Computer Science Department
cs.salemstate.edu

ITE315 Information Security **4 cr.**

Catalog description:

The course covers a unified view of information security that examines the closely related areas of information security, software security, networks, web security, and forensics using a common set of underlying security principles. Students will get an understanding of how to model secure environments and how to implement these starting from standalone computers, operating systems, and then going towards distributed networks and web. Each of the security areas is examined in sufficient detail for students to understand the complexity of modern threats and the corresponding sophistication of the software and hardware that is designed to counter these threats. Three lecture hours and three hours of scheduled laboratory per week.

Prerequisites: ITE310

Course Narrative

Security and information assurance have risen sharply in importance in recent years. Since protection is only as good as the weakest point in the system, security and assurance present particular challenges in IT, where the scope of concern encompasses the total system [1].

The emphasis of this course is on presenting a thorough understanding of fundamentals of security, policies, operational issues, vulnerabilities, security models, mechanisms, and countermeasures in order to create a secure IT infrastructure. Security is important at various layers under the umbrella of information security. These layers include security for standalone computers, operating systems, software programs, networks, web systems, and databases. Security is a major component of any IT infrastructure. It thus becomes important to understand the principles of securing IT environments and networks. IT professionals need to understand the underlying principles that make a secure environment.

While security considerations are important to any computing professional, they become even more important for IT graduates [1]. This course goes into details of various security attacks and threats as well as security mechanisms and countermeasures.

Goals:

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

G1: understand various terminologies, concepts, and protocols associated with securing information systems.
G2: identify basic issues, problems, and solutions in designing and building information systems and technologies taking into consideration security vulnerabilities of its separate components and of the computing environment as a whole;
G3: describe all elements (software, hardware, organizational structures) used in creating information

security solutions and discuss the methods used to protect them against external attacks;

G4: describe rules, regulations, legal issues, and necessary administrative measures required to build a secure computing environment;

Course Objectives:

Upon successful completion of the course, a student will have demonstrated the ability to:

O1: apply correct technical terminology when analyzing requirements, describing the main issues, and designing solutions for information security;

O2: identify all necessary components of information security systems and explain methods and technologies that are used in designing these systems and demonstrate application of these techniques in practical exercises;

O3: analyze and apply assessment techniques that allow objective evaluation of the characteristics and vulnerabilities of IT environment, and to develop skills in using these techniques to design a practical solution based on the requirements of an organization or customer;

O4: utilize knowledge and understanding of standards used in the creation of secure systems;

O5: analyze customer's requirements and specifications, formulate specifications for a secure environment (design blueprints, component specification, policies and procedures, etc.) and communicate (verbally and in writing) clearly and concisely these requirements to system managers, administrators, business users, etc.;

O6: understand the legal, ethical, and professional issues in information security and be able to perform risk management.

Program Objective / Course Objective matrix (For ABET Accreditation Purposes)

(The following Matrix maps the Program Objectives for Information Technology Program outlined by Accreditation Board of Engineering Technology (ABET) with the Course Objectives. The check marks below the course objective represent that those course objectives accomplish specific program objectives set forth by ABET. The program objectives that have a * in front of them means that that course does not address those program objectives.)

Program Objective	**O1**	**O2**	**O3**	**O4**	**O5**	**O6**
PO-A: An ability to apply knowledge of computing and mathematics appropriate to the program's student outcomes and to the discipline.	✓	✓	✓	✓	✓	✓
PO-B: An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution.				✓	✓	✓
PO-C: An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs.		✓	✓	✓	✓	✓
PO-D: An ability to function effectively on teams to accomplish a common goal.		✓	✓			✓
PO-E: An understanding of professional, ethical, legal, security and social issues and responsibilities.	✓	✓			✓	✓
PO-F: An ability to communicate effectively with a range of audiences.	✓				✓	✓

Program Objective	O1	O2	O3	O4	O5	O6
PO-G: An ability to analyze the local and global impact of computing on individuals, organizations, and society.	✓	✓			✓	✓
***PO-H:** Recognition of the need for and an ability to engage in continuing professional development.						
PO-I: An ability to use current techniques, skills, and tools necessary for computing practice.	✓	✓	✓			
PO-J: An ability to use and apply current technical concepts and practices in the core information technologies.	✓	✓	✓	✓	✓	✓
PO-K: An ability to identify and analyze user needs and take them into account in the selection, creation, evaluation and administration of computer-based systems.	✓	✓			✓	✓
PO-L: An ability to effectively integrate IT-based solutions into the user environment.		✓	✓			✓
PO-M: An understanding of best practices and standards and their application.					✓	✓
PO-N: An ability to assist in the creation of an effective project plan.					✓	✓

Course topics:

- Information Security Overview IAS1(2), IAS11(1)
  - What Is Security?
  - History of Security
  - Key Information Security Concepts
    - data security, storage security, computer security, network security, enterprise security, global security
  - Modeling Security environments
    - Layered Security architecture (from standalone computer to distributed information systems)
    - Access control model (users, employees, administration, developers, etc.)
    - Asset protection model (confidentiality, integrity, availability, access control)
    - Effect of Security on characteristics of computing environment (accessibility, reliability, performance, etc.)
    - Security management model (secure environment design, administration, policies and procedures, etc.)

- Threats and Types of Attacks, Risk Analysis IAS1(1), IAS3(0.5), IAS10(1)
  - Threats and Vulnerabilities (computers, networks, people, organizations)
  - Attacks (participants, tools, mechanisms) IAS5(2)
    - Hackers (classification, motivations, activities)
    - Types of attacks (classification of methods and mechanisms – what assets are attacked and how attacks are perpetrated)
    - What is attacked and why (computers, communication pathways, data storage, information processing centers, individuals, etc.)
    - Software tools used to administer attacks
    - Social engineering

- Creating a secure information environment IAS4(4)
  - Principles of designing a secure environment (from a personal network to enterprise-wide security)
  - Policies and Procedures (formal modeling and examples)
  - Technical measures (intranets, extranets, honeypots, security perimeter, etc.)
  - Administrative measures (user education, access control, definition of disaster recovery policies, specification of security testing procedures, etc.)
  - Mechanisms and tools of Secure environment testing
  - Administration of security (who are the players and who is responsible - participants, responsibilities, relations, reporting structure)
  - Disaster recovery planning and managing

- Information Security Technology IAS6(2), IAS8(1), IAS9(1)

  - Authentication, Authorization, and Access Control IAS2(2), IAS3(0.5)
    - Classification of authentication mechanisms (Usernames and Passwords, Certificate-Based, Biometrics, etc.)
    - Authorization and access control
    - Monitoring access control

  - Data Security IAS2(2.5), IAS5(1), IAS3(0.5),
    - Securing Data
    - Approaches to Securing Data
      - Databases, Applications, Networks, Computers, Storage
    - Cryptography
      - Fundamentals of Cryptography
      - Symmetric-Key algorithm
      - Public (asymmetric) Key algorithm
      - Public Key Infrastructures
      - Certificates

  - Standalone computer security IAS3(0.5), PT1(1.5), IAS2(1)
    - Specifics of OS (Windows, Unix, PDAs)
    - User access control
    - Resource protection methods
    - User authorization database and access control matrix

  - Software Security Practices IAS2(0.5), IPT5(5)
    - Software Security (standards and models)
    - Countermeasures

  - Malicious software (viruses, worms, trojans, rootkits, etc.) and countermeasures IAS2(1)

  - Network Security NET4(2), IAS2(1.5), IAS3(1)
    - Communication channel security (wire-based and wireless) Firewalls

        - Intrusion Detection and Prevention
        - VPNs (architecture and management)
        - Attacks (methods and tools) Classification
            - Probing (methods and tools)
            - Active (DOS, intrusion, impersonation, etc.)
            - Impersonation, playback, modification, etc.
            - Others – classify
    - Website security WS5(2)
        - Secure website principles (what must be secure)
        - Website-specific attack methods and tools

    - Forensics IAS7(2)
        - Legal systems
        - Digital forensics and its relationship to other forensic disciplines
        - Rules of evidence
        - Search and seizure
        - Digital evidence
        - Media analysis

    - Scanning and Analysis Tools: The following tools can be introduced in lecture/labs as and when required, as well as used to set up security based labs, Port Scanners, Firewall Analysis Tools, Operating System Detection Tools, Vulnerability Scanners, Packet Sniffers, Wireless Security Tools

Student Experiences

Organization of the course

The course consists of lectures, labs, homework assignments, quizzes, and two exams – a midterm and a final. Lectures include exercises that may consist of:

- Discussions of the material presented during lectures
- Analysis of security threats and writing of reports that offer solutions used to mitigate these threats
- Usage of tools available to IT professionals to analyze information and examine security threats.

Group discussion time and group presentations that will be conducted as part of the scheduled laboratory sessions are an integral component of the course, serving to reinforce the concepts and techniques presented during lectures.

Assignments:

Homework assignments include analysis of security components and design of solutions for security-related tasks, as well as exercises in using security tools. Assignments require students to use information given during the lectures and in textbooks. Regular writing assignments include but are not limited to:

- analysis and evaluation of methodologies used in building secure networked environments;
- proposals to solve different security problems formulated by the instructor;

Specific requirements for each assignment will be stated when the assignment is distributed.

Labs:

Weekly labs consist of hands-on exercises that include:

- Analyzing different information security issues, threats, attacks, vulnerabilities, and implementation using information security tools and writing reports
- Using security-related tools to test network security defenses

Quizzes, Tests, and Examinations: There will be quizzes, a midterm, and a cumulative final.

Grading: Final grades will be determined on the basis of the following approximate weights:

- Laboratory exercises 25%
- Homework assignments 25%
- Quizzes 20%
- Midterm exam 15%
- Final exam 15%

Course Objective / Assessment Mechanism matrix

	Lab assignments	Homework assignment	Quizzes	Midterm exam	Final Exam
O1	✓	✓	✓	✓	✓
O2		✓	✓	✓	✓
O3	✓	✓		✓	✓
O4	✓	✓	✓		
O5	✓	✓			
O6	✓	✓			

Bibliography:

- C.P. Pfleeger, S.L. Pfleeger, Security in Computing, Fifth Edition, McGraw-Hill, ISBN-13: 978-0134085043, 2015.
- Whitman, Mattord, Principles of Information Security, Fifth Edition, Cengage, ISBN-13: 9781285448367, 2015.
- Peter Kim, The Hacker Playbook 2: Practical Guide To Penetration Testing, CreateSpace, ISBN-13: 978-1512214567, 2015
- Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 5th Edition, ISBN-13: 978-1305093911, 2014.
- Mark Rhodes-Ousley, Information Security: The Complete Reference, Second Edition, McGraw-Hill, ISBN-13: 9780071784351, 2013.
- J. Andress. The Basics of Information Security. First edition. Syngress, 2011.
- Michael E. Whitman, Herbert J. Mattord, Hands-On Information Security Lab Manual, 3rd Edition, ISBN-13: 978-1435441569, 2010.
- C. W. Axelrod, J. L. Bayuk, D. Schutzer. Enterprise Information Security and Privacy. First Edition. Artech House, 2009.
- M. Whitman, R.D. Austin, G. Holden. Guide to Firewalls and Network Security. Second Edition. Course Technology, 2009.
- Miller, Gregg, Security Administrator Street smarts. A real world guide to COMPTIA Security+ skills. Sybex, ISBN-13: 978-1118061169, 2009.

- Michael Gregg. Build your own security lab. A field guide for network testing. Wiley, ISBN: 978-0-470-17986-4, 2008.

References

1. Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programs in Information Technology, Association for Computing Machinery (ACM).