Master of Technology in Computer Technology

Second Year First Semester Examination

2024

Subject: Network Security

Time: 3 Hours | Full Marks: 100

Answer All Questions

1. (a) Distinguish between passive attacks and active attacks. What are the various forms of these two attacks? Briefly explain.
   (b) Explain how confidentiality and authentication can be achieved using public-key cryptography.
   (c) Explain how digital signature of a message is generated .
   (d) What is the difference between a "Known-Plaintext" attack and a "Chosen-Plaintext" attack? Which one is more easy and beneficial from a cryptanalyst point of view and why? Justify your answer.
   (e) Explain what is meant by weak collision resistance of a hash function. Explain what would have happened if a hash function is not weak collision resistant?
   (f) Differentiate between block ciphers and stream ciphers.

   4+3+3+4+3+3=20

2. (a) What are the different entities in Kerberos authentication system? State the roles of each.
   (b) An enterprise network system uses Kerberos authentication system to authenticate users to different services (i.e. http, ftp, mail, print etc.). Identify different authentication messages exchanged between the Kerberos client in one of the users machine and other servers when the user
      (i) First logs into the system
      (ii) Uses mail service
      (iii) Uses http service
      (iv) Uses mail service again

      Describe the content of each message.
   (c) In the above authentication scenario what will happen if the Ticket Granting Server is absent.
   (d) What are the drawbacks of Kerberos authentication system?

   4+10+3+3=20

3. (a) Explain how PGP provides the security services confidentiality, authentication, and message integrity.
   (b) Explain the necessity of Radix-64 conversion in PGP operation.
   (c) How does PGP generate per session symmetric key?
   (d) How does a PGP client retrieves private keys from PGP Private Key Ring?
   (e) What are the significances of the Owner Trust, Key Legitimacy and Signature Trust fields of PGP public key-rings?

   4+3+3+4+6=20

4. (a) Describe how a firewall can achieve the following design objectives?
   (i) Service control
   (ii) Direction control
   (iii) User control
   (iv) Behavior control
   (b) What is the difference between a packet filtering firewall and a stateful inspection firewall?
   (c) Explain the "default-deny" and "default-allow" options of filtering packets through a firewall. What are the pros and cons, if any?
   (d) What is the usefulness of host based firewalls?
   (e) Differentiate between Correlation Anomaly and Redundancy Anomaly in firewall rule set. Provide a suitable example.

   6+4+3+2+5=20

5. (a) Differentiate between a SSL connection and a SSL session.
   (b) Explain how SSL record protocol provides confidentiality and integrity services?
   (c) Explain how two parties A and B can establish a shared secret key K between themselves using Diffie-Hellman Key Exchange protocol.
   (d) Describe how an active attacker can mount a Man in The Middle attack against this protocol. State one way to prevent this kind of attack.
   (e) Explain how the pre master secret is established in SSL handshake protocol using each of the following key exchange algorithms
   (i) Ephemeral Diffie-Hellman
   (ii) Anonymous Diffie-Hellman

   3+3+4+6+4=20

6. (a) How does IPSec differ from SSL? Which security services does IPSec provide?
   (b) Mention some example scenarios where IPSec is useful.
   (c) Differentiate between the transport and tunnel mode of IPSec operation.
   (d) Explain how Message Authentication Code (MAC) is generated in both AH and ESP.
   (e) Explain how ESP provides limited traffic flow confidentiality.

   3+4+3+6+4=20

7. (a) Describe the usage of a digital certificate?
   (b) Describe the X.509 digital certificate format.
   (c) Identify cases when revocation of user certificates is necessary and briefly describe how it is done.
   (d) Assume you can only use a hash function H and a symmetric-key encryption algorithm that takes a secret key K. Show how would you transmit a message M from user A to user B so that the following are guaranteed: (i) Message Authentication and Integrity (ii) Confidentiality (iii) Message Authentication, Integrity and Confidentiality.
   (e) Assume you can only use a hash function H and a secret key S. Show how would you transmit a message M from user A to user B so that both message authentication and integrity are guaranteed. You should not use any encryption.

   3+4+3+6+4=20