CSE 551 (Official)

CSE 551: Introduction to Information Security

Description

Introduction to security of digital information including: threats, regulations, risk management, attack detection and response, cryptography, forensics, and technical training and certification.

Level, Credits, Class Time Distribution, Prerequisites

Level	Credits	Class Time Distribution	Prerequisites
U	3	3 cl	314 or 321 or 502 or AMIS 531 or equivalent, and second writing course; or permission of instructor

Quarters Offered

- Wi

General Information, Exclusions, Cross-listings, etc.

Intended Learning Outcomes

- Master information security governance, and related legal and regulatory issues.
- Master understanding of external and internal information security threats to an organization.
- Be familiar with the structure of policies, standards and guidelines.
- Be familiar with information security awareness and a clear understanding of its importance.
- Be familiar with how threats to an organization are discovered, analyzed, and dealt with.

Texts and Other Course Materials

- *Principles of Information Security, Thomson/Course Technology, ISBN 0-619-06318-1, 2003* - Michael E. Whitman and Herbert J. Mattord
- *Security Architecture: Design, Deployment and Operations, McGraw-Hill Osborne Media; ISBN: 0072133856; 1st edition (July 30, 2001) (Optional)* - Christopher King, Ertem Osmanoglu, Curtis Dalton

Topics

Number of Hours	Topic
3	Primer: information security and network basics; information security and its role in an organization; legal and regulatory issues; government homeland security initiatives and how they impact business

	and individuals
3	Threats; internal threats: employees, contractors, third parties; external threats: criminals, corporate espionage, hackers, cyber warfare, cyber terrorism; psychology of computer criminals and info-terrorists and associated ethical issues
6	Governance, policies, standards, and guidelines; architecture; awareness
10	Risk management, vulnerability assessment and intrusion detection; malicious code protection; content filtering; internet DMZ and related components; incident response; application security
3	Cryptography; forensics
3	Information security directions; technical training and certifications; what's next
2	Review and exam

Representative Lab Assignments

- None

Grades

Homework assignments	15%
Paper and presentation	15%
Participation	10%
Midterm exam	20%
Final exam	40%

Relationship to ABET Criterion 3

a	b	c	d	e	f	g	h	i	j	k
*	*	*	*	*	**	*	*	*	**	*

Relationship to CSE Program Outcomes/Objectives

1a	1b	1c	2a	2b	2c	3a	3b	4a	4b	5a	5b	5c
*	*	*	*			**	**	*	*	*	*	*

Course Coordinator: Dong Xuan
Prepared by Bruce Weide
Last modified: Oct 3 2005 2:41PM