

CSCE 522: INFORMATION SECURITY PRINCIPLES

Catalog Course Description:

522—Information Security Principles. (3) (Prereq: CSCE 311 or MGSC 596) 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.

Prerequisite(s) By Topic:

Introduction to operating systems (CSE students)

Introduction to database management systems (non-CSE students)

Textbook(s) and Other Required Material:

Charles P. Pfleeger and Shari Lawrence Pfleeger, *Security in Computing*, 3rd edition, Pearson Prentice Hall, Upper Saddle River, NJ, 2003.

Computing Platform: Windows XP; UNIX

Course Objectives: {Assessment Methods Shown in Braces}

1. Identify common risks, threats, and countermeasures related to computing systems {tests, assignments}
2. Apply knowledge of computer security to personal computer use {tests, assignments}
3. Analyze computing situations with respect to security risks, threats, and countermeasures, including the tradeoffs between security and system functionality {tests, assignments, projects}
4. Work with others to design and/or implement security measures {projects}

Topics Covered:

1. Basic security concepts (3 hours)
2. Cryptography (6 hours)
3. Information security (2 hours)
4. Statistical database security (2 hours)
5. Access control (6 hours)
6. Network and Internet security (4 hours)
7. Program security (4 hours)
8. Intrusion detection (2 hours)
9. Fault tolerance and recovery (2 hours)
10. Information warfare (3 hours)
11. Security administration (5 hours)
12. Reviews, examinations, etc. (4 hours)

Laboratory Projects and Other Student Work:

Students work in teams to complete at least one substantial laboratory project involving the design, implementation, and/or evaluation of some aspect of a security system; an oral presentation is given on the project. In addition, written assignments and at least one exam (in addition to the final) are required.

Graduate students complete a more difficult project and are graded on a different scale from undergraduates.

Syllabus Flexibility: Medium

Relationship of Course to Program Outcomes:

The contribution of each course objective to meeting the program outcomes is indicated with the scale:

3 = major contributor, 2 = moderate contributor, 1 = minor contributor. Blank if not related.

Course Objectives	Program Outcomes										
	1. Logic & Math	2. Computing Fundamentals	3. Apply Computing Principles	4. Work on teams	5. Communicate Effectively	6. Liberal arts & Soc. Sciences	7. Basic Science and Lab Procedures	8. Learn New Tools & Processes	9. Employed upon Graduation	10. Application Area	11. Electronics and Digital Sys Design
1. Identify common risks, threats, and countermeasures related to computing systems	1	2	3	1	1	1		2	2		
2. Apply knowledge of computer security to personal computer use		2	3	1	1			3	2		
3. Analyze computing situations with respect to security risks, threats, and countermeasures, including the tradeoffs between security and system functionality	1	2	3	2	2	1	1	2	2		
4. Work with others to design and/or implement security measures			3	3	3	1		2	3		

Estimated Computing Category Content (Semester hours):

Area	Core	Advanced	Area	Core	Advanced
Algorithms		1	Data Structures		
Software Design		2	Programming Languages		
Computer Architecture					

Estimated Information Systems Category Content (Semester hours):

Area	Core	Advanced	Area	Core	Advanced
Hardware and Software			Networking and Telecommunications		1
Modern Programming Language			Analysis and Design		
Data Management		1	Role of IS in an Organization		
Quantitative Analysis			Information Systems Environment		1

Oral and Written Communication:

Both an oral and a written report are required for the course project.

Social and Ethical Issues:

A wide range of issues related to security and privacy

Theoretical Content:

Introduction to mathematical foundations of cryptography and access control.

Analysis and Design:

Design and evaluation of security systems and components

Class/Laboratory Schedule:

Lecture: 3 periods of 50 minutes or 2 periods of 75 minutes per week

Course Coordinator: Csilla Farkas

Acknowledgement of Funding Support:

Development of this course was supported in part by the National Science Foundation (NSF) under Grant No. IIS-0237782. The material presented here does not necessarily reflect the views of the National Science Foundation.

Modification and Approval History

Prepared June 2005 by Caroline Eastman based upon original course proposal and course information from Csilla Farkas