

Fall 2015/16 IS 493 Syllabus

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

TA: Abdulaziz Alajaji Office:

Course mechanics

- Classes: Mon 10:00-11:50
 Wed 10:00-10:50
- 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 exam: TBD
- **Final exam: Sunday Dec 20th 2015**

Overview

This course introduces security issues in various aspects of computing, particularly security fundamentals, security in programs, operating systems, networks, databases, and Internet applications, and symmetric and asymmetric cryptography.

In addition, students will undertake two security projects: 1) Exploitation and 2) Defense. In the Exploitation project, and only for educational purposes, students will use an attack image, such as Kali Linux or BeEF, to find and exploit a vulnerability, such as existing vulnerabilities in Metasploitable 2 image (a deliberately vulnerable Linux environment). In the Defense project, students will implement a cryptosystem (e.g., RSA, Elliptic curve, Hill cipher, etc.), demonstrating both encryption and decryption processes.

Students completing this course should be better able to build more protective system designs following structured and engineered methods. Students will also learn to implement basic crypto primitives and conduct high-level research in security and privacy issues.

Intended audience

Third or fourth year IS students, or first year IS graduate students

Prerequisites

Operating Systems (CSC227), Data Communications and Computer Networks (IS370), Database Management Systems (IS335), programming skills.

Outline

- Introduction to information security and privacy concepts and terminology (1.5 hours)
- The meaning of computer security, comparing security with privacy, attacks and methods of defense (1.5 hours)
- Elementary cryptography such as Hill Cipher, vigenere Cipher, symmetric and asymmetric cryptosystems such as RSA, Diffie-Hellman, DES, Triple DES, AES (15 hours)
- Program security (Address space layout randomization, XSS Controls, Client-Server Side Mediation) , secure programs, nonmalicious program errors, malicious code, controls against program threats (6 hours)
- Operating system security (Paging, Segmentation , memory and address protection, access controls, user authentication, trusted OSs (6 hours)
- Database security and privacy, reliability and integrity, sensitive data and inference (5 hours)

- Network Security, threats in network, firewalls, intrusion detection systems (5 hours)
- Administering security, planning, risk analysis, policies, physical security (6 hours)

Textbooks

1. Security in Computing, 4th Edition by Charles P. Pfleeger
2. Computer Security, 3rd Edition by Dieter Gollmann, Wiley, 2011
3. 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. Computer Security: Art and Science by Matt Bishop, 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)

Other resources

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

Grading Policy

Grades will be calculated as follows:

- Midterm exam (20%)
- Exploitation project (10%)
- Defense project (10%)
- Tutorials (10%)
- Assignments (5%)
- Quizzes (5%)
- Final exam (40%)