

Syllabus for INFA620 (Network and Internet Security)

Course Description

(Formerly TLMN 672.) An introduction to the security concepts needed for the design, use, and implementation of secure voice and data communications networks, including the Internet. A brief review of networking technology and standards (including an introduction to Internet communication protocols) is provided. Specific security subjects addressed include defense models, security policy development, authentication and authorization controls, firewalls, packet filtering, virtual private networks (VPNs), and wireless network security.

Course Goals/Objectives

Upon successful completion of this course, the student should be able to:

1. Illustrate and explain fundamental architectures of networks and the Internet as well as their underlying protocols.
2. Identify and define security issues, problems and vulnerabilities in voice, data, and wireless networks.
3. Define, evaluate, and compare prevalent information assurance solutions for voice, data, and wireless networks.
4. Describe and analyze Internet security issues and available countermeasures.
5. Apply industry standard security concepts and techniques to specific network environments.
6. Evaluate trends in network security policies and technology as well as their impact on the future of network development.

Course Materials

American Psychological Association. (2001). Publication manual of the American Psychological Association (5th ed.). Washington, D.C.: APA. ISBN: 1-55798-791-2

Bragg, Rhodes-Ousley, and Strassbert. (2004). Network Security: The Complete Reference. Emeryville, California: McGraw-Hill/Osborne. ISBN: 0-07-222697-8

Grading Criteria

Section removed.

Academic Policies and Procedures

Section removed.

Project Descriptions

Details on the Analytic Research Paper:

- A. Length and Style: The body of an analytic research paper should be 10 pages in length and typed using the APA Guide. Student projects distill fundamental issues, discuss the various available solutions, discuss the benefits and limitations of the available solutions, and provide a new solution and justification. Student papers must state a thesis, and based on the research, attempt to prove or disprove that thesis. An adequate literature search will include a few books and journal articles (or other relevant documents). A search of Internet documentation is required. Students should develop a conclusion which synthesizes the literature in such a way as to demonstrate new knowledge.

- B. Term Paper Process: Students are required to use the structured approach to project construction to aid them in completing a successful paper. Students must turn in several interim products (deliverables) which are part of the term paper grade.
Session 3: Student proposes a research paper topic for approval.
Session 6: Student submits a sample bibliography.
Session 9: Student submits a paper progress report.
Session 12: Student submits the research paper.

- C. Evaluation Criteria and Feedback: The litmus test of a good research project is: "Does my research project provide the professor with new insight on my topic?" An e-mail evaluation of the paper will be provided along with the final grade.

- D. Standards for Papers: (Repeated from the UMUC Policies Entry.) Effective managers and leaders are also effective communicators. Written communication is an important element of the total communication process. The Graduate School recognizes and expects exemplary writing to be the norm for course work. All individual and group papers must demonstrate graduate level writing ability and comply with the format requirements of the Publications Manual of the American Psychological

Association (5th edition). Careful attention should be given to source citations, proper listing of references, and the presentation of tables and graphs. Format and graphics, however, are not always transmitted well over the Internet: there are dozens of ways in which hardware, software and networks may be incompatible. A student may mail an additional copy of his/ her research paper to the professor by Postal Service when graphics present a problem.

E. Policy and Academic Integrity (Plagiarism): (Repeated from the UMUC Policies Entry.)

Plagiarism is the intentional or unintentional presentation of another person's idea or product as one's own. Plagiarism includes, but is not limited to the following: copying verbatim all or part of another's written work; using phrases, charts, figures, illustrations, or mathematical or scientific solutions without citing the source; and paraphrasing ideas, conclusions, or research without citing the source. Students can avoid unintentional plagiarism by carefully accepted scholarly practices. Notes taken for papers and research projects should accurately record sources of material to be cited, quoted, paraphrased, or summarized, and papers should acknowledge these sources in footnotes. The penalties on plagiarism include a zero or a grade "F" on the work in question, a grade "F" in the course, suspension with a file letter, suspension with a transcript notation, or expulsion.

Course Schedule

Week	Session Dates	Readings, Assignments, and Due Dates
1	09/04/2007	Session 1: Introduction to the Course Bragg and others, Chapter 1
2	09/11/2007	Session 2: Network Security Foundations: Risk Analysis and Defense Models Bragg and others, Chapter 2
3	09/18/2007	Session 3: Network Security Foundations: Security Policy Development Bragg and others, Chapter 3 Due: Paper topic
4	09/25/2007	Session 4: Network Security Foundations: Security Organization Bragg and others, Chapter 4
5	10/02/2007	Session 5: Access Control: Physical Security Bragg and others, Chapter 5 Bishop, Chapter 5
6	10/09/2007	Session 6: Access Control: Authentication and

		Authorization Controls Bragg and others, Chapter 6 Bishop, Chapter 6 Due: Sample Bibliography
7	10/16/2007	Session 7: Midterm Exam
8	10/23/2007	Session 8: Access Control: Data Security Architecture Bragg and others, Chapter 7 Bishop, Chapter 7
9	10/30/2007	Session 9: Access Control: Security Management Architecture Bragg and others, Chapter 8 Due: Progress Report
10	11/06/2007	Session 10: Network Architecture: Network Design Considerations and Network Device Security Bragg and others, Chapters 9-10
11	11/13/2007	Session 11: Network Architecture: Firewalls and Virtual Private Network Security Bragg and others, Chapters 11-12
12	11/20/2007	Session 12: Network Architecture: Wireless Network Security and Intrusion Detection Systems Bragg and others, Chapters 13-14 Due: Research Paper
13	11/27/2007	Session 13: Final Exam
14	12/04/2007	Session 14: Network Architecture: Integrity and Availability Architecture, and Network Role-Based Security Bragg and others, Chapters 15-16
15		