California State University San Marcos • **COURSE CHANGE(S)** • **FORM C-2**

ORIGINATOR'S SECTION:		
1. College: ☐ CHABSS ☐ CoBA ☐ CoEHHS ☒ CSM	**Desired Term and Year of Implementation (e.g., Fall 2008):** Spring 2017	
2. Current Course abbreviation and Number: **MCS 510 (Security in Computer Networks)**		

TYPE OF CHANGE(S). Check √ all that apply.

Course Number Change	☐	**Delete Prerequisite**	☐	**Other Prerequisite Change**	☐
Course Title Change	☐	**Add Corequisite**	☐	**Grading Method Change**	☐
Unit Value Change	☐	**Delete Corequisite**	☐	**Mode of Instruction Change (C/S Number)**	☐
Description Change	☒	**Add Consent for Enrollment**	☐	**Consider for G.E.** If yes, also fill out appropriate GE form.	☐
Add Prerequisite	☐	**Delete Consent for Enrollment**	☐	**Cross-list**	☐

Information in this section– both current and new – is required only for items checked (√) above.

CURRENT INFORMATION:	**NEW INFORMATION:**
	Course abbreviation and Number:
3. Title:	**Title:** ***(Titles using jargon, slang, copyrighted names, trade names, or any non-essential punctuation may not be used.)***
4. Abbreviated Title for Banner ***(no more than 25 characters):***	**Abbreviated Title for PeopleSoft:** ***(no more than 25 characters, including spaces)***
5. Number of Units:	**Number of Units:**
6. Catalog Description: Theoretical and practical aspects of security in computer networks, including wired and wireless networks. Topics will include: the basic concepts of communication networks and an introduction to TCP/IP architecture, the fundamental techniques and protocols used to insure secure communications, the common attacks and defenses, and the vulnerability assessment of network systems. Students will learn various aspects of security in computer networks, and the best techniques and tools against network attacks. *Prerequisite: MATH 503.*	**Catalog Description:** ***(Not to exceed 80 words; language should conform to catalog copy. Please consult the catalog for models of style and format; include all necessary information regarding consent for enrollment, pre- and/or corequisites, repeated enrollment, crosslisting, as detailed below. Such information does <u>not</u> count toward the 80-word limit.)*** Theoretical and practical aspects of security in computer networks, including wired and wireless networks. Topics will include: the fundamental techniques and protocols used to insure secure communications, the common attacks and defenses, and the vulnerability assessment of network systems. Students will learn to apply and operationalize network security technologies and techniques. *Prerequisite: MATH 503.*

7. Mode of Instruction* (*See pages 17-23 at http://www.calstate.edu/cim/data-elem-dic/APDB-Transaction-DED-SectionV.pdf for definitions of the Course Classification Numbers)*

Type of Instruction	**Number of CrediUnits**	**Instructional Mode (Course Classification Number)**
Lecture		
Activity		
Lab		

Type of Instruction	**Number of Credit Units**	**Instructional Mode (Course Classification Number)**
Lecture		
Activity		
Lab		

8. Grading Method:*	**Grading Method:***
☐ Normal (N) *(Allows Letter Grade +/-, and Credit/No Credit)*	☐ Normal (N) *(Allows Letter Grade +/-, and Credit/No Credit)*
☐ Normal Plus Report-in-Progress (NP) *(Allows Letter Grade +/-, Credit/No Credit, and Report-in-Progress)*	☐ Normal Plus Report-in-Progress (NP) *(Allows Letter Grade +/-, Credit/No Credit, and Report-in-Progress)*
☐ Credit/No Credit Only (C)	☐ Credit/No Credit Only (C)
☐ Credit/No Credit or Report-in-Progress Only (CP))	☐ Credit/No Credit or Report-in-Progress Only (CP))

*If Originator is uncertain of this entry, please consult with Program Director/Chair.

CURRENT INFORMATION:	NEW INFORMATION:
9. If the NP or CP grading system was selected, please explain the need for this grade option.	
10. Course Requires Consent for Enrollment? ☐ Yes ☐ No ☐ Faculty ☐ Credential Analyst ☐ Dean ☐ Program/Department/Director/Chair	**Course Requires Consent for Enrollment?** ☐ Yes ☐ No ☐ Faculty ☐ Credential Analyst ☐ Dean ☐ Program/Department/Director/Chair
11. Course Can be Taken for Credit More than Once? ☐ Yes ☐ No If yes, how many times (including first offering)	**Course Can be Taken for Credit More than Once?** ☐ Yes ☐ No If yes, how many times (including first offering)
12. Is Course Cross Listed: ☐ Yes ☐ No If yes, indicate which course	**Is Course Cross-listed?** ☐ Yes ☐ No If yes, indicate which course and check "yes" in item #17 below.
13. Prerequisite(s):	**Prerequisite(s):**
14. Corequisite(s):	**Corequisite(s):**
15. Documentation attached: ☐ Syllabus ☒ Detailed Course Outline	

PROGRAM DIRECTOR/CHAIR - COLLEGE CURRICULUM COMMITTEE SECTION:
(Mandatory information – all items in this section must be completed.)

16. Does this course fulfill a requirement for any major (i.e. core course or elective for a major, majors in other departments, minors in other departments? ☒ **Yes** ☐ **No**
If yes, please specify:
Master in Cybersecurity – a required course

17. Does this course change impact other discipline(s)? ***(If there is any uncertainty as to whether a particular discipline is affected, check "yes" and obtain signature.)*** Check "yes" if the course is cross-listed. ☐ **Yes** ☒ **No**
If yes, obtain signature(s). Any objections should be stated in writing and attached to this form.

_____ Discipline _____ Signature _____ Date _____Support _____Oppose

_____ Discipline _____ Signature _____ Date _____Support _____Oppose

18. Reason(s) for changing this course:
The basic concepts in the current description are already part of the admission requirement. And it was lacking the most important application and operationalization part.

SIGNATURES : (COLLEGE LEVEL) :

Rika Yoshii 3-23-16
1. Originator (Please Print) Date

2. Program Director/Chair 5-3-16 Date

3. College Curriculum Committee 5/2/2016 Date

4. College Dean (or Designee) 5/3/16 Date

(UNIVERSITY LEVEL)

5. UCC Committee Chair Date

6. Vice President for Academic Affairs (or Designee) Date

7. President (or Designee) Date

RECEIVED
MAY 03 2016
BY:

Course Outline: MCS 510 Security in Computer Networks (3)

Course Description:
Theoretical and practical aspects of security in computer networks, including wired and wireless networks. Topics will include: the fundamental techniques and protocols used to insure secure communications, the common attacks and defenses, and the vulnerability assessment of network systems. Students will learn to apply and operationalize network security technologies and techniques.

Prerequisite:
MATH 503 Cryptography

3 unit lecture only

Textbooks:
·Information Security: Principles and Practice, 2nd edition, Mark Stamp, Wiley 2011.
• Network Security, Firewalls, and VPNs, 2nd edition, J. Michael Stewart, Jones & Bartlett Learning 2014

List of Topics:
- ·Security of TCP/IP protocols
- ·Network security attacks and defenses
- ·Web security
- ·Internet worms, viruses, spyware
- ·Spam, phishing, botnets, denial of service
- ·TCP/IP and DNS security
- ·Firewalls and intrusion detection systems
- ·VPN fundamentals, management, and technology concerns
- ·Wireless security
- How to operationalize security decisions and techniques

Student learning outcomes:
Upon successful completion of the course, students will be knowledgeable of the practical elements of networks security and related design. They will be able to:
1. Recognize design and analysis of network security architectures, protocols, and services in both wired and wireless networks.
2. Identify network security standards, their functionality and limitations.
3. Identify network attacks and analyze defense techniques against them.
4. Apply and operationalize network security technologies and techniques.
5. Communicate their analyses and decisions effectively.

Typical Evaluation Components:
Homework Assignments (15%): To be completed individually.
Programming Projects (15%): In groups of two or less.
Midterm (30%): Covers security protocols and software.
Final Exam (40%): Covers all material. Emphasis on the parts after the midterm.