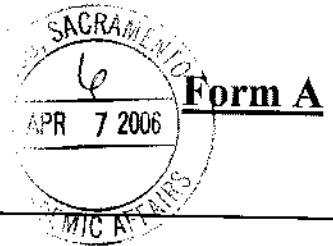




ECS

Academic Affairs - Course Proposal

CALIFORNIA STATE UNIVERSITY, SACRAMENTO



Academic Unit: Computer Science		Department Chair: Du Zhang	
Type of Course Proposal: New <input checked="" type="checkbox"/> Change <input type="checkbox"/> Deletion <input type="checkbox"/>		Date: March 9, 2006	
Does this course fulfill a requirement for single-subject or multiple subject credential students? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>		For Catalog Copy: Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	CCE: Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
		Semester Effective: Fall <input checked="" type="checkbox"/> Spring <input type="checkbox"/> 2006	
Prefix & No. CSC 115	Title: Internet Security	Units: 3	
Change to:			
Prefix & No.	Title:	Units:	

JUSTIFICATION:

This course is part of the proposed Minor in Information Security and Computer Forensics, which is intended for students in Criminal Justice and related fields. Information Assurance and Security is an area of emerging significance; the proposed minor is intended to educate future professionals in computer and telecommunications crime investigation and evidence processing. Additionally, Computer Science hopes to reverse its present negative trend in enrollment by taking this interdisciplinary approach.

NEW COURSE DESCRIPTION: (Not to exceed 80 words, and language should conform to catalog copy.)

See <http://www.csus.edu/aca/univmanual/crspsl.htm> - Guidelines for Catalog Course Description

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.

Note:

Prerequisite: CSC 114

Corequisite:

CAN (California Articulation Number):

Graded: Letter Credit/No Credit **Instructor Approval?** Yes No

Course Classification: 04 **Title for SIS+ (not more than 25 characters)**
INTERNET SECURITY

Cross Listed? Yes No **If yes, with what course:**

How Many Times Can This Course be Taken for Credit? Once

ECS

FOR NEW COURSE PROPOSALS OR SUBSTANTIVE CHANGES ONLY:

Description of the Expected Learning Outcomes: Describe outcomes using the following format: "Students will be able to: 1), 2), etc." See the example at <http://www.csus.edu/acaf/example.htm>

Students will gain:

A thorough understanding of:

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

A basic understanding of:

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

Exposure to:

1. History of network attacks
2. Career paths in network security
3. Ethical issues related to network security

**Attach a list of the required/recommended course readings and activities [Note: it is understood that these are updated and modified as needed by the instructor(s).] This attachment should be forwarded only to your Dean's office, not Academic Affairs.

Assessment Strategies: A description of the assessment strategies (e.g., portfolios, examinations, performances, pre- and post-tests, conferences with students, student papers) which will be used by the instructor to determine the extent to which students have achieved the learning outcomes noted above:

Examinations, lab projects, term paper

For whom is this course being developed?

Majors in the Dept ___ Majors of other Depts Minors in the Dept ___ General Education ___ Other ___

Is this course required in a degree program (major, minor, graduate degree, certificate)? Yes No ___

If yes, identify program(s): **Minor in Information Security and Computer Forensics**

Does the proposed change or addition cause a significant increase in the use of College or University resources (lab room, computer facilities, faculty, etc.)? Yes ___ No

If yes, attach a description of resources needed and verify that resources are available.

Indicate which department or programs will be affected by the proposed course (if any). _____

The Department Chair's signature below indicates that affected programs have been sent a copy of this proposal form.

Approvals: If proposed change, new course or deletion is approved, sign and date below. If not approved, forward without signing to the next reviewing authority, and attach an explanatory memorandum to the original copy.

Signatures:

	Date
Department Chair:	3/9/2006
College Dean or Associate Dean:	04-06-06
CPSP (for school personnel courses ONLY)	
Associate Vice President and Dean for Academic Programs	

Distribution: Academic Affairs (original), Department Chair and College Dean. Dean's office to send original after approval to Jerri McAtee, at zip 6016. An electronic copy must also be sent to mcaateeji@csus.edu.

New Course Proposal

CSC 115 – Internet Security

By Isaac Ghansah and Ju-Yeon Jo

Internet Security is an emerging field of computer and information technology with a concentration on security issues pertinent to the Internet such as network and protocol vulnerabilities, network attacks and defenses, and secure protocols. Internet Security is increasingly critical due to the growth in malicious and criminal activities on the Internet. Currently there is a shortage of network security experts trained to fight these malicious activities. This course is designed to increase awareness of dangerous network security issues, identify security problems, and learn to prevent or minimize those problems. As a result, the course will contribute to an increase in trained professionals in network security. This course covers vulnerabilities in communication protocols, how attackers exploit those vulnerabilities in protocols or network configurations, and how to use countermeasures to defend against attacks.

COURSE DESCRIPTION

Department and Course Number: CSC 115

Course Coordinator: Isaac Ghansah

Course Title: Internet Security

Total Credits: 3

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: CSC 114

Textbook: R. Panko, *Corporate Computer and Network Security*, Prentice Hall, 2004

References

- Charlie Kaufman, Radia Perlman, Mike Speciner, *Network Security: Private Communication in a Public World*, 2nd Ed., Prentice Hall, 2002
- McClure, Scambray, and Kurtz, *Hacking Exposed (Network Security Secrets & Solutions)*, 5th Ed., Osborne-McGraw Hill, 2005
- William Stallings, *Network Security Essentials*, 2nd Ed., Prentice Hall, 2002
- William Stallings, *Cryptography and Network Security: Principles and Practice*, 3rd Ed., Prentice Hall, 2002

Course Goals

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

Prerequisites by Topic

Thorough understanding of:

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

Basic understanding of:

1. Internet security
2. Host security
3. Tools for information security
4. Web client and server software

Exposure to:

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

Major Topics Covered in the Course

- Introduction to security (1 week)
 - Basic security concepts
 - Threats, vulnerabilities, and attacks
 - Confidentiality, authentication, message integrity, availability
- 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
- 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
- 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
- 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

- 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
- Wireless / mobile network security (2 weeks)
 - Types of wireless networks
 - Wireless network attacks and defenses
 - Secure ad hoc network routing
- Students' presentations (1 week)
- Exams, reviews and evaluations (1 week)

Outcomes

Thorough understanding of:

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

Basic understanding of:

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

Exposure to:

1. History of network attacks
2. Career paths in network security
3. 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 CSAB Category Content

	CORE	ADVANCED		CORE	ADVANCED
Data Structures	_____	_____	Computer Org & Architecture	_____	_____
Algorithms	_____	_____			
Software Design	_____	_____	Concepts of Programming Languages	_____	_____

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.

2/24/06