QUESTION BANK

Year: III II Branch: CSE Subject: IS Name of the Faculty: E. Jagadeeswara Rao

UNIT – I

SYLLABUS:

Security Attacks (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms, A model for Inter network security, Internet Standards and RFC's, Buffer overflow & format string vulnerabilities, TCP session hijacking, ARP attacks, route table modification, UDP hijacking, and man-in-the-middle attacks.

QUESTIONS:

1. Define a Security attack. Explain in detail about the various types of attacks an Inter network is vulnerable to? [Apr/May 2009]
2. Write about Man-in-the-middle attacks? [Apr/May 2009]
3. Explain the Security services mentioned in X.800 in detail? [Apr/May 2009]
4. Explain the process of standardization process of Internet standards? [Nov/Dec 2008]
5. Describe the Internet standards and RFC's? [Nov/Dec 2008]
6. Explain how Address Resolution Protocol table becomes a victim for attacks? [Nov/Dec 2009]
7. "Gaining control over the Routing tables at layer 3 is one of the attacks" Explain how Route table's modification is crucial? [Nov/Dec 2008]
8. Explain how Buffer overflow is created for any known platforms (e.g. WINDOWS NT / LINUX)?
9. Describe the various Security Services? [Nov/Dec 2008]
10. Compare TCP session hijacking and UDP hijacking? [Nov/Dec 2009]
11. What is a Security attack? Give the classification of the Security attacks? [Nov/Dec 2008]
12. Discuss the following terms in detail with relevant examples: [Apr/May 2010]
    i. Interruption
    ii. Interception
    iii. Modification
    iv. Fabrication
13. Write in detail about security mechanisms? [Apr/May 2010]
14. Discuss a model for Inter network security and Internet Standards? [Apr/May 2010]
15. Explain various ciphering techniques in detail? [Nov/Dec 2008]

UNIT – II

SYLLABUS:

Conventional Encryption Principles, Conventional encryption algorithms, cipher block modes of operation, location of encryption devices, key distribution Approaches of Message Authentication, Secure Hash Functions and HMAC.

QUESTIONS:

1. Explain the Secure Hash Algorithm (SHA-1) in detail with an example [Apr/May 2009]
2. Discuss why Encryption is the most resorted security tool. Explain the conventional encryption principles. [Apr/May 2009]
3. Explain how message authentication is provided without message encryption. [Nov/Dec 2009]
4. Describe Feistel's cipher structure with a neat illustration. [Nov/Dec 2008]
5. Explain terms related to key distribution methods: [Apr/May 2010]
    i. Session key
    ii. Master key
    iii. Key distribution centre
    iv. Security service module
6. Compare and contrast between Cryptography and Cryptology. [Nov/Dec 2009]
7. Explain the various Key distribution methods? [Nov/Dec 2009]
8. Differentiate between the symmetric block ciphers and symmetric stream ciphers. [Nov/Dec 2008]
10. Write about Key distribution? [Nov/Dec 2009]
11. Compare AES cipher versus RC4 encryption algorithm? [Nov/Dec 2009]
12. Compare and contrast SHA-1 and HMAC functions? [Nov/Dec 2008]
13. Differentiate between the symmetric block ciphers and symmetric stream ciphers. [Nov/Dec 2009]
14. With neat illustration explain Advanced Encryption Standard algorithm (AES)? [Apr/May 2010]
15. Explain the importance of Secure Hash functions with relevant examples? [Apr/May 2010]

UNIT – III

SYLLABUS:

Public key cryptography principles, public key cryptography algorithms, digital signatures, digital Certificates, Certificate Authority and key management Kerberos, X.509 Directory Authentication Service.

QUESTIONS:

1. Explain the procedure involved in RSA public-key encryption algorithm. [Apr/May 2009]
2. Explain what Kerberos is and give its requirements. [Apr/May 2009]
3. Explain the procedure involved in RSA public-key encryption algorithm. [Nov/Dec 2008]
4. Perform the RSA algorithm on the given data and explain how encryption and decryption are performed on the message: p = 3; q = 11; e = 7; M = 5. [Apr/May 2009]
5. Describe the Digital certificates. [Nov/Dec 2008]

6. Alice and Bob wish to share private messages, where each of them of two separate keys generated. What kind of strategy would you suggest to ensure confidentiality, key management and authentication for the conversation between Alice and Bob? Explain the strategy and also highlight the design issues related to the strategy proposed. [Nov/Dec 2008]

7. Describe the X.509 version 3 in detail. [Apr/May 2010]

8. Describe Differences between Kerberos version 4 and version 5. [Nov/Dec 2009]

9. Describe Kerberos version 5 Authentication Dialogue. [Nov/Dec 2009]

10. Describe Kerberos version 4 Authentication Dialogue. [Apr/May 2010]

11. Describe Public key cryptography principles. [Aug/Sep 2008]

12. Explain X.509 Directory Authentication procedures. [Aug/Sep 2008]

13. Describe Diffie-Hellman Key exchange algorithm in detail. [Apr/May 2010]

UNIT – IV

SYLLABUS:

Email privacy: Pretty Good Privacy (PGP) and S/MIME.

QUESTIONS:

1. Discuss the following in relation with S/MIME: [Apr/May 2009]
    i. RFC 822
    ii. MIME Header fields
    iii. MIME Content types
2. Explain the following terms in relation with the e-mail software - PGP: [Apr/May 2009]
    i. E-mail compatibility
    ii. Segmentation and reassembly.
3. Describe how authentication and confidentiality are handled in S/MIME. [Apr/May 2009]
4. Describe clearly the Public key management in PGP. [Apr/May 2009]
5. Show how the S/MIME certification process is carried out. [Apr/May 2010]
6. Clearly explain in detail the Multipurpose Internet Mail Extensions (MIME). [Aug/Sep 2008]
7. Explain the general format of a PGP message with a pictorial representation. [Apr/May 2008]
8. What is a Certification Authority and explain its role in S/MIME. [Apr/May 2010]
9. Compare and contrast the key management in PGP and S/MIME. [Nov/Dec 2009]
10. Write about how PGP messages are created. [Nov/Dec 2009]
11. What is Radix-64 format? Explain how both PGP and S/MIME perform the Radix-64 conversion is performed. [Apr/May 2010]
12. Describe the five principal services that Pretty Good Privacy (PGP) provides. [Apr/May 2010]