CSE 5473 (Approved): Network Security

Course Description

Security threats and services, elements of cryptography, protocols for security services, network and internet security, advanced security issues and technologies.

Prior Course Number: CSE 651
Transcript Abbreviation: Netw Security
Grading Plan: Letter Grade
Course Deliveries: Classroom
Course Levels: Undergrad, Graduate
Student Ranks: Senior, Masters, Doctoral
Course Offerings: Autumn, Spring
Flex Scheduled Course: Never
Course Frequency: Every Year
Course Length: 14 Week
Credits: 3.0
Repeatable: No
Time Distribution: 3.0 hr Lec
Expected out-of-class hours per week: 6.0
Graded Component: Lecture
Credit by Examination: No
Admission Condition: No
Off Campus: Never
Campus Locations: Columbus
Prerequisites and Co-requisites: CSE 3461 or CSE 5461 or CSE 677
Exclusions: Not open to students with credit for CSE 651
Cross-Listings:

The course is required for this unit's degrees, majors, and/or minors: No
The course is a GEC: No
The course is an elective (for this or other units) or is a service course for other units: Yes

Subject/CIP Code: 14.0901
Subsidy Level: Doctoral Course

Programs

Abbreviation	Description
BS CSE	BS Computer Science and Engineering
MS CSE	MS Computer Science and Engineering
PhD CSE	PhD Computer Science and Engineering

Course Goals

Be competent with some protocols for security services.
Be competent with network security threats and countermeasures.
Be familiar with fundamentals of cryptography.
Be familiar with network security designs using available secure solutions (such as PGP, SSL, IPSec, and firewalls).
Be familiar with advanced security issues and technologies (such as DDoS attack detection and containment, anonymous communications, and security properties testing, verification and design).

Be exposed to original research in network security.

Course Topics

Topic	Lec	Rec	Lab	Cli	IS	Sem	FE	Wor
Security threats and services	3.0							
Elements of cryptography: (1) Classic ciphers, modern ciphers, stream ciphers and block ciphers; (2) Secret key (symmetric): DES/AES and public key (asymmetric): RSA	10.0							
Protocols for security services: (1) Key distribution and management, (2) Data integrity and message authentication codes, (3) User authentication; (4) Non-repudiation and digital signatures	10.0							
Network and internet security: (1) Transport-level security, (2) Wireless network security, (3) Email security, (4) IP security	10.0							
Advanced security issues and technologies such as firewalls, intrusion detection, active worm defense, DDoS attacks and defense, anonymous communications, security in routing (OSPF and BGP), sensor network security	9.0							

Grades

Aspect	Percent
Homework assignments and lab exercises	35%
Midterm exam	35%
Research project	30%

Representative Textbooks and Other Course Materials

Title	Author
Cryptography and Network Security: Principles and Practice	William Stallings
Applied Cryptography (2nd Edition)	Paul Campbell, et al.
Network Security: Private Communication in a Public World	Charlie Kaufman, Radia Perlman and Mike Speciner

ABET-EAC Criterion 3 Outcomes

Course Contribution		College Outcome
***	a	An ability to apply knowledge of mathematics, science, and engineering.
***	b	An ability to design and conduct experiments, as well as to analyze and interpret data.
***	c	An ability to design a system, component, or process to meet desired needs.
***	d	An ability to function on multi-disciplinary teams.
***	e	An ability to identify, formulate, and solve engineering problems.
*	f	An understanding of professional and ethical responsibility.
*	g	An ability to communicate effectively.
*	h	The broad education necessary to understand the impact of engineering solutions in a global and societal context.
*	i	A recognition of the need for, and an ability to engage in life-long learning.
***	j	A knowledge of contemporary issues.

Course Contribution		College Outcome
***	k	An ability to use the techniques, skills, and modern engineering tools necessary for engineering practice.

BS CSE Program Outcomes

Course Contribution		Program Outcome
***	a	an ability to apply knowledge of computing, mathematics including discrete mathematics as well as probability and statistics, science, and engineering;
***	b	an ability to design and conduct experiments, as well as to analyze and interpret data;
***	c	an ability to design, implement, and evaluate a software or a software/hardware system, component, or process to meet desired needs within realistic constraints such as memory, runtime efficiency, as well as appropriate constraints related to economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability considerations;
***	d	an ability to function on multi-disciplinary teams;
***	e	an ability to identify, formulate, and solve engineering problems;
*	f	an understanding of professional, ethical, legal, security and social issues and responsibilities;
*	g	an ability to communicate effectively with a range of audiences;
*	h	an ability to analyze the local and global impact of computing on individuals, organizations, and society;
*	i	a recognition of the need for, and an ability to engage in life-long learning and continuing professional development;
***	j	a knowledge of contemporary issues;
***	k	an ability to use the techniques, skills, and modern engineering tools necessary for practice as a CSE professional;
***	l	an ability to analyze a problem, and identify and define the computing requirements appropriate to its solution;
**	m	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;
**	n	an ability to apply design and development principles in the construction of software systems of varying complexity.

Prepared by: Anish Arora