

COURSE DESCRIPTION

Dept., Number	CSC 115	Course Title	Internet Security
Semester hours	3	Course Coordinator	Isaac Ghansah
		URL (if any):	http://gaia.ecs.csus.edu/~ghansahi/

Catalog Description

Study of Internet security problems and discussion of potential solutions: network vulnerabilities and attacks, secure communication and use of cryptography, Internet security protocols and tools to defend against network attacks, network intrusion detection, and wireless network security. Survey and use of software tools for network security. Prerequisite: At least a C- grade in CSC 114.

Textbook

Raymond Panko, Corporate Computer and Network Security, Prentice-Hall, 2004.

References

Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: Private Communication in a Public World, 2nd Ed., Prentice Hall, 2002.

Stuart McClure, Joel Scambray, and George Kurtz, Hacking Exposed: Network Security Secrets & Solutions, 5th Ed., Osborne-McGraw Hill, 2005.

William Stallings, Cryptography and Network Security: Principles and Practice, 3rd Ed., Prentice Hall, 2002.

William Stallings, Network Security Essentials, 2nd Ed., Prentice Hall, 2002.

Course Goals

1. To develop knowledge of contemporary risks in networks and attack procedures.
2. To understand Internet protocols in order to protect networks from attack.
3. To understand security protocols which protect networks from attack.
4. To develop understanding of how cryptography is used in Internet protocols for secure communication.
5. To develop proficiency in use of various software tools for Internet security.
6. To provide an overview of wireless network security.

Prerequisites by Topic

Thorough understanding of:

- Information Assurance and Security best practices.
- Threats, risks, and vulnerabilities to information systems; countermeasures available to address these threats.

Basic understanding of:

- Internet security.

- Host security.
- Tools for information security.
- Web client and server software.

Exposure to:

- Cyber Forensics.
- TCP/IP protocol suite.
- Career paths in information security.
- Ethical issues related to information security.
- Web programming (e.g. Javascript, XML, etc).

Major Topics Covered in the Course

1. Introduction to security (1 week).
Basic security concepts.
Threats, vulnerabilities, and attacks.
Confidentiality, authentication, message integrity, availability.
2. Review of computer networks and TCP/IP protocol suite (1 week).
Standards and layers.
Internet Protocol (IP) and Transmission Control Protocol (TCP).
User Datagram Protocol (UDP).
ICMP for supervisory information.
3. Secure communication (2 weeks).
Symmetric encryption.
Public key encryption.
Public key infrastructure (PKI).
Authentication.
Message digest, digital signature, digital certificates and standards.
Kerberos key exchange.
Encryption standards (DES, AES, RSA, etc.) and case studies.
4. Internet security (2.5 weeks).
SSL / TLS.
Secure shell, secure FTP.
Secure E-Mail (PGP).
IPsec, VPN.
Secure internet routing (BGP, OSPF).
Survey and demonstration of software tools for Internet security.
Web application security.
5. Network attacks (2.5 weeks).
Malicious programs (e.g., viruses, worms, Trojan horses).

Buffer overflow attack.
Hacking methods and software tools.
Denial-of-service attacks and distributed denial-of-service attacks.
IP spoofing and IP/attacks traceback.
Routing protocol attacks.
“Spam” email.
Steganography.
Windows and Unix vulnerabilities – case studies and software tools.

6. Protection of networks from attacks (2 weeks).
 - Firewalls.
 - Intrusion detection systems.
 - Network intrusion detection systems and tools such as *snort*.
 - Honeypot.
 - Anti-virus software.
 - Access control.
 - Trusted operating systems principles.
 - Auditing and monitoring examples.
7. Wireless / mobile network security (2 weeks).
 - Types of wireless networks.
 - Wireless network attacks and defenses.
 - Secure ad hoc network routing.
8. Students’ presentations (1 week).
9. Exams, reviews and evaluations (1 week).

Outcomes

Thorough understanding of:

- Network and Internet security threats.
- Network attacks – techniques and countermeasures.
- Cryptography-based protocols at multiple layers of the TCP/IP stack.

Basic understanding of:

- Wireless network security.
- Freeware and commercially available software tools for Internet security.

Exposure to:

- History of network attacks.
- Career paths in network security.
- Ethical issues related to network security.

Laboratory Projects

1. Use of software tools such as GNU Privacy Guard (GPG) to implement encryption/decryption.
2. Password cracking.
3. Network footprinting, scanning, and enumeration.
4. Configuring personal firewalls.
5. Sniffing network traffic.
6. Host hardening in Windows and Linux.
7. Use of software tools for network vulnerability assessment, packet crafting for attacks, network sniffing, and intrusion detection.

Estimated Curriculum Category Content (Semester hours)

<i>Area</i>	<i>Core</i>	<i>Advanced</i>	<i>Area</i>	<i>Core</i>	<i>Advanced</i>
Algorithms			Data Structures		
Software Design			Prog. Languages		
Comp. Arch.					

Oral and Written Communications

Students will be required to write a term paper on Internet Security issues.

Social and Ethical Issues

It will be made clear that students should not use their knowledge and skills with any malicious intent against the university network, any other networks, physical computing resources, or humans. Students will be required to sign an agreement to observe a set of legal and ethical guidelines.

Theoretical Content

The course uses cryptographic algorithms applied to secure communication and outlines a statistical basis for intrusion detection.

Problem Analysis

Each network attack method will be analyzed in a rigorous manner. Effectiveness of defensive measures shall be evaluated.

Solution Design

Students will learn how to discover vulnerabilities and how to develop techniques to protect the networks.