Computer Science Department
cs.salemstate.edu

CSC435 Computer and Network Security Engineering **3 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 in IT infrastructures. The course uses an in-depth approach to analysis of 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.

Prerequisites: CSC 315A; CSC 279 strongly recommended.

Goals:

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

CG01: clearly explain the concept of cryptography and demonstrate knowledge of algorithms and the design principles of software used in cryptography;
CG02: demonstrate understanding of guidelines and proficiency in following the principles of secure programming;
CG03: analyze software from a security prospective 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:

CO01: worked with multiple encryption techniques and algorithms used in security protocols and products;
CO02: used programming tools and proper coding procedures to build secure software;
CO03: applied proper security assessment methods and used appropriate security testing tools in order to evaluate vulnerabilities in software and suggest methods of fixing security-related flaws;
CO04: demonstrated knowledge of the security deficiencies of TCP/IP protocols and analyzed protocol-level attacks that exploit these vulnerabilities;
CO05: learned design and implementation of software products employed to protect data and computer systems in IT environments;

Course Objective / Assessment Mechanism matrix

Program Objective (condensed form)	CO01	CO02	CO03	CO04	CO05
PO-A: apply knowledge of computing and math	✓	✓	✓	✓	✓
PO-B: analyze a problem and define its computing requirements	✓	✓	✓	✓	✓
PO-C: design, implement and evaluate applications		✓	✓		✓
PO-D: function effectively in teams to accomplish a common goal					

Program Objective (condensed form)	CO01	CO02	CO03	CO04	CO05
PO-E: professional, ethical, and social responsibilities			✓		✓
PO-F: communicate effectively with a range of audiences				✓	
PO-G: local and global impact of computing on people and society			✓		✓
PO-H: need for continuing professional development		✓			✓
PO-I: use current techniques, skills, and tools	✓	✓	✓		✓
PO-J: apply theory and principles to model and design systems	✓	✓	✓	✓	
PO-K: apply design and development principles in constructing software		✓			
note - full statements of the **P**rogram **O**utcomes (objectives) for the Computer Science Major can be found in the document *Computer Science Major Program Educational Objectives and Program Outcomes* on the Assessment page of the Computer Science Major (cs.salemstate.edu)					

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 in C and Java security platform (J2SE)
- 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. Weekly labs consist of hands-on exercises that include examination of security software and usage of different security tools. Homework assignments, given weekly, consist of doing research on different aspects of computer and network security. Individual and group projects include analyzing and solving security-related tasks.

Assignments: There will be 4 home assignments that include code analysis of security software products. (including code analysis) and projects that cover principles and rules of creating secure software presented during the course.

Projects: there will be two programming projects that include writing secure software according to the principles learned during the course.

Labs: There will be one security lab each week. Each lab will be defined through a set of actions and results that cover material learned during the week. All labs will be conducted within an environment specifically created for this course.

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

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

- Laboratory exercises 10%
- Home assignments 10%
- Quizzes 20%
- Projects 20%
- Midterm exam 20%
- Final exam 20%

Course Objective / Assessment Mechanism matrix

	Lab assignments	Homework assignments	Quizzes	Projects	Midterm exam	Final Exam
CO01			✓		✓	✓
CO02	✓	✓	✓	✓	✓	✓
CO03		✓		✓	✓	✓
CO04	✓		✓		✓	✓
CO05			✓	✓	✓	✓

Bibliography:

Doraswamy, N; Harkins, D. IPsec. **The New Security Standard for the Internet.** Prentice Hall, 2003.

Frankel, Sheila. **Demystifying the IPsec Puzzle).** Artech House, 2001.

Garfinkel, Simson; Spafford, Gene; Schwartz, Alan. **Practical UNIX and Internet Security. Third Edition.** O'Reilly, 2003.

Gollman, Dieter. **Computer Security**. Wiley, 2006.

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

McGraw, Gary. **Building Secure Software: How to Avoid Security Problems the Right Way**. Addison-Wesley Professional Computing Series, 2001.

Mel, H. X; Baker, Doris. **Cryptography Decrypted. Fifth Edition.** Addison-Wesley Professional, 2001.

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

Spafford, Gene; Garfunkel, Simson; Schwartz, Alan. **Secure Programming Techniques.** O'Reilly, 2003.

Viega, John; Messier, Matt. **Secure Programming Cookbook for C and C++: Recipes for Cryptography, Authentication, Input Validation & More.** O'Reilly Media, 2003

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

Whitman, Michael. **Principles of Information Security.** Cengage Learning, 2009.

Tools and Web resources

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 (http://catalog.salemstate.edu/content.php?catoid=13&navoid=1295#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,* ***do not 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 standing class communication protocols. 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/or Internet access.

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 email.