

Fall 2014/2015, IS 536 Section 236—Syllabus (tentative)

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

Course mechanics

- Classes: Wed 04:00-06:30, Studio # 4
- 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: 26 November 2014

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	
7	Administering security, planning, risk analysis, policies, physical security	

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	CH3: LEGAL AND REGULATORY REQUIREMENTS	1 student	Main textbook chapters
2	CH4: ROLES & RESPONSIBILITIES		
3	CH5: STRATEGIC METRICS	2 students	

4	CH6: INFORMATION SECURITY OUTCOMES		"Information Security Governance: A Practical Development and Implementation Approach"	
5	CH7: SECURITY GOVERNANCE OBJECTIVES	3 students		
6	CH8: RISK MANAGEMENT OBJECTIVES			
7	CH9: CURRENT STATE			
8	CH10: DEVELOPING A SECURITY STRATEGY	2 students		
9	CH11: SAMPLE STRATEGY DEVELOPMENT			
10	CH12: IMPLEMENTING STRATEGY	2 student		
11	CH13: SECURITY PROGRAM DEVELOPMENT METRICS			
13	CH14: INFORMATION SECURITY MANAGEMENT METRICS	3 students		
14	CH15: INCIDENT MANAGEMENT AND RESPONSE METRICS			
15	ISO27001	2 students		ISO documents

Part III: Project or topic research and presentation

Seq #	Paper	Domain
1	Organized in groups of THREE students, 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.	<p>Project: information security governance.</p> <p>Topic research: any area under/related to security and privacy—subject to prior approval.</p> <p>-----</p> <p>Sample subjects (for both projects and topic research):</p> <ul style="list-style-type: none"> • ISO27001 • ISO27002 • SANS Critical Controls @ http://www.sans.org/critical-security-controls • HIPPA

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%