

COURSE DESCRIPTION

Department and Course Number	CS 436	Course Coordinator	Warner
Course Title	Computer Security	Total Credits	3

Current Catalog Description

Study of computer security including assurance, authorization, authentication, key distribution, encryption, threats including phishing and key logging, and related distributed computing issues. Theory and practical applications.

Textbook *Introduction to Computer Security*. Dieter Gollman, Wiley Press. ISBN 0-470-86293-9, 2006.

Reference *Security Engineering: A Guide to Building Dependable Distributed Systems*. Ross Anderson. Wiley Press. ISBN 0-471-38922-6, 2001. (online at: <http://www.cl.cam.ac.uk/~rja14/book.html>)

Course Goals

Students who complete this course will learn the foundations of computer security, including major kinds of threats, key protocols and algorithms for encryption/decryption, and design principles for assurance. Key frameworks for integrity and confidentiality are part of the material presented. Practical connection of this knowledge to real systems is a further learning goal and an important component of this course, including but not limited practical aspects of to Kerberos, LDAP/Active Directory, and PKI/RSA/PGP/OpenPGP.

Prerequisites by Topic

Algorithms and Data Structures

Computer Organization and Assembly Language Programming

Major Topics Covered in the Course

- 1. Computer Security Fundamentals: Confidentiality, Integrity, Availability*
- 2. Concepts: Assurance, Threats, Trust*
- 3. Basics of cryptography, digital signatures, identity*
- 4. Policies and Mechanisms for Security*
- 5. Authentication, Authorization, Access Control*
- 6. Kinds of Security, Intrusions*
- 7. Covert channels, kinds of attack, highlights of network security*

Laboratory projects (specify number of weeks on each)

None

Estimate CSAB Category Content

	CORE	ADVANCED		CORE	ADVANCED
Data Structures	0	6	Computer Organization and Architecture	0	7
Algorithms Software Design	0	6	Concepts of Programming Languages	0	0

Oral and Written Communications

none

Social and Ethical Issues

Social and ethical issues are part and parcel of computer security, since many aspects involve unethical activities of attackers. These issues are interwoven into at least 20% of the lecture material.

Theoretical Content

Theory involving methodology for security, for secure protocols/algorithms, and evaluation of secure system designs comprise a significant component of this course, at least 50% of lecture hours.

Problem Analysis

Analysis of cryptographical algorithms and protocols is part of homework problems assigned.

Solution Design

Defining secure protocols, from protocol building blocks and concepts, for secure communication, is part of design activity in homework.