

Code No: 07A7EC39

R07**Set No. 2**

IV B.Tech I Semester Examinations, November 2010
INFORMATION SECURITY
Information Technology

Time: 3 hours**Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

1. (a) Define a Security attack. Explain in detail about the various types of attacks an Internetwork is vulnerable to.
 (b) Write about Man-in-the-middle attacks. [10+6]
2. (a) What are the fields present in SSL record protocol header? Mention their sizes and purpose?
 (b) Discuss the purpose of change cipher spec protocol and alert protocol in detail? [6+10]
3. (a) What is a bastion host? List the common characteristics of a bastion host?
 (b) Explain the concept of reference monitor in detail with a neat sketch? [8+8]
4. (a) Discuss in detail about network management architecture?
 (b) What are the deficiencies of SNMPV1?
 (c) Give a brief note of distributed network management. [8+4+4]
5. (a) What is Key exchange? What is its importance? Discuss the Diffie-Hellman key exchange algorithm.
 (b) Explain the Digital Signature Algorithm (DSA) with a relevant example. [8+8]
6. Clearly explain in detail the Multipurpose Internet Mail Extensions (MIME). [16]
7. (a) With neat illustration explain Advanced Encryption Standard algorithm (AES).
 (b) Explain the importance of Secure Hash functions with relevant examples. [8+8]
8. (a) End-to-end authentication and encryption are desired between two hosts. Draw figures that show
 - i. Transport adjacency, with encryption applied before authentication.
 - ii. A transport SA bundled inside a tunnel SA, with encryption applied before authentication.
 - iii. A transport SA bundled inside a tunnel SA, with authentication applied before authentication.
 (b) What is the purpose of padding field in ESP packet? [12+4]

Code No: 07A7EC39

R07**Set No. 4**

IV B.Tech I Semester Examinations, November 2010
INFORMATION SECURITY
Information Technology

Time: 3 hours**Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

1. (a) Discuss in detail the three firewall configurations?
 (b) List the limitations of firewalls. [12+4]
2. (a) Describe the various SET participants?
 (b) How SSL sessions and connections are related to each other? Discuss about connection state parameters in detail? [8+8]
3. (a) Discuss the benefits of IPSec?
 (b) Explain in detail the combinations of SAs listed in IP SEC architecture document? [6+10]
4. (a) Explain why PGP generates a signature before applying the compression.
 (b) Discuss the requirement of segmentation and reassembly function in PGP. [8+8]
5. (a) What is an access policy? On what factors does access determination depends?
 (b) Discuss the two techniques for developing an effective and efficient proactive password checker? [8+8]
6. (a) Illustrate clearly and explain how Cipher Feedback mode performs encryption and decryption.
 (b) Write about Message authentication:
 - i. Using Conventional Encryption
 - ii. Without Message Encryption. [8+8]
7. (a) "Gaining control over the Routing tables at layer 3 is one of the attacks" - explain how Route tables modification is crucial.
 (b) Explain how Buffer overflow is created for any known platforms (eg., WINDOWS NT / LINUX). [8+8]
8. (a) Perform the RSA algorithm on the given data and explain how encryption and decryption are performed on the message: $p = 17$; $q = 31$; $e = 7$; $M = 2$.
 (b) Compare and contrast the version 4 and version 5 of Kerberos in terms of the Authentication Dialogue. [8+8]

Code No: 07A7EC39

R07**Set No. 1**

IV B.Tech I Semester Examinations, November 2010
INFORMATION SECURITY
Information Technology

Time: 3 hours**Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

1. Discuss in detail the concept of trusted systems? Explain Trojan Horse defense Is done using trusted systems? [16]
2. (a) Explain the procedure involved in RSA public-key encryption algorithm.
(b) Explain what Kerberos is and give its requirements. [8+8]
3. (a) Explain about the Security Mechanisms.
(b) Explain TCP session hijacking with Packet Blocking. [8+8]
4. (a) Explain the conventional encryption principles with a neat illustration.
(b) Differentiate between Message authentication and User authentication. [8+8]
5. (a) What is WWW? What are the challenges web presents? Discuss?
(b) Explain how SSL makes use of TCP to provide a reliable end-to-end secure service. [6+10]
6. (a) Explain in detail Anti-Replay mechanism in AH?
(b) What is a cookie? How are they used in thwarting clogging attacks in Oakley algorithm? [8+8]
7. (a) Draw the figure showing VACM logic and explain?
(b) The encryption scheme used for UNIX passwords is one way; it is not possible to reverse it. Therefore, would it be accurate to say that this is, in fact, a hash code rather than an encryption of the password. [8+8]
8. (a) Explain how the session key generation is crucial in PGP and list the various algorithms used to generate the session key.
(b) Compare and contrast the way the certificates are handled in PGP and S/MIME. [8+8]

Code No: 07A7EC39

R07**Set No. 3**

IV B.Tech I Semester Examinations, November 2010
INFORMATION SECURITY
Information Technology

Time: 3 hours**Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

1. (a) What is a firewall? What is its functionality? What are its limitations?
(b) What are the three main components of distributed intrusion detection? Discuss about agent architecture? [8+8]
2. (a) Discuss in detail SNMPV1 community facility?
(b) Explain Digital Immune System with a neat diagram. [8+8]
3. (a) Explain about how the Internet standards and RFCs.
(b) Explain how Address Resolution Protocol table becomes a victim for attacks. [8+8]
4. (a) Draw the diagrams showing the relative location of security facilities in TCP/IP protocol stack? Discuss the advantages of each?
(b) What is SSL session? Can a session be shared among multiple connections? What are the parameters that define a session state? [8+8]
5. (a) Explain the structure of the Conventional Public-key encryption with relevant illustrations.
(b) Write about the X.509 certification service. [8+8]
6. (a) Explain clearly with relevant illustration how authentication is addressed in PGP.
(b) Explain how the exchange of secret key takes place between 'X' and 'Y' users of S/MIME. [8+8]
7. (a) Show how RC4 algorithm exhibits the symmetric stream cipher concept.
(b) Discuss the requirements for Hash function. [8+8]
8. (a) Explain the parameters associated with each security association in a nominal security Association Database?
(b) Explain how man-in-the-middle attack can be done on Diffie-Hellman algorithm? What features are added in Oakley protocol to counter this attack? [8+8]
