

Maryland in Europe Graduate Programs
Bowie State University

Information Systems Security
INSS 635

7/8, 21/22 JUN; 12/13, 26/27 JUL 2003
Wuerzburg, Leighton Education Center
Saturday & Sunday, 0900 to 1600

Instructor: Scott Jarrow
Mailing Address: UMUC Central Germany, Unit 29216, APO AE 09102
Email Address: sjarrow@faculty.ed.umuc.edu
Consultation: Students may request individual discussions before or after class, or by appointment. I will be on post Saturday and Sunday during weekend classes.

Course Description: 3 semester hours credit. *Prerequisites: Either INSS 510, INSS 520, INSS 530, or permission of the instructor.* Introduces ADP audit and control methods, with emphasis on information systems controls. ADP security, type of ADP audit, concepts, and techniques used in ADP audits are discussed. It also examines exposure to risk assessment and professional standards in the field of ADP auditing and internal control policy and procedures.

Course Goals/Objectives:

Upon completion of the course, participants should:

1. Understand management responsibilities and information system security practices
2. Understand controlling access to a system
3. Understand the complex problems of security in telecommunications and networks
4. Understand cryptography as a tool of information security
5. Understand building security into the fundamental architecture of hardware and systems software
6. Understand how to protect a facility's computer operations, including its data media and personnel
7. Understand developing applications with security designed into them
8. Understand ensuring business continuity with disaster and recovery plans
9. Understand the role of ethics and the law in issues of information systems security
10. Understand physical security of system sites

Objectives: At the conclusion of this course the student will be able to:

1. Evaluate an organization's security practices
2. Create a checklist of needed security controls for corporate resources
3. Grasp information security as it applies to telecommunications
4. Select from different encryption schemes the best one for a particular application
5. Comprehend where security is to be applied in IT architecture
6. Secure computing resources from threats inside and outside the organization
7. Supervise the development of applications to include built-in security
8. Set up a backup and recovery plan for critical corporate data
9. Make judgements regarding ethical/legal implications of Info. security systems

Text: Krutz, R. and Vines, R. (2001). *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*. New York: John Wiley and Sons.

Grading Information: Grades for this course will be assigned as follows:

A	92% +	C	70 – 79%
B	80 – 91%	F	Below 70% F(a) or regular non-attendance F(n)

Course Requirements:

Midterm Exam will cover both text and lectures. It will consist of objective questions and essay questions. The Final Exam will have essay questions of the type found in the MIS Graduate program comprehensive exams.

Class attendance is expected. Students are responsible for all material covered during lectures and discussions, as well as assigned textbook readings. Class participation is encouraged, especially when discussing issues where there are differing sources of information and points of view. In order to have lively and effective class discussions, students should read the assigned material and think about it before class.

Students will be graded primarily on their written work. Good presentation skills are also important, however, and will help contribute to the grade.

Individual Case Study	10%
Class Participation	5%
Midterm Examination:	25%
Final Examination:	30%
Team Project:	30%

Project Description: There will be a Team Project for INSS 635 students. A possible group project task would be to put together a security and/or recovery plan for an organization or enterprise or explore the security vulnerabilities of an organization.

As an example of a current and relevant research topic, the draft of "The National Strategy to Secure Cyberspace" was released for public comment by the President's Critical Infrastructure Protection Board on 18 September 2002.

More detailed plans for these assignments will be developed during our first weekend class.

Projected Course Schedule:

Module	Topics	Assigned readings/Assignments due
7 June	Course and Class Introductions Security Management Practices & Access Control Systems	Chapters 1 & 2
8 June	Telecommunications Network Security	Chapter 3
21 June	Cryptography	Chapter 4
22 June	Security Architecture & Models Review	Chapter 5 <i>Midterm Exam, 22 June</i>
12 July	Operations Security & Applications and Systems Development	Chapters 6 & 7
13 July	Continuity Planning and Disaster Recovery	Chapter 8
26 July	Law, Investigation, Ethics & Physical Security	Chapters 9 & 10
27 July	Research & Project Presentations and Discussions Course Review	<i>Final Exam, 27 July</i>

Academic Policies: Please refer to the UMUC Maryland in Europe Graduate Catalog, available online at http://www.ed.umuc.edu/visit/pubs/catalog/grad_02-03.pdf or from your local Education Center, for information on the following:

- Academic Integrity**
- Course Load**
- Exception to Policy**
- Grade Appeal Process**
- Make-up Examinations**
- Nondiscrimination**
- Students with Disabilities**

CODE OF CIVILITY

To promote a positive, collegial atmosphere among students, faculty, and staff, Maryland in Europe has developed the following Code of Civility:

Respect

Treat all students, faculty, and staff with respect and in a professional and courteous manner at all times and in all communications, whether in person or in written communication (including e-mail).

Kindness

Refrain from using profanities, insults, or other disparaging remarks.

Truth

Endeavor to cite only the truth and not knowingly misrepresent, mischaracterize, or misquote information received from others.

Responsibility

Take responsibility for our own actions instead of blaming others.

Cooperation

Work together with other students, faculty, and staff in a spirit of cooperation toward our common goals of seeking and providing quality education.

Privacy

Strive to uphold the right to privacy and not talk about others.

Nondiscrimination

Respect the differences in people and their ideas and opinions and reject bigotry.

Additional Information:

Written assignments:

Black ink on white A4 or 8.5x11 paper, in a standard typewriter face such as Courier, or 11- or 12-point Times New Roman. Line spacing double-spaced or 1.5.

No color or graphics, except for (1) charts or maps generated by the student to convey substantive information; or (2) as an artifact of the subject being studied, in support of a point discovered or being argued by the student.

Where there has been research, be sure to acknowledge your sources, using the APA style. See -- www.umuc.edu/library/guides/apa.html

Attendance:

Class attendance is expected. Students are responsible for all material covered during lectures and discussions, as well as assigned textbook readings.

Academic Honesty:

Students are expected to do their own work. Cheating on tests, plagiarism on written assignments, or any other form of academic dishonesty will result in a "0" for the assignment for the first violation, a second violation will entail more serious penalties at the discretion of the instructor. Note that a D or an F usually results in at least 60 or 50

points, where violation of academic honesty results in none. See the European Division Catalog for the UMUC policy on academic dishonesty and plagiarism.

Assignments/Test Schedules:

Students are expected to hand in all assignments and complete all tests on the days they are due. If a student fails to complete any assignment or test, the resulting grade will be a "0," rather than an "F." Any other assignments will be marked down half a letter grade for each week the assignment is late. Major tests can be made up only if prior arrangements are made with the instructor.

Mutual Respect for Classmates and Teammates:

All of us are expected to conduct ourselves with appropriate mutual respect and basic fairness in all matters related to class and project work with no one unduly burdened, and no one treated in other than a professional, collegial manner. Harassment, bias or intimidation in any form will not be tolerated and should be reported to the instructor as soon as practical. See Student Handbook for Maryland policy statements on nondiscrimination and sexual harassment.

About Your Instructor: Scott Jarrow has a broad background in teaching and in the field of high tech. He graduated with a Bachelors degree in Basic Sciences in 1977 from the USAF Academy, with a Computer Science discipline. He began teaching microcomputers and programming for Central Texas College at the Pacific Far East campus in 1987. He returned to the U.S. in 1989 and received a Masters degree in Management Information Systems from Bowie State University in 1991. He then returned overseas to Europe to teach for University of Maryland from 1991 to 1994 as an IFSM and CMIS lecturer in Germany and Great Britain. From 1994 to 2000, he worked as a defense contractor in the U.S. and in private industry for City and County governments as a systems analyst/systems engineer. He formed his own company and worked independently in a variety of private business ventures from 2001 to 2002. In 2002, he returned to Europe to teach for UMUC and Bowie State University.