Computer Science Department
cs.salemstate.edu

CSC435 Computer and Network Security **4 cr.**

Instructor: TBA **Office:** location **Phone:** (978) 542-extension
email: TBA@salemstate.edu **Office Hours:** days and times

Section	Time	Room	Final Exam
nn	days and times	location	date and time
Lnn	days and times	location	

Catalog description:

This course offers a detailed analysis of security problems and the corresponding methods used to create practical, working solutions to problems in computer and network security. Topics include secure software design, architecture of security products, and organization and administration of information security solutions, secure operating systems, secure communication protocols, and secure software. Through laboratory exercises students will develop expertise in the use of contemporary security tools for protecting computers and computer networks. Three lecture hours and three hours of scheduled laboratory per week.

Prerequisites: CSC 315A. Not open to students who have received credit for ITE 315.

Goals:

Upon completion of the course, a student should be able to do the following:

CG01: explain the concept of cryptography and demonstrate knowledge of algorithms and the design principles of software used in cryptography;
CG02: demonstrate understanding of and proficiency in the principles of secure programming;
CG03: analyze software from a security perspective and demonstrate proficiency in using secure coding practices;
CG04: demonstrate understanding of security deficiencies of TCP/IP protocols and the ability to analyze protocol-level attacks that exploit these vulnerabilities;
CG05: apply methods and procedures used in security assessment and security testing.

Objectives:

Upon successful completion of the course, a student will have demonstrated the ability to:
CO01: use encryption techniques and algorithms in the design of security protocols;
CO02: use programming tools and proper coding procedures to build secure software;
CO03: apply proper security assessment methods and use appropriate security testing tools in order to evaluate vulnerabilities in software and suggest methods of fixing security related flaws;
CO04: identify the security deficiencies of TCP/IP protocols and analyze protocol-level attacks that exploit these vulnerabilities;
CO05: apply security principles and use appropriate computer security products in systems design.

Student Outcome (SO) vs. Course Objectives matrix

SO	CO01	CO02	CO03	CO04	CO05
SO-1	□	□	□	□	□
SO-2	□	□	□	□	□
SO-3			□	□	□
SO-4		□	□		□
SO-5					
SO-6	□	□	□	□	□

Notes:

SO-1: Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.

SO-2: Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.

SO-3: Communicate effectively in a variety of professional contexts.

SO-4: Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.

SO-5: Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.

SO-6: Apply computer science theory and software development fundamentals to produce computing-based solutions.

Course topics:

- Review of necessary concepts
  - Programming networking applications — PL1 (2)
  - TCP/IP family of protocols and the Internet — NC2 (2)
  - Computer architecture and Operating Systems — AR9(1), OS2 (1)
- Problems and Solutions in Computer and Network Security
  - Security vulnerabilities, attackers and their attacks — NC3(3), AR6 (3)
  - Security models, identification mechanisms, access control — OS7(2)
  - Secure operating systems — NC3(1),OS2(1),OS7(1)
- Concepts and mathematics of encryption — AL9 (2)
  - Introduction into cryptography
  - Symmetric and public key encryption
  - Digital signatures
  - Hashing algorithms and use of hashing in encryption
- Principles, guidelines, and practices of secure programming — SE5(1),SE6(2),SE8(2)
  - Concepts and principles of secure programming
  - Discussion of main issues in secure programming (Authentication, Authorization, Data validation, Session management, Logging, Error handling, Code Quality)
  - Processes and technical controls necessary to develop secure software.
  - Secure programming
- Network Security — NC3 (8)
  - Architecture and implementation of firewalls
  - Vulnerabilities of TCP/IP protocols and techniques that exploit them
  - Analysis of IPsec design, architecture, and implementation.
  - The Internet key exchange protocols
  - IPsec deployment issues and deployment scenarios
- Web security — NC4(1),NC5(1),NC8(1),IM1(1)
  - Web client-server data and control flow
  - Basic ideas in WWW security
  - Introduction into Secure Socket Layer (SSL) and SSL programming
  - Web servers and Web security management
- Security of IT infrastructures — NC3(2), NC8(2), NC9(2)
  - Architecture of Public Key Infrastructure (PKI)
  - PKI Protocols and Standards, PKI-enabled services, and certificate management
  - Anatomy of a Virtual Private Network
  - Architecture and organization of IT infrastructure defense products (demilitarize zones, intrusion detection systems, firewalls, network address translation, secure DNS, secure authentication, etc.)
  - Evaluating and testing network and system security

Organization of the course

The course consists of lectures, labs, homework assignments, quizzes, and two exams – a midterm and a final. Lectures are accompanied by live demonstration of security products and solutions. Labs consist of hands-on exercises that include examination of security vulnerabilities and usage of different techniques to exploit them and secure systems from them. Homework assignments, consist of doing research on different aspects of computer and network security. Individual and group projects include analyzing and solving security-related tasks.

Labs and Homework: There will be a collection of computer security lab and homework assignments. Assignments will be defined through a set of tasks that cover material learned during the course. All labs will be conducted within an environment specifically created for this course.

Term Project: there will a term project that includes writing secure software according to the principles learned during the course.

Exams and quizzes: There will be a midterm examination, quizzes, and a comprehensive written two-hour final examination.

Grading: Final grades will be determined using the following approximate weights:

- Labs and Homework 40%
- Term Project 15%
- Exams and Quizzes 45%

Course Objective / Assessment Mechanism matrix

	Labs and Homework	Projects	Exams & Quizzes
CO01	✓		✓
CO02	✓	✓	✓
CO03	✓	✓	✓
CO04	✓		✓
CO05		✓	✓

Bibliography:

Bishop, Matt. **Computer Security. Second Edition.** Addison-Wesley Professional, 2018.

Du, W. **Computer Security: A Hands-on Approach. Second Edition.** Wenliang Du, 2019.

Garfinkel, Simson; Spafford, Gene; Schwartz, Alan. **Practical UNIX and Internet Security. Third Edition.** O'Reilly, 2011.

Gollman, Dieter. **Computer Security**. **Third Edition.** Wiley, 2011.

Goodrich, M; Tamassia, R. **Introduction to Computer Security.** Pearson, 2010.

Grembi, Jason. **Secure Software Development: A Security Programmer's Guide.** Delmar Cengage Learning, 2008.

Palmer, Michael. **Guide to Operating System Security.** Course Technology, 2009.

Stallings, W; Brown, L. **Computer Security: Principles and Practice (4th Edition).** Pearson, 2017.

Stallings, W. **Cryptography and Network Security: Principles and Practice (7th Edition).** Pearson, 2016.

Whitman, Michael *et al*.**. Guide to Firewalls and Network Security. Second Edition.** Course Technology, 2009.

Whitman, Michael E.; Mattord, Herbert J. **Principles of Information Security. Sixth Edition.** Cengage Learning, 2017.

Tools and Web resources

SEED Labs: http://www.cis.syr.edu/~wedu/seed/labs.html

OverTheWire: http://overthewire.org/wargames/

An illustrated guide to IPsec: http://www.unixwiz.net/techtips/iguide-ipsec.html

Secure Programming for Linux and Unix: http://www.dwheeler.com/secure-programs/

O'Reilly Secure programming cookbook for C and C++ (online book)

Secure programming: http://www.freebsd.org/doc/en/books/developers-handbook/secure.html

Utility for network exploration: http://nmap.org/

Network security lectures: http://www.cis.ufl.edu/~nemo/security/

Backtrack remote penetration toolset: www.remote-exploit.org

An illustrated guide to IPsec: http://www.unixwiz.net/techtips/iguide-ipsec.html

Academic Integrity Statement:

"Salem State University assumes that all students come to the University with serious educational intent and expects them to be mature, responsible individuals who will exhibit high standards of honesty and personal conduct in their academic life. All forms of academic dishonesty are considered to be serious offences against the University community. The University will apply sanctions when student conduct interferes with the University primary responsibility of ensuring its educational objectives." Consult the University catalog for further details on Academic Integrity Regulations and, in particular, the University definition of academic dishonesty.

The Academic Integrity Policy and Regulations can be found in the University Catalog and on the University website (https://catalog.salemstate.edu/content.php?catoid=38&navoid=8211#Academic_Integrity). The formal regulations are extensive and detailed - familiarize yourself with them if you have not previously done so. A concise summary of and direct quote from the regulations: "Materials (written or otherwise) submitted to fulfill academic requirements must represent a student's own efforts". *Submission of other's work as one's own without proper attribution is in direct violation of the University's Policy* and will be dealt with according to the University's formal Procedures. *Copying without attribution is considered cheating in an academic environment - simply put,* ***don't do it!***

University-Declared Critical Emergency Statement:

In the event of a university-declared emergency, Salem State University reserves the right to alter this course plan. Students should refer to www.salemstate.edu for further information and updates. The course attendance policy stays in effect until there is a university-declared critical emergency.

In the event of an emergency, please refer to the alternative educational plans for this course, which will be distributed via the class listserv. Students should review the plans and act accordingly. Any required material that may be necessary will have been previously distributed to students electronically or will be made available as needed via email and email attachments.

Equal Access Statement:

"Salem State University is committed to providing equal access to the educational experience for all students in compliance with Section 504 of The Rehabilitation Act and The Americans with Disabilities Act and to providing all reasonable academic accommodations, aids and adjustments. **Any student who has a documented disability requiring an accommodation, aid or adjustment should speak with the instructor immediately.** Students with Disabilities who have not previously done so should provide documentation to and schedule an appointment with the Office for Students with Disabilities and obtain appropriate services."

Note: This syllabus represents the intended structure of the course for the semester. If changes are necessary, students will be notified in writing and via all regular class communication mechanisms.

.