



# College of Business

Department of Computer Science and Information Systems

## MURRAY STATE UNIVERSITY

### COURSE SYLLABUS

TSM615 (Spring 2010)

Information System Security

---

---

**DEPARTMENT:** Computer Science and Information Systems

**COURSE NUMBER:** TSM 615

**CREDIT HOURS:** 3

- I. **TITLE:** Information System Security.
- II. **CATALOG DESCRIPTION:** Graduate-level study of modern computer, network, and information systems security. This course presents systems oriented approaches to network defense, malicious software, and data encryption. Topics include: network intrusion prevention and detection; incident response; worms; viruses; Trojan horses; public key encryption; message authentication; and privacy issues. Throughout the presentation of security issues, discussion will focus on the cost of security to business and society at large.
- III. **PURPOSE:** Establish a clear understanding of potential threats to modern computer, network, and information systems, the defense mechanisms available, and the cost of adequate security.
- IV. **COURSE OBJECTIVES:** To provide the graduate level computer information system student an understanding of the technology involved in the modern threats to computers, networks, and information systems, and the systems oriented approaches to protecting against those threats. At the conclusion of the course, students should be able to recognize and document threats to computers, networks, and information systems, and prescribe appropriate defenses and responses.
- V. **CONTENT OUTLINE**
  - A. Overview of Information Systems Security and Vulnerabilities
    - a. The Value of Information
    - b. Computer Availability and Data Consistency
  - B. Privacy and Assurance
    - a. Cryptographic Tools
    - b. Authentication
    - c. Access Control
  - C. Database Security
  - D. Malicious Software
  - E. Denial of Service
  - F. Intrusion Prevention and Detection

- G. Firewalls
- H. Trusted Computing
- I. Buffer Overflow
- J. Software Security
- K. Security Audit
- L. Windows and Linux Security
- M. Student Presentations and Case Studies on Information Security

**VI. INSTRUCTIONAL ACTIVITIES** Lecture, discussion, and individual research. There will be weekly reading assignments and individual or group projects.

**VII. FIELD, CLINICAL, AND/OR LABORATORY EXPERIENCES:** Students will work with threat and counter measure technology. Each student will select, research, and report on a modern threat to computer, network, or information system security; the potential impact and cost of the threat; and a technological approach or product addressing this threat. Topics must be approved by the instructor. Students will prepare and submit a paper on their approved topic, and will prepare and make presentations to the class on their research.

**VIII. RESOURCES:** Web-Page references: Students in the on-line section must have: **high-speed internet access; web-cam and headset.** For all students: Microsoft Office software (or ability to read and create Office compatible documents).

<http://estudy.murraystate.edu/webapps/portal/frameset.jsp> – MSU Blackboard

**IX. GRADING PROCEDURES:**

Grading Scale: **92**-100% A  
80-**91**% B  
70-79% C  
60-69% D  
Below 60% E

Students will be graded on participation, presentations, papers, and examinations.

1. Tests (probably 3) – 60%.
2. Paper and presentations on selected information security topic – 25%.
3. Other Assignments, Participation, Quiz's – 15%
4. Grievance and Appeals Policy: <http://www.murraystate.edu/cbpa/PDF/Appeals.pdf>.

**X. ATTENDANCE POLICY:** This course will adhere to the policy published in the current MSU Bulletin. This is a combined on-campus and online class. There will be weekly on-campus lectures/discussions which will be broadcast to the web through Blackboard and Elluminate. Each student is expected to participate to the maximum extent possible.

**XI. ACADEMIC HONESTY POLICY:** Automated tools will be used to check papers and assignments for plagiarism. The Murray State University College of Business (MSU CoB) Academic Honesty Policy is viewable online at: <http://www.murraystate.edu/cbpa/PDF/Honesty.pdf>. Cheating, plagiarism, submitting

another person's material as one's own, or doing work for another person for academic credit are all impermissible. This includes the use of unauthorized books, notebooks, people, or other sources in order to secure or give help during an examination, the unauthorized copying of examinations, assignments, reports, or term papers, laboratory reports, drawings or the presentation of unacknowledged material as if it were the student's own work. Disciplinary action may result in no credit for an assignment or exam and/or failure of the course. All instances of academic dishonesty will receive appropriate punitive action from the instructor of this course and the names of the students involved will be reported to the Dean in all instances. The MSU CoB Ethics policy is viewable online at: <http://www.murraystate.edu/cbpa/PDF/Ethics.pdf>

**XII. TEXT AND REFERENCES:** Computer Security Principles and Practices, Willam Stallings, Lawrie Brown, Prentice Hall ISBN: 978-0-13-600424-0.

**XIII. PREREQUISITES:** Graduate Student Status.

**XIV. STATEMENT OF AFFIRMATIVE ACTION AND EQUAL OPPORTUNITY:** Murray State University does not discriminate on grounds of race, color, gender, sexual orientation, religion, national origin, age, handicap, or veteran's status in providing any educational or other benefits services of Murray State University to students or those applying for admission at Murray State University. Murray State University attempts to provide equal opportunity in all areas of student admissions, financial aid, employment, and placement and provides upon request, reasonable accommodation including auxiliary aids and services necessary to afford individuals with disabilities an equal opportunity to participate in all programs and activities.

**XV. Spring 2010 Office hours:** Mon and Wed 8:30-11:00 AM, Tues and Thursday 1:00 – 3:30 PM.