Code No: R5411206

IV B.Tech I Semester(R05) Regular & Supplementary Examinations, December 2009
INFORMATION SECURITY
(Computer Science & System Engineering and Information Technology)
Time: 3 hours Max Marks: 80
Answer any FIVE Questions
All Questions carry equal marks

1. (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]

2. (a) Differentiate between the symmetric block ciphers and symmetric stream ciphers.

   (b) Write about Key distribution. [8+8]

3. (a) 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.

   (b) Describe the X.509 version 3 in detail. [8+8]

4. (a) What is Radix-64 format? Explain how both PGP and S/MIME perform the Radix-64 conversion is performed.

   (b) Describe the five principal services that Pretty Good Privacy (PGP) provides. [8+8]

5. (a) Explain about various drafts published by the IP Security Protocol working group?

   (b) Draw IPSec authentication header format? Discuss the purpose of each field? [8+8]

6. (a) What are the services provided by SSL record protocol for SSL connections?

   (b) Discuss about SSL record protocol payload in detail with diagrams? [6+10]

7. (a) What is an access policy? On what factors does access determination depends?

   (b) Discuss the two techniques for developing an effective an efficient proactive password checker? [8+8]

8. (a) List the design goals for a firewall?

   (b) What are false Positives and false Negatives?

   (c) What are the Properties that a Multilevel Secure System must enforce? [6+4+6]

Code No: R5411206 2

IV B.Tech I Semester(R05) Regular & Supplementary Examinations, December 2009
INFORMATION SECURITY
(Computer Science & System Engineering and Information Technology)
Time: 3 hours Max Marks: 80
Answer any FIVE Questions
All Questions carry equal marks

KOTTAM INSTITUTIONS

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) Explain the Feistel cipher structure.

   (b) With a clear diagram explain how Cipher Block Chaining mode is performed. [8+8]

3. (a) Explain the procedure involved in RSA public-key encryption algorithm.

   (b) Explain what Kerberos is and give its requirements. [8+8]

4. (a) What is Radix-64 format? Explain how both PGP and S/MIME perform the Radix-64 conversion is performed.

   (b) Describe the five principal services that Pretty Good Privacy (PGP) provides. [8+8]

5. (a) What are SA selectors? How there are used in filtering outgoing traffic to map it a particular SA?

   (b) What are the features of Oakley algorithm? Discuss the three basic requirements that must be satisfied in cookie generation.[8+8]

6. Discuss the features of SSL that counters man-in-the-middle attack, IP spoofing, IP hijacking and brute-force attacks to web security?[16]

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 the working of Packet-filtering router?

   (b) Explain the general model of access control as exercised by DBMS? [8+8]

Code No: R5411206 3

IV B.Tech I Semester(R05) Regular & Supplementary Examinations, December 2009
INFORMATION SECURITY
(Computer Science & System Engineering and Information Technology)
Time: 3 hours Max Marks: 80
Answer any FIVE Questions
All Questions carry equal marks

1. (a) Explain about how the Internet standards and RFCs.
   (b) Explain how Address Resolution Protocol table becomes a victim for attacks. [8+8]

2. (a) Compare AES cipher versus RC4 encryption algorithm.
   (b) Compare and contrast SHA-1 and HMAC functions. [8+8]

3. (a) Explain the procedure involved in RSA public-key encryption algorithm.
   (b) Explain what Kerberos is and give its requirements. [8+8]

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) Discuss the scope of ESP encryption and authentication in both IPV4 and IPV6?
   (b) Explain about transport adjacency and transport tunnel bundle? [8+8]

6. (a) Explain in detail how payment processing is done in SET?
   (b) What is the significance of change cipher specification protocol? [12+4]

7. (a) Explain in detail message processing model?
   (b) Give a note on the malicious program that need a host program and that do not replicate?[8+8]

8. (a) What are two default policies that can be taken in a packet filter if there is no match to any rule? Which is more conservative? Explain with example rule sets both the policies?
   (b) What are the advantages of decomposing a user operation into elementary actions?
   (c) What are false negatives and false positives? [6+6+4]

Code No: R5411206 4

IV B.Tech I Semester(R05) Regular & Supplementary Examinations, December 2009
INFORMATION SECURITY
(Computer Science & System Engineering and 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) List advantages and disadvantages of Electronic Codebook (ECB) mode.

   (b) Explain the various approaches to Message authentication. [8+8]

3. (a) Explain the procedure involved in RSA public-key encryption algorithm.

   (b) Explain what Kerberos is and give its requirements. [8+8]

4. (a) What is Radix-64 format? Explain how both PGP and S/MIME perform the Radix-64 conversion is performed.

   (b) Describe the five principal services that Pretty Good Privacy (PGP) provides. [8+8]

5. (a) Discuss how sequence number field of Authentication header is used to thwart replay attacks?

   (b) What is a cookie? ISAKMP mandates that the cookie generation satisfy three basic requirements. What are they? Explain?[8+8]

6. (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]

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) What are two default policies that can be taken in a packet filter if there is no match to any rule? Which is more conservative? Explain with example rule sets both the policies?

   (b) What are the advantages of decomposing a user operation into elementary actions?

   (c) What are false negatives and false positives? [6+6+4]