

| | |
|---------------------------------------|---|
| Course | ITM5600 - Information and Communications Security |
| Term | Fall 2, 2009 |
| Instructor | Name: <u>Barry Levine</u> Phone: <u>(915) 474-3797</u> Email: <u>levineba@webster.edu</u> |
| Catalog Description | This course focuses on the analysis and management of information and information systems security including processes, technology, and facilities. |
| Prerequisites | ITM5000 – Information Technology Management - Overview |
| Course Level Learning Outcomes | <p>After completing this course, students will:</p> <ul style="list-style-type: none"> • <i>know and explain the important technical and management terminology, concepts, principles, techniques, and theories related to the technical aspects of information and communications security management.</i> • <i>be able to effectively apply important technical and management concepts, principles, practices, techniques, and theories needed to critically analyze an organization's information and communications security requirements.</i> • <i>be able to effectively apply important technical and management concepts, principles, practices, techniques, and theories needed to design and recommend appropriate security solutions.</i> • <i>be able to effectively apply important technical and management concepts, principles, practices, techniques, and theories needed to manage the implementation and on-going administration of recommended security solutions.</i> |
| Materials | <p><u>REQUIRED TEXTS:</u> "Security in Distributed Computing", Bruce, Glenn and Dempsey, Rob; Prentice-Hall PTR; Latest Edition</p> <p><u>TBA:</u> Articles from various publications that are most appropriate to the weekly topic will be delivered in photocopy form, e-mail, or as internet addresses. Students are encouraged to recommend sources that will benefit our understanding of the weekly topics.</p> |

Materials (cont.)

In addition, students are expected to stay abreast of current events relevant to this class. Each class will begin with a discussion of current events that will be led by students – participation in this discussion will count towards the Class Participation and Discussion grade.

SUPPLEMENTAL READINGS AND WEBSITES:

Websites:

Networked Systems Survivability Program of the Software Engineering Institute of Carnegie-Mellon University (CERT-CC)

<http://www.cert.org/> and

<http://www.sei.cmu.edu/organization/programs/nss/nss.html>

VISA Cardholder Information Security Program (CISP).

http://www.usa.visa.com/business/accepting Visa/ops_risk_management/cisp.html

Honeypots Revealed

<http://www.securitydocs.com/library/2692>

...and other readings/websites as assigned.

Grading

- A) Quizzes; Class Participation 20%
- B) Midterm Paper & Group Presentation 25%
- C) Security Strategy Paper & Group Presentation 25%
- D) Final examination 30%

Grade distribution for this course is as follows:

| Grade | Score Range |
|-------|-------------|
| A | 95 - 100 |
| A- | 91 - 94 |
| B+ | 87 - 90 |
| B | 83 - 86 |
| B- | 79 - 82 |
| C | 70 - 78 |
| F | 0 - 69 |

The GRADUATE catalog provides these guidelines and grading options:

- **A/A-** Superior graduate work
- **B+/B/B-** Satisfactory graduate work
- **C** Work that is barely adequate as graduate-level performance
- **CR** Work that is performed as satisfactory graduate work (B- or better). A grade of "CR" is reserved for courses designated by a department, involving internships, a thesis, practicums, or specified courses.
- **F** Work that is unsatisfactory

| | |
|--|---|
| | <p>and in the time allotted, a grade of “F” will be submitted. The instructor on a case-by-case basis will consider extensions of the time period required for completion. After one year, any grade of “I” not changed to another grade becomes final.</p> <p>Special Services If you have registered as a student with a documented disability and are entitled to classroom or testing accommodations, please inform the instructor at the beginning of the course of the accommodations you will require in this class so that these can be provided.</p> <p>Disturbances Since every student is entitled to full participation in class without interruption, disruption of class by inconsiderate behavior is not acceptable. Students are expected to treat the instructor and other students with dignity and respect, especially in cases where a diversity of opinion arises. Students who engage in disruptive behavior are subject to disciplinary action, including removal from the course.</p> <p>Student Assignments Retained From time to time, student assignments or projects will be retained by The Department for the purpose of academic assessment. In every case, should the assignment or project be shared outside the academic Department, the student's name and all identifying information about that student will be redacted from the assignment or project.</p> <p>Contact Hours for this Course It is essential that all classes meet for the full instructional time as scheduled. A class cannot be shortened in length. If a class session is cancelled for any reason, it must be rescheduled.</p> |
|--|---|

| | |
|-------------------------------|--|
| <p>Course Policies</p> | <p>This class will cover a range of contemporary topics relating to information and communications security and therefore will rely heavily on assigned readings. The instructor will distribute these readings throughout the week before each class. Each week, the class will be organized around lectures, specific case studies, and discussion questions based on the course readings. These will normally be distributed at the end of the prior class or assigned via email shortly thereafter. To receive a satisfactory discussion grade students must read the assigned material and come prepared to address the discussion questions. This applies to the first week as well.</p> |
|-------------------------------|--|

| | |
|--|--|
| | <p>Webster University’s policy on plagiarism or cheating is “Students who are discovered cheating or committing plagiarism will be awarded a failing grade for the course, and may be subject to dismissal or further discipline.”</p> <p>Webster University’s policy on class attendance is “Students are expected to attend all class sessions of every course. In the case of unavoidable absence, the student must contact the instructor. The student is subject to appropriate academic penalty for incomplete or unacceptable makeup work, or for excessive or unexcused absences.”</p> <p>“If a student is absent, the instructor is to assign makeup work, which may exceed the material presented that week. If a student has two absences, the instructor has the option to lower the student’s grade one letter grade and to inform the student of the action. If the student has three absences, the instructor has the option to assign a grade of “F” and to inform the student of the action. It is the student’s responsibility to withdraw from the course.”</p> <p><i>Furthermore, students are expected to stay abreast of current events relevant to this class. Each class will begin with a discussion of current events that will be led by students – participation in this discussion will count towards the Class Participation and Discussion grade.</i></p> |
|--|--|

| | |
|-------------------------------|---|
| <p>Weekly Schedule</p> | <p><u>Week 1 - Part One: Understanding the Problem</u></p> <p>Topic: Introduction to Computing Security and the examination of the business issues associated with security. Identify the business drivers and issues which define the organizational requirements for IS security. Examine the challenges associated with distributed security and describe the most pressing problems of trust and security encountered.</p> <p>Learning Activities: Lecture, Discussion</p> <p>Homework Due: Read chapters 1 and 2.</p> <p><u>Note: Be sure to review this weekly schedule in its entirety so that you are aware of the Security Audit & Strategy paper and presentation due in Week 8; possibly week 7 depending on the number of students in the class.</u></p> <p><u>Week 2 - Part Two: Foundations</u></p> <p>Topic: Examine the concepts supporting computing security. Define the key terms of trust and security. Discuss the foundations and architecture that lead to the development of security policies. Define the structure and components of a security architecture</p> |
|-------------------------------|---|

| | |
|--|--|
| <p>Weekly Schedule (cont.)</p> | <p>model and a security policy.</p> |
| | <p>Learning Activities: Quiz, Lecture, Discussion</p> |
| | <p>Homework Due: Read chapters 3 to 6. Access a CERT website and present a synopsis of a current network security issue or problem.</p> |
| | <p><u>Week 3 - Part Three: Technologies</u></p> |
| | <p>Topic: Discuss the concepts of trusted networks and the security implication of TCP/IP protocols in a distributed environment. Develop an understanding of the common network operating systems and their common security issues. Examine the components of client/server computing systems, the trust issues presented by them, and the interfaces and security services provided by middleware.</p> |
| <p>Learning Activities: Quiz, Lecture, Discussion</p> | |
| <p>Homework Due: Read chapters 7 to 9. Conduct an Internet research on the topics “IP Port Scan” and “Ping of Death” and write a paper with an executive summary on each cause of the potential vulnerability, its potential impact and measures of protection that are available and feasible.</p> | |
| <p><u>Week 4 - Part Three Continued: UNIX Security</u></p> | |
| <p>Topic: Examine the concepts of the open systems operating system environment and the security and trust issues associated with these and UNIX in particular. Identify and discuss the security services contained in UNIX systems and their weak points. Identify security solutions for UNIX implementations and the accompanying policies and guidelines that must support these solutions.</p> | |
| <p>Learning Activities: Quiz, Lecture, Discussion</p> | |
| <p>Homework Due: Read chapters 10 to 12. Access a CERT website and present a synopsis of a current UNIX security issue or problem and propose specific, viable solutions.</p> | |
| <p><u>Week 5 - Part Three Continued: Windows NT and Internet Security</u></p> | |
| <p>Topic: Examine the concepts and architecture of the Microsoft Windows NT operating system. Identify the security features and issues associated with WIN NT. Learn how to invoke the security controls contained with WIN NT. Discuss the structure and services provided by the Internet architecture and the security issues and problems associated with it.</p> | |

| | |
|---|---|
| <p>Weekly Schedule (cont.)</p> | <p>Learning Activities: Quiz, Lecture, Discussion, Individual Student Presentations</p> <p>Homework Due: Read chapters 13 and 14.</p> <p>Group Project: Develop a management review paper on the VISA “Cardholder Information Security Program (CISP)” and present in class.</p> <p>MIDTERM EXAMINATION: The CISP Paper and Presentation count as Midterm Examination.</p> <p><u>Week 6 - Part Three Continued: Cryptology</u></p> <p>Topic: Examine the concepts of cryptology and the principles of encryption. Study the concepts of Private Key and Public Key encryption. Discuss the management concepts and concerns of the use of encryption keys and their evaluation techniques. Learn the methodologies and examine the issues associated with digital signatures. Examine the concepts, architectures and security issues associated with Distributed Computing Environments (DCE), distributed databases and on-line transaction processing.</p> <p>Learning Activities: Quiz, Lecture, Discussion</p> <p>Homework Due: Read chapters 15 to 19. Present an in-depth analysis of a current security issue that involves a cryptological problem or solution.</p> <p><u>Week 7 - Part Four: Solving the Problem.</u></p> <p>Topic: Learn how to develop secure applications and identify the role and rule-based security concepts. Examine secure examples presently in use. Discuss the detailed aspects of the requirements and implementation of security systems and the management of these</p> |
|---|---|

| | |
|---------------------------------------|--|
| <p>Weekly Schedule (cont.)</p> | <p>systems.</p> <p>Learning Activities: Quiz, Lecture, Discussion</p> <p>Homework Due: Read chapters 20 to 22.</p> <p><u>Week 8 - Part Four Continued: Development and Auditing of Security Strategies</u></p> <p>Topic: Discuss the concepts of Security Strategies and how to develop and implement them. Examine the uses of security audits and the criteria used in the protection of information systems. Discuss emerging IS security concepts, threats and evolving procedures along with their resultant management implications.</p> <p>Presentations: Present a <i>Security Audit & Strategy for the Protection of an Information System</i> using charts, graphs, slides and text in effective media formats. Submit a formal paper on this topic in APA format.</p> <p>Learning Activities: Quiz, Lecture, Group Presentations</p> <p>Homework Due: Read chapter 23 to 25. Prepare for Final Exam.</p> <p><u>Note:</u> All presentations are group presentations. Presentations are limited to 20 minutes each. Additional time used may result in point deduction.</p> <p><u>WEEK 9 – Final Exam</u></p> <p>Assessment: Cumulative written exam covering chapters 1 through 22</p> <p>Time allowed: 4 hours</p> |
| <p>Additional Information</p> | <p><u>GUIDANCE ON ORAL PRESENTATION:</u> (Weeks 5 & 8)</p> <p>Oral presentations will be strictly limited to 20 minutes (practice beforehand!), followed by 10-15 minutes of questions and discussion. Students may use any presentation aids deemed necessary (PowerPoint, handouts, etc.).</p> <p>XI. <u>GUIDANCE ON RESEARCH PAPERS:</u> (Due week 8)</p> <p>Papers are expected to be roughly 20 pages in length, double-spaced, with full citations (proper citation will be considered in the paper grade).</p> <p>This syllabus may be revised at the discretion of the instructor without the prior notification or consent of the student.</p> |