

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 655

1. **Abbreviated Course Title:** Computer Security Topics
2. **Full Course Title:** Computer Security Topics
3. **Credits:** Three (3) graduate degree credits, 45 contact hours. Online or on-campus formats will be offered in the future.
4. **Catalog Description:** Content varies depending on faculty interests, research developments, and student demand, as current topics of advanced research in computer security are examined. Representative topics include but are not limited to formal models for computer security, multilevel data models, and multilevel database management system architectures.
5. **Course Prerequisites:** None
6. **Rationale:** This course is designed to address, analyze and discuss relevant current issues and the changes that affect the field of cyber security. All organizations as well as individuals must be kept informed of the important dimensions and relevant issues and changes of our network, information-based society for their safety. Cyber security significantly impact national and corporate security entities, it is also an ever-changing field and as such it is critical that students and practitioners alike be kept informed of the current issues, and its possible direction.

Students aspiring to advance or seek a career in the security field or law enforcement should have a thorough understanding of current and relevant issues and changes in cyber Security and how it ties in with national and corporate security, as it affects all sectors of our information-based, technically reliant society.

7. **Student Learning Outcomes and Course Goals:** Students who successfully complete this course will be able to...
 - A. ANALYZE various responsibilities of those involved with Cyber Security.
 - B. ANALYZE the current policies and procedures that impacts on an organization's information/cyber security systems.
 - C. SYNTHESIZE knowledge of current issues involved with hard and software utilized in cyber security.
 - D. ASSESS whether or not an organization's information/cyber security system is current and operating with the best available technology.
 - E. ASSESS the vulnerabilities of information/cyber systems during regular intervals and/or when significant changes have been made affecting these systems.

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 655

- F. APPRAISE the importance of keeping current of new policies, procedures, hard and software when managing an information technology/cyber security system.
- G. EVALUATE the resources currently being used on a regular basis.
- H. EXPLAIN security concurrency control protocols.
- I. IDENTIFY the levels of and prioritize the most current vulnerabilities and threats to information-based systems.
- J. CRITIQUE the formal models for computer security.
- K. DEMONSTRATE the ability to manage multi-level data models and architecture.
- L. PREDICT current changes that might lead to legislation that might affect information assurance/cyber security systems.
- M. FACILITATE the appropriate use of information based/cyber security systems.
- N. DISTINGUISH components of a distributed secure system architecture.
- O. INFER the importance of maintaining regular liaisons with information/cyber security professionals.
- P. DISCERN the responsibilities of and importance that executive management has in fully supporting cyber security professionals.

8. Instructional Procedures:

- Lecture
- Hands-on in class/lab exercises
- Group discussion and interaction
- Group and individual assignments/projects
- Student presentations

9. Course Content:

UNIT	TOPIC	SUBTOPICS	OUTCOMES
1	Introduction	Technology is Ever-changing	A,D
2	Information-based Systems	Security; Assurance	D,E,M
3	Current Issues in Cyber Security	Certification and Accreditation	D,E,
4	Formal Models for Computer Security	Confidentiality; Commercial; Integrity;	J

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 655

		Information Flow Models	
5	Multi-level Data Models	Life Cycle System	K
6	Multi-level Database Management System Architecture	Systems Approach	K
7	Secure Concurrency Control Protocols	Locking Techniques	H
8	Mid-term Project/Examination		A,D,E,H,J,K,M
9	Distributed Secure System Architecture	Defense in Depth; Access Controls	N
10	Analysis of Current Policies and Procedures	Implementation; Enforcement; Reporting	B,F
11	Analysis of Current Hard and Software Needs	Asset Management; Hardware and Software	B,F
12	Requirements Analysis	Needs Assessment	A,B,C,D,E,G,H,I
13	Communicating With Other Security Sectors	Security networks	O
14	Current Legislation Affecting Info Systems	Security Laws; Licensing; Piracy;	L
15	Final Project/Examination		A through P

Due to the nature of IA/Cyber Security courses, use of personal computers and University computer labs are **REQUIRED**. See CITI and computer lab links:

- <http://www.njcu.edu/programs/citi/>
- <http://www.njcu.edu/ac/home.htm>
- <http://www.njcu.edu/ac/labs/proflabs.htm>

10. Undergraduate General Studies Courses: (Not Applicable)

11. Graduate Course Status: This course is part of a carefully planned program sequence that embraces graduate-level pedagogy. Specifically, the design includes a curriculum core, specialization and capstone for each graduate student. Item #6 covers the content rationale of this course and this item emphasizes the graduate status. Professional Security Studies prepares students to be critical thinkers, defined as employing higher-order thinking: emphasizing application, analysis, synthesis and evaluation. As a graduate course, research is the common thread during the entire curriculum. Additionally, a team approach is integrated throughout as teamwork is the reality of the Professional Security field.

Students are required to address, analyze and discuss relevant current issues and the changes that affect the field of cyber security, in areas that include formal models for computer security, multilevel data models, multilevel database management system architectures, secure concurrency control protocols, distributed secure system

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 655

architectures, integrity models and mechanisms, security policy, and requirement analysis.

12. Programmatic/Departmental Outcomes:

Programmatic: This course fulfills the mission of the Security Program to provide students with greater knowledge, skills and abilities in the field of Professional Security Studies that will enable them to...

- Become lifelong learners for personal and professional enrichment
- Be effective and productive leaders and/or managers in their respective careers in the security field

Departmental: Students completing a course of studies in the graduate Security Studies Program must address, analyze and discuss relevant current issues and the changes that affect the field of cyber security, in areas that include formal models for computer security, multilevel data models, multilevel database management system architectures, secure concurrency control protocols, distributed secure system architectures, integrity models and mechanisms, security policy, and requirement analysis. This course is necessary for students specializing in information assurance/cyber security, and reflects the comprehensive, challenging nature and quality of the Professional Security Studies Department.

13. Degree Requirements: This course has been included as a required course for those specializing in the Cyber Security track in the Professional Security Studies Program.

14. Specialized Accreditation, Certification, and Licensure: This course in has been mapped against the National Security Agency's (NSA) certification requirements for *Information Systems Security Officers, CNSSI 4014* (Committee on National Security Systems Instructions – CNSSI).

15. Assessment/Evaluation of Student Outcomes and Determining Student Grades:
a. Describe how students will be assessed on an ongoing basis and how their performance will be evaluated. Describe examinations, term or research papers, special projects, class performance, seminar presentations, and portfolios in relation to student learning outcomes (Item 7). Include type of examination, nature of papers and projects, etc.

The following sets forth the assessment/evaluation tool being used and the nature of the assignment(s) used to evaluate student outcomes:

ASSESSMENT/EVALUATION	NATURE OF ASSIGNMENTS USED TO
-----------------------	-------------------------------

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 655

TOOL	EVALUATE STUDENT OUTCOMES
Class Participation	-Class discussions of assigned readings -Presentation of group responses to issues discussed in each class
Exams	-Written essay examinations to mid-term and final examination
Oral Presentations	-Individual presentation of research paper(s) -Presentation of group project
Research Paper(s) & Project(s)	-Individually assigned research paper(s) -Participation in group project

b. Please indicate the percentage assigned to each assessment/evaluation tool.

ASSESSMENT/EVALUATION TOOL	% OF TOTAL GRADE	OUTCOMES
Class Participation	20 %	C,J,L,M,N,O,P
Exams	30 %	A,B,F,G,H,I
Oral Presentations	20 %	C,H,I,J,K,L,M,N,O,P
Research Paper(s) & Project(s)	30 %	A,B,C,D,E,F,L,M,N,O,P

16. Bibliography:

a. Required Text(s):

Bishop, M. (2003). *Computer Security: Art and Science*. Boston: Addison Wesley.

Kelly, L. & McCumber, J. (2004). *Assessing and Managing Security Risks in IT Systems*. Boca Raton, FL: CRC Press.

Stallings, W. (2002). *Cryptology and Network Security: Principles and Practice*. Harlow, CA: Pearson.

Additional Required Readings:

Buchmann, J. (2004). *Introduction to Cryptography, 2nd ed*. New York: Springer, Verlag.

Litchko, J. & Payne, A. (2004). *Know Cyber Risk: By Managing Your IT Security*. Kensington, MD: Know Book Publishing.

Additional Required Resources: IA/Cyber Security Education Resources and Links for central access point for all historical documents (THESE ARE REQUIRED FOR ALL IA/CYBER SECURITY COURSES!!!):

<http://web.njcu.edu/sites/profstudies/securitystudies/Content/links.asp>

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 655

b. Supporting Bibliography:

- Anderson, J. (1972), *Computer Security Technology Planning Study Volume II, ESD-TR-73-51, Vol. II, Electronic Systems Division*. Bedford, MA: Air Force Systems Command, Hanscom Field.
- Anderson, J. (1980). *Computer Security Threat Monitoring and Surveillance*. Fort Washington, PA: James P. Anderson Co.
- Anderson, R. & Wiley, J. (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Upper Saddle River, NJ: Prentice Hall.
- Bisbey . & Hollingworth, D. (May 1978). *Protection Analysis: Final Report, ISI/SR-78-13*. Marina Del Rey, CA: University of Southern California/Information Sciences Institute.
- Bisbey II, R. et al. (1976). *Data Dependency Analysis, ISI/RR-76-45*. Marina Del Rey, CA: University of Southern California/Information Sciences Institute.
- Bishop, M. (2003). *Computer Security: Art and Science*. Boston: Addison Wesley.
- Buchmann, J. (2004). *Introduction to Cryptography, 2nd ed*. New York: Springer, Verlag.
- Carlstedt, J., et al. (1975). *Directed Protection Evaluation, ISI/RR-75-31*. Marina Del Rey, CA: University of Southern California/Information Sciences Institute.
- Carlstedt, J. (1978). *Protection Errors in Operating Systems: Serialization, ISI/SR-78-9*. Marina Del Rey, CA: University of Southern California/Information Sciences Institute.
- Department of Defense. (1985). *Computer System Evaluation Criteria, DOD 5200.28-STD*. Ft. Meade, MD: National Computer Security Center.
- Gollmann, D. & Wiley, J. (1999). *Computer Security*. Hoboken, NJ: John W. Wiley & Sons Incorporated.
- Hollingworth, D. & Bisbey II R. (1978). *Protection Errors in Operating Systems: Allocation/Deallocation Residuals, ISI/SR-76-7*. Marina Del Rey, CA: University of Southern California/Information Sciences Institute.
- Kelly, L. & McCumber, J. (2004). *Assessing and Managing Security Risks in IT Systems*. Boca Raton, FL: CRC Press.
- Litchko, J. & Payne, A. (2004). *Know Cyber Risk: By Managing Your IT Security*.

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 655

- Kensington, MD: Know Book Publishing.
- Mitnick, K.D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Hoboken, NJ: John Wiley & Sons, Inc.
- Peltier, T. R. (2000). *Information Security Risks Analysis*. New York, NY: CRC Press.
- Perlman, R. & Skoudis, E. (2001). *Computer Hack: A Step By Step Guide to Computer Attacks and Effective Defenses*. Harlow, CA: Pearson.
- Pfleeger, C. P. & Pfleeger, S. L. (2002). *Security in Computing*. Upper Saddle River, NJ: Prentice Hall.
- Phillips, B. (2001). *The Complete Book of Electronic Security*. New York: McGraw-Hill.
- Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. Hoboken, NJ: John Wiley & Sons, Inc.
- Stallings, W. (2002). *Cryptography and Network Security: Principles and Practice*. Harlow, CA: Pearson.
- Stein, L. D. (1997). *Web Security-A Step By Step Reference Guide*. Boston: Addison, Wesley.
- Stinson, D. (2002). *Cryptography: Theory and Practice*. New York: CRC Press.
- Vacca, J. R. (2002). *Computer Forensics: Computer Crime Scene Investigation*. Hingham, MA: Charles River Media
- c. Relevant Periodical Sources:**
American Society for Industrial Security, International. *Security Journal*.
American Society for Industrial Security, International. *Security Management*.
Business News Publishing Company. *Security*.
Federal Bureau of Investigation. *The Law Enforcement Bulletin*.
[Http://www.wired.com](http://www.wired.com). *Wired*.
- d. Relevant Online Materials (if not noted above):**
American Society for Industrial Security, International: <http://www.asisonline.org>
Computer Security Organizations: www.sans.org
Federal Bureau of Investigation: <http://www.fbi.gov>
Improving CyberSecurity Research in the United States:
http://www7.nationalacademies.org/cstb/project_cybersecurity.html
Journal of Security Administrators: www.wiu.edu/users/mfkac/jsa
National Security Agency: <http://www.nsa.gov>

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Graduate
SECU 655

Society of Competitive Intelligence Professionals: www.scip.org

17. Enrollment and Scheduling: This course will be offered once a year with a minimum of 10 students and a maximum of 25 per class.

18. Resources:

- a. Supplies & Materials: Smart Board and/or projector for power point, blackboard, chalk and erasers
- b. Equipment:
 - 1.) Smart board and/or projector for power point
 - 2.) Dedicated Information Technology Classroom
- c. Space Allocation: Dedicated space to handle information technology/cyber security laboratory classroom as instructors will need the latest hard and software that will enable them to provide students with the knowledge, skills and abilities necessary in this field

19. Budget: The department's current budget will need to be augmented to cover cost of laboratory classroom and materials.