B.E. Computer Science & Engineering Fourth Year First Semester Examination 2024

COMPUTER AND NETWOR SECURITY (Hons.)

Time: 3 hours Full Marks: 100

Group A (Total Marks: 30) [CO1]
Answer Question No. 1 OR Question no. 2.

1. [4+4+5+4+3+3+2+2+3=30]

a) What is *integrity*? What are the types of integrity?
b) How can you differentiate between *disruption* and *userpation*? Give suitable examples for each.
c) Why and how would you use Diffie Hellman algorithm?
d) What is *cryptographic hash collision*? What is the requirement of *strong collision resistance* property for hash function?
e) Consider a situation in which a user needs to log into the system from home/workplace/office canteen/office café. What type of *access control* would be suitable and why?
f) On what aspects of security would military security policy look into primarily? Justify your answer.
g) How can *replay attacks* be detected?
h) What are the threats to *passwords*?
i) What are the contents of *digital certificate*? Who can issue these certificates?

2. [4+4+5+4+3+3+2+2+3=30]

a) Why is *availability* considered to be an aspect of security? What are the other aspects of security?
b) How can you differentiate between *disclosure* and *deception*? Explain briefly with suitable examples.
c) How is RSA used for generating key pair? How are encryption and decryption done in Public Key cryptosystem?
d) What is the *second pre-image resistance* property of hash function? How does *keyed hash function* work?
e) Consider a situation in which a user is a student at his/her college and then enrolls in research at the same college and later on becomes a staff of the same college. What type of *access control* would be suitable and why?
f) On what aspects of security would company security policy look into primarily? Justify your answer.
g) What practice should be followed as principles of operation?
h) What are the different types of *user authentication*?
i) What is *smart card*? Why is it used?

Group B (Total Marks: 40) [CO2]

Answer Question No. 3 [Compulsory] AND

Answer Question No. 4 OR Question no. 5.

3. [(2+3)+(2+2)+(4+3)+(2+2)=20]

a) Why is there a requirement of third party in the *classical key exchange* protocol? What are the problems with *classical key exchange* protocol?

b) What type of protocol is *Kerberos*? From what threat/attack are *Kerberos* messages protected?

c) What algorithms are used in IPsec? Mention their purposes. What is *security association* (SA)?

d) What security service does *Transport Layer Security* (TLS) provide? What does the TLS *Cipher Suite* contain?

4. [3+(4+2)+5+(5+1)=20]

a) What drawback of *classical key exchange protocol* is addressed by *Needham Schroeder* protocol and how?

b) How is *client service authorization* done in *Kerberos*? What does the *Key Distribution Centre* (KDC) in *Kerberos* generate for the network entities?

c) What are the modes of operation in IPsec? Explain the modes and mention their usages.

d) What happens in the *Negotiation* phase? Name the protocol of which this is a part.

5. [5+(2+2)+(3+2)+(3+2+1)=20]

a) What does *Otway-Rees* protocol do? Do you find any disadvantage of this protocol? Why or why not?

b) What happens after a client puts a service request in *Kerberos*? Why is the *Key Distribution Centre* (KDC) considered to be a point of failure in *Kerberos*?

c) In what ways do *Authentication Header* (AH) and *Encapsulating Security Payload* (ESP) differ? Can both be applied to the same packet? Justify your answer.

d) What are the tasks of the *Record* protocol? What does the *Alert* protocol do? Name the protocol of which these two protocols are parts.

Group C (Total Marks: 20) [CO3]

Answer Question Nos. 6 AND 7 [Both Compulsory]

6. [3+2=05]

a) What are the various attack techniques of *Denial of Service* (DoS)?

b) Why is *Distributed Denial of Service* (DDoS) hard to deal with?

7. Answer any THREE (3) Questions from the following: [5X3=15]

a) What is *clone phishing*? What is the possible solution for dealing with *birthday attack*?

b) How does *Trojan Horse* work? Why may it be difficult to detect?

c) What is the role of a *recursive DNS server* in DoS/DDoS attack?

d) Briefly explain the working of any one DoS attack defense technique.

e) What is *Man-In-The-Middle* (MITM) attack? What is *spyware*?

f) How does a *worm* work and spread?

Group D (Total Marks: 10) [CO4]

8. Answer any TWO (2) Questions from the following: [5X2=10]

a) How is confidentiality maintained in Pretty Good Privacy (PGP)?

b) How does a Host Intrusion Detection System work?

c) What is *firewall*? Mention a typical rule for a firewall.

d) What is *Virtual Private Network* (VPN)?