UNIT – V: E-Mail Security, IP Security & Case Studies

1. PGP stands for:
A) Private Good Privacy
B) Pretty Good Privacy
C) Protected Group Privacy
D) Public Good Privacy

Answer: B

2. PGP is primarily used for:
A) Database Security
B) Email Security
C) Network Routing
D) Operating Systems

Answer: B

3. PGP combines which cryptographic techniques?
A) Only Symmetric Cryptography
B) Only Asymmetric Cryptography
C) Hybrid Cryptography
D) Hashing Only

Answer: C

4. Which service is provided by PGP?
A) Confidentiality
B) Authentication
C) Integrity
D) All of the Above

Answer: D

5. S/MIME stands for:
A) Secure Mail Internet Message Extension
B) Secure Multipurpose Internet Mail Extensions
C) Security MIME Extension
D) Secure Message Internet Mail Extension

Answer: B

6. S/MIME is based on:
A) X.509 Certificates
B) DES
C) RC4
D) IDEA

Answer: A

7. Which of the following secures e-mail messages?
A) SSH
B) TLS
C) PGP
D) FTP

Answer: C

8. Digital signatures in e-mail provide:
A) Compression
B) Authentication
C) Routing
D) Storage

Answer: B

9. Which standard is widely used in commercial e-mail security?
A) S/MIME
B) TCP
C) UDP
D) SMTP

Answer: A

10. PGP uses a combination of public key and:
A) Stream Key Cryptography
B) Symmetric Key Cryptography
C) Hashing Only
D) Transposition

Answer: B

IP Security (IPSec)

IP Security Overview & Architecture

11. IPSec operates at which OSI layer?
A) Application Layer
B) Transport Layer
C) Network Layer
D) Data Link Layer

Answer: C

12. IPSec is designed to provide security for:
A) IP Packets
B) Email Messages
C) Databases
D) Web Pages

Answer: A

13. IPSec provides:
A) Authentication
B) Confidentiality
C) Integrity
D) All of the Above

Answer: D

14. The architecture of IPSec is defined by:
A) Security Associations (SA)
B) FTP
C) SMTP
D) DNS

Answer: A

15. A Security Association (SA) is identified by:
A) SPI
B) TCP Port Number
C) MAC Address
D) URL

Answer: A

Authentication Header (AH)

16. AH stands for:
A) Authentication Header
B) Access Header
C) Authorization Header
D) Application Header

Answer: A

17. AH provides:
A) Authentication and Integrity
B) Encryption Only
C) Compression
D) Routing

Answer: A

18. AH protects against:
A) Replay Attacks
B) Packet Loss
C) Congestion
D) Fragmentation

Answer: A

19. AH does not provide:
A) Integrity
B) Authentication
C) Confidentiality
D) Replay Protection

Answer: C

20. Which field is used to detect replay attacks in AH?
A) Sequence Number
B) TTL
C) Port Number
D) Checksum

Answer: A

Encapsulating Security Payload (ESP)

21. ESP stands for:
A) Encryption Security Payload
B) Encapsulating Security Payload

C) Encapsulation Security Protocol
D) Encoded Security Payload

Answer: B

22. ESP provides:
A) Confidentiality
B) Integrity
C) Authentication
D) All of the Above

Answer: D

23. Which IPSec protocol encrypts packet data?
A) AH
B) ESP
C) SSL
D) SMTP

Answer: B

24. ESP can operate in:
A) Transport Mode
B) Tunnel Mode
C) Both A and B
D) None of the Above

Answer: C

25. Tunnel mode is commonly used in:
A) VPNs
B) LAN Switching
C) Routing Tables
D) Databases

Answer: A

Combining Security Associations

26. Multiple Security Associations used together are called:
A) SA Bundle
B) Security Chain
C) Packet Chain
D) Crypto Link

Answer: A

27. Combining AH and ESP can provide:
A) Authentication
B) Confidentiality
C) Integrity
D) All of the Above

Answer: D

Internet Key Exchange (IKE)

28. IKE stands for:
A) Internet Key Encryption

B) Internet Key Exchange
C) Internal Key Exchange
D) Integrated Key Exchange

Answer: B

29. IKE is used for:
A) Key Management
B) Routing
C) Compression
D) Storage

Answer: A

30. IKE automates the creation of:
A) Security Associations
B) Routers
C) Databases
D) Switches

Answer: A

31. Secure Multiparty Computation allows parties to:
A) Share private keys
B) Compute jointly without revealing inputs
C) Encrypt emails
D) Route packets

Answer: B

32. Main goal of Secure Multiparty Computation is:
A) Privacy Preservation
B) Compression
C) Routing
D) Storage

Answer: A

33. Secure Multiparty Computation is useful in:
A) Secure Voting Systems
B) Data Analytics
C) Auctions
D) All of the Above

Answer: D

34. Virtual Elections require:
A) Confidentiality
B) Integrity
C) Voter Authentication
D) All of the Above

Answer: D

35. Electronic voting systems should ensure:
A) Vote Privacy
B) Vote Integrity

C) Verifiability
D) All of the Above

Answer: D

36. Digital signatures help virtual elections by providing:
A) Authentication
B) Compression
C) Routing
D) Switching

Answer: A

Single Sign-On (SSO)

37. SSO stands for:
A) Single Sign-On
B) Secure Sign-On
C) System Sign-On
D) Security Service Option

Answer: A

38. SSO allows users to:
A) Use multiple passwords
B) Authenticate once and access multiple services
C) Access only one application
D) Avoid authentication

Answer: B

39. An advantage of SSO is:
A) Reduced Password Fatigue
B) Increased Network Traffic
C) More Passwords
D) Less Security

Answer: A

40. Which protocol is commonly used in SSO systems?
A) Kerberos
B) FTP
C) ARP
D) ICMP

Answer: A

41. Secure payment transactions require:
A) Authentication
B) Confidentiality
C) Integrity
D) All of the Above

Answer: D

42. Encryption in banking transactions ensures:
A) Confidentiality
B) Compression

C) Routing
D) Fragmentation

Answer: A

43. Digital signatures in payment systems provide:
A) Non-repudiation
B) Compression
C) Routing
D) Data Storage

Answer: A

44. Secure banking systems commonly use:
A) PKI B) Hub Networks
C) FTP D) Telnet

Answer: A

45. XSS stands for:
A) Cross-Site Scripting
B) Cross-System Security
C) Extended Security Service
D) Cross-Site Scanning

Answer: A

46. XSS is primarily a:
A) Network Attack
B) Web Application Vulnerability
C) Physical Attack
D) Wireless Attack

Answer: B

47. Stored XSS attacks store malicious scripts in:
A) Database B) Router
C) Switch D) Firewall

Answer: A

48. Reflected XSS occurs when malicious code is:
A) Stored permanently
B) Reflected from a web server response
C) Encrypted
D) Compressed

Answer: B

49. XSS attacks often target:
A) User Browsers
B) Routers
C) Databases
D) Switches

Answer: A

50. A common defense against XSS is:
A) Input Validation and Output Encoding

B) Increasing Bandwidth
C) Packet Fragmentation
D) Data Compression

Answer: A