Instructor Information:

Someswar Kesh, Office: WDE 2705, Phone: 660-441-0721, E-Mail: kesh@ucmo.edu
Office Hours: 8:30 A.M – 10:30 M, W, 8:30-11:30 Tu
Other times by appointment

Text:

Guide to Network Defense and Countermeasures
Randy Weaver

Course Description:

This course provides an in-depth knowledge of managing corporate information systems with an emphasis on security. Both managerial and technical aspects of IT security will be discussed.

Course Objectives:

The objectives of the course are:

1. Introduce the students to the concepts of Information Security
2. Learn about planning for information security and contingency planning
3. In-depth knowledge of security management models and practices
4. In-depth knowledge of risk management models
5. Use network analysis and design tools
6. Design a network defense and protection mechanisms
7. Design and configure firewalls
8. Understand and use encryption schemes
9. Understand and use intrusion detection
10. Use risk analysis

Course Outcomes:

After successful completion of the course students should be able to:

1. Perform contingency planning
2. Apply security management models for developing
3. Develop a network defense and protection mechanism
4. Configure firewalls
5. Compare and apply various encryption mechanisms
6. Perform risk analysis for information security
Outcome measurement

All outcomes will be measured by tests and successful completion of assignments.

Teaching methods:

Lectures and class discussions

Attendance policy:

Students are expected to attend classes on a regular basis and participate in class discussions.

Honesty policy:

Students are expected to follow the university regulations and policies. Consult the student handbook for further information.

Tests and assignments policy:

Tests will be given on the dates announced by the instructor. A make up test will be considered only in case of a serious emergency. Assignments will be due on the date specified. There will be a 10 percent penalty per day for late submission. Final exam will be held as per schedule.

Grading:

1 Test and one final exam: 200 points
Presentations: 75 points, class participation: 25 points; Total 100 points.
Research paper: 100 points
Total: 400 points
(more information regarding research paper expectations will be provided later).

Grading: A: >90, B: 80-89%, C: 70-79%, D: 60-69%, F <60%
The instructor reserves the right to curve the grades, if necessary.

Schedule of Topics:

Lecture Topics:

Introduction
Elements of Computer Security
Security Policy
Security Program Management
Risk Management
Security Planning
Preparing for Contingencies and Disasters
Technical controls
Cryptography

Reference Materials for Lecture Topics:

http://books.google.com/books?id=gPonBssSm0kC&pg=PA8&lpg=PA8&dq=cia+triangle+information+security&source=bl&ots=cZ98PNsBl_&sig=Usin7YXu8rgJA3

http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/

Additional material, if needed will be provided by the instructor.

Presentation Topics:

Each group will be assigned a presentation topic that will generally follow the topics outlined in the text.
Final exam will be held as per schedule.

Research: All students taking the course for graduate credit will have to submit an in-depth research paper. Appropriate topics, length, format etc. will be discussed in class. The instructor will recommend topics on which the student may work. The student may also select a topic with the approval of the instructor. These topics will be based on relevance to the course and currency. The student will select one of the topics and develop a research proposal and submit it to the instructor for approval. Once approved, the student may proceed to complete the research within the allotted time.

IMPORTANT:

This class has a prerequisite of CIS 2665: Principles of Data Communications and LAN or equivalent