[CSE6072]: [Computer Security]

Programme: UG Year: UG 3rd Semester: UG 5th
Course: Core Credits: 3 Hours: 40

Course Context and Overview (100 words):

The course will provide an overview of main problems and techniques of computer security. It will introduce the key security management issues, such as threats, attacks, objectives and measures. Computer Security is concerned with the protection of computer systems and their data from threats which may compromise integrity, availability, or confidentiality; the focus is on threats of a malicious nature rather than accidental. This course aims to give a broad understanding of computer security. Topics include basic computer security concepts, fundamentals of cryptography, system and software security, Network and Web security and explain the requirements and techniques for security management, including security policies, risk analysis, and physical threats and controls.

Prerequisites Courses:

Basics of Programming Language, Operating Systems and Basic Awareness of Networking.

Course outcomes (COs):

On completion of this course, the students will have the ability to:
CO1 State the basic concepts in information security, including threats, threat models, security policies and security mechanisms.
CO2 Explain basic concepts related to cryptography, including plain-text, cipher-text, symmetric cryptography, asymmetric cryptography, digital signature, and modes of encryption operations.
CO3 Explain and exploit common vulnerabilities in system and mobile, including buffer overflow vulnerabilities, rooting, privilege escalation etc.
CO4 Explain and demonstrate the concepts of web and database security including malicious code, including virus, Trojan horse, and worms, side channel attacks, sql- injection etc.
CO5 Identify the threats to networks and web including interception, fabrication, interruption, browser and email attacks.
CO6 Analyze the requirements and techniques for security management, including security policies, risk, and physical threats and controls.

Course Topics:

Contents	**Lecture Hours**
UNIT – 1: Computer Security Concepts and Technologies • Overview of Computer Security • Threats • Threat Models • Security Functional Requirements: Confidentiality, Integrity (fraud), Availability, Authentication, Accountability, Non-repudiation • Basics of Cryptography • Cryptographic toolkit • Types of cryptography	10
UNIT-2: System and Mobile security	

System Security: • Buffer Overflow vulnerability and attack • Return to libc attack • Defence mechanism Mobile Security • Rooting attacks • Repackaging attacks • Privilege Escalation Attacks • Defence Mechanism	10
UNIT-3: Web and Database Security	8
Web Security: • Browser Attacks • Web Attacks Targeting Users • Email Attacks • Side-channel Attacks • Malicious code: viruses, Trojan horses, worms Database Security • SQL Injection Attacks	
UNIT-4: Network Security	6
Network Security: • Interception: Eavesdropping and Wiretapping • Modification, Fabrication: Data Corruption • Interruption: Loss of Service • Port Scanning • Networking attack defenses	
UNIT-5: Security Management and Advanced Security Threats	6
• Security policies • Risk analysis • Physical threats and controls • Legal aspects of security • Privacy and ethics • Security Threats due to emerging technologies	

Textbook references (IEEE format):

Text Book:

1. Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies, *Security in Computing*, 5th Edition, Prentice Hall Press Upper Saddle River, NJ, USA, 2015.

Reference books:

1. Dieter Gollmann, *Computer Security*, 3rd Edition, John Wiley & Sons UK, 2011
2. Stallings William, Lawrie Brown, *Computer security: principles and practice*, 3rd

Edition, Pearson Education, 2015.

3. Lecture Notes, Recent Research Papers and White Papers.

Additional Resources (Video Lectures, Web resources etc.): NPTEL Video Lectures

Evaluation Methods:

Component	Weightage (%)
Surprise Quiz1	20%
Surprise Quiz2	
Midterm	30%
Endterm	50%

Prepared By: Shweta Bhandari and Hemant Kumar Mehta,
Last Update: 09/Jul/2018