Master Course Syllabus
School of Engineering and Computer Science
Washington State University Vancouver
CS 427
Computer Security
3 Semester Hours
(3 lecture hours)

Catalog Description
Computer security concepts, models and mechanisms; encryption technology, formal models, policy and ethical implications.

Prerequisite Courses
- CS 166 with a C or better
- CS 360 with a C or better
- Senior Standing

Prerequisite Topics
- Abstract Algebra, Probability Theory
- Proficient in at least one high level programming language.
- Implementation of common data structures for lists, trees, and graphs
- Use of Linux or Windows environment for coding, compilation, debugging and testing

Measured Course Outcomes
Students taking this course will:
1. Identify which cryptographic services, such as confidentiality, authentication, integrity, etc., are appropriate to best build security into computer systems. (Contributes to performance criterion 1-c.)
2. Implement advanced cryptographic algorithms. (Contributes to performance criterion 6-c.)

Required Textbooks
Cryptography and Network Security (Principles and Practices), William Stallings, Prentice Hall.

Reference Material

Major Topics Covered in the Course
1. An examination of conventional encryption algorithms and related mathematical theory, as well as design principles.
2. An examination of cryptographic services like confidentiality, authentication, integrity and non-repudiation, and cryptographic mechanisms like public-key encryption algorithms, block ciphers including AES, hash functions, digital signatures and key distribution protocols and mechanisms including public-key certificates.
3. An overview of network security tools and applications including Transport level security (SSL/TSL, HTTPS and SSH), IP Security (IPSEC) and Web security.

4. Examine system-level security issues, including the threat of and countermeasures for intruders and use of firewalls and trusted systems.

Projects

Programming projects are to be developed by students individually.

Programming Project Area	Weeks
Software Design	1
Programming	4

Projects include implementing at least one symmetric encryption-decryption algorithm and one asymmetric (public/private) key algorithm.

Design, Implementation and Analysis

Students use mathematical techniques to analyze computational problems associated with encryption and decryption. A variety of cryptographic protocols, and the extent to which they provide security, are also extensively analyzed on homework exercises and exam questions. The instructor performs analysis of representative problems in class.

Additionally, programming assignments require students to analyze software requirements, in order to successfully implement the projects.

CS2013

This course provides coverage of CS2013 knowledge areas. Values listed are minimum course hours dedicated to the topic, percentages indicate the fraction of CS2013 knowledge area topics covered (acceptable values are: <25%, 25-75%, >75%, or 100%).

Area	Tier 1	Tier 2	Elective
IAS/Foundational Concepts in Security	4 (>75%)		N
IAS/Threats and Attacks		1 (<25%)	N
IAS/Network Security		4 (>75%)	N
IAS/Cryptography		3 (100%)	3 (>75%) Y

Course Coordinator:	Paul Bonamy
Last Updated:	September 23, 2020
Syllabus Version Number:	2.2