



College of Business

Department of Computer Science and Information Systems

MURRAY STATE UNIVERSITY

COURSE SYLLABUS

TSM441 (SPRING 2010)

Advanced Information Security

DEPARTMENT: Computer Science and Information Systems

COURSE NUMBER: TSM 441

CREDIT HOURS: 3

- I. **TITLE:** Advanced Information Security.
- II. **CATALOG DESCRIPTION:** An introduction to advanced aspects of Information Security and Assurance. This course provides the students with an understanding of the issues associated with computer and network forensics, malicious software, and encryption systems.
- III. **PURPOSE:** The purpose of the course is to provide the student with an overview of the techniques involved in forensics for computer and network incident handling; minimizing malicious code damage; and the use and management of data encryption systems.
- IV. **COURSE OBJECTIVES:** By the completion of the course, students will be able to:
 - A. Identify the steps involved in computer forensics
 - B. Plan for incident handling with the use of computer forensics
 - C. Understand malicious software and determine how to combat it
 - D. Identify and use different encryption algorithms for identification and authentication
 - E. Understand how encryption is used to secure data
- V. **CONTENT OUTLINE**
 - A. Computer Forensics
 - a. Overview of Computer Forensics as a Profession
 - b. Computer Investigations
 - c. Working with Different Operating Systems
 - d. Forensic Tools
 - e. Digital Evidence
 - f. Data Acquisition
 - g. Writing Investigative Reports
 - B. Malicious Software
 - a. History of Malicious Software
 - b. Viruses
 - c. Worms
 - d. Malicious Mobile Code
 - e. Backdoors
 - f. Rootkits

- C. Encryption
 - a. Encryption System Management

VI. INSTRUCTIONAL ACTIVITIES: Lecture, Discussion, Case Studies, Hands-on Exercises, and Problem-based Learning.

VII. FIELD, CLINICAL, AND/OR LABORATORY EXPERIENCES: Weekly lab for case studies and hands-on exercises.

VIII. RESOURCES: Web-Page references:

<http://estudy.murraystate.edu> – MSU Blackboard

<http://www.sans.org> - Sans Institute

<http://infosyssec.net>

<http://csrc.nist.gov/publications/PubsSPs.html>

<http://www.crime-research.org/>

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. Lab Work, Homework/quizzes, and attendance - 30%.
2. Tests - 60% (probably 3)
3. Term Paper - 10%.

Grievance and Appeals Policy: <http://www.murraystate.edu/cbpa/PDF/Appeals.pdf>.

X. ATTENDANCE POLICY: This course will adhere to the attendance policy published in the current MSU Bulletin. Lecture attendance is mandatory and will be checked. Students that have 3 unexcused absences will lose 1 exam point for each additional unexcused absence up to a total of 5 absences. Students will lose 2 exam points for each additional unexcused absence in excess of 5. Lab attendance will not be checked but students are expected to participate in the scheduled lab time on a regular basis and complete all required lab work by the due dates, regardless of whether the work is completed during the scheduled lab or on their own work schedules.

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: There are two texts.

- A. Nelson, et al: Guide to Computer Forensics and Investigations, 3rd Edition, ISBN 978-1-4180-6733-5.
- B. Skoudis, Malware: Fighting Malicious Code, ISBN 013101405-6

RECOMMENDATION READING:

- a. Grimes, Roger A., Malicious Mobile Code, O'Reilly Publishers, ISBN# 9781565926820.
- b. Jones, Robert, Internet Forensics, O'Reilly, ISBN# 9780596100063.
- c. HoneyNet Project, Know Your Enemy, ISBN# 0321166469.
- d. Ferguson and Schneier, Practical Cryptography, ISBN# 047122894-X.

XIII. PREREQUISITES: TSM 352.

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 Thurs 1:00 – 3:30 PM.

TELECOMMUNICATIONS SYSTEMS PROGRAM SECURITY AGREEMENT

As a student of Murray State University's Telecommunications Systems Management Program, I understand that I will receive instruction which will convey knowledge of security and protection services and which will also by nature convey how illegal actions could be performed so that I will be able to defend against them.

Therefore, I agree, now and in the future, not to use this knowledge for illegal or unethical purposes and to abide by all applicable standards and laws, whether they are city, state, national, or international.

Further, I agree that:

- I will promote good information security concepts and practices.
- I will perform all professional activities and duties in accordance with the law and the highest ethical principles.
- I will give preference to the laws of the jurisdiction in which service is being rendered when resolving differing laws in different jurisdictions.
- I will not engage in or be a party to unethical or unlawful acts that negatively affect the community, my own or others professional reputation, or the information security discipline.
- I will not misuse any information or privileges I am afforded as part of my education.

Student's Signature

Student's Name (Printed)

Date