L	T	P	C
3	1	0	4

Course Code: INT313

COMPUTER SYSTEM SECURITY

Course Objectives

This course will help the learner to understand the key features of computer systems security and discuss the Security Design, Security Policies with Network and database security.

UNIT - I **15 Periods**

Overview of Security Parameters: Confidentiality - integrity and availability - Security violation and threats - Security policy and procedure - Assumptions and Trust - Security Assurance - Implementation and Operational Issues - Security Life Cycle. **Access Control Models:** Discretionary - mandatory - roll-based and task-based models - unified models - access control algebra - temporal and spatio-temporal models.

UNIT - II **15 Periods**

Security Policies: Types - Role of trust and access control - Examples. **Confidentiality policies-** The Bell-LaPadula Model, Examples. **integrity policies** - Biba Integrity Model - Low-Water-Mark and Ring Policy Models- Lipner's Integrity Matrix , Lipner's Use of the Bell-LaPadula, Lipner's Full and Clark-Wilson Integrity models. **hybrid policies** - Chinese Wall Model, Formal Model, Bell-LaPadula and Chinese Wall - Clark-Wilson and Chinese Wall model. **Non-Interference And Policy Composition -** Deterministic Noninterference - Unwinding Theorem - international standards.

UNIT - III **15 Periods**

Systems Design: Design principles. **Representing Identity**- files and objects - Users - Groups and roles - Naming and certificate - identity on the web. **Control of Access and Information flow**, **confinement problem**- Isolation and covert channels - Composition of Deterministic Non-Interference-Secure Systems and Deducibly Secure Systems. **Assurance**: Building systems with assurance - formal methods - evaluating systems.

UNIT - IV **15 Periods**

Logic-based System: Malicious logic, vulnerability analysis, auditing, intrusion detection. Applications: Network security, operating system security, user security, program security. Special Topics: Data privacy, introduction to digital forensics, enterprise security specification. **Operating Systems Security:** Security Architecture, Analysis of Security in Linux/Windows. **Database Security:** Security Architecture, Enterprise security, Database auditing.

TEXTBOOKS

1. Mark Stamp, *Information Security: Principles and Practice*, Wiley Publications, Second Edition, 2011
2. Ross Anderson, *Security Engineering A Guide to Building Dependable Distributed Systems*, Wiley Publications, Third Edition, 2020.
3. M. Bishop, *Computer Security: Art and Science*, Second Edition, Pearson Education, 2019.

REFERENCES

1. C.P. Pfleeger, S.L. Pfleeger, J. Margulies, *Security in Computing*, Pearson Education, Fifth Edition, 2015,
2. David Wheeler, *Secure Programming: HowTo*,2015
3. Michael Zalewski, *Browser Security Handbook*, Google Inc., 2009
4. M. Gertz, S. Jajodia, *Handbook of Database Security, Application and Trends*, Springer, 2008.

UNITWISE LEARNING OUTCOMES

Upon successful completion of each unit, the learner will be able to

Unit I	• Understand the basics of computer system security • Aware of various access control models.
Unit II	• Identify different kinds of security policies • Know the security policy models , international standards.
Unit III	• Comprehend system design identity • Grasp control access , confinement problem and Assurance
Unit IV	• Become aware of vulnerability with intrusion detection • Gain knowledge about operating system and database security.

COURSE LEARNING OUTCOMES

Upon successful completion of the course, the learner will be able to

- Explain the needs of computer and Information security.
- Understand the various Information security policies.
- analyse the various security policy models for designing security techniques.
- Understand the basics of security design principles with various models for information security
- Gain knowledge to analyse the security issues in database and operating system
- Defend the importance of enforcing security in information communication