# CSE3052/CSE329: COMPUTER SECURITY

Programme: B.Tech (CSE) Year: 3 Semester:5
Course: Program Core Credits: 3 Hours: 40

**Course Context and Overview (100 words):**
The course will introduce an overview of well-known problems and techniques of computer security. This would introduce the key security management issues, such as threats, attacks, objectives and measures. Computer Security is concerned with the protection of computer systems and associated data from threats which may compromise integrity, availability, or confidentiality. The focus is on threats of a malicious nature not the accidental threats. This course aims to give a broad understanding of computer security. Topics include basic computer security concepts, Cryptographic tools/primitives, system and software security and network. It also covers the requirements and techniques for security management, including security policies, risk analysis, physical threats and controls.

**Prerequisites Courses:** Computer Programming, Operating Systems, Computer Networks.

## Course outcomes (COs):

| The Outcomes of this Course are |
|---|
| **CO1:** Students be able to recognize the security threats against computer systems, and have at least a high-level idea of the ways to address them. |
| **CO2:** Students be able to apply techniques and design principles underlying security solutions, including aspects of cryptography and security protocols. |
| **CO3:** Students be able to analyze simple security protocols using a formal method. |
| **CO4:** Apply Cryptographic technique and mechanism to achieve security goals and formulate efficient mechanism to solve security issue. |
| **CO5:** Understand Operating system security and trusted system. |

## Course Topics

| Contents | | Lecture Hours | |
|---|---|---|---|
| **UNIT – 1 (Introduction to Computer Security)** | | | 4 |
| 1.1 | The Challenges of Computer Security, A Model for Computer Security, **Security** Functional Requirements- (Confidentiality, Authentication, Non-repudiation, | 2 | |

| | | | |
|---|---|---|---|
| | Data integrity) | | |
| 1.2 | **Threats, Attacks, and Assets-** Threat and Attack, Threats and Assets<br><br>**Fundamental Security Design Principles** | 2 | |
| **UNIT-2 (Cryptographic Tools/Primitives)** | | | |
| 2.1 | **Confidentiality with Symmetric Encryption:** Symmetric Encryption, Symmetric Block Encryption Algorithms, Stream Ciphers | 2 | 10 |
| 2.2 | **Message Authentication and Hash Functions:** Authentication Using Symmetric Encryption, Message Authentication without Message Encryption, Secure Hash Functions and applications of Hash Functions | 2 | |
| 2.4 | **Public-Key Encryption :**Public-Key Encryption Structure<br>Applications for Public-Key Cryptosystems, Requirements for Public-Key Cryptography Asymmetric Encryption Algorithms | 2 | |
| 2.5 | **Digital Signatures and Key Management :**Digital Signature, Public-Key Certificates, Symmetric Key Exchange Using Public-Key Encryption, Digital Envelopes | 2 | |
| **UNIT-3 User Authentication** | | | 08 |
| 3.1 | **Electronic User Authentication Principles :** A Model for Electronic User Authentication, Means of Authentication, Risk Assessment for User Authentication | 2 | |
| 3.2 | **Password-Based Authentication:** The Vulnerability of Passwords<br>The Use of Hashed Passwords, Password Cracking of User-Chosen Passwords | 2 | |
| 3.3 | Password File Access Control, Password Selection Strategies | 2 | |
| 3.4 | **Remote User Authentication:** Password Protocol, Token Protocol, Static Biometric Protocol, Dynamic Biometric Protocol | 2 | |
| **UNIT-4 Access Control** | | | 6 |
| 4.1 | **Access Control Principles :**Access Control Context, Access Control Policies | 2 | |
| 4.3 | **Discretionary Access Control:** An Access Control Model, Protection Domains | 2 | |
| 4.4 | **Example: Unix File Access Control:** Traditional UNIX File Access Control<br>Access Control Lists in UNIX | 2 | |
| **UNIT-5 Operating System Security** | | | 6 |
| 5.1 | Introduction to Operating System Security, System Security Planning, Operating Systems Hardening, Application Security, | 2 | |
| 5.2 | Security Maintenance, Linux/Unix Security, | 2 | |
| 5.3 | Windows Security, Virtualization Security | 2 | |
| **UNIT-6:Network Security** | | | 6 |
| 5.3 | **Internet Security Protocols and Standards** -Secure E-Mail and S/MIME, Domain Keys Identified Mail, | 2 | |

| | | | |
|---|---|---|---|
| 5.4 | Secure Sockets Layer (SSL) and Transport Layer Security (TLS HTTPS, IPv4 and IPv6 Security | 2 | |
| 5.5 | **Internet Authentication Applications :** Kerberos, X.509, Public-Key Infrastructure | 2 | |

**Textbook references (IEEE format):**
**Text Book:**

1. William Stallings, Lawrie Brown, *"Computer Security- Principles and Practice",* Third Edition, 2015

**Reference books:**

1. Dieter Gollman , "*Computer Security"* Wiley; 3rd edition (February 28, 2011)
2. Douglas R.Stinson, *"Cryptography-Theory & Practices"*, 3rd edition CRC press 2005.

**Evaluation Methods:**

| Item | Weightage |
|---|---|
| Quiz-I | 05 |
| Project | 15 |
| Mid Term | 30 |
| End Term | 50 |

**Prepared By: Jayaprakash Kar**
**18th March 2019**