ISA 562, Spring 2019

1. Catalog Description

Credits: 3 (NR)

Course Description: A technical introduction to the theory and practice of information security, which serves as the first security course for the MS-ISA degree, is required as a prerequisite for all subsequent ISA courses (at the 600 and 700 levels) and subsumes most topics covered by the CISSP examination. Also serves as an entry-level course available to non-ISA students, including MS-CS, MS-IS, and MS-SWE students.

Last day to add / drop classes without penalty: 01/26/2016
Drop with Tuition Penalty (and final drop deadline) Dates: 02/19/2016
Prerequisite(s): INFS 501, 515, 519, and SWE 510, or permission of instructor.

2. Class Administration

Class Times: Monday 4.30-7.10
Location: Arts and Design Building L008

Instructor: Duminda Wijesekera
Email: dwijesek@gmu.edu
Phone: 703-993-5030
Office Hours: Monday 3.30-4.00 and 7.30-8.00. (Before and after class)
Office Hour Location: Research Building 436

Teaching Assistant: Padmawathi Duggireddy
Email: pduggire@masonlive.gmu.edu
Office Hours: Thursday 4.00-6.00 pm
Location: Engineering 5321

Course Administration: Consisting of 13 lectures, 6 home works (5 best scores per each student counts for the grade), one mid-term (in class) and one final exam (in class).
Grade Calculation: 40% homework, 30% midterm, 30% final exam
Grading: The TA will grade all home works, the instructor will grade all exams are graded and assign the final grades.
Standard of Homework Submissions: Expect to be written using a word processor (Word or Latex), individually written and submitted using the blackboard system. All homework are to be submitted on the due date, and later submissions may occur a penalty at the discretion of the TA or the instructor.
Course Text: Network Security (Private Communication in a PUBLIC World) by C. Kaufman, R. Perlman and M Speciner
Material for First 3 Lectures: Notes by Prof Fred. B Schneider at Cornell University:

Go to his web page http://www.cs.cornell.edu/fbs/fullist.html. Get contents under the heading Draft chapters for a textbook on cybersecurity (as yet, untitled)

Cryptography Material For Lecture 03/02: http://cseweb.ucsd.edu/~mihir/cse207

3. Tentative Course Syllabus

Note: The following tentative syllabus may change based on student background, interests and phase of the class. I may attempt to cover Chapter 8 from Cornell in one day.

Day of Class	Topic	Chapters from textbook and other reading material	Home work Out	Home work In
01/28	Introduction, Access Control	Chapter 1 and Chapter 7 from Fred Schneider (chptrIntro), (chptrDisc)	HW 1	
02/04	Access Control Mechanisms Foundational Results	Chapter 7 and Chapter 8 from Fred Schneider (chptrDisc)		
02/11	Probability and Number Theory Review	Chapter 7 textbook	HW 2	HW 1
02/18	Cryptography & Secret keys	Chapter 2 from the textbook		
02/25	Hashes and Message Digests	Chapters 3 and 4 from the textbook (Block Cyphers and Modes of Operation)	HW 3	HW 2
03/04	**Mid-term 1**	**Mid-term 1**		
03/18	Hash Algorithms	Chapters 5 from textbook		
03/25	Public Key Algorithms	Chapter 6 from textbook	HW 4	HW 3
04/1	Handshake & Strong Password Protocols	Chapter 11 and Chapter 12		
04/08	Kerberose	Chapter 13 and 14	HW 5	HW 4
04/15	IP Sec	Chapter 17 and 18		
04/22	SSL/TLS	Chapter 19	HW 6	HW 5
04/29	IDS Systems/Web Issue	Chapter 23 & 25		
05/06	File System Security	Unix, Windows and trusted storage		HW 6
05/14	**Final Exam**	**Final Exam**		