CSCE 522: Information Security Principles

1. Course number and name: CSCE 522: Information Security Principles

2. Credit: 3-hrs; Contact: 3 lectures of 50 minutes each or 2 lectures of 75 minutes each per week

3. Instructor: Fall 2010: Csilla Farkas

4. Text book: Charles P. Pfleeger and Shari Lawrence Pfleeger, *Security in Computing*, 4th Edition, Prentice Hall, 2006, ISBN-10: 0132390779.

5. Specific course information
   a. Catalog description: Threats to information resources and appropriate countermeasures. Cryptography, identification and authentication, access control models and mechanisms, multilevel database security, steganography, Internet security, and intrusion detection and prevention.
   b. Prerequisites: CSCE 311 or MGSC 596
   c. Required in CIS curricula

6. Specific goals for the course
   a. Specific outcomes of instruction:
      1. Identify common risks, threats, and countermeasures related to computing systems.
      2. Apply knowledge of computer security to personal computer use.
      3. Analyze computing situations with respect to security risks, threats, and countermeasures, including the tradeoffs between security and system functionality.
      4. Work with others to design and/or implement security measures.
   b. Relation of course outcomes to Student Outcomes: CE: see page 2; CS & CIS: see page 3

7. Topics covered and approximate weight (14 weeks, 3 hours/week, 42 hours total)
   1. Basic security concepts
   2. Cryptography
   3. Information security
   4. Statistical database security
   5. Access control
   6. Network and Internet security
   7. Program security
   8. Intrusion detection
   9. Fault tolerance and recovery
   10. Information warfare

11. Security administration

c.

Computer Engineering

Relation of Course Outcomes to EAC Student Outcomes*

Course Outcomes (CE)	Student Outcomes											
	(a) apply knowledge of mathematics, science, and engineering	(b) design and conduct experiments, … interpret data	(c) design a system, component, or process to meet desired needs …	(d) function on multidisciplinary teams	(e) identify, formulate, and solve engineering problems	(f) an understanding of professional and ethical responsibility	(g) communicate effectively	(h) the broad education to understand the impact of engineering solutions …	(i) a recognition of the need for, and an ability to engage in life-long learning	(j) a knowledge of contemporary issues	(k) use the techniques, skills, and modern engineering tools ….	(CE) demonstrate knowledge of discrete mathematics [CE]
Criteria	a	b	c	d	e	f	g	h	i	j	k	CE
1. Identify common risks, threats, and countermeasures related to computing systems.		2	2		3			1	1	3		
2. Apply knowledge of computer security to personal computer use.	3				1					1		
3. Analyze computing situations with respect to security risks, threats, and countermeasures, including the tradeoffs between security and system functionality.	3	2	3		3		1			2	2	1
4. Work with others to design and/or implement security measures.		3	3	1	3	2	1			3	3	

* 3 = major contributor, 2 = moderate contributor, 1 = minor contributor; blank if not related

d.

Computer Science & Computer Information Systems

Relation of Course Outcomes to CAC Student Outcomes*

Course Outcomes (CS & CIS)	Student Outcomes											
	All									CS		CIS
	(a) apply knowledge of computing and mathematics appropriate to the discipline	(b) analyze a problem, and identify and define the computing requirements …	c) design, implement, and evaluate a computer-based system, …	(d) function effectively on teams to accomplish a common goal	(e) An understanding of professional, ethical, legal, … responsibilities	(f) communicate effectively with a range of audiences	(g) analyze the local and global impact of computing on … society	(h) Recognition of the need for … continuing professional development	(i) current techniques, skills, and tools necessary for computing practice	(j) apply mathematical foundations, algorithmic principles, and CS theory …	(k) apply design and development principles	(j) An understand processes that support the information systems environment.
Criteria	a	b	c	d	e	f	g	h	i	j	k	j
1. Identify common risks, threats, and countermeasures related to computing systems.		3	2				2	1			2	2
2. Apply knowledge of computer security to personal computer use.	3	1					2					1
3. Analyze computing situations with respect to security risks, threats, and countermeasures, including the tradeoffs between security and system functionality.	3	3	3			1			2	1	3	3
4. Work with others to design and/or implement security measures.		3	3	3	2	1			3			3

* 3 = major contributor, 2 = moderate contributor, 1 = minor contributor; blank if not related