Managing EC Security

57. An organizations evaluates its security risks by determining assets, the vulnerabilities of their system, and the potential threats to these vulnerabilities. This is an example of:

    a. assessment.
    b. planning.
    c. implementation.
    d. monitoring.

    Answer: a **Reference**: Security Risk Management

58. A company works to develop a set of policies defining which threats are tolerable and which are not. This is an example of:

    a. assessment.
    b. planning.
    c. implementation.
    d. monitoring.

    Answer: b **Reference**: Security Risk Management

59. In security risk management, a tolerable risk:

    a. doesn't exist. There is no such thing as a tolerable risk.
    b. is one where the cost of implementation is very low.
    c. is a risk that is highly likely to result in data loss.
    d. is a risk where the safeguard cost is very high or the likelihood of attack is low.

    Answer: d **Reference**: Security Risk Management

60. The phase of security risk management when a company chooses particular technologies to counter high-priority threats is called:

    a. assessment.
    b. planning.
    c. implementation.
    d. monitoring.

    Answer: c **Reference**: Security Risk Management

61. The process of identifying legitimate parties to a transaction is called:

    a. assessment.
    b. verification.
    c. authentication.
    d. monitoring.

    Answer: c **Reference**: Authentication

63. Once authenticated, a security system must often limit the actions of the authenticated parties to a subset of the total actions that can be taken on a system. To accomplish this task, a company needs a(n):

a. biometric system.
b. access control mechanism.
c. virus protection program.
d. monitoring system.

Answer: b **Reference**: Authentication

64. Before gaining access to a building, a worker must place her identification card in a reader. The reader determines whether this employee has authority to enter the door, then either releases the lock or sounds an alarm. The identification card is an example of a(n):

a. biometric system.
b. active token.
c. passive token.
d. public key infrastructure.

Answer: c **Reference**: Authentication

65. Before gaining access to a building, a worker must place her palm on a pad. The palm reader scans her hand, compares her scan to a database, and determines whether this employee has authority to enter the door, then either releases the lock or sounds an alarm. This is an example of a(n):

a. physiological biometric.
b. active token.
c. behavioral biometric.
d. passive token

Answer: a **Reference**: Authentication

66. In cryptography, the original message in human-readable form is called:

a. key.
b. plaintext.
c. ciphertext.
d. encrypted text.

Answer: b **Reference**: Private and Public Key Encryption

67. The mathematical formula used to move between plaintext to ciphertext and vice versa is called:

    a. the encryption algorithm.
    b. the key.
    c. the conversion code.
    d. the cipher.

    Answer: a **Reference**: Private and Public Key Encryption

68. An encryption key system in which the same key is used to encrypt and decrypt the message is called the:

    a. public key.
    b. asymmetric key.
    c. data key.
    d. symmetric key.

    Answer: d **Reference**: Symmetric (Private) Key System

69. One encryption key system sends the same public key to all users who use the key to encrypt messages. The resulting ciphertext, however, can't be read without a private key known only by the sender. This encryption scheme is known as:

    a. private key.
    b. data key.
    c. asymmetric key.
    d. symmetric key.

    Answer: c **Reference**: Public (Asymmetric) Key Encryption

70. The secret code used to encrypt and decrypt a message is called the:

    a. cipher.
    b. key.
    c. algorithm.
    d. digital signature.

    Answer: b **Reference**: Private and Public Key Encryption

71. The purpose of a digital certificate is to:

    a. verify that the holder of a public or private key is who they claim to be.
    b. verify the time a message was sent.
    c. verify the domain name of the computer that sent a message.
    d. encrypt data so that it cannot be easily intercepted by hackers.

    Answer: a **Reference**: Public Key Infrastructure

72. Third parties who issue digital certificates are called:

    a. certificate brokers.
    b. certificate processors.
    c. certificate issuers.
    d. certificate authorities.

    Answer: d **Reference**: Digital Certificates and Certificate Authorities

73. A protocol developed by Netscape which handles data encryption in a transparent manner within the Web browser is called:

    a. Netscape Navigator.
    b. secure socket layer.
    c. IPSec.
    d. Verisign.

    Answer: b **Reference**: Secure Socket Layer

74. A network node consisting of both hardware and software that isolates a private network from a public network is called a(n):

    a. public key.
    b. physical biometric.
    c. firewall.
    d. packet filter.

    Answer: c **Reference**: Firewalls

75. 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 are called:

    a. secure sockets.
    b. address filters.
    c. proxies.
    d. packet-filtering routers.

    Answer: d **Reference**: Firewalls

76. On the Internet, data is broken into pieces as it is routed from one computer to another. These chunks of data are called:

    a. packets.
    b. sockets
    c. proxies.
    d. routers.

    Answer: a **Reference**: Firewalls

77. Firewalls that block data and requests depending on the type of application being accessed are called:

    a. packet filters.
    b. bastion gateways.
    c. Application-level proxies.
    d. routers.

    Answer: c **Reference**: Firewalls

78. The process of encrypting data packets then encapsulating them in packets for transmission on the Internet is called:

    a. protocol tunneling.
    b. packet filtering.
    c. VPN.
    d. intrusion detection.

    Answer: a **Reference**: VPNs

79. If a company has a well-formulated security policy and sophisticated security technology in place:

    a. it should be safe from data loss or damage from attacks.
    b. it is still vulnerable to attack.
    c. it will automatically know if an intruder has violated the system.
    d. it is not fully protected until each user has a personal firewall.

    Answer: a **Reference**: Intrusion Detection Systems

80. 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 is called:

    a. virus protection.
    b. an intrusion detection system.
    c. a firewall.
    d. PKE.

    Answer: b **Reference**: Intrusion Detection Systems

Essay Questions

81. Distinguish between a technical and nontechnical attack, and give an example of each.

Answer: In a nontechnical attack, the attacker tricks people into revealing sensitive information and performing actions that can be used to compromise network security. No programming or technical expertise is required. Social engineering is an example.

Software and systems expertise are used to perpetrate a technical attack. Examples include DoS attacks, DDos attacks, worms, Trojan horses, and viruses.

Reference: Types of Threats and Attacks

82. List three common mistakes made by companies in e-security.

Answer: Three of the following:
1. Undervaluing the firm's information.
2. Narrowly defined security boundaries.
3. Reactive security management.
4. Dated security management procedures.
5. Lack of communication about security management responsibilities.

Reference: Managing EC Security

83. What are the four phases in risk management? Give a brief description of each phase.

Answer:
1. Assessment – Evaluate assets, vulnerabilities, and potential threats.
2. Planning – Arrive at a set of policies which establishes which threats are tolerable and which aren't.
3. Implementation – Chose specific technologies to address serious threats.
4. Monitoring – An ongoing process in which the company decides what is working and what isn't, as well as what new technologies are available and which new threats are emerging.

Reference: Security Risk Management

84. What are the five elements of an authentication system?

Answer:
1. A person or group to be authenticated.
2. A distinguishing characteristic that differentiates group members.
3. Someone responsible for the system being used.
4. An authentication mechanism for verifying the presence of the distinguishing characteristic.
5. An access control mechanism which limits the activities of an authenticated person.

Reference: Authentication

85. Explain firewalls and Virtual Private Networks, and how they can be used to limit the likelihood of attack.

Answer: A firewall is a network node consisting of both hardware and software that isolates a private network from a public network. By creating a firewall, a company attempts to control what information can be received and how it can be received.

A VPN uses the public Internet to carry information but remains private by using a combination of encryption to scramble communications, authentication to ensure that the information has not been tampered with and comes from a legitimate source, and access control to verify the identity of anyone using the network. This combination makes unauthorized access, eavesdropping, and sending unwanted data more difficult.

Reference: Securing EC Networks