

Information Security

Prepared by Dr. Ahmed Omar

IT373

Information Security

Lecture 0



Information Security

Lecture 0

IT373

Information Security

Prepared by
Dr. Ahmed Omar



Course Outline

Develop an understanding of *information assurance* as practiced in computer operating systems, software and web applications, gain familiarity with common attacking techniques such as virus, Trojan, worms and memory exploits defenses against them, develop a basic understanding of cryptography, how it has evolved, and two key encryption techniques used today(DEA, RSA).

Learning Outcomes

Upon completion of this course, the student will be able to:

- Describe Computer security concepts.
- Describe OSI security architecture.
- Explain information assurance as practiced in software and web applications.
- Describe cryptography and how it has evolved.
- Apply two key encryption techniques used today (DEA, RSA).
- Develop a basic understanding of Message Authentication (MAC)
- Apply Message Integrity (Secure Hash Algorithms: SHA-1)
- Apply Digital signatures (ELGamal digital signature scheme and Digital Signature Standard)
- Explain malicious software, viruses, viruses' countermeasures, worms.
- study ways of attaching a virus to a program.

Learning Outcomes

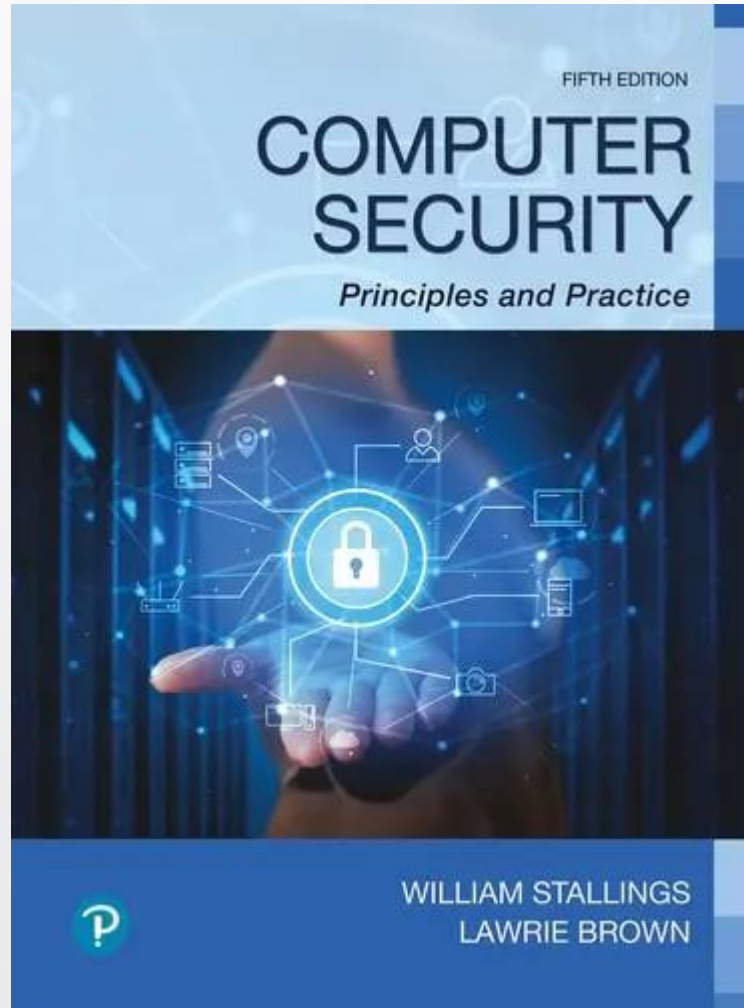
Upon completion of this course, the student will be able to:

- explain the sources of viruses and how to countermeasure them.
- List types of security policies, high- and low-level policy languages, operational issues.
- explain security feature in Linux.
- apply security feature in windows.
- explain the vulnerabilities in programs.
- explain Buffer Overflow, Cross-site Scripting (XSS) and SQL Injection.
- study cybercrime and computer crime, intellectual property (copyright).
- explain the problem of intrusion (behavior and techniques).
- classify intrusion detection techniques (statistical and rule-based)
- explain password management.

Week	Topics
1	Orientation week
2	Foundations of Information Security & Assurance
3	Symmetric Encryption & Standards
4	Asymmetric Cryptography & Key Management
5	Message Authentication & Digital Signatures
6	Malicious Software & Countermeasures
7	Operating System Security
8	Application & Web Security
9	Network Security & Protocols
10	Intrusion Detection & Cybercrime
11	Security Policies and Operational Issues
12	Revision
13	Final Exam



Course Plan



Reference

Computer Security Principles and Practice, 5th edition

❖ **80 Marks**

- 10 weekly short exams
- 8 Marks for each Exam.

❖ **20 Marks**

- Final Examination



Assessment



Thank You