### Course Change Proposal

**Form A**

<table>
<thead>
<tr>
<th>Academic Group (College):</th>
<th>Academic Organization (Department):</th>
<th>Date:</th>
<th>Submitted by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering and Computer Science</td>
<td>Computer Science</td>
<td>January 18, 2011</td>
<td>Issac Ghansah</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of Course Proposal:</th>
<th>Department Chair: Cui Zhang</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>New _ X_ Change <em>X</em> Deletion <em>X</em></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Does this course fulfill a requirement for single-subject or multiple subject credential students?</th>
<th>For Catalog Copy: Yes <em>X</em> No <em>X</em></th>
<th>Semester Effective:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes <em>X</em> No <em>X</em></td>
<td></td>
<td>Fall <em>X</em> Spring <em>X</em>, 2011</td>
</tr>
</tbody>
</table>

| This course replaces experimental course Subject Area (prefix) and Catalog Nbr (course number): |
|---------------------------------|-----------------------------|
| If changing an existing course, should new version be considered a repeat of the original version? If so, the same Course ID will be maintained. If not, a new Course ID will be assigned. Note: In PeopleSoft terminology, the Course ID is the unique system identifier, not the Catalog Nbr. | Yes _X_ No _X_ |

| Change from: |
|--------------------------|-----------------------------|---|
| Subject Area (prefix) & Catalog Nbr (course no.): | Title: | Units: |
| CSC 115 | Internet Security | 3 |

| Change to: |
|--------------------------|-----------------------------|---|
| Subject Area (prefix) & Catalog Nbr (course no.): | Title: | Units: |
| same | same | same |

### JUSTIFICATION:

Change in prerequisite only. Current catalog prerequisite is CSC 114. The new catalog prerequisite is CSC 1 and one of the following: CSC 8 or CSC 8S or CSC 80; or instructor’s permission. The current prerequisites are too restrictive. Experience has shown that no material from CSC 114 is needed in CSC 115. This change will allow non-major students more flexibility in taking this service course.

### NEW COURSE DESCRIPTION:

(Not to exceed 80 words, and language should conform to catalog copy. See http://www.csus.edu/umanual/acad.htm - Guidelines for Catalog Course Description)

N/A

### Note:

- **Prerequisite:** CSC 1 and one of the following: CSC 8 or CSC 8S or CSC 80; or instructor’s permission
- **Enforced at Registration:** Yes _X_ No _X_
- **Corequisite:**
- **Instructor Approval Required?** Yes _X_ No _X_
- **Graded:** Letter _X_ Credit/No Credit _X_  
- **Course Classification** (e.g., lecture, lab, seminar, discussion): Title for CMS (not more than 30 characters)
- **Cross Listed?** Yes _X_ No _X_  
- **How Many Times Can This Course be Taken for Credit?** _X_
- **Can the course be taken for Credit more than once during the same term?** Yes _X_ No _X_
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

**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:

**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):

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.**

**Accessibility:** Following course approval, and prior to the start of the semester in which the new or revised course will be taught for the first time, an accessibility checklist [available at http://www.csus.edu/accessibility/checklist.html] shall be completed and submitted to the appropriate Dean’s office. An accessible syllabus shall also be made available online, preferably prior to the start of that semester’s open registration period.

**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:**

<table>
<thead>
<tr>
<th>Department Chair:</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2/1/2011</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>College Dean or Associate Dean:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2/1/11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CPSP (for school personnel courses ONLY)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1/1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Associate Vice President and Dean for Academic Programs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Distribution: Academic Affairs (original), Department Chair and College Dean. Dean’s office to send original after approval to Academic Affairs, at mail zip 6016. An electronic copy must also be sent.

5/20/2010
COURSE DESCRIPTION

Dept., Number: CSC 115  
Semester hours: 3  
Course Title: Internet Security  
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: CSC 1 and CSC 8 or CSC 8S or CSC 80 or Instructor's permission.

Textbook


References


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.
course Description for CSC 115
April 25, 2008
Page 2 of 4

- 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)

<table>
<thead>
<tr>
<th>Area</th>
<th>Core</th>
<th>Advanced</th>
<th>Area</th>
<th>Core</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithms</td>
<td></td>
<td></td>
<td>Data Structures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Design</td>
<td></td>
<td></td>
<td>Prog. Languages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp. Arch.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

/aa