CSET 4850 Computer Network Security (4 semester credit hours)

CSET Elective
IT Elective

Current Catalog Description:

Theory and practice of network security. Topics include firewalls, Windows, UNIX and TCP/IP network security. Security auditing, attacks, viruses, intrusion detection and threat analysis will also be covered.

Textbooks:

Matt Bishop, *Introduction to Computer Security*, Addison-Wesley, November 5, 2004, ISBN 0-321-24744-2.

References:

Course web pages: http://cset.sp.utoledo.edu/~wsun/cset4850/

Related Program Outcomes (a, b, c, f, i and k):

CSET Program Outcomes are (a, b, c, f, i and k)
IT Program Outcomes are (a, b, c, f, and i)

Course Objectives:

After successful completion of this course, students will be able to:

- Understand secret key, message digest, and public key algorithms, and how each is used
- Understand and be able to use authentication and key agreement protocols.
- Identify attacks and efficiently block the attacks.
- Develop firewall based solutions against security threats, employ access control techniques to the existing computer platforms such as UNIX.
- Study a security related problem and recommend solutions.

Major Topics Covered in the Course

Topic	Lecture Hours
Introduction, Ethics and Expectation Fundamentals of network Security	3
Access control	1.5
Security Policies	6
Symmetric Key Cryptography	1.5
Public Key Cryptography	1.5
Key Management and Public Key Infrastructure (PKI)	1.5
Authentication	1.5
Security Design Principles	1.5
Confinement Problem	1.5
Auditing	1.5
Malicious Logic	3
Intrusion Detection	3
Network Security	4.5
System Security	3
Program Security	3
Advanced Research Topics	7.5
Total	45

Laboratory Projects:

	Laboratory/Project	
	Title	Major Tasks
LAB 1	Network and Service Configuration	Get familiar with VNetLab platform; figure out the topology of given virtual network using network tools; configure routing tables; setup dynamic services such as Web, SSH and NFS server.
LAB 2	Hide and Seek: a network discovery game.	Part I, one group prepares the network with a random set of services and dynamic traffic and then hands over to the other group for discovery; Part II, each group uses network tools such as nmap to discover the given unknown network.
LAB 3	Firewall configuration using iptables	Develop a set of iptable rules according to the given specifications.
Final Project	Each student will research on a specific security related topic of his/her interest, provide presentation and reports. Selected projects include study of spyware, smart grid security, log analysis, FPGA security, etc.	

Oral and Written Communications

Lab reports and final project report/presentation.

Social and Ethical Issues

Topics like legal background for regulation of the Internet, Fourth Amendment Law and electronic surveillance, fundamentals of privacy law will be cited and discussed in class and homework will be assigned.

Theoretical Content

Various levels of Cryptographic algorithms will be discussed in the class (refer to the content table).

- Classical Cryptosystems: Shift ciphers, Affine cipher, Vigenere Cipher, One-time pads linear feedback shift registers.
- Number Theory: Modular arithmetic, Modular exponentiation, Fermat and Euler theorem.
- Symmetric Encryption: A simplified DES-type algorithm, DES, Modes of operation.
- Public Key Cryptography: RSA algorithm, Primality testing, Factoring, Public Key Cryptosystems.
- Digital Signatures: RSA signatures, ElGamal signatures, Hash functions (MD5 and SHA).
- Key Establishment and Authentication Systems: Kerberos, Public Key Infrastructure, Password Systems and Unix Salt.

Problem Analysis

Analysis plays an important role in system security implementation. Analysis such as the nature of the attack, the security property of a given system is examined in the homework and lab projects.

Solution Design

Students will be presented various kinds of different security policies and mechanisms. Students need to develop solutions to meet their specific security requirements.

Course Coordinator:

Hong Wang (hong.wang2@utoledo.edu)
8-13-2007
Modified by Weiqing Sun (Weiqing.Sun@utoledo.edu)
02-24-2011

CSET	CSET Student Outcomes:	Course Outcomes	Assessment Methods
a	An ability to select and apply knowledge of computing and mathematics appropriate to the discipline. More specifically, 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.	Use contemporary encryption algorithms.	Evaluation of questions in quizzes and homework assignments associated with cryptography.
b	An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution.	Research interesting security problems.	Evaluation of final projects.
c	An ability to design, implement and evaluate a computer-based system, process, component, or program to meet desired needs. More specifically, an ability to apply design and development principles in the construction of software systems of varying complexity.	Solve practical security problems in a lab setting.	Evaluation of hands-on lab projects.
d	An ability to function effectively as a member or leader on technical teams to accomplish a common goal.		
e	An understanding of professional, ethical, legal, security and social issues and responsibilities including a respect for diversity.		
f	An ability to communicate effectively with a range of audiences using a range of modalities including written, oral and graphical.	Develop and deliver reasonable project reports and presentations.	Evaluation of students' project reports and presentations.
g	An ability to analyze the local and global impact of computing on individuals, organizations, and society.		
h	Recognition and understanding of the need for and an ability to engage in self-directed continuing professional development.		
i	An ability to select and apply current techniques, skills, and tools necessary for computing practice.	An understanding of the analytical and laboratory skills associated with computer and network security.	Evaluation of homework assignments, projects and quizzes.
j	An ability to conduct standard tests and measurements; to conduct, analyze, and interpret experiments; and to apply experimental results to improve processes.		
k	A commitment to quality, timeliness, and continuous improvement.	Submit projects on time and continuously improve their projects once design issues are identified.	Evaluate students' efforts in meeting deadline and improving their laboratory projects.

IT	IT Student Outcomes:	Course Outcomes	Assessment Methods
a	An ability to select and apply knowledge of computing and mathematics appropriate to the discipline. Specifically, an ability to use and apply current technical concepts and practices in the core information technologies. [IT-j]	Use contemporary encryption algorithms.	Evaluation of questions in quizzes and homework assignments associated with cryptography.
b	An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution.	Research interesting security problems.	Evaluation of final projects.
c	An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs. And, an ability to identify and analyze user needs and take them into account in the selection, creation, evaluation and administration of computer-based systems. [IT-k]	Solve practical security problems in a lab setting.	Evaluation of hands-on lab projects.
d	An ability to function effectively as a member or leader on technical teams to accomplish a common goal.		
e	An understanding of professional, ethical, legal, security and social issues and responsibilities including a respect for diversity.		
f	An ability to communicate effectively with a range of audiences using a range of modalities including written, oral and graphical.	Develop and deliver reasonable project reports and presentations.	Evaluation of students' project reports and presentations.
g	An ability to analyze the local and global impact of computing on individuals, organizations, and society.		
h	Recognition and understanding of the need for and an ability to engage in self-directed continuing professional development.		
i	An ability to select and apply current techniques, skills, and tools necessary for computing practice. And an ability to effectively integrate IT-based solutions into the user environment. [IT-l]	An understanding of the analytical and laboratory skills associated with computer and network security.	Evaluation of homework assignments, projects and quizzes.
j	An understanding of best practices and their application. [IT-m]		
k	An ability to assist in the creation of an effective project plan. [IT-n]		