Subject : Network Security
Code : XCS593
Department : MSc SE
Semester : Nineth

Name of Staff: Anusha Linda Kostka
Department : MSc SE/CT/IT

Part A (2 marks)

1. What are the various layers of an OSI reference model?
   Application, Presentation, Session, transport, Network, Data Link, Physical layers.

2. What are important layer 4 protocols?
   TCP and UDP

3. What is a passive attack?
   A passive attack is one in which the intruder eavesdrops but does not modify the message stream in any way.

4. What is an active attack?
   An active attack is the one in which the intruder may transmit messages, replay old messages, modify messages in transit.

5. Difference between authentication and authorization?
   Authentication – who you are.
   Authorization – what you are allowed to do.
6. Define a virus.
   A virus is a set of instructions when executed inserts copies of itself into other programs.

7. What is a worm?
   It is a program that replicates itself by installing copies of itself on other machines across a network.
8. What is zombie?
   They are malicious instructions installed on a system that can be triggered to carry out an attack with less traceability.

9. What is a trapdoor?
   It is an undocumented entry point intentionally written into a program, for debugging purposes.

10. What are digital pest?
    All kinds of malicious software,' are digital pests.

11. What is a polymorphic virus?
    To evade detection of viruses, polymorphic viruses are devised.

12. What are non-discretionary access controls?
    They enforce a policy where users might be allowed to use information themselves but not to make a copy of it.

13. What are the components of security label?
    a. Security level.
    b. Categories
14. What is a security level?
    It is an integer which consists of unclassified, confidential, secret and topsecret.

15. What are categories?
    Categories are known as compartments which describe kinds of information.

16. Define discretionary?
    Someone who owns a resource can make a decision as who is allowed to use it.

17. What is a covert channel?
It is a method for a Trojan horse to circumvent the automatic confinement of information within a security perimeter.

18. Give an example of covert channel?
    a. Timing channel.
    b. Storage channel

19. What are the services provided by cryptography?
    a. Integrity checking
    b. Authentication

20. What is a ciphertext?
        The mangled information is the cipher text.

21. What is encryption?
    The process of producing ciphertext from plaintext is known as encryption.

22. What is decryption?
The reverse process ids called decryption

23. What are the basic attacks of breaking an encryption scheme?
    Ciphertextonly, known plaintext, chosen plaintext.

24. What are the types of cryptographic functions?
    a. Secret key cryptography
    b. Public key
    c. Hash functions

25. What is permutation?
    A permutation specifies k input bits and the output position to which it goes.

26. What are the operations of IDEA?
    a. Bitwise exclusive
    b. Slightly modified add
    c. Slightly modified multiply

27. How many rounds are present in IDEA?
    17 rounds

28. What are the operations of AES?
    a. Exclusive or
    b. Octet for octet substitution
    c. Rearrangement of octets rotating a row or column by number of cells
    d. Mixcolumn.

29. How is a mixcolumn implemented?
    It is a single table containing 256 4 octet columns. Each of the 4 octets is used as an index to retrieve column from the table.

30. What are the various modes of operation?
    a. Electronic code book
    b. Cipher block chaining
    c. Cipher feedback mode
    d. Counter mode
    e. Output feedback mode

31. What is the min problem with Cipher block chaining?
    Efficiency

32. What are the various modular arithmetic?
    a. Modular Addition
    b. Modular multiplication
    c. Modular exponentiation.

33. What is the length of RSA?
    512 bits

34. How efficient are RSA operations?
    a. Exponentiating with big numbers
    b. Generating RSA keys

35. How are RSA keys generated?
    a. Finding big primes p and q
    b. Finding d and e

36. Define relatively prime.
    They donot share any common factors other than 1

37. What is an additive inverse?
    It is the number you have to add to x to get 0.

38. What is multiplicative inverse?
    The number which you have to multiply x to get 1.

39. What are the important capabilities of authentication?
    a. To store high quality cryptographic key
    b. To perform cryptographic operations

40. What are the Main techniques of authentication?
    a. What you know
    b. What you have
    c. What you are

41. What is an authentication token?
    A authentication token is a physical device that a person carries around and uses in authenticating.

42. Give an example of authentication token?
    Smart Card

43. What is a smart card?
    It is a device about the size of the size of credit card but with an embedded CPU and memory.

44. What are the various forms of smart cards?
    a. PIN protected memory cards
    b. Cryptographic challenge/response cards
    c. Cryptographic calculator

45. What is authentication?
Authentication is a process of reliably verifying the identity of someone.

46. What are the forms of authentication?
    a. Password based authentication
    b. Address based
    c. Cryptographic

47. What is a password based authentication?
    It refers to a secret quantity that you state to prove you know it.

48. What is an online attack?
    The system makes it impossible to guess too many passwords.

49. How is a password stored?
    a. Information is configured into a server.
    b. Authentication storage node stores the information and server retrieves it
    c. Authentication facilitator node does the authentication.

50. What is an address based authentication?
    It does not rely on sending password around the network but assumes that the identity can be inferred from the network address from which the packets arrive.

51. What is a KDC?
    It is a Key Distribution Center which knows the keys for all the nodes.

52. What is a certification authority?
    It generates certificates that are signed messages specifying a name and the corresponding public key.

53. Where are the certificates stored?
        Certificates are stored in a directory service.

54. State 2 advantages of CAs over KDCs?
    a. The CA does not need to be online
    b. Certificates are not security sensitive

55. What is Kerberos?
    It is a secret key based service for providing authentication in a network.

56. What are the versions of Kerberos?
    Version 4 and 5

57. How is a Kerberos implemented?
58. It is implemented using KDC that runs on a secure node somewhere on the network and a library of subroutines.
59. What is a ticket?
    The message consisting of the session key encrypted with Bs master key is the ticket.

60. What is a KDC master key?
    To keep the KDC database secure the stored master keys are stored encrypted by a key known as KDC master key.

61. What are credentials?
    a. SESSION KEY
    b. TICKET GRANTING TICKET

62. What does a TGT contain?
    a. Session key
    b. User name
    c. Expiration time.

63. What is an IPSec Security Association?
    It is a cryptographically protected connection.
64. What are types of IPsec headers?
    AH and ESP

65. Difference between AH and ESP?
    a. AH – provides integrity protection only
    b. ESP – provides encryption to integrity protection.

66. What are the modes of IPsec protection to a packet?
    a. Transport mode
    b. Tunnel mode

67. What is a transport mode?
    It refers to adding the IPsec information between Ip header and the remainder of the packet.

68. What is a tunnel mode?
    It refers to keeping the original IP packet intact and adding a new IP header and the IPsec information outside.

69. What are the fields of IPV4 header?
    a. Version
    b. Header length
    c. Type of service
    d. Length of header plus data
    e. Packet identification
    f. Flags
    g. Fragment offset
    h. Hops
    i. Protocol;
    j. Header checksum
    k. Source address
    l. Destination address
    m. Options

70. What are the fields of IPV6 header?
    a. Version
    b. Payload Header
    c. next header
    d. Hops
    e. Source address
    f. Destination address.

71. What are the fields in Authentication header?
    a. Next header
    b. Payload length
    c. SPI
    d. Sequence number
    e. Authentication data

72. What are the fields in ESP?
    a. SPI
    b. Sequence number
    c. IV
    d. Data
    e. Padding
    f. Padding length
    g. Next header
    h. Authentication data

73. What are the various secure mail standards?
    S/MIME, PEM , PGP

74. What is a distribution list?
    It is a name that stands for a set of recipients.

75. What are the ways of implementing distribution lists?
    a. Remote Explorer method
    b. Local Explorer method

76. What are the advantages of local explorer method?
    a. Easier to prevent mail forwarding loops
    b. It is possible for the sender to prevent duplicate copies being sent to individuals on multiple lists.

77. What are the advantages of remote explorer method?
    a. Allows you to end to a list whose membership you are not allowed to know.
    b. If organized geographically, send only one copy of messageto a remote area.
78. State 2 reasons for needing multiple MTAs along a path from the source to the destination?
    a. Path from source to destination may be intermittent.
    b. For security reasons it might need to authenticate other MTAs as well as user machines.

79. What are the features of security of electronic mails?
    a. PRIVACY
    b. Authentication
    c. Integrity
    d. Non repudiation
    e. Proof of submission
    f. Proof of delivery

80. Define anonymity\
    The ability to send a message so that the recipient can't find out the identity of the sender.

81. What is privacy?
    It is the ability to keep anyone but the intended recipient from reading the message.

82. Define authentication?
    It is the reassurance to the recipient of the identity of the sender.

83. What is third party authentication?
    The ability of the recipient to prove the third party that the sender send the message.

84. What is containment?
    The ability of the network to keep certain security levels of information from leaking out of a particular region.

85. What is audit?
    The ability of the network to record events that might have some security relevance.

86. Define repudiation?
    It is the act of denying that you sent a message.

87. What is self destruct?
    It is an option allowing a sender to specify that a message should be destroyed after delivery to the recipient.

88. What is accounting?
    The ability of the mail system to maintain system usage statistics.

89. What are the keys established in security services?
    a. Public keys
    b. Secret keys

90. What is a firewall?
    A firewall is a computer that sits between your internal network and the rest of the network and attempts to prevent bad things from happening.

91. What is a stateful packet filter?
    A packet filter that remembers what has happened in the recent past and changes its filtering rules dynamically as a result.

92. What is bastion host?
    An application gateway is the bastion host.

93. What is DMZ?
    The portion of the network between the two firewalls is Demilitarized zone(DMZ)

94. What is a tunnel?
    It is a point to point connection in which the actual communication occurs across the network.

95. what is a deniel of service attack?
    It is the one in which the attacker prevents good guys from accessing a service, but does not enable unauthorized access to any services.

96. What is a distributed denial of service attack?
    In this form of attack it breaks into lots of innocent machines and installs software on them to attack the victim machine. The innocent machines are called zombies or drones.

97. What is a spider or robot?
    This is an automated program used by search engines to search through the web and the index information so that when someone does the search for specific information the search engine can return the answer quickly

98. What are the types of HTTP request types?
    GET and POST

99. What is a cookie?
    It is a data structure created by the server and stored at the client.

100. What are the ways of correlating information in cookies?
    a. Server logs
    b. Eavesdropping
    c. Proxy logs
    d. Redirects or embedded images
    e. Software at the client

Part B (16 marks)

1. What are the types of cryptographic functions ? Explain each.
    a. Secret key cryptography
        i. Security issues
        ii. Transmitting over insecure channel
        iii. Secure storage on insecure media
        iv. Authentication
        v. Integrity check

    b. Public key cryptography
        i. Security issues
        ii. Transmitting over an insecure channel
        iii. Secure storage on insecure media
        iv. Authentication

    c. Hash Algorithms
        i. Password Hashing
        ii. Message integrity
        iii. Message fingerprint
        iv. Downline load security
        v. Digital Signature Efficiency

2. Explain public key cryptography in detail.
        i. Security issues
        ii. Transmitting over an insecure channel
        iii. Secure storage on insecure media
        iv. Authentication

3. Explain Data Encryption standard in detail.
    a. 64 bit input subjected to initial permutation to obtain 64 bit result
    b. 56 bit key is used to generate 16 48 bit per round keys.
    c. Permutation of the data
    d. Generating per round keys
    e. DES Round
    f. The Mangler Function
    g. Weak and Semi weak keys

4. Explain the various modes of operation?
    a. Electronic code block
    b. Cipher block chaining- if same block repeats in the plaintext it will not cause repeat in the ciphertext.
        i. Modifying ciphertext blocks
        ii. Rearranging ciphertext blocks
    c. Cipher Feedback mode – similar to OFB
    d. Output Feedback mode- stream cipher
    e. Counter mode

5. What are the types of authentication? Explain each.
    a. Password based- It refers to a secret quantity that you state to prove you know it.
        i. Off and Online password guessing
        ii. Storing user passwords
            1. Information is configured into a server.
            2. Authentication storage node stores the information and server retrieves it
            3. Authentication facilitator node does the authentication.
    b. Address based – It does not rely on sending password around the network but assumes that the identity can be inferred from the network address from which the packets arrive.
        i. Implementation in Unix
        ii. Network address impersonation
    c. Cryptographic authentication protocols.

6. Explain password based authentication in detail.
    Password based- It refers to a secret quantity that you state to prove you know it.
        i. Off and Online password guessing
        ii. Storing user passwords
            1. Information is configured into a server.
            2. Authentication storage node stores the information and server retrieves it
            3. Authentication facilitator node does the authentication.

7. What are authentication tokens? Explain with examples.
    A authentication token is a physical device that a person carries around and uses in authenticating.
    example of authentication token
    Smart Card
    It is a device about the size of the size of credit card but with an embedded CPU and memory.
    The various forms of smart cards?
    a. PINprotected memory cards
    b. Cryptographic challenge/response cards
    c. Cryptographic calculator

8. Explain trusted intermediaries in detail.
    a. Key distribution Center
    b. Certification Authorities
    c. Certificate Revocation
    d. Multiple Trusted intermediaries
        i. Multiple KDC Domains
        ii. Multiple CA Domains

9. Explain RSA Algorithm in detail.
    a. Generate a public key, e
    b. Generate a private key, d
    c. Encrypt a message, m
    d. Decrypt a message, c
    e. Sign a message, s
    f. Verify the signature

10. How efficient are RSA operations?
    a. Exponentiating with big numbers
    b. Generating RSA keys

    RSA keys generated

    a. Finding big primes p and q
    b. Finding d and eg public/private key
    c. Calculate a message digest
    d. Compute the signature
    e. Transmit the messagesm, per message public number, the signature x
    f. Verify the signature.

11. Explain DSS Algorithm in detail.
    a. Generate p and q
    b. Generate g
    c. Choose a long term public/private key
    d. Choose a per ms
12. Explain Kerberos in detail.

    Kerberos- It is a secret key based service for providing authentication in a network.

    a. Tickets and Ticket granting ticket
    b. Configuration

13. How will you log into the network using Kerberos?
    a. Obtaining a session key and TGT
        i. Seesion key
        ii. TGT, username, expiration time
        iii. Talking to a remote node

14. Difference between IPv4 and IPv6?

    Fields of IPV4 header

    a. Version
    b. Header length
    c. Type of service
    d. Length of header plus data
    e. Packet identification
    f. Flags
    g. Fragment offset

h. Hops
i. Protocol;
j. Header checksum
k. Source address
l. Destination address
m. Options

Fields of IPV6 header?

n. Version
o. Payload Header
p. next header
q. Hops
r. Source address
s. Destination address.

15. Briefly explain Authentication header?
    a. Next header
    b. Payload length
    c. SPI
    d. Sequence number
    e. Authentication data

16. Briefly explain the fields in ESP?
    a. SPI
    b. Sequence number
    c. IV
    d. Data
    e. Padding
    f. Padding length
    g. Next header
    h. Authentication data

17. Give a brief note on Cookies.
    a. The cookie is a data structure created by the server and stored at the client.
    b. Alternatives to cookies.
    c. Cookie rules
    d. Tracking users
        i. Server logs
        ii. Eavesdropping
        iii. Proxy logs
        iv. Redirects or embedded images
        v. Software at the client.

18. Briefly explain firewalls.

1. A firewall is a computer that sits between your internal network and the rest of the network and attempts to prevent bad things from happening.
2. A packet filter that remembers what has happened in the recent past and changes its filtering rules dynamically as a result.
3. An application gateway is the bastion host.
4. The portion of the network between the two firewalls is Demilitarized zone(DMZ).
5. Encrypted tunnels

19. What are security services of Electronic mail.Define each?

anonymity\

The ability to send a message so that the recipient can't find out the identity of the sender.

privacy

It is the ability to keep anyone but the intended recipient from reading the message.

authentication

It is the reassurance to the recipient of the identity of the sender.

third party authentication

The ability of the recipient to prove the third party that the sender send the message.

Containment

The ability of the network to keep certain security levels of information from leaking out of a particular region.\

audit

The ability of the network to record events that might have some security relevance.

Repudiation

It is the act of denying that you sent a message.

self destruct

It is an option allowing a sender to specify that a message should be destroyed after delivery to the recipient.

accounting

The ability of the mail system to maintain system usage statistics.

20. Structure of PEM message.
    a. Different types can be combined into a message
        i. Ordinary unsecured data
        ii. Integrity protected unmodified data
        iii. Integrity protected encoded data
        iv. Encoded encrypted integrity protected data.