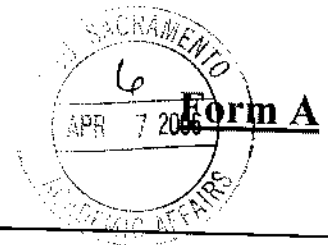


ECS

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 114	Title: Fundamentals of Information Assurance & 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/acaf/univmanual/crspsl.htm> - Guidelines for Catalog Course Description

Topics include the security principle of success, architecture and models, business continuity planning, cryptography, application development security, access control, operating systems security, database security, introduction to computer forensics, web security, Internet security protocols, and security management. Course includes projects involving practical computer security tools.

Note:

Prerequisite: CSC 010, CSC 080

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)**
FNDMNTLS INFO ASSUR & SEC

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

A basic understanding of:

1. Internet/web security
2. Host security
3. Tools for information security

Exposure to:

1. Cyber forensics
2. TCP/IP protocol suite
3. Career paths in information security
4. Ethical issues related to information security
5. Policy and administration of site 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 X Minors in the Dept ___ General Education ___ Other ___

Is this course required in a degree program (major, minor, graduate degree, certificate)? Yes X 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 X


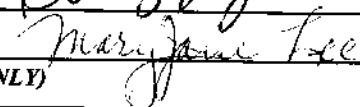
If yes, attach a description of resources needed and verify that resources are available.

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 mcateeji@csus.edu.

New Course Proposal

CSC 114 – Fundamentals of Information Assurance & Security

By Isaac Ghansah

This document comprises a proposal for a new course to be part of the Minor in the Computer Science Department titled Information Security and Computer Forensics. This proposed course represents an introduction to a number of key topics related to the field of information assurance and security, as well as legal issues involved in computer systems security.

COURSE DESCRIPTION

Department and Course Number: CSC 114

Course Coordinator: Isaac Ghansah

Course Title: Fundamentals of Information Assurance and Security

Total Credits: 3

Catalog Description: Topics include security principle of success, architecture and models, business continuity planning, cryptography, application development security, access control, operating systems security, database security, introduction to computer forensics, web security, Internet security protocols, and security management. Course includes projects involving practical computer security tools. Prerequisite: CSC 010, CSC 080

Textbook: M. Jerkow and J. Breithaupt, *Information Security Principles and Practices*, Prentice Hall, 2006

References

- C. Easton, *Computer Security Fundamentals*, Prentice Hall, 2006
- Cliff Stoll, *The Cuckoo's Egg*, Pocket Books, 1990
- C. Pfleeger and S. Pfleeger, *Security in Computing*, 3rd Ed., Prentice Hall, 2003

Course Goals

- To develop knowledge of information security and assurance best practices.
- To develop understanding of the importance of securing information efficiently, the threats, risks, and vulnerabilities to information, and the controls available to address these threats.
- To study management practices and proficiency in the use of selected software tools for securing systems.

Prerequisites by Topic

Thorough understanding of:

1. Webpage design and layout including HTML tables and forms

Basic understanding of:

1. Fundamental properties of algorithms and programming
2. How to use Windows and/or Linux operating systems

Exposure to:

1. Elementary working knowledge of a commonly used applications programming language
2. Internet protocols such as HTTP and TCP/IP

Major Topics Covered in the Course

- Introduction to Information Assurance and Security, threats to information, importance of information security (3 hours)
- Risk assessment and security management (3 hours)
- How contemporary computer systems are organized (1 hour)
- Access control techniques and models including 2-factor authentication, social engineering, and biometrics (3 hours)
- Telecommunications, network security and network fundamentals: logical and physical topologies, introduction to TCP/IP, and hardware architecture (6 hours)
- Cryptography including Advanced Encryption Standard (3 hours)
- Security architecture and models (3 hours)
- Operations security (3 hours)
- Applications, system development, and database security (3 hours)
- Business continuity planning – disaster recovery planning (3 hours)
- Law, investigation, ethics, U.S. Patriot Act, Digital Millennium Copyright Act (DMCA), and recent rulings (3 hours)
- Introduction to host-based perimeter detection and network-based perimeter detection, physical security (3 hours)
- Methods of attacks, Honeypots and Honeynets, firewalls and perimeters, trap and trace tools such as Echelon (3 hours)
- Government information assurance regulations (3 hours)
- System security engineering, future threats and countermeasures (2 hours)

Outcomes

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/web security
2. Host security
3. Tools for information security

Exposure to:

1. Cyber forensics
2. TCP/IP protocol suite
3. Career paths in information security
4. Ethical issues related to information security
5. Policy and administration of site security

Laboratory Projects

- Windows and Linux/Unix vulnerability analysis
- Internet research and reporting on security topics such as biometrics, computer system laws, certifications, security advisories, etc.
- Linux and Windows security tools and techniques
- Security reporting, monitoring and auditing
- File system security and cryptography
- Use of hands-on hacking tools such as nmap
- Firewalls, personal and commercial grade

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 information security issues.

Social and Ethical Issues

It will be made clear that the 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 covers an overview of cryptographic algorithms and applies cryptography to secure communication applications. Access control principles are also covered.

Problem Analysis

A given configured system will be analyzed in a rigorous manner to determine to what extent it is secure.

Solution Design

Students will learn how to discover security weaknesses and mitigate the identified weakness in the system.

2/24/06