National University of Computer & Emerging Sciences

Department of Computer Science

CS3002: Information Security

Fall 2024

Instructor

Name: Dr. Ammar Haider

TA Name: TBA

Email address: ammar.haider@nu.edu.pk

Office Location: Block F, First floor, Room 26

Office Hours: Open

Course Objectives/Goals

This course serves as a comprehensive overview to the field of information security at senior undergraduate level. At the end of the course the students will be able to:

	BT Level	PLO Mapping
1. **Explain** key concepts of information security such as design principles, cryptography, risk management.	2	1
2. **Discuss** legal, ethical, and professional issues in information security.	2	6
3. **Analyze** real world scenarios, model them using security measures, and apply various security and risk management tools for achieving information security and privacy.	3	2
4. **Identify** appropriate techniques to tackle and solve problems of real life in the discipline of information security.	4	3

The course will broadly cover the following topics:

- Information security foundations
- Security design principles and mechanisms
- Symmetric and asymmetric cryptography
- Hash functions, digital signatures, key management,
- Authentication and access control
- Software security, vulnerabilities and protections, malware
- Database security
- Network security, firewalls
- Intrusion detection
- Security policies, policy formation and enforcement

- Risk assessment
- Cybercrime, law and ethics in information security
- Privacy and anonymity of data

Reference Textbooks

- Computer Security: Principles and Practice (SPP), 4th ed. by William Stallings and Lawrie Brown
- Cryptography and Network Security (CNS), 8th ed. By William Stallings
- Principles of Information Security, 6th ed. by M. Whitman and H. Mattord
- $(ISC)^2$ CISSP: Official Study Guide, 8th edition
- Computer Security, 3rd edition by Dieter Gollmann
- Computer Security Fundamentals, 3rd edition by William Easttom

Tentative Grading Criteria

- 3-4 Assignments — 10%
- 4 Quizzes — 10%
- 2 Midterm Exams — 25%
- Course Project — 10%
- Final Exam — 45%

Grading Scheme: Absolute

Tentative Weekly Schedule

Timeline	Content Covered
Lecture 1	**Course Introduction** • Introducing syllabus, policies, and projects. • An overview of basic information security principles (with practical examples): confidentiality, integrity, availability, authentication, authorization and non-repudiation. • Component of an Information system
Lecture 2	**Security Design Principles** Discussion and evaluation of following primitives: Least-privilege, fail-safe defaults, complete mediation, separation of privilege, economy of mechanism, open design
Lecture 3	**Cryptography** Introduction to Cryptography: Symmetric cipher model, Substitution techniques (Caesar cipher, Monoalphabetic cipher)
Lecture 4	**Cryptography-II** Substitution techniques (Vigenere cipher, One-time pad) Transposition techniques (Rail fence cipher, Row transposition cipher)
Lecture 5	**Cryptography-II** Block cipher structure and design principle, Feistel cipher structure, the data encryption standard, DES (encryption, key generation)

Lecture 6	**Cryptography-III** AES structure, transformation, key expansion mechanism, AES example and implementation Stream ciphers introduction
Lecture 7	**Cryptography-IV** Introduction to Public Key cryptography RSA: principles, RSA algorithm Diffie-hellman key exchange algorithm with example, Man-in-the-middle attack in diffie-hellman
Lecture 8	**Cryptography-V** Hash functions, applications, Hash properties (preimage resistant, second preimage resistant, collision resistant) Message authentication code, requirements & properties of MAC HMAC algorithm & structure
Lecture 9	**Cryptography-VI** Digital Signature, requirements & properties of DS Public key infrastructure (PKI), elements of PKI, X.509, Digital certificates
Lecture 10	**Revision**
First Mid-term Exam	
Lecture 11	**Software Security** Malware, types of malware (virus, worms, trojan horse, adware, spyware, backdoor, ransomware, rootkits, bootkits), malware analysis & countermeasures
Lecture 12	**Software Security-II** Control Hijacking: Integer overflow String format vulnerabilities & countermeasures
Lecture 13	**Software Security-III** Control Hijacking: Buffer overflow countermeasures
Lecture 14	**Database Security** Basics SQL Injection Attack, techniques, types of attack Countermeasures, database access control
Lecture 15	**Database Security-II** Database inference attacks & counter measures Database encryption methods
Lecture 16	**Web Security** Background

	Cross Site Request Forgery (CSRF) Attack Countermeasures (STP, origin header, referrer header)
Lecture 17	**Web Security-II** Cross Site Scripting (XSS) Attack Types of XSS (reflected, stored, DOM based) countermeasures (encoding, validation, input handling contexts, secure input handing)
Lecture 18	**User Authentication** Types (password, biometric, symmetric/asymmetric) Kerberos (overview, key exchange protocol)
Lecture 19	**Access Control** Access control policies Discretionary and Role-based Access Control
Lecture 20	**Revision**
Second Mid-term Exam	
Lecture 21	**Network Security** Secure Socket Layer (SSL) SSL certificate, architecture, handshake
Lecture 22	**Network Security-II** IP security (IPSec) IPsec modes (transport, tunnel), architecture, AH, ESP
Lecture 23	**Network Security-III** Intrusion Detection Systems (IDS) Components of IDS, classification of IDS (anomaly, signature, hybrid), types (host-based, network based)
Lecture 24	**Network Security-IV** Firewalls, Types of firewall (packet-filtering, stateful packet inspection, application proxy, circuit-level proxy) Location of firewall
Lecture 25	**Theoretical models of Access Control** Confidentiality policies (BLP model) Integrity policies (Biba Model) Integrity policies (Clark-Wilson model) Hybrid policies (Chinese Wall model)
Lecture 26	**Cybercrime Laws and Ethics** Pakistan cybercrime act and the role of investigative agencies. Ethical perspective of research studies and experimentation (data privacy and anonymization techniques). Intellectual property, copyright, patent, trade secret.

Lecture 27 - onwards	**Revision & Project Evaluations**
Final Examination	