

Course Information Sheet

CSCI 4250

Computer Security

Brief Course Description (50-words or less)

Basic concepts of computer security and the theory and current practices of authentication, authorization, and privacy mechanisms in modern operating systems and networks.

Extended Course Description / Comments

This course is part of the BS-CS Teamwork Requirement; students In CSCI 4250 are required to work in teams of size greater than 2.

Use this section to put additional information that's relevant to whom this course is targeting

Pre-Requisites and/or Co-Requisites

CSCI 4730
Operating Systems

Or CSCI 4760
Computer Networks

Approved Textbooks

(if more than one listed, the textbook used is up to the instructor's discretion)

Author(s): Jon Erickson
Title: Hacking: The Art of Exploitation
Edition: 2
ISBN-13: 978-1593271442

Author(s): Charlie Kaufman, Radia Perlman, and Mike Speciner
Title: Network Security: Private Communication in a Public World
Edition: 2
ISBN-13: 978-0130460196

Specific Learning Outcomes (Performance Indicators)

These are a (non-exhaustive) list of specific, measurable outcomes, as they relate to course and program objectives.

This course presents the strengths and weakness of security mechanisms that are built into existing system and networks. The course will make students aware of the common programming mistakes that could lead to potential security compromises and help them avoid these situations. At the end of the semester, all students will be able to do the following:

1. Classify symmetric and asymmetric cryptography algorithms and explain the difference between them.
2. List the fundamental goals of computer and network security.
3. Explain the points of strength and weakness of different authentication and authorization mechanisms.
4. Give examples of common software vulnerabilities.
5. Explain and implement common computer security attack and/or defense techniques.
6. Explain the process of malware infection on computer system and networks.

Relationship Between Student Outcomes and Learning Outcomes

		<i>Student Outcomes</i>										
		a	b	c	d	e	f	g	h	i	j	k
<i>Learning Outcomes</i>	1			•		•				•		
	2					•				•		
	3									•		
	4					•		•				
	5			•		•				•		
	6					•		•				

Student Outcomes

- a. An ability to apply knowledge of computing and mathematics appropriate to the discipline.
- b. An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution.
- c. An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs.
- d. An ability to function effectively on teams to accomplish a common goal.
- e. An understanding of professional, ethical, legal, security and social issues and responsibilities.
- f. An ability to communicate effectively with a range of audiences.
- g. An ability to analyze the local and global impact of computing on individuals, organizations, and society.
- h. Recognition of the need for and an ability to engage in continuing professional development.
- i. An ability to use current techniques, skills, and tools necessary for computing practice.
- j. An ability to apply mathematical foundations, algorithmic principles, and computer science theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices.
- k. An ability to apply design and development principles in the construction of software systems of varying complexity.

Major Topics Covered
(Approximate Course Hours)

3 credit hours = 37.5 contact hours
4 credit hours = 50 contact hours

Note: Exams count as a major topic covered

Security Principle and Goals (3-hours)
Symmetric Cryptography (4-hours)
Public-key based Cryptography (4-hours)
Access Control (6-hours)
Secure Network Protocols (such as SSL/TLS, IPsec) (10-hours)
Application Security (such as Email and Web) (10-hours)
Security in Software Development (10-hours)
Trends in the Computer Security Arms Race (3-hours)

Assessment Plan for this Course

Each time this course is offered, the class is initially informed of the Course Outcomes listed in this document, and they are included in the syllabus. At the end of the semester, an anonymous survey is administered to the class where each student is asked to rate how well the outcome was achieved. The choices provided use a 5-point Likert scale containing the following options: Strongly agree, Agree, Neither agree or disagree, disagree, and strongly disagree. The results of the anonymous survey are tabulated and results returned to the instructor of the course.

The course instructor takes the results of the survey, combined with sample student responses to homework and final exam questions corresponding to course outcomes, and reports these results to the ABET committee. If necessary, the instructor also writes a recommendation to the ABET committee for better achieving the course outcomes the next time the course is offered.

How Data is Used to Assess Program Outcomes

Each course Learning Outcome, listed above, directly supports one or more of the Student Outcomes, as is listed in "Relationships between Learning Outcomes and Student Outcomes". For CSCI 4250, Student Outcomes (c), (e), (g), and (i) are supported.

**Course Master
Course History**

Dr. Kang Li
08/2005 Course Approval in CAPA
02/2012 Course Information Sheet Prepared
12/7/2012 Course added to BS-CS Teamwork Requirement block