M.Sc.(CA)(3rd Semester)

040020315: Network Security

Question Bank

Unit 1: Introduction to Network Security

Short questions

1. What are the characteristics of CIA triad?
2. What are the key principles of security?
3. How access control differ from availability?
4. Why are some attack called passive attack?
5. What is cipher text?
6. Write difference between substitution cipher and transposition cipher.
7. What are the two different uses of public key cryptography related to key distribution?
8. What are the requirements of a hash function?
9. Give an example of simple hash function.
10. Which attack is related to integrity?
11. Which public key cryptosystem can be used for digital signature?
12. Which are the require point for secure use of symmetric encryption?

Long questions

1. Discuss the reason behind the significance of authentication? Explain simple mechanism of authentication.
2. In real life, how is message integrity ensured?
3. Explain challenges of computer security.
4. Give an example where integrity is required but not confidentiality.
5. Draw and explain model for network security.
6. Distinguish between symmetric and asymmetric key cryptography.
7. From a bank's perspective, which is usually more important, the integrity of itscustomer's data or the confidentiality of the data? From the perspective of the bank's customer, which is more important?
8. Explain Feistal cipher structure principle with diagram.
9. List and briefly define categories of security service.
10. Write difference between symmetric Vs Public Key cryptography, which method is more convenient?

Multiple choice questions

1. In computer security, _____ means that computer system assets can be modified only by authorized parities.
   - A. Confidentiality
   - B. Integrity
   - C. Availability
   - D. Authenticity

2. In computer security, _____ means that the information in a computer system only be accessible for reading by authorized parities.
   - A. Confidentiality
   - B. Integrity
   - C. Availability
   - D. Authenticity

3- One of Goals Of secure computing is :
   - A. Confidentiality
   - B. Interruption
   - C. Modification
   - D. All A,B & C

4. Integrity:
   - A. Viewing, printing
   - B. Separation and protection of the resources
   - C. Access to computing resources without difficulties.

5. Cipher text is:
   - A. The encrypted form.
   - B. A system of encryption and decryption

C. Hidden writing.

6. Threats are categorized as:
   A. Passive or active
   B. Traffic
   C. Masquerade
   D. Both A and B
7. Release of message contents means:
   A. Obtain information that is being transmitted.
   B. Telephone conversation, email message and transferred files.
   C. Attack that have a specific target
   D. All of above
8. The basic elements of model of access control are:
   A. Subject, Object, Access right
   B. Capability list, Object, Access right
   C. Centralized, Decentralized
   D. All of above
9. In asymmetric key cryptography, the private key is kept by
   A. sender
   B. receiver
   C. sender and receiver
   D. all the connected devices to the network
10. Which one of the following algorithm is not used in asymmetric-key cryptography?
   A. RSA algorithm
   B. diffie-hellman algorithm
   C. electronic code book algorithm
   D. All of above
11. In cryptography, the order of the letters in a message is rearranged by
   A. transpositional ciphers
   B. substitution ciphers
   C. both (a) and (b)
   D. none of the mentioned
12. Cryptanalysis is used
   A. to find some insecurity in a cryptographic scheme
   B. to increase the speed
   C. to encrypt the data
   D. none of the mentioned

Fill in the blanks

1. _____ consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized use of a computer network and network-accessible resources.
2. The protection afforded to an automated information system in order to attain the applicable objectives of preserving the _____, availability and confidentiality of information system resources .
3. _____ is the protection of transmitted data from passive attack.
4. The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources known as _____.
5. _____ is the prevention of the unauthorized use of a resource
6. The process of attempting to discover the plaintext or key is known as _____.
7. Strategy used by _____ depend on the nature of encryption scheme and the information available to cryptanalyst.
8. A public key is denoted as _____ & private key as _____.
9. Most symmetric block ciphers are based on _____ structure.
10. In asymmetric key cryptography _____keys are required per user.
11. _____ keys are required for two people to communicate via a cipher?

Unit 2: Key Distribution and User Authentication

Short questions

1. Which are the two ways to distribute the public keys?
2. List ways in which secret keys can be distributed to two communicating parties.
3. Write difference between session key and a master key.
4. Which are the operations performed by key distribution center?
5. Which are the possible threats occur in kerberos?
6. What entities constitute a full-service Kerberos environment?
7. Write difference between version 4 and version 5 of Kerberos.
8. What is realm?
9. What is the use of ticket granting server?
10. Write two requirements to use asymmetric encryption in secure manner.
11. How is an X.509 certificate revoked?
12. List elements of X.509 format.
13. Which element store name of the user in X.509 certificate?
14. Which are the functions used in public key infrastructure?
15. Which element is used for user to modify his or her password?

Long questions

1. How to distribute key using symmetric encryption?
2. How does a client communicate with a server using Kerberos protocol? Explain in detail.
3. Explain how authentication performed in Kerberos.
4. How to distribute key using asymmetric encryption?
5. Explain the hierarchy used to store and retrieve certificate in X.509 directory service.
6. With a neat sketch explain public-key infrastructure.
7. List principle element of identify management. With neat sketch explain architecture of identify management.

Multiple choice questions

1. What is not a role of encryption ?
   a) It is used to protect data from unauthorized access during transmission.
   b) It is used to ensure user authentication.
   c) It is used to ensure data integrity.
   d) It is used to ensure data corruption doesn't happens.
2. SHA-1 produces _____bit of hash.
   a) 128 b) 160
   c) 150 d) 112
3. Which of the following is not a component of public key infrastructure?
   a) Register
   b) CA
   c) End Entity
   d) RA
4. Which trusted third party assigns a symmetric key to two parties?
   a) KDC b) KDD
   c) CA d) RSA
5. Which of the following is not a principle element of federated identity management?
   a) authentication
   b) authorization
   c) accounting
   d) password
6. Why clocks are used in a Kerberos authentication system?
   a) To ensure proper connections.
   b) To ensure tickets expire correctly.
   c) To generate the seed value for the encryptions keys.
   d) To benchmark and set the optimal encryption algorithm.
7. Which of the following factors must be considered when implementing Kerberos authentication?
   a) Kerberos can be susceptible to man in the middle attacks to gain unauthorized access.
   b) Kerberos tickets can be spoofed using replay attacks to network resources.
   c) Kerberos requires a centrally managed database of all user and resource passwords.

d) Kerberos uses clear text passwords.

8. You work as the Security Administrator at Company.com. You want to ensure that only encrypted passwords are used during authentication. Which authentication protocol should you use?
   a) PPTP (Point-to-Point Tunneling Protocol) b) SMTP (Simple Mail Transfer Protocol)
   c) Kerberos d) CHAP (Challenge Handshake Authentication Protocol)
9. When does CHAP (Challenge Handshake Authentication Protocol) perform the handshake process?
   a) When establishing a connection and at anytime after the connection is established.
   b) Only when establishing a connection and disconnecting.
   c) Only when establishing a connection.
   d) Only when disconnecting.
10. Which of the following represents a process that takes plaintext and transforms into a short code?
   a) Public Key Infrastructure
   b) Symmetric key Infrastructure
   c) Hashing
   d) Digital Signature
11. One of the most widely used public-key algorithms today is called
   a) SSL.
   b) PKI.
   c) RSA.
   d) hash code.

Fill in the blanks

1. A _____ key is a key used between entities for the purpose of distributing session keys.
2. The _____ determine which systems are allowed to communicate with each other.
3. Kerberos is a key distribution and user authentication service developed at _____.
4. Kerberos provide _____ authentication server whose function is to use authenticate users to server and server to users.
5. The client choice _____for an encryption key to be used to protect this specific application session in kerberos.
6. _____ define the framework for the provision authentication services by the X.500 directory to its users.
7. PKI as the set of hardware, software, people, policies and _____ needed to create , manage, store, distribute and revoke.
8. The _____ is often associated with the end entity registration process but can assist in a number of other areas as well.
9. Two CAs exchange information used in establishing a _____.
10. A _____ is an identity holder.
11. The identity _____ associate authentication information with principal, as well as attributes and one or more identifier.
12. An _____ service manages the creation and maintenance attribute.

Unit 3: Transport-Level Security and Email Security

Short questions

1. Which are the threats occur in web
2. What is secure socket layer?
3. List two services provided by SSL connection.
4. Which are the operation performed by SSL record protocol?
5. Write difference between SSL connection and SSL session.
6. Which are the authentication method used in authentication protocol?
7. Which are the services provided by PGP?
8. What is S/MIME?
9. What is port forwarding?
10. Which are the information stored in public-key ring?
11. List information stored in private-key ring.
12. What is the purpose of DKIM?
13. List difference MIME content type.
14. What are the five principles service provided by PGP?

Long questions

1. With a neat sketch explain secure socket layer.

2. List and briefly define the parameters that define an SSL connection.
3. List and briefly define the parameters that define an SSL session.
4. Write steps for SSL Record Protocol transmission.
5. Explain S/MIME in detail.
6. Which services provided by SSL Record protocol? Explain any three services.
7. Explain HTTPS.
8. Write phase of Handshake protocol. Explain any two phases in detail.
9. Why does PGP generate a signature before applying compression?
10. Which are the key components of internet mail architecture? Explain in detail.

Multiple choice questions

1. Which of the security provide at the transport layer?
   a) SSL b) TLS c)PGP d) SSH
2. _____ is designed to provide security and compression services to data generated from the application layer.
   a) SSL b) TLS c)PGP d) SSH
3. The combination of key exchange, hash, and encryption algorithms defines a _____ for each SSL session.
   a) List of protocols b) Cipher suite c) List of keys d) Session key
4. One of the security protocol for the e-mail system is
   a) IPSec b) SSL c) PGP d) S/MIME
5. In PGP, to exchange e-mail messages, a user needs which types of ring.
   a) Secret b) Public c)Session d) Master
6. Which of the following is used to single path from the fully trusted authority to any certificate?
   a) X.509 b) PGP c)KDC d) CA
7. Which cryptography SSH to authenticate the remote computer?
   a) public-key cryptography
   b) private-key cryptography
   c) hash function
   d) both (a) and (b)
8. Which one of the following authentication method is used by SSH?
   a) public-key b) host based
   c) password d) all of the mentioned
9. PGP encrypt data by using block cipher called
   a) international data encryption algorithm.
   b) private data encryption algorithm.
   c) internet data encryption algorithm.
   d) public data encryption algorithm.
10. For secure EDI transmission on Internat
   a) MIME is used.
   b) S/MIME is used.
   d) PGP is used
   d) TCP/IP is used.
11. Pretty good privacy (PGP) is used in
   a) browser security
   b) email security
   c) FTP security
   d) TCP security
12. Which of the following function is not provided by S/MIME?
   a) Enveloped Data
   b) Signed Data
   c) Clear-signed Data
   d) Unsigned Data
13. Which of the following information is not stored in private key ring?
   a) Timestamp
   b) KeyID
   c) Private key
   d) Signature

Fill in the blanks

1. _____ is the standard security technology for establishing an encrypted link between a web server and a browser.
2. Secure Sockets Layer (SSL) is a protocol developed by _____ for transmitting private documents via the Internet.
3. The _____ Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.
4. Handshake Protocol also defines a shared secret key that is used to form a_____.
5. The _____ Protocol is one of the three SSL-specific protocols that use the SSL Record Protocol,
6. The Alert Protocol is used to convey_____ alerts to the peer entity.
7. HTTPS (HTTP over SSL) refers to the combination of HTTP and _____ to implement secure communication between a Web browser and a Web server.
8. _____ is a protocol for secure network communications designed to be relatively simple and inexpensive to implement.
9. PGP provides a confidentiality and _____ service that can be used for electronic mail and file storage applications.
10. PGP generates a key and_____ key encrypts the message.
11. S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the _____ Internet e-mail format standard.
12. S/MIME secures a MIME _____ with a _____, encryption, or both.
13. _____ is a specification for cryptographically signing email messages, permitting a signing domain to claim responsibility for a message in the mail stream.
14. The _____ is a directory lookup service that provides a mapping between the name of a host on the Internet and its numerical address.

Unit 4:Wireless Network Security

Short questions

1. What is the basic building block of an 802.11 WLAN>
2. Define: extended service set.
3. Write format of MAC protocol data unit.
4. What security areas are addressed by IEEE 802.11i?
5. Which are the security provide in discovery phase?
6. List two ways to manage key.
7. Write difference between TKIP and CCMP?
8. Which protocol is used to protect data in IEEE 802.11i?
9. Give difference between an HTML filter and WAP Proxy.
10. Which are the services provided by WSP?
11. List keys used in WLTS.

Long questions

1. Which are the services provided by IEEE 802.11. Explain any two services in detail.
2. How is the concept of an association related to that mobility?
3. Describe the four IEEE 802.11i phases of operation.
4. When would each of three WTP transaction classes be used?
5. Which are the security services provided by WLTS? Explain any two services.
6. Explain four protocol elements used in WLTS.
7. Describe three alternative approaches to providing WAP end-to-end security.

Multiple choice questions

1. In IEEE 802.11, when a frame is going from a station to an AP, the address flag is
   a) 01.
   b) 10.
   c) 11.
   d) 00.
2. In IEEE 802.11, a BSS without an AP is called
   a) an infrastructure network.
   b) an ad hoc architecture.
   c) private network.
   d) All of above.
3. In IEEE 802.11, a station with _____ mobility is either stationary (not moving) or moving only inside a BSS.
   a) ESS-transition

b) no-transition
c) BSS-transition
d) None of the above

4. In IEEE 802.11, communication between two stations in two different BSSs usually occurs via two
a) ESSs.
b) APs.
c) BSSs.
d) ASSs.

5. In IEEE 802.11, a _____ is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).
a) BSS
b) CSS
c) ESS
d) ASS

6. The IEEE 802.11 standard for wireless LANs defines two services: _____ and _____.
a) ESS; SSS
b) BSS; ESS
b) BSS; ASS
d) BSS; DCF

7. What is the access point (AP) in wireless LAN?
a) Device that allows wireless devices to connect to a wired network
b) Wireless devices itself
c) Proxy server
d) All of above.

8. In wireless distribution system,
a) multiple access point are inter-connected with each other.
b) there is no access point.
c) only one access point exists.
d) only one access point used.

9. Which one of the following event is not possible in wireless LAN.
a) collision detection
b) Acknowledgement of data frames
c) Multi-mode data transmission
d) All of above.

10. What is Wired Equivalent Privacy (WEP) ?
a) Security algorithm for ethernet
b) Security algorithm for wireless networks
c) Security algorithm for usb communication
d) Security algorithm for ethernet

11. What is WPA?
a) wi-fi protected access
b) wired protected access
c) wired process access
d) wi-fi process access

12. Wireless Application Protocol (WAP) has several layers. Which of the following is the security layer?
a) Wireless Security Layer (WSL)
b) Wireless Transport Layer (WTL)
c) Wireless Transport Layer Security (WTLS)
d) Wireless Security Layer Transport (WSLT)

13. WPA2 is used for security in
a) ethernet.
b) bluetooth.
c) wi-fi.
d) internet.

14. Extensible authentication protocol is authentication framework frequently used in
a) wired personal area network.
b) wireless networks.

c) wired local area network.
d) All of above.

Fill in the blanks

1. _____ is a committee that has developed standards for a wide range of local area networks (LANs).
2. The Wi-Fi _____ is concerned with a range of market areas for WLANs, including enterprise, home, and hot spots.
3. The _____ layer receives data from a higher-layer protocol, typically the Logical Link Control (LLC) layer, in the form of a block of data known as the MAC service data unit (MSDU).
4. The _____ layer is responsible for detecting errors and discarding any frames that contain errors.
5. An _____ service set (ESS) consists of two or more basic service sets interconnected by a distribution system.
6. Reassociation enables an established association to be transferred from one AP to another, allowing a mobile station to move from one _____ to another.
7. _____ is a notification from either a station or an AP that an existing association is terminated.
8. Distribution is the primary service used by stations to exchange_____ when the _____ must traverse the DS to get from a station in one BSS to a station in another BSS.
9. A _____ protocol is used to define an exchange between a user and an AS that provides mutual authentication and generates temporary keys to be used between the client and the AP over the wireless link.
10. A _____ is a secret key shared by the AP and a STA, and installed in some fashion outside the scope of IEEE 802.11i.
11. _____ is designed to require only software changes to devices that are implemented with the older wireless LAN security approach called Wired Equivalent Privacy (WEP).
12. TKIP adds a _____ bit message integrity code (MIC), generated by an algorithm, called Michael, to the 802.11 MAC frame after the data field.
13. Wireless Transport Layer Security (WTLS) provides security services between the mobile device (client) and the WAP_____.
14. The WAP Programming Model is based on three elements: the client, the_____, and the original server
15. _____ markup language was designed to describe content and format for presenting data on devices with limited bandwidth, limited screen size, and limited user input capability.

Unit 5:IP Security

Short questions

1. Why IP security necessary?
2. How IP security achieved?
3. List application of IPSec.
4. Write advantage of IPSec.
5. Give example of application of IPSec.
6. Which services provided by IPSec?
7. Differentiate the packet structure of ESP and AH.
8. Why does ESP including a padding field?
9. Which are the basic approaches to bundling SAs?
10. Which are the three different authentication method can be used with IKE key management?

Long questions

1. What is the purpose security association? Explain database of security association.
2. Explain ESP header format and discuss the inbound and outbound processing of IPSec
3. Explain roles of the Oakley key determination protocol and ISAKMP in IPSec.
4. Where does the IPSec reside in a protocol stack?
5. Can IP security used to secure Wi-Fi network? Justify.
6. Explain key determine protocol.

Multiple choice questions

1. IPSec is designed to provide the security at the
   a) transport layer.
   b) network layer.
   c) application layer.
   d) session layer.
2. In tunnel mode IPsec protects the
   a) entire IP packet.

b) IP header.
c) IP payload.
d) IP footer.

3. IPSec defines two protocols: _____ and _____.
a) AH; SSL
b) PGP; ESP
c) AH; ESP
d) PGP; SSL

4. Which of the following provides authentication at the IP level?
a) AH
b) ESP
c) PGP
d) SSL

5. Which of the following provides either authentication or encryption, or both, for packets at the IP level?
a) AH
b) ESP
c) PGP
d) SSL

6. IPSec uses a set of SAs called the _____.
a) SAD
b) SAB
c) SADB
d) SADE

7. Which of the following protocol designed to create security associations, both inbound and outbound.
a) SA
b) CA
c) KDC
d) IKE

8. IKE creates SAs for
a) VP.
b) IPSec.
c) PGP.
d) SSL.

9. IKE uses _____.
a) Oakley
b) SKEME
c) ISAKMP
d) all of the above

10. What are the two modes of IP security?
a) transport and certificate
b) transport and tunnel
c) tunnel and certificate
d) transport and pre-shared

11. The _____ is used to provide integrity check, authentication and encryption to IP datagram.
a) SSL
b) ESP
c) TSL
d) PSL

12. Which of the following protocol designed by Internet Engineering Task Force(IETF) to provide security for a packet at the Network level?
a) IPsec
b) Netsec
c) Packetsec
d) Protocolsec

Fill in the blanks

1. IP-level security encompasses three functional areas: authentication, _____, and key management.
2. The _____ mechanism assures that a received packet was transmitted by the party identified as the source

in the packet header, and that the packet has not been altered in transit.
3. The _____ networking device will typically encrypt and compress all traffic going into the WAN, and decrypt and decompress traffic coming from the WAN.
4. _____ is an extension header for message authentication
5. ESP consists of an encapsulating _____ and _____ used to provide encryption or combined encryption/authentication.
6. _____ is a collection of documents describing the key management schemes for use with IPsec.
7. Tunnel mode ESP is used to encrypt an entire _____ packet.
8. _____can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality.
9. The _____ is used to provide integrity check, authentication and encryption to IP datagram.
10. The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for Internet key management and provides the specific protocol support, defining procedures and packet formats to establish, _____, modify, and delete security associations.
11. The _____ exchange can be used to establish further SAs for protecting traffic.

Unit 6: Intruders and Firewalls

Short questions

1. What are the two common techniques used to protect a password file?
2. List three benefits that can be provided by intrusion detection system.
3. What open standards exist for IDSs?
4. What metrics are useful for profile based intrusion detection?
5. Write difference between rule-based anomaly detection and rule-based penetration identification.
6. What is the salt in the context of UNIX password management?
7. List three design goal of firewall.
8. Which are the techniques used by firewall to control access and enforce a security policy?
9. Write weakness of a packet filtering firewall.
10. What are the common characteristics of a bastion host?
11. What is an application gateway?
12. Why is it useful to have host-based firewall?
13. Differentiate IDS and firewall.
14. Name some packet screening tools.

Long questions

1. List and briefly define three classes of intruders.
2. What are the two common exploit? How does the system get hacked?
3. State the components of IDS and explain their function.
4. Compare the features of host-based IDS and network based IDS. Why, when and where to use host-based IDS.
5. How honeypots used for securing the network system?
6. List and briefly define four techniques used to avoid guessable password.
7. State the advantage and disadvantage of using firewall.
8. What is IP address Spoofing? How can it be prevented using firewalls?
9. What is the difference between a packet filtering firewall and stateful inspection firewall?
10. Are gateway different from firewall? Justify the answer.

1. What primary advantage does an IPS offer over IDS that makes it a crucial component of a security strategy?
    a) The amount of logs generated
    b) The speed at which attacks can be mitigated
    c) The lower price tag
    d) A reduced quantity of false positives
2. Which of the following is not an important failure mode for an intrusion detection system?
    a) False positives
    b) Subversion errors
    c) False negatives
    d)Synchronization errors
3. Which of the following detection mechanisms might an IPS employ?
    a) packet anomaly detection
    b) generic pattern matching
    c) TCP connection analysis
    d) All of the above

4. At which two traffic layers do most commercial IDSes generate signatures?
   a) application layer
   b) network layer
   c) session layer
   d) transport layer
5. An IDS follows a two-step process consisting of a passive component and an active component. Which of the following is part of the active component?
   a) Inspection of password files to detect inadvisable passwords
   b) Mechanisms put in place to reenact known methods of attack and record system responses
   c) Inspection of system to detect policy violations
   d) Inspection of configuration files to detect inadvisable settings
6. Which of the following is used to provide a baseline measure for comparison of IDSes?
   a) crossover error rate
   b) false negative rate
   c) false positive rate
   d) bit error rate
7. Network layer firewall works as a
   a) frame filter.
   b) packet filter.
   c) block filter.
   d) All of above.
8. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as
   a) chock point.
   b) meeting point.
   c) firewall point.
   d) secure point.
9. Which of the following is / are the types of firewall?
   a) Packet Filtering Firewall
   b) Dual Homed Gateway Firewall
   c) Screen Host Firewall
   d) All of the above
10. In packet-filtering router, the following information can be external from the packet header.
i) Source IP address ii) Destination IP address
iii) TCP/UDP source port iv) ICMP message type
v) TCP/UDP destination port
   a) i, ii, iii and iv only
   b) i, iii, iv and v only
   c) ii, iii, iv and v only
   d) All i, ii, iii, iv and v
11. Network layer firewall has two sub-categories as
   a) stateful firewall and stateless firewall
   b) bit oriented firewall and byte oriented firewall
   c) frame firewall and packet firewall
   d) screen host firewall and statefull firewall

Fill in the blanks

1. The objective of the _____ is to gain access to a system or to increase the range of privileges accessible on a system.
2. _____anomaly detection collect data relating to the behavior of legitimate users, then use statistical tests to determine with a high level of confidence whether new behavior is legitimate user behavior or not.
3. Profile based develop profile of activity of each user and use to _____ changes in the behavior
4. Rule-based detection attempt to define a set of rules used to decide if given behavior is an _____.
5. A fundamental tool for intrusion detection is the _____.
6. _____ audit records implement collection facility to generates custom audit records with desired info, advantage is it can be vendor independent and portable.
7. A _____ password checking strategy is one in which the system periodically runs its own password cracker to find guessable passwords.

8. A _____ is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter, forming a single choke point where security and audit can be imposed.
9. A packet-filtering router applies a set of rules to each incoming and outgoing IP packet to forward or _____the packet.
10. An _____ gateway (or proxy server), acts as a relay of application-level traffic.
11. A _____ firewall is a software module used to secure an individual host. Such modules are available in many operating systems or can be provided as an add-on package.
12. A _____ firewall controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side.