11464: INFORMATION SYSTEMS SECURITY

Syllabus-ISS-Fall 2021-2022

Syllabus-ISS-Fall 2021-2022

By

Mustafa Al-Fayoumi

Outline

- □ Course Overview
- □ Course Description
- □ Course contents
- □ Learning outcomes
- □ Teaching methods
- □ Textbooks and materials
- □ Assessment Policy
- □ Class Rules

Course Overview

- This course is a service course for all students of CS, CE, SE, DS&AI as a compulsory requirements and as an elective course for SE of the third and fourth year level.
- So, I can say, this course is the first one for all students that handle Information security. Therefore this course will be a heavy course.
- This course aims to provide a deep and comprehensive study of the security principles and practices of information systems.
- Therefore, this course covers the major aspects of information security, computer security and network security.

Course Description

- □ This course aims to provide a deep and comprehensive study of the security principles and practices of information systems.
- □ Topics include security threats, vulnerabilities and countermeasures, attacks, security services (confidentiality, integrity, availability, non-repudiation, accountability), cryptography: classical encryption techniques, block ciphers and stream ciphers, symmetric-key and asymmetric-key cryptography, authentication and digital signature, key management and cryptographic protocol, DES and AES, Block cipher operation modes, asymmetric ciphers: RSA, Diffie-Hellman key exchange, hash functions, MAC functions, digital signature: digital Signature Standard DSS, key management and distribution, X.509 certificates, user authentication, access control, security in operating systems, web security: SSL and TLS, electronic mail security (PGP. MOME), malicious software, and firewalls.

Course Description

- At the end of this course, students are expected to be familiar with many of the basic principles and practices in information systems security. In particular, understand what the foundational theory is behind information security:
  - What the common threats are,
  - What are the basic principles and techniques when designing a secure system, and
  - How to gauge (measure) the protection and limitations provided by today's technology

Course contents

- As you know, Information security covers many different topics and because we only have one course and one semester, we select just a subset of topics that we can cover. These topics cover the major aspects of information security.
  - Overview of information systems Security
  - Cryptography Tools
    - Number Theory
    - Classical Encryption Techniques
    - Cryptographic Algorithms: Symmetric Ciphers
    - Cryptographic Algorithms: Asymmetric Ciphers
  - User Authentication
  - Access control: Access - control principles and policies
  - Operating System Security
  - Firewalls and Intrusion Prevention System (IPS)
  - Network Security

Course contents

- Topic #1: **Overview of information systems Security**
  - In this topic we will start by giving some definitions of what do we mean by Information security, computer security, and network security, and then introduce some different concepts and terminology.
  - Also we introduce the key security requirements of confidentiality, integrity, and availability, and then the security services, type of security vulnerability, threats + attacks and countermeasures.

Course contents

- Topic # 2: **Cryptography Tools**
  - In this topic we will explain the basic cryptography terminology
  - Introduce the cipher types (symmetric and asymmetric) – (stream and block cipher)
  - Discuss the use of secure hash function for message authentication and other applications of secure hash functions.
  - Overview of the digital signature mechanism and explain the concept of digital certificate and key exchange protocol and digital envelops.

Course contents

- Topic # 3: **Number Theory – Mathematical principle of Cryptography**

  - Number theory is important thing in cryptography algorithms
  - This topic provides sufficient breadth and depth of coverage of relevant number theory topics for understanding the wide range of applications in cryptography.
  - Subtopics here will be:
    - The concept of divisibility and division algorithm
    - Operations of the Euclidean alg.
    - Concept of Modular arithmetic
    - Key concepts relating to prime number (generation and testing)
    - Some theorems like: Fermat and Euler's theorem, integer factorization problem, discrete logarithm problem, additional inverse, and multiplicative inverse.

Course contents

- Topic # 4: **Classical Encryption Techniques**
  - Overview of the main concepts of symmetric cryptography.
  - Explain the difference between cryptanalysis and brute force attack
  - Explain the difference between substitution and transposition cipher.
    - Substitution Techniques
      - Caesar Cipher – addition and multiplication
      - Monoalphabetic Cipher – Digram and trigram
      - Playfair Cipher
      - Polyalphabetic Ciphers - Vigenère Cipher
      - One-Time Pad
    - Transposition Techniques – rail fence and double
  - Block cipher: the objective of this topic is to illustrate the principle of modern symmetric cipher. For this purpose we will focus on the most widely used symmetric cipher like:
    - Simplified DES
    - The Data Encryption Standard (DES)
    - Some math - finite fields
    - Advanced Encryption Standard (AES)

Course contents

- Topic # 5: **Public Key Cryptography**
  - We will present an overview of the basic principle of public key cryptosystems, and then we will explain the two distinct uses public key cryptosystems.
  - Finally, we will present the best known algorithms as example of public key cryptosystems as RSA and DSA.

Course contents

- Topic # 6: **Use Authentication**
  - In most IS contexts, user authentication is the fundamental building block and primary line of defense.
  - So, here we will discuss the four general means of authentication a user's identity.

Course contents

- Topic # 7: **Access Control**
  - The access control is a central element of computer system security.
  - So, the primary objectives of IS are to prevent unauthorized users from gaining access to resources.
  - In this topic, we will present the 4 major categories of access control policies: DAC, MAC, RBAC, ABAC.

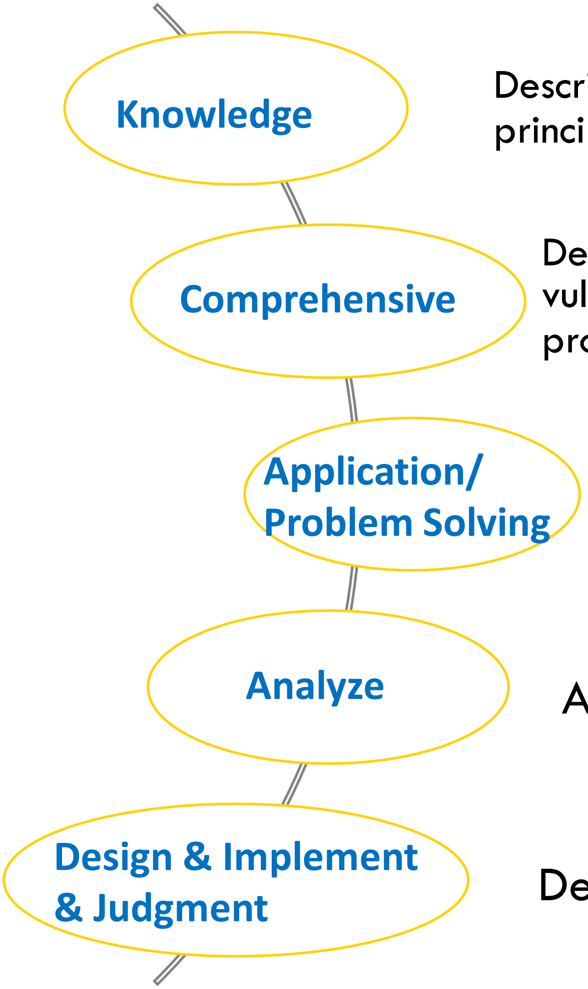
Course contents

- Topic # 8: **Operating System Security**
  - In this topic, we will discuss how to provide systems security as a hardening process that includes planning, installation and configuration, update, and maintenance of the OS.

Course contents

- Topic # 9: **Firewalls**
  - Firewalls can be an effective means of protecting a local system or Network of systems from network-based security threats, while at the same time affording access to the outside word via WAN (Wide Area networks) and the internet.
  - So, in this topic we will explain the role of firewalls as apart of IS strategy.

Course Learning outcomes (CLOs)



Knowledge

Describe the main security objectives and define basic security concepts and principles

Comprehensive

Demonstrate the ability to identify a variety of generic security threats, vulnerabilities, and attacks, and identify and analyze particular security problems for a given application

Application/ Problem Solving

Apply mathematical foundations, algorithm principles, and computer science theory in topics such as cryptographic operations and security architecture.

Analyze

Analyses the common network vulnerabilities and attacks.

Design & Implement & Judgment

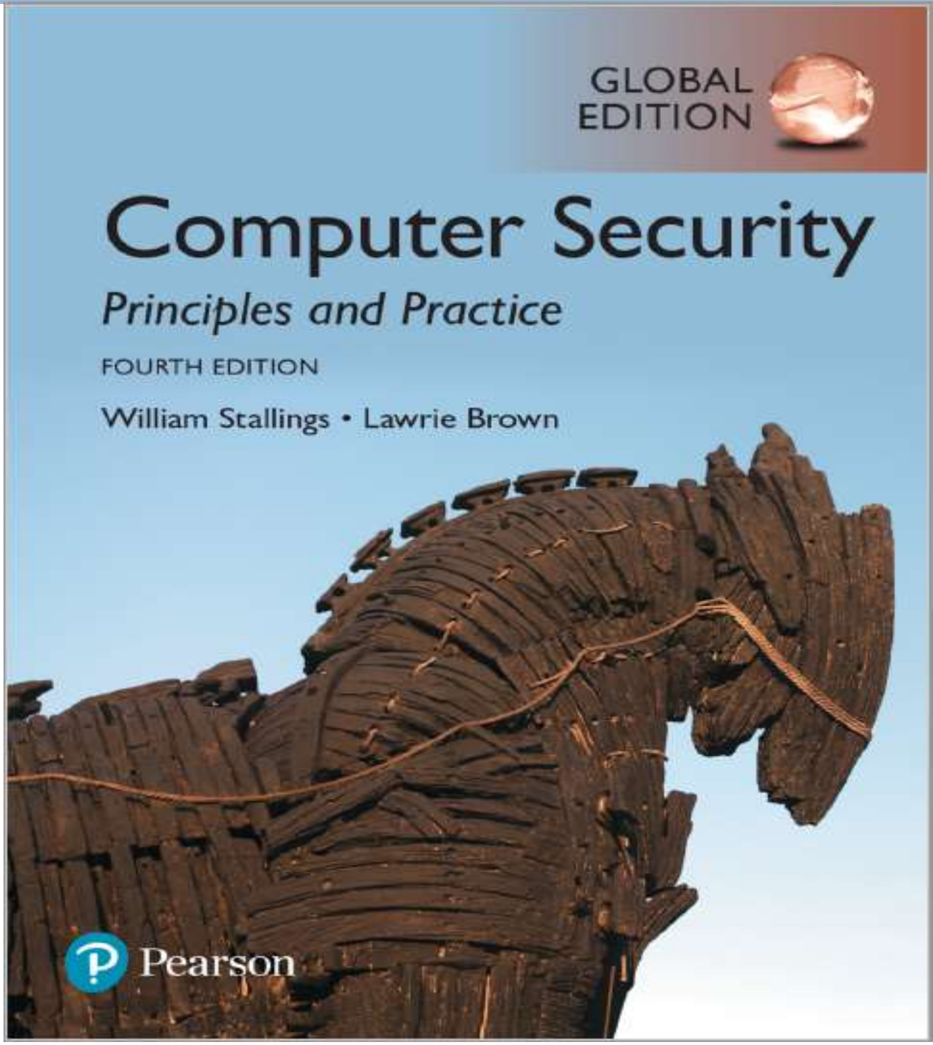
Design, implement and evaluate a secure network system..

Teaching methods

- □ Lectures
- □ Assignments
- □ Discussion
- □ Project: Individual and team
- □ E-learning (LMS)

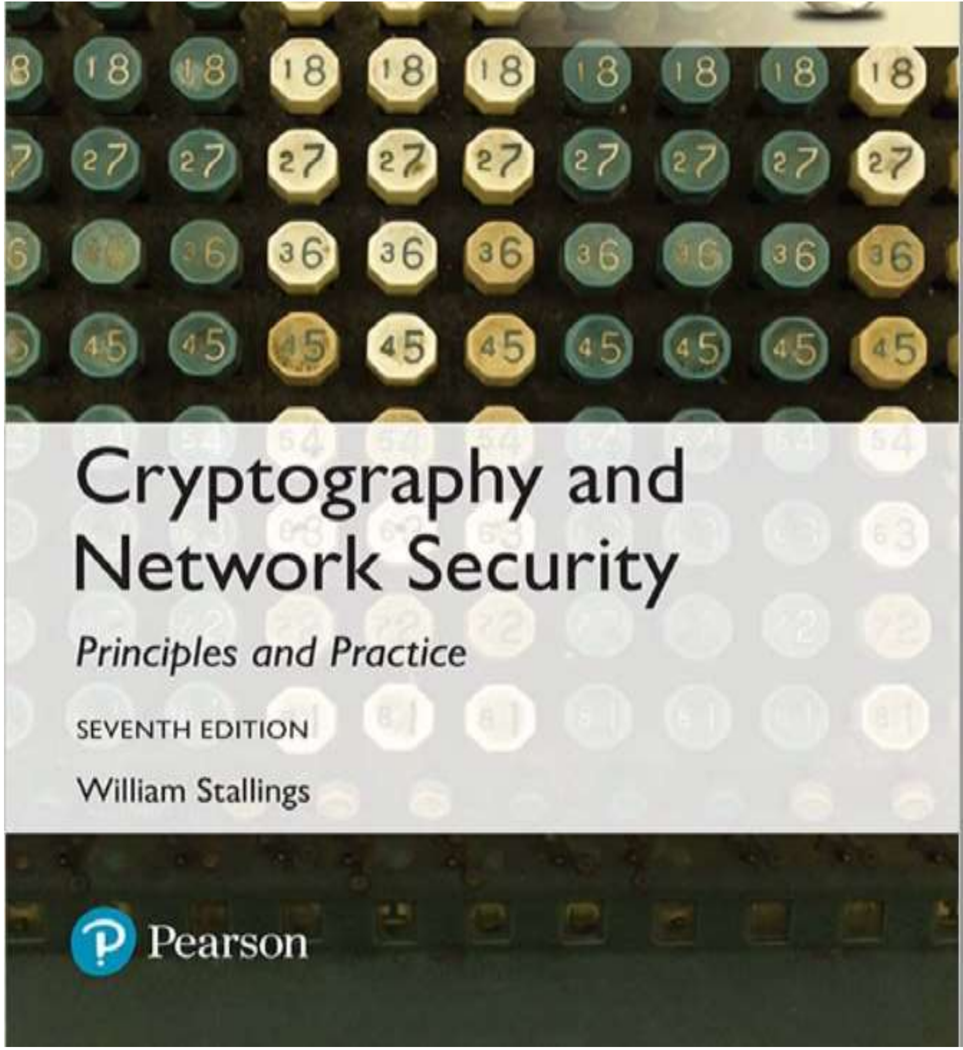
Textbooks and materials

Computer Security: Principles and Practice 4/E, by William Stallings & Lawrie Brown. Pearson Press, 2018.



Textbooks and materials

Cryptography and Network Security: Principles and Practice, 7th Edition by William Stallings. Pearson Press, 2017



Shannon's principle of Confusion and diffusion

Assessment Tool	Expected Due Date	Weight
Participation, Home Works, Quizzes and Project	All Course duration	20%
First exam	TBA	20%
Second Exam	TBA	20%
Final Exam	16th week	40%

Class Rules

- Any student who get 7 absences will definitely fail in this course.
- Do not show late to this course.
- Switch OFF your mobiles.

Thank You