Fall 2014/2015 IS622 Syllabus

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

Course mechanics

- Classes: Tue 11:00-01:30
- 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!

Overview

The objective of this course is to explore some of the advanced topics in information security arena adopting a research-centric approach. The deliverables of this course consist of four main components: 1) Introductory lectures to security in today's computing, covering various aspects of security such as security fundamentals, security in programs, operating systems, networks and databases. 2) A brief overview and discussions of research methods and resources for graduate studies. 3) A thorough study of selected topics in security in a research-based setting. Examples of selected topics may include research work in security engineering, security economics, computer security and privacy, C4I systems, usable security and privacy, and security modeling and evaluation methods. 4) A research paper component.

Students completing this course should be better able to explore and conduct structured research into those multidisciplinary areas of security and privacy in today's computing environments. This course also aims at advancing research and presentation skills, thesis and paper writing, and paper critique abilities.

Intended audience

Graduate students.

Prerequisites

Fundamentals of operating systems (e.g., CSC227), data communications and computer networks (e.g., IS370), database management systems (e.g., IS335), basic modeling and programming skills.

Modes of study

Discussions, research work, presentations, and lecturing.

Outline

The deliverables of this course consists of four main parts:

Part I: Introductory lectures to security fundamentals		
Seq #	Subject	Resource type
1	Introduction to information security and privacy concepts and terminology, comparing security with privacy, attacks and methods of defense	
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, memory and address protection, access controls, user authentication, trusted OSs	ppt slides
5	Database Security and Privacy, reliability and 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: presentation and discussion of selected resources for PhD-level research methods			
Seq #	Title	Method	Date
1	U of Berkeley: Armando's Paper Writing and Presentations Page http://www.cs.berkeley.edu/~fox/paper_writing.html	Paper writing and presentation skills	
2	The illustrated guide to a Ph.D by Matthew Might http://matt.might.net/articles/phd-school-in-pictures/	PhD track	
3	How to Write a Great Research Paper http://www.youtube.com/watch?v=g3dkRsTqdDA	Research paper	
4	U of Toronto: How Theses Get Written: Some Cool Tips! Dr. Steve Easterbrook http://www.cs.toronto.edu/~sme/presentations/thesiswriting.pdf	Thesis writing	
5	U of Cambridge: How to write a great research paper http://www.youtube.com/watch?v=g3dkRsTqdDA	Research paper	

6	U of Michigan: https://open.umich.edu/sites/default/files/Topic8Assignment-CritiqueArticle.pdf	Paper critique	

Part III: Paper critique: total of four selected scientific papers			
Seq #	Paper	Domain	Due date
1	Yee, Ka-Ping. "Aligning security and usability." IEEE Security & Privacy 2.5 (2004): 48-55.	Usable security and privacy	
2	Chiasson, Sonia, Paul C. van Oorschot, and Robert Biddle. "A Usability Study and Critique of Two Password Managers." Usenix Security. Vol. 6. 2006.	Usable security and privacy	
3	A. Whitten and J. D. Tygar, "Why johnny can't encrypt: A usability evaluation of PGP 5.0," in Proceedings of the 8th USENIX Security Symposium, 1999	Usable security and privacy	
4	Anderson, Ross. "Why information security is hard-an economic perspective." Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual. IEEE, 2001.	Security economics	
5	K. J. S. Hoo, "How much is enough? A risk-management approach to computer security," in Workshop on Economics and Information Security, UC Berkeley, CA, 2000.	Security economics/risk management	
6	R. Anderson and T. Moore, "The Economics of Information Security," Science, vol. 314, pp. 610-613, 2006.	Security economics	
7	Sandhu, Ravi S., and Pierangela Samarati. "Access control: principle and practice." Communications Magazine, IEEE 32.9 (1994): 40-48.	Access controls	
8	A. Avizienis, J. -. Laprie, B. Randell and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, pp. 11-33, 2004.	Dependable and secure computing	
9	Schneier, Bruce. "Attack trees." Dr. Dobb's journal 24.12 (1999): 21-29.	Security modeling and evaluation methods	
10	Torres-Toledano, José Gerardo, and Luis Enrique Sucar. "Bayesian networks for reliability analysis of complex systems." Progress in Artificial Intelligence—IBERAMIA 98. Springer Berlin Heidelberg, 1998. 195-206.	Security modeling and evaluation methods	

11	D. M. Nicol, W. H. Sanders and K. S. Trivedi, "Model-based evaluation: from dependability to security," IEEE Transactions on Dependable and Secure Computing, vol. 1, pp. 48-65, 2004.	Security modeling and evaluation methods	
12	B. Littlewood, S. Brocklehurst, N. Fenton, P. Mellor, S. Page, D. Wright, J. Dobson, J. McDermid and D. Gollmann, "Towards Operational Measures of Computer Security," Journal of Computer Security, vol. 2, pp. 3, 1993	Security modeling and evaluation methods	
13	A Vouk, Mladen. "Cloud computing–issues, research and implementations." CIT. Journal of Computing and Information Technology 16.4 (2008): 235-246.	Cloud computing	
14	A journal paper of your choice (max. one journal)	Subject to approval	

Part IV: research paper				
Seq #	Paper	Domain	Submission date	Presentation date
1	Each student is required to write a complete research paper before end of term. In addition, sharing progress and discussions will be conducted on a weekly basis along other course materials with the class.	Any area under/related to security and privacy (subject to approval)	December 9th 2014	December 16th 2014

Textbooks

This course is not designed to follow a particular textbook(s), rather as a research-oriented course it will be mostly based on research papers in the selected areas of study. However, for interested readers, the following list contains the most popular textbooks used in international graduate schools.

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
4. Security Engineering, Ross Anderson, Wiley, 2001, http://www.cl.cam.ac.uk/~rja14/book.html
5. Computer Security: Principles and Practice by William Stallings and Lawrie Brown
6. Computer Security: Art and Science by Matt Bishop, Addison-Wesley, 2003.
   book info @ http://nob.cs.ucdavis.edu/book/book-aands/index.html
7. Handbook of Information and Communication Security, Springer, Peter Stavroulakis and Mark Stamp (Editors)

Other online 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.

Paper critique resources

1. http://www.citewrite.qut.edu.au/write/critique.jsp
2. http://www.uis.edu/ctl/wp-content/uploads/sites/76/2013/03/Howtocritiqueajournalarticle.pdf
3. https://open.umich.edu/sites/default/files/Topic8Assignment-CritiqueArticle.pdf

Grading Policy (tentative)

Grades will be calculated as follows:

- Research paper (50%)
- Paper critique—total of 4 papers (40%)
- Final presentation (10%)