Fall 2015/16, IS 536 —Syllabus (tentative)

Instructor: **Dr. Saad Alaboodi** **Office: 2025** **Email: Salaboodi <at> ksu.edu.sa**

Course mechanics

- Classes: Mon 04:00-06:30
- This course will use KSU LMS (as much as possible!) @ https://lms.ksu.edu.sa
- It is your responsibility to keep up with the course updates
- Feedback is highly encouraged and appreciated
- Mobile phone policy: phones must be switched off/in silent mode!
- Midterm: Monday Nov 2nd 2015
- Final Exam: Monday December 21st 2015

Overview

This course first introduces the full spectrum of security controls necessary for establishing governance program in computing environments, i.e., technological, administrative, and physical, including security fundamentals, security in programs, operating systems, networks, and databases, cryptography, and security auditing. It then explores security governance domain, covering its objectives, metrics, roles and responsibilities, and risk management.

Students completing this course should be better able to develop and evaluate security governance program using structured and widely-accepted methodologies.

Intended audience

Upper year undergrad or graduate students.

Prerequisites

Fundamentals of operating systems (e.g., CSC227), computer networks (e.g., IS370), and database management systems (e.g., IS335).

Main textbook

Information Security Governance: A Practical Development and Implementation Approach, by Krag Brotby, ISBN: 978-0-470-13118-3.

Additional textbooks

1) Principles of Information Security, Fourth Edition by Michael E. Whitman and Herbert J. Mattord
2) Security in Computing, 4th Edition by Charles P. Pfleeger
3) Computer Security, 3rd Edition by Dieter Gollmann, Wiley, 2011
4) Information Security: Principles and Practice, Second Edition, Wiley-Inter Science, 2011, by Mark Stamp

Extra reading

1) Security Engineering, Ross Anderson, Wiley, 2001, http://www.cl.cam.ac.uk/~rja14/book.html
2) Computer Security: Principles and Practice by William Stallings and Lawrie Brown

3) Matt Bishop: Computer Security, Art and Science Addison-Wesley, 2003.
book info @ http://nob.cs.ucdavis.edu/book/book-aands/index.html
4) Handbook of Information and Communication Security, Springer, Peter Stavroulakis and Mark Stamp (Editors): Electronic copy available.

Other Resources

- Schneier on Security, http://www.schneier.com/blog/. A blog covering current computer security and privacy issues.
- The RISKS Digest, http://catless.ncl.ac.uk/Risks. A forum on risks to the public in computers and related systems.
- BugTraq, http://www.securityfocus.com/archive/1. A full disclosure moderated mailing list for the detailed discussion and announcement of computer security vulnerabilities.

Modes of study
Lectures, research work, presentations, and discussions.

Outline
The deliverables of this course consists of three main parts:

Part I: Introductory lectures (selective topics)		
Seq #	Subject	Resource type
1	Introduction to information security and privacy concepts and terminology, comparing security with privacy, attacks and methods of defense	ppt slides
2	Elementary cryptography, symmetric and asymmetric cryptosystems	
3	Program security, secure programs, nonmalicious program errors, malicious code, controls against program threats	
4	Operating system security, access controls, user authentication	
5	Database Security and Privacy, integrity, sensitive data and inference	
6	Network Security, threats in network, firewalls, intrusion detection systems	

Part II: Security governance program Each student (or a group of students) will present and discuss in class one section from the main textbook (or additional course materials as indicated).			
Seq #	**Subject**	**Distribution**	**Resource**
1	CH1 Governance Overview	Instructor	Main textbook chapters "Information Security Governance: A Practical Development and Implementation Approach"
2	CH2 Why Governance?		
3	CH3: LEGAL AND REGULATORY REQUIREMENTS	1 student	
4	CH4: ROLES & RESPONSIBILITIES		
5	CH5: STRATEGIC METRICS	2 students	

6	CH6: INFORMATION SECURITY OUTCOMES		
7	CH7: SECURITY GOVERNANCE OBJECTIVES	3 students	
8	CH8: RISK MANAGEMENT OBJECTIVES		
9	CH9: CURRENT STATE		
10	CH10: DEVELOPING A SECURITY STRATEGY	2 students	
11	CH11: SAMPLE STRATEGY DEVELOPMENT		
12	CH12: IMPLEMENTING STRATEGY	2 student	
13	CH13: SECURITY PROGRAM DEVELOPMENT METRICS		
14	CH14: INFORMATION SECURITY MANAGEMENT METRICS	3 students	
15	CH15: INCIDENT MANAGEMENT AND RESPONSE METRICS		
16	ISO27001	2 students	ISO documents

Part III: Project or topic research and presentation		
Seq #	Paper	Domain
1	Organized in groups of THREE students (maximum), each group will choose to either work on a project or topic research. The group will submit a project/topic report, and present and discuss their work and findings in class.	**Project:** information security governance **Topic research:** any area under/related to security and privacy—subject to prior approval. --- Sample subjects (for both projects and topic research): • ISO27001 • ISO27002 • SANS Critical Controls @ http://www.sans.org/critical-security-controls • HIPPA • SSE-CMM

Grading Policy

Grades will be calculated as follows:

- Midterm exam: 20%
- Final exam: 40%
- Module assignment and presentation (Part II): 20%
- Project/topic research and presentation (Part III): 20%