Information Security

EG3203CT

Year: III **Total: 5 hours /week**

Part: II **Lecture: 3 hours/week**

Tutorial: hours/week

Practical: hours/week

Lab: 2 hours/week

Course description:

This course is designed to introduce basics of Information Security in digital world. It deals with elementary cryptography, protection mechanisms against threats and ways to administer security tools.

Course objectives:

After completion of this course students will be able to:

1. Find information vulnerability and attacks.
2. Use encryption techniques.
3. Get knowledge of program security, network security and database security.

Course Contents:

Theory

Unit 1. Introduction **[2 Hrs.]**

- 1.1. Information System
- 1.2. Data and Information
- 1.3. Vulnerability and attacks
- 1.4. Security Goals
- 1.5. Security services and mechanisms

Unit 2. Cryptographic Techniques **[10 Hrs.]**

- 2.1. Conventional Cryptographic Techniques
  - 2.1.1. Conventional substitution and transposition ciphers
  - 2.1.2. One-time pad
  - 2.1.3. Block cipher and stream cipher
  - 2.1.4. Steganography
- 2.2. Symmetric and Asymmetric Cryptographic Techniques
  - 2.2.1. Rivest, Shamir, and Adleman (RSA)
  - 2.2.2. Data Encryption Standard (DES)
  - 2.2.3. Advanced Encryption Standard (AES)

Unit 3. Authentication and Digital Signatures **[4 Hrs.]**

- 3.1. Use of Cryptography for authentication
- 3.2. Secure Hash function
- 3.3. Key management-Kerberos

Unit 4. Application Security **[4 Hrs.]**

- 4.1. Types
- 4.2. Security in cloud
- 4.3. Mobile application security
- 4.4. Web application security

Unit 5. Program Security **[4 Hrs.]**

5.1. Non-malicious Program errors
  5.1.1. Buffer overflow
  5.1.2. Incomplete mediation
  5.1.3. Time-of-check to Time-of-use errors
5.2. Viruses
5.3. Trapdoors
5.4. Salami attack
5.5. Man-in-the-middle attacks
5.6. Covert channels

Unit 6. Security in Networks **[8 Hrs.]**

6.1. Threats in networks
6.2. Network Security Controls
  6.2.1. Architecture
  6.2.2. Encryption
  6.2.3. Content Integrity
  6.2.4. Strong Authentication
  6.2.5. Access Controls (Physical and Logical)
  6.2.6. Wireless Security
  6.2.7. Honeypots
  6.2.8. Traffic flow security
6.3. Firewalls
  6.3.1. Design and Types of Firewalls
  6.3.2. Personal Firewalls
  6.3.3. Intrusion Detection System (IDS) and its types
  6.3.4. Intrusion Protection System (IPS)
6.4. Email Security
  6.4.1. PGP
  6.4.2. S/MIME

Unit 7. Database Security **[5 Hrs.]**

7.1. Security requirements
7.2. Reliability and integrity
7.3. Sensitive data
7.4. Inference
7.5. Multilevel database
7.6. Proposals for multilevel security

Unit 8. Security Administration **[8 Hrs.]**

8.1. Security Planning
8.2. Risk Analysis
8.3. Organizational Security policies
8.4. Physical Security
8.5. Legal Privacy and Ethical Issues in Computer Security:
  8.5.1. Protecting Programs and data
  8.5.2. Information and the law
  8.5.3. Rights of Employees and Employers
  8.5.4. Software failures
  8.5.5. Computer Crime

8.5.6. Privacy
8.5.7. Ethical issues in Computer Security
8.5.8. Case studies of ethics

Practical: **[30 Hrs.]**

1. Implement Caesar Cipher.
2. Implement substitution cipher.
3. Implement different cryptographic algorithm (RSA, DES, AES)
4. Implement Firewall.
5. Implement Access control.
6. Implement Digital Signature.

Final written exam evaluation scheme			
Unit	**Title**	**Hours**	**Marks Distribution***
1	Introduction	2	4
2	Cryptographic Techniques	10	18
3	Authentication and Digital Signatures	4	7
4	Application Security	4	7
5	Program Security	4	7
6	Security in Networks	8	14
7	Database Security	5	9
8	Administering Security	8	14
	Total	**45**	**80**

* There may be minor deviation in marks distribution.

References:

1. Security in Computing, Fourth Edition, by Charles P. Pfleeger, Pearson Education
2. Cryptography and Network Security Principles and Practice, Fourth or Fifth Edition, William Stallings, Pearson
3. Modern Cryptography: Theory and Practice, by Wenbo Mao, Prentice Hall.
4. Network Security Essentials: Applications and Standards, by William Stallings. Prentice Hall.