Regn. No. □□□□□□□□□

Manipal Institute of Technology

(Constituent Institute of Manipal University)

II SEMESTER M.TECH (CSIS/CSE) DEGREE EXAMINATIONS, MAY 2016
SUBJECT : NETWORK SECURITY(CSE 524/CSE 554)
REVISED CREDIT SYSTEM
DATE: 07-05-2016

TIME:03 HOURS MAX.MARKS : 50

Instructions to Candidates:

- Answer ANY FIVE FULL questions.
- Missing data, if any, may be suitably assumed.

1A. List the various security mechanisms that could be used to provide each of the following security services and explain. 4M
i. Peer Entity Authentication
ii. Traffic Flow Confidentiality
iii. Nonrepudiation

1B. What is a distributed intrusion detection system? Explain the major issues that need to be considered in the design of a distributed intrusion detection system 2M

1C. Explain the following malicious software 4M
i. Trojan Horse ii. Logic Bomb
What threats do they cause?

2A. What are Packet filtering firewalls? Explain with an example. List the advantages and limitations of Packet filtering firewalls. 4M

2B. Explain the following advanced functionalities of Firewalls 3M
i. Authentication and Authorization
ii. Network Address Translation
iii. Server Load Balancing

2C. Explain the various modules of Checkpoint Firewall 3M

3A. Explain with examples, the various statistical tests that can be performed over the metrics to detect intrusions. 4M

3B. Explain the four techniques that could be used to eliminate guessable passwords. 3M

3C. With a neat diagram, explain the architecture and operation of a proactive worm containment system 3M

4A. With a neat time line diagram explain the SSL handshake protocol. 4M

4B. Show how someone who knows both Alice's and Bob's Public encryption keys (and neither side's private key) can construct an entire IKE exchange based on public encryption keys that appears to be between Alice and Bob. 4M

4C. Explain the tunnel and transport modes of operation of IPSec 2M

5A. Suppose if Alice's aggressive-mode IKE connection initiate is refused, Alice starts up another aggressive-mode connection initiate with her next (and weaker) choice of Diffie-Hellman group, rather than starting a main-mode exchange telling Bob all her supported Diffie-Hellman groups. What is the vulnerability, given an active attacker? 2M

5B. With necessary diagrams, specify the Kerberos V4 messages involved from the time a user first walks up to a workstation to the time the user is successfully talking to somebody. 4M

5C. Explain the information contained in the Tickets and the authenticators in Kerberos V5. 4M

6A. What are renewable and postdated tickets? How are they implemented in Kerberos V5? 3M

6B. With neat diagrams, explain how key rings are used in message transmission and reception to implement the various PGP crypto services 5M

6C. What is the significance of specifying the network layer addresses in tickets in Kerberos V4 implementation? 2M