The University of Georgia

Department of Computer Science

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	N/A
Pre-Requisites and/or Co-Requisites	CSCI 4730 Operating Systems Or CSCI 4760 Computer Networks
Required, Elective or Selected Elective	Selected Elective Course
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)	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

		Student Outcomes										
		a	b	c	d	e	f	g	h	i	j	k
Learning Outcomes				●		●				●		
						●				●		
										●		
						●		●				
				●		●				●		
	6					●		●				

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)

Course Master

Dr. Kang Li