S6 B.Tech CSE

19CSE311 – COMPUTER SECURITY

(3-0-0) – Credit-3

Table of Contents

01

Course Description

Course Description

- This course provides basic knowledge and skills in the fundamental theories and practices of cyber security.
- It provides an overview of the field of security and assurance emphasizing the need to protect information being transmitted electronically

- **CO1:** Understand the fundamental concepts of computer security and apply to different components of computing systems
- **CO2:** Understand basic cryptographic techniques
- **CO3:** Understand how malicious attacks, threats, security and protocol vulnerabilities impact a system’s Infrastructure.
- **CO4:** Demonstrate knowledge in terms of relevance and potential of computer security for a given application
- **CO5:** Apply authentication services and mechanisms
- **CO6:** Understand email security services and mechanisms
- **CO7:** Develop an understanding of security policies (such as authentication, integrity and confidentiality), as well as protocols to implement such policies in the form of message exchanges
- **CO8:** Comprehend and apply web security services and mechanisms for E-commerce applications

Course Outcomes

CO1: Understand the fundamental concepts of computer security and apply to different components of computing systems.

- **CO2:** Understand basic cryptographic techniques.
- **CO3:** Understand how malicious attacks, threats, security and protocol vulnerabilities impact a system's Infrastructure.
- **CO4:** Demonstrate knowledge in terms of relevance and potential of computer security for a given application.
- **CO5**: Apply authentication services and mechanisms.
- **CO6**: Understand email security services and mechanisms.

02

Course Syllabus

Course Syllabus

UNIT I: Basics of Computer Security: Overview – Definition of terms – Security goals – Shortcomings – Attack and defense – Malicious code – Worms – Intruders – Error detection and correction Encryption and Cryptography: Ciphers and codes – Public key algorithms – Key distribution – Digital signatures.

UNIT II: Security Services: Authentication and Key Exchange Protocols - Access control matrix – User authentication – Directory authentication service – Diffie-Hellman key exchange – Kerberos.

UNIT III: System security and Security models: Disaster recovery - Protection policies. E-mail Security: Pretty good privacy - Database Security: Integrity constraints - Multi-phase commit protocols - Networks Security: Threats in networks - DS authentication -Web and Electronic Commerce: Secure socket layer - Client-side certificates - Trusted Systems : Memory protection.

03

Text Books

Text Book/References

1. **Stallings William, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson/Prentice- Hall, 2018.**
2. **Forouzan B A, Cryptography and Network Security, Special Indian Edition, Tata McGraw Hill, 2007.**
3. **Padmanabhan TR, Shyamala C K, and Harini N, Cryptography and Security, First Edition, Wiley India Publications,2011**

04

Evaluation Pattern

Evaluation Policy

50 (Internal Assessment) + 50 (End Semester)

Evaluation Policy	Components	Marks	Total
Continuous Assessment	Assignment(#2)	10 Marks	20 Marks
	Quizzes(#4)-Best of 3	10 Marks	
Mid Term Exam	Online Exam	20 Marks	30 Marks
	Viva	10 Marks	
End Semester Exam	Online Exam	20 Marks	50 Marks
	Viva	30 Marks	
	Total		50 Marks(Internal)+ 50 Marks(External)

Thank You & Stay Safe