



King Fahd University of Petroleum & Minerals
College of Computer Sciences and Engineering
Information and Computer Science Department

SEC 511: Principles of Information Assurance and Security (3-0-3)

Syllabus – First Semester 2015-2016 (151)

Website: Blackboard Learn 9.1 (<https://blackboard.kfupm.edu.sa/>)

Class Time, Venue and Instructor Information:

Sec.	Time	Venue	Instructor	Office Hours
01	MW 08:00-09:15pm	24-104	Dr. EL-SAYED M. EL-ALFY Office: 22-108 Phone: 013-860-1930 E-mail: alfy@kfupm.edu.sa	MW: 9:15-10:00PM Or by appointment

Course Catalog Description

Introduction to information assurance and security. Information confidentiality, availability, and integrity. Security systems lifecycle. Risks, attacks, and the need for security. Legal, ethical, and professional issues in information security. Risk management including identification and assessment. Security technologies and tools. Security laws, audit and control. Cryptography foundations, algorithms and applications. Physical security, security and personnel, security implementation and management. Securing critical infrastructure. Trust and security in collaborative environments.

Pre-requisites: Graduate Standing

Course Objectives

- ▶ This course is an introductory course to information assurance and security (IAS). It provides a wide coverage of a variety of technical and administrative aspects of IAS.

Course Learning Outcomes

Upon completion of the course, you should be able to:

1. Demonstrate the ability to use security lingo and terminology.
2. Identify and describe key issues associated with IAS
3. Explain potential threats, risks and attacks to information assets.
4. Describe the lifecycle of information security systems.
5. Discuss various security methods, procedures and tools for detection and reaction to threats.
6. Effectively use common tools for information assurance and security
7. Describe various administrative, legal, ethical and professional issues and liabilities related to IAS in computer and network environment, and best practices to write a security policy.
8. Gain skills and demonstrate ability to conduct research in the field of IAS.

Required Material

- ▶ No official textbook for the course. However, a number of selected book chapters and papers will be identified throughout the semester.
- ▶ Lecture notes and some recommended websites

Other Recommended References

- ▶ [Principles of Information Security](#), 5/E, Michael E. Whitman, Herbert J. Mattord, Cengage Learning, January 2014.
- ▶ [Computer and Information Security Handbook](#), John R. Vacca (Ed.), MK, Elsevier, 2013. [Available thr [sciencedirect.com](#)]
- ▶ [Cryptography & Network Security](#), Behrouz Forouzan, McGraw-Hill, 2008.
- ▶ [Cryptography and Network Security: Principles and Practice](#), 6/E, [William Stallings](#), Prentice Hall, 2014.
- ▶ [Security+ Guide to Network Security Fundamentals](#), 5/E, Mark Ciampa, Course Technology, 2014.
- ▶ [Hacking Exposed: Network Security Secrets and Solutions](#), 7/E, Stuart McClure, Joel Scambray, George Kurtz, McGraw-Hill Osborne, 2012.
- ▶ [Hacking Exposed Malware and Rootkits](#), Michael Davis, Sean Bodmer, Aaron LeMasters, McGraw-Hill Osborne, 2009.
- ▶ [Hacking Exposed Web Applications](#), 3/E, Joel Scambray, Vincent Liu, Caleb Sima, McGraw-Hill Osborne, 2010.
- ▶ [Computer Viruses and Malware](#), John Aycock, Advances in Information Security, Springer, 2006.

Assessment Plan

Assessment Tool	Weight
Coursework: Blogs, Assignments, Presentations & Quizzes	15 %
Term Project	30 %
Midterm Exam (9 th week on Wednesday, Nov. 17)	25 %
Final Exam (semi-comprehensive) [As announced by the registrar: Dec. 17@7PM]	30 %

Tentative Topics Covered and Some References:

- ▶ Research skills: Writing academic papers, Latex, GNUPlot. (Plenty of online resources)
- ▶ Introduction to Information Assurance and Security (Ch. 1, Principles of Information Security)
- ▶ Overview of Cryptography (Selected chapters from Cryptography and Network Security Book).
- ▶ Securing Organizations (Ch.1, Security Handbook)
- ▶ System Intrusions (Ch. 3, 4, Security Handbook)
- ▶ Firewalls (Ch. 21, Security Handbook)
- ▶ Mathematical Model to Security Policies
- ▶ Malware (Ch. 2,3, Computer Virus and Malware Book)
- ▶ Web Application Security (OWASP Resources)
- ▶ Computer and Network Forensics (Ch. 19, 20, Security Handbook)
- ▶ Trust and security in collaborative environments
- ▶ Legal, Ethical, and Professional Issues (Ch. 3, Principles of Information Security, Saudi Laws).

Course Policies

- **Course website & participation:** Students are required to periodically check the course website and download course material as needed. Several resources will be posted through the website as well. Blackboard **CE 9.1** will be used for communication and interaction, posting and

submitting assignments, posting grades, posting sample exams, etc. It is expected that you get benefit from the discussion board by raising questions or answering questions put by others.

- **Attendance:** Regular attendance is a university requirement; hence attendance will be checked at the beginning of each lecture and lab. Late arrivals will disrupt the class session. Hence, two late attendances will be considered as one absence. Missing more than 6 unexcused lectures will result in a DN grade without prior warning. To avoid being considered as absent, an official excuse must be shown no later than one week of returning to classes.
- **No makeup of homework, quizzes or exams will be given.**
- **Re-grading policy:** If you have a complaint about any of your grades, discuss it with the instructor no later than a week of distributing the grades (except for the final the date will be announced). Only legitimate concerns on grading should be discussed.
- **Office hours:** Students are encouraged to use the office hours to clarify any part of the material that is not clear; however the instructor will only provide hints if it is an assigned task but not solve it.
- **Academic honesty:** Students are expected to abide by all the university regulations on academic honesty. Cheating will be reported to the Department Chairman and will be severely penalized. Although collaboration and sharing knowledge is highly encouraged, copying others' work without proper citation, either in part or full, is considered plagiarism. Whenever in doubt, review the university guidelines or consult the instructor. Cheating in whatever form will result in F grade.
- **Courtesy:** Students are expected to be courteous toward the instructor and their classmates throughout the duration of this course. Talking while someone else is speaking will not be tolerated. Furthermore, all cell phones must be turned off during class and exams. In addition, students are expected to be in class on time. More importantly, you are not allowed to leave the class unless it is an urgent matter. To contact your instructor, please use email through Blackboard and avoid using phone calls or written notes whenever possible.

☺☺☺ **Best luck!!** ☺☺☺