AP5007 SECURE COMPUTING SYSTEMS

DETAILED SYLLABUS

UNIT I COMPUTER SECURITY AND MANAGEMENT

Overview of Computer Security, Threats, Malware, Vulnerabilities, Authentication, Access Control, Security Management Models, Security Management Practices, Protection Mechanisms, Legal aspects of security, Ethical Hacking.

UNIT II HARDWARE SECURITY

Need for Hardware Security, Computer Memory and storage, Bus and Interconnection, I/O and Network Interface, CPU; Side channel Analysis: Power Analysis Attack, Timing Attack, Fault attack. Countermeasures of Side Channel Attack, Secure Hardware Intellectual Properties, Physically Unclonable Functions(PUFs), Secure PUF.

UNIT III ASSEMBLY AND OPERATING SYSTEMS SECURITY

Opcode, Operands, Addressing Modes, Stack and Buffer Overflow, FIFO and M/M/1 Problem, Kernel, Drivers and OS Security; Secure Design Principles, Trusted Operating Systems, Trusted System Functions

UNIT IV ADVANCED COMPUTER ARCHITECTURE

Security aspects : Multiprocessors, parallel processing, Ubiquitous computing, Grid, Distributed and cloud computing, Internet computing, Virtualization

UNIT V NETWORK AND WEBSECURITY

TCP/IP Protocol, Network switches, Routers, Gateways, Wireless Networks and Network Address Translation (NAT); Network Security Issues in TCP/IP, Threat Models, Denial of Service Attacks, Firewalls, Intrusion Detection, Browser Attacks, Web Attacks Targeting Users, Email Attacks, Secure Shell (SSH), HTTPS

REFERENCES:

1. Charles B. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing", Fourth Edition, Pearson Education, 2007

2. Debdeep Mukhopadhyay, Rajat Subhra Chakraborty, "Hardware Security – Design Threats and Safeguards", CRC Press, 2015

3. Michael Whitman, Herbert J. Mattord, "Management of Information Security", Third Edition, Course Technology, 2010

4. Shuangbao Wang, Robert S.Ledley, Computer Architecture and Security, Wiley, 2013

5. William Stallings, "Network Security Essentials, Applications and Standards", Dorling Kindersley I P Ltd, Delhi, 2008.