College of San Mateo
Official Course Outline

1. **COURSE ID:** CIS 479 **TITLE:** Computer and Network Security
   Units: 3.0 units **Hours/Semester:** 48.0-54.0 Lecture hours; and 96.0-108.0 Homework hours
   Method of Grading: Grade Option (Letter Grade or Pass/No Pass)
   Corequisite: Completion or concurrent enrollment in CIS 151.

2. **COURSE DESIGNATION:**
   Degree Credit
   Transfer credit: CSU; UC

3. **COURSE DESCRIPTIONS:**
   Catalog Description:
   This course covers the concepts of vulnerabilities, threats, attacks, security measures and mechanisms in computer networks. The course will introduce the fundamental concepts of security technology and the applications of these technologies. Topics include fundamental cryptography, authentication, encryption, digital signatures, digital certificates and network security protocols such as IP Sec, SSL.

4. **STUDENT LEARNING OUTCOME(S) (SLO'S):**
   Upon successful completion of this course, a student will meet the following outcomes:
   1. Evaluate the impact of a security design
   2. Design remote services and DNS/SNMP security
   3. Assess the network security risks and provide a plan for secure communication channels
   4. Describe the fundamentals of cryptography
   5. Describe the popular computer and network security mechanisms and protocols
   6. Analyze, implement and maintain security requirements and mechanisms in various computer systems and networks

5. **SPECIFIC INSTRUCTIONAL OBJECTIVES:**
   Upon successful completion of this course, a student will be able to:
   1. Analyze a client's company model and processes
   2. Analyze a client's management model
   3. Design an appropriate security solution for client organization
   4. Evaluate the impact of a security design
   5. Design remote services and DNS/SNMP security
   6. Assess the network security risks and provide a plan for secure communication channels

6. **COURSE CONTENT:**
   Lecture Content:
   - Overview of cryptography
   - Modern ciphers , symmetric and asymmetric ciphers (DES, AES, RSA)
   - Public key systems, digital signatures
   - Authentication, digital certificates, hash and MAC
   - Key management, Diffi-Hellman key exchange
   - Basic web security model
   - HTTPS: goals and pitfalls
   - Web application security
   - Session management and user authentication
   - Content Security Policies (CSP), Web workers, and extensions
   - Security issues in Internet protocols: TCP, DNS, and routing
   - Network security protocols: IP Sec, SSL, SSH,
   - Network defense tools: Firewalls, VPNs, Intrusion Detection, and filters
   - Concepts of vulnerabilities, threats, attacks, security measures and mechanisms in both computer systems and networks
   - Unwanted traffic: denial of service attacks
   - Control hijacking attacks: exploits
   - Control hijacking attacks: defenses
   - Principle of least privilege, access control, and operating systems security

- Dealing with legacy code: sandboxing and isolation
- Exploitation techniques and fuzzing
- Tools for improving system security
- Mobile platform security models: Android and iOS
- Mobile threats and malware

7. **REPRESENTATIVE METHODS OF INSTRUCTION:**
   Typical methods of instruction may include:
   A. Lecture
   B. Directed Study
   C. Discussion
   D. Guest Speakers
   E. Work Experience
   F. Other (Specify): Short in-class projects

8. **REPRESENTATIVE ASSIGNMENTS**
   Representative assignments in this course may include, but are not limited to the following:
   Writing Assignments:
   Written assignments include commentaries on situational events proposed at the end of chapters. These force the student to absorb and assimilate the material in a trouble shooting scenario.
   Reading Assignments:
   Students read a chapter from the text each week. Chapters are 30-35 pages of technical material. Students are expected to complete the accompanying hands-on exercises associated with each chapter.

9. **REPRESENTATIVE METHODS OF EVALUATION**
   Representative methods of evaluation may include:
   A. Class Participation
   B. Class Performance
   C. Class Work
   D. Exams/Tests
   E. Homework
   F. Papers
   G. Projects
   H. Quizzes
   I. Individual assignments and course projects.

10. **REPRESENTATIVE TEXT(S):**
    Possible textbooks include:
    A. Stalling, William. *Network Security Essentials Application and Standards*, Sixth Edition ed. Pearson, 2017
    B. Katz Jonathan, Lindel Yehuda. *Model Cryptography*, Second Edition ed. CRC Press, 2015
    C. Smart Nigel. *Cryptography Made Simple*, ed. Springer, 2016

Origination Date: January 2019
Curriculum Committee Approval Date: April 2019
Effective Term: Fall 2020
Course Originator: Kamran Eftekhari