


QFO-AP-FI-MO02	اسم النموذج: Course Syllabus	 Philadelphia University
رقم الاصدار: 1 (Revision)	الجهة المصدرة: كلية تكنولوجيا المعلومات	
التاريخ: 2017/11/05	الجهة المدققة: عمادة التطوير والجودة	
عدد صفحات النموذج:		

Course Title: Information Security	Course code:731443
Course Level: 4	Course prerequisite (s) and/or corequisite (s):711232
Lecture Time:11:10	Credit hours:3

**Academic
Staff
Specifics**

Name	Rank	Office Number and Location	Office Hours	E-mail Address
Dr. Amer AbuAli	Associate prof.	331	10-11:00,12-1	aabuali@philadelphia.edu.jo

Course module description:

The aim of this course is to provide the basic knowledge about computing systems security. The topics covered in this course include cryptography fundamentals, threats to computer systems, authentication of computer systems, access control, intrusion detection, program security, operating system security, database security, network & distributed systems security fundamentals and security evaluation criteria. While the course does provide all the necessary mathematical background in cryptography, it concentrates more on the systems security aspects. Therefore the primary focus will be on the design of computing systems from the security perspective.

Course module objectives:

At the end of this module, student will be able to:

1. Understand the principles and practices of cryptographic techniques; (A)
2. Understand a variety of generic security threats and vulnerabilities, and identify and analyse particular security problems for a given application; (A and B)
3. Understand the design of security protocols and mechanisms for the provision of security services needed for secure networked applications; (A)
4. Appreciate the application of security techniques and technologies in solving real-life security problems in practical systems; (A)
5. Apply appropriate security techniques to solve security problems; (B and C)

Course/ module components

- Books (title , author (s), publisher, year of publication)

Security in Computing, Charles Pfleeger, Prentice Hall International, 2007

- Support material (s) (vcs, acs, etc).
- Study guide (s) (if applicable)
- Homework and laboratory guide (s) if (applicable).

Teaching methods:

Lectures, discussion groups, tutorials, problem solving, debates, etc.

Learning outcomes:

- Knowledge and understanding
- Cognitive skills (thinking and analysis).
- Communication skills (personal and academic).

Understand a variety of generic security threats and vulnerabilities, and identify and analyse particular security problems for a given

- Practical and subject specific skills (Transferable Skills).

Appreciate the application of security techniques and technologies in solving real-life security problems in practical systems

Assessment instruments

- Short reports and/ or presentations, and/ or Short research projects
- Quizzes.
- Home works
- Final examination: 50 marks

<u>Allocation of Marks</u>	
Assessment Instruments	Mark
First examination	20
Second examination	20
Final examination: 50 marks	40
Reports, research projects, Quizzes, Home works, Projects	20
Total	100

Documentation and academic honesty

- Documentation style (with illustrative examples)
- Protection by copyright
- Avoiding plagiarism.

Course/module academic calendar

week	Basic and support material to be covered	Homework/reports and their due dates
(1)	Introduction to Computer Security	Assignment: Why we using security
(2)	Cryptography Fundamentals I	A simple algorithm for encryption
(3)	Cryptography Fundamentals II	Assignment: Write three programs to encrypt and decrypt some words
(4)	Tutorial 1, Security Protocols I	Implementation of the protocols
(5)	Security Protocols II, Tutorial 2	
(6)	Program Security, Tutorial 3	
(7)	Viruses	Tutorial of last viruses
(8)	Operating Systems Security II	Implementation of the Operating Systems
(9)	Database Security	
(10)	Network Security I	Implementation of networks
(11)	Network Security II	
(12)	Security policies, Standards & Assurance	Assignment : Evaluation of methods of defense
(13)	Security: Current issues & Trends	
(15)	Revision	
(16)	Final Examination	

Expected workload:

On average students need to spend 2 hours of study and preparation for each 50-minute lecture/tutorial.

Attendance policy:

Absence from lectures and/or tutorials shall not exceed 15%. Students who exceed the 15% limit without a medical or emergency excuse acceptable to and approved by the Dean of the relevant college/faculty shall not be allowed to take the final examination and shall receive a mark of zero for the course. If the excuse is approved by the Dean, the student shall be considered to have withdrawn from the course.

Module references

Books

Cryptography and network Security: Principles and Practice, William Stallings, 2nd Edition, Printice Hall , ***Unix Security Reference Manual, Windows Security Reference Manual,Java Security Reference Manual***