LNMIIT, Jaipur
Department of Computer Science & Engineering

Programme: M. Tech. (CSE)	Course Title: Information Security and Privacy			Course Code: CSE XXXX
Type of Course: **Program Core**	**Prerequisites:** Computer Security			**Total Contact Hours:** **40**
Year/Semester: **1/Odd**	**Lecture Hrs/Week:** **3**	**Tutorial Hrs/Week:** **0**	**Practical Hrs/Week:** **0**	**Credits:** **3**

Learning Objective:

The course aims to provide a basic understanding of information security and privacy. This course allows us to understand what threats may exist to our system and how do we begin to reason about potential attacks. Concepts of security policies and models that formulate these policies to work well in practice will be discussed. The course will dive into the core concepts of cryptography and will explore different notions of privacy. How some extent of privacy can be achieved by anonymity techniques will also be discussed. Core concepts of software validity and rights will be discussed in this course. The course will familiarize students with the security mindset while remaining ethical. This course will help prepare students for careers and further course work in cybersecurity, computer science and information technology.

Course outcomes (COs):

On completion of this course, the students will have the ability to:		Bloom's Level
CO-1	Define the core concepts of information security and privacy to achieve security goals and solve related issues.	**1,2**
CO-2	Explain the core concepts of Privacy, Anonymity, Software Validity and Rights.	**1,2**
CO-3	Analyze the threat model and potential attacks to the system.	**4**
CO-4	Evaluate and reason about the existing security policies and model.	**4,5**
CO-5	Apply a security mindset while remaining ethical	**3**
CO-6	Design a modern and secure architecture for the real-world systems	**3,4**

Course Topics	Lecture Hours	
UNIT – I: Introduction to Information Security and Privacy	6	6
1.1 Importance of Security and Privacy 1.2 Threats Vulnerabilities & Attacks 1.3 Security Policies and Trust Mechanism	2	
1.4 Specification, Design & Implementation 1.5 Principles to Secure Design	2	
1.6 Threat Modeling	2	

1.7 Attack Trees		
Unit II: Cryptography	8	8
2.1 Closed and Open Design	2	
2.2 Symmetric/Private Key Model and their applications, DES, Triple DES	3	
2.3 Asymmetric cryptography models, Digital Signatures, Cryptographic Hashes, PKI, Digital Certificates	3	
Unit III: Containerization	5	5
3.1 Resource Isolation 3.2 Virtualization 3.3 PL Virtual Machines 3.4 Software Fault Isolation 3.5 Native Client	5	
Unit IV: Privacy and Anonymity	6	6
4.1 Privacy 4.1.1 Contextual Integrity 4.1.2 Differential Privacy	3	
4.2 Anonymity and Mixing Concepts: 4.2.1 Anonymity with Tor 4.2.2 Anonymity Nets 4.2.3 Anonymity Relay.	3	
Unit V: Software Validity and Rights	10	10
5.1 Digital Right Management, 5.2 Implementation of DRM in different media types	3	
5.3 Trusted Computing 5.4 Trusted Platform Module	2	
5.5 Software Watermarking and its techniques and attacks	3	
5.6 Steganography 5.7 Software Anti-Piracy	2	
UNIT – VI: Security and Privacy: Ethics and Legality	5	5
6.1 Security Acts and Policies in Practice 6.1.1 GDPR, PDP and CCP Act	3	
6.2 Security, Privacy, Ethics and Legality 6.3 Case Study	2	

Textbook references:

Text Book:

1. Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security*, 6th Edition, Cengage Learning, 2017
2. David Kim and Michael G. Solomon, *Fundamentals of Information Systems Security*, 3rd Edition, Jones & Bartlett Learning, 2016
3. Thomas J. Shaw, *Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists*, 1st Edition, American Bar Association, 2012

Reference books:

1. Jason Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, 1st Edition, Syngress, 2011
2. Kevin Mitnick, *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data*, 1st Edition, Little, Brown and Company, 2017

Evaluation Method	
Item	**Weightage (%)**
Quizzes/ Term Paper /Attendance	40
Midterm	25
Final Examination	35

*Please note, as per the existing institute's attendance policy the student should have a minimum of 75% attendance. Students who fail to attend a minimum of 75% lectures will be debarred from the End Term/Final/Comprehensive examination.

CO and PO Correlation Matrix

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3			1					1		3	1		3
CO2	3	3			1					1		3	1		3
CO3	3	3		1	1					1		3	2		3
CO4	3	2		1	1			3		1		3	3	2	3
CO5	3	3	2	1	1	2		3		1		3	3	2	3
CO6	3	3	3	1	1	2		3		1		3	3	2	3

Last Updated On: 16th June 2021

Updated By: Shweta Bhandari

Approved By: