M. TECH PRINTING ENGINEERING AND GRAPHIC

Network Security

Time – 3 Hours **Full Marks – 100**

Answer any five questions
Answer all parts of a question together

1.

a. What are the different components 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 http service
iii. Uses mail service
iv. Uses http 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. Explain how password validation is performed in Kerberos.

4+8+3+3=20

2.

a. Differentiate between discretionary access control and mandatory access control.

b. What do you mean by protection state of a system?

c. Consider the following access matrix in Lampson, Graham and Denning's Model of Discretionary Access Control (DAC) mechanism.

	Subjects		Files	
	Amal	Bimal	F1	F2
Amal			owner, write*	read
Bimal				

Show the actions taken by the DAC mechanism (in terms of authorization action and changes to the access control matrix) in response to the following commands issued by subjects. Provide necessary explanation in each case.

i. Amal creates a file F3
ii. Amal creates a subject Chinmoy
iii. Amal wants to transfer write* on F1 to Bimal
iv. Amal wants to transfer read on F2 to Chinmoy
v. Bimal wants to transfer write on F1 to Chinmoy
vi. Amal wants to know what type of access Chinmoy has over file F1

d. What are role hierarchies in RBAC? Explain with a suitable example.

e. Discuss different types of constraints in RBAC.

2+2+9+3+4=20

3.

a. Differentiate between the transport and tunnel mode of IPSec operation.
b. Explain how ESP provides limited traffic flow confidentiality.
c. Differentiate between the authentication services provided by AH and ESP.
d. Define security association and security policy. Explain their purposes with relation to IPSec.
e. Explain how the pre master secret is established in SSL handshake protocol using each of the following key exchange algorithms
    i. RSA
    ii. Ephemeral Diffie-Hellman
    iii. Anonymous Diffie-Hellman

3+4+3+4+6=20

4.

a. What is a secure hash function? State some desirable properties of it.
b. Describe different ways in which message authentication codes can be generated?
c. What are digital envelops? How is it useful?
d. Compare known plaintext and chosen plaintext attacks on encrypted messages.
e. Explain the role of a certification authority (CA) in X.509 authentication scheme.
f. Identify cases when revocation of user certificates is necessary and briefly describe how it is done.

3+6+3+3+2+3=20

5.

a. Explain how PGP (Pretty Good Privacy) achieves both confidentiality and authenticity on the same message.
b. Explain the necessity of Radix-64 conversion in PGP operation.
c. How does PGP generate per session symmetric key?
d. Explain how PGP prevents replay attacks.
e. How does a PGP client retrieve private keys from PGP Private Key Ring?
f. What are the significances of the Owner Trust, Key Legitimacy and Signature Trust fields of PGP public key-rings. Explain how PGP processes trust on a public key based on these fields.

4+2+2+2+4+6=20

6.

a. Explain how two parties A and B can establish a shared secret S between themselves using Diffie-Hellman Key Exchange protocol. Explain why a passive attacker is not able to recover the secret S by observing the communications between A and B.
b. What is Message Authentication Code (MAC)? Describe how MAC is generated in SSL.
c. What is a packet filtering firewall? Describe two possible attacks against packet filtering firewalls.
d. What is an application level gateway? State its advantages and disadvantages.
e. Explain with suitable example, each of the following firewall rule anomalies
    i. Shadowing anomaly
    ii. Correlation anomaly
    iii. Generalization anomaly

5+3+4+2+6=20