University of Dhaka
Institute of Information Technology

Course Title: Information Security
Course Code: SE 411
Credit Hours: Three (3)

Course Instructor

Mohammed Shafiul Alam Khan, PhD (Information Security)
Professor,
Institute of Information Technology (IIT)
University of Dhaka, Dhaka -1000, Bangladesh
Email: shafiul@du.ac.bd

Course Overview

This course is an introduction to the broad field of computer, network, and data security. Upon completion of this course, the students

- should able to explain concepts related to applied cryptography.
- should know the algorithms of symmetric cryptography, asymmetric cryptography, and digital signatures.
- should explain the theory behind the security of different cryptographic algorithms.
- should explain common network vulnerabilities and attacks, defense mechanisms against network attacks, and cryptographic protection mechanisms.

Course Objective

- To understand how the knowledge of information security can counteract attempts to the attacks of valuable information technology assets
- To understand the basic software tools for assessing the security posture of a computer or a network
- To acknowledge the students about the fundamentals of cryptography and how cryptography serves as the central language of information security.
- To understanding how issues of privacy affect information security.

Course Content

Theory

- Introduction to Information Security: Security attacks [active, passive, brute force, cryptanalysis, insider], security services [CIA, AAA], security terminologies [adversary, vulnerability, threat, attack], assumption and trust, security policy and mechanism, threat analysis, attacker modeling
- Authentication Mechanism, Password-based authentication, Biometric authentication, Challenge-Response authentication, One-way authentication, Mutual authentication, Multifactor authentication
- Introduction to Cryptography: Plaintext, ciphertext, encryption, decryption, symmetric and asymmetric encryptions, block cipher and stream ciphers**,** historical cipher techniques

- Modern Cryptography: DES, need for 3DES, computationally secure cipher, unconditionally secure cipher, types of attack on cryptographic text, cipher mode of operation
- Cryptographic algorithm: Detail operation of AES, AES variants
- Cryptographic algorithm: Introduction to modular arithmetic, detail operation of RSA
- Hash: Properties of Hash functions, hash algorithm variants, details of SHA 512
- Diffie Hellman (DH) key exchange protocol, Problems in DH key exchange protocol. Man-in-the-Middle attack
- Digital Signature, RSA-based Digital Signature Generation and Verification
- Human Factors in Information Security: Why human is the weakest point in Information security; Social Engineering Attacks, techniques and prevention mechanisms.
- Cyber Security Controls: Physical, Technical, Procedural, Legal.
- Cyber Security Terminology, reporting software flaws, computer crime, and difference between law and ethics.

Lab

- Implementation of any tradition
- AES Implementation
- RSA Algorithm
- SHA 512 Implementation
- Using Security Tools: Introduction to Nmap
- Nmap analysis detail
- Packet analysis

Text Books

- Cryptography and Network Security- Principles and Practice, William Stallings
- Computer Security- Principles and Practice, William Stallings and Lawrie Brown
- Introduction to Computer Security, Matt Bishop

Reference Books

- Security in Computing, Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies
- Computer Security: Art and Science, Matt Bishop
- Network Security: Private Communication in a Public World, Charlie Kaufman, Radia Periman, and Mike Speciner.

Message to the Participants

- Participants are expected to attend all classes. Due to emergency, if anyone miss any lecture, recovering missed lecture content or assignment information is the responsibility of the participant. However, facilitator will cooperate to get the missing content.
- Two-way communications will be emphasized and classes will be made participatory in consultation with the participants in the class.
- Students require forming a group of Four (4) students for group activities (i.e. analyzing real world cases and so on) reflecting learning of the course

Assessment and Grading Policy

The components in evaluation for the theory course are as follows [1].

- Class attendance: 5%
- Assignments (including presentation): 5%
- Lab: 20%
- In course examinations (Mid + Class Test): 20%
- Final examination: 50%

[1] The weightage can vary up to +/- 5%

Final Grade will be calculated as per University rules which is as follows,