Regn. No. | | | | | | | | | |

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

A Constituent Institution of Manipal University

II SEMESTER M.TECH (COMPUTER SCIENCE AND INFORMATION SECURITY)
DEGREE EXAMINATIONS, APRIL/MAY 2017
SUBJECT : INTRUSION DETECTION SYSTEMS(CSE 5250)
REVISED CREDIT SYSTEM
DATE: 29-04-2017

TIME:03 HOURS MAX.MARKS : 50

Instructions to Candidates:

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

1A.	Explain Intrusion Detection Expert System[IDES] model briefly.	3M
1B.	Draw Distributed Intrusion Detection System[DIDS] Architecture and Explain.	4M
1C.	Define "security triad": Confidentiality, Integrity, Availability.	3M
2A.	Explain Architecture, Monitoring strategy and Analysis type of a Intrusion Detection System with a neat Diagram	4M
2B.	Discuss Pros and Cons of Operating System Audit trails.	3M
2C.	What is the Advantage and Disadvantage of System logs as information Sources in Intrusion Detection Systems?	3M
3A.	Explain the steps involved in building a Behavior Classification Engine for misuse detection and Anomaly Detection.	4M
3B.	Explain Non-Parametric Statistical Measures for Anomaly Detection.	2M
3C.	Explain Agent-Based Intrusion Detection with the help of a Diagram.	4M
4A.	Explain different Types of Responses in Intrusion detection System.	3M
4B.	What are the Scalability Issues in Intrusion Detection Systems?	3M
4C.	What are the problems in Design and Development of Operating Systems as proposed by RISOS team that may lead to the origin of security problems in Intrusion Detection Systems?	4M
5A.	What do you mean by Extrusion Detection? What is the difference between Intrusion Detection and Extrusion detection? Explain with a simple network diagram.	3M
5B.	What are the four forms of Network Data that used to implement Network Security Monitoring? Explain in Detail.	3M
5C.	Explain Extrusion Detection with Full Content Data with the help of Diagram.	4M