Syllabus: INT684 Foundations of Information Systems Security

Instructor Information

Name: Keyu Jiang, Ph.D.
Department: Information Networking and Telecommunications
Contact information: email: kjiang@fhsu.edu
Phone: 785.628.4684
Fax: 785.628.4098
Web Site: blackboard.fhsu.edu

Online Resources:

Please refer to https://sites.google.com/site/professorjiang/ia-links.

Course Description:
This course is intended as an introduction of the many facets of information security. It approaches information security from a holistic perspective and emphasizes that security encompasses more than just hardware and software. The course provides an introduction to the technological tools used to protect information including software, hardware, and network tools. It also addresses protocols, processes, human systems, security management practices, and other non-technological elements. This course introduces the upper division/graduate sequence in information assurance.

Foundations of Information Systems Security is intended as an overview of the many facets of Information Security. This course will enable the student to see the information security “big picture” more clearly and that security encompasses more than just hardware and software. The student will also be exposed to career possibilities that were not visible to them before.

This course is developed loosely around the Common Body of Knowledge required to become a Certified Information Systems Security Professional (CISSP). A CISSP is required to provide documented evidence of a minimum of three (3) years of experience working in various areas of Information Security. This course is not intended as a CISSP boot camp. The ten (10) areas covered in the CISSP Common Body of Knowledge are areas that would benefit people working in or pursuing jobs in Business, Management, Computer Science, Management Information Systems, Telecommunications, Data Communications, Networking, Engineering Technology, Security, Government, Legal, Law Enforcement, and even Healthcare Management; to name a few.


Course Requirements: Complete all online assignments, quizzes, and exams, and participate in online problem solving and discussion. All instruction will take place via the Blackboard website. Each week, you will be directed toward new course materials, assignments, discussions and assessments. Students are required to do course work at the level of the degree for which they are enrolled. This is especially true for the written assignment for this course. Graduate students will complete assignments in addition to those of undergraduate students.
For Graduate Students: You will be required to perform at a level significantly higher than that required of undergraduate students. Your work will be required to show mastery of the subject matter; your assignments will be required to show thorough research and demonstrate a comprehensive, synthetic viewpoint of the subject matter and original, important thought. Your assignments will be graded using higher standards than the standards used in grading upper division undergraduates taking this course.

Graduate students are required to write a research paper. Papers should be at least 15 pages long, single spaced, 12 font of Time New Roman, in APA format with at least 15 references. The instructor reserves the right to require revisions to the paper. This is a required assignment for all students enrolled in graduate sections of this course. Failure to complete a satisfactory research paper will prevent the student from passing the course.

**Evaluation:** Will be based on quizzes, assignments, discussion participation, a paper and exams. The grading scale is as follows:

A=90-100  
B=80-89  
C=70-79  
D=60-69  
U=0-59

**Attendance:** Attendance will be based on your participation in online discussion and on your timeliness in turning in assignments. You should check the web site at least once a week. New announcements and assignments will be posted every Monday, and the assignments will usually be due before the midnight on the following Monday, if not other specified. If you have an emergency that will keep you from getting an assignment done on time, send an email to let me know.

**ADDITIONAL INFORMATION / INSTRUCTIONS**

Some additional readings included in the course schedule may require you to use the library's website as well. I also reserve the right to add or change readings during the course of this class. FHSU’s Blackboard system will serve as the backbone of this class. Since you have enrolled for this virtual course, I assume you are proficient enough with Blackboard to use it. If you are not, it is your responsibility to learn the login and navigation procedures of the Blackboard system. Please call 1-800-628-FHSU for technical support or e-mail mailto: support@fhsu.edu. As the instructor of this class, I have no technical expertise in Blackboard. Any technical questions should be directed to the Support staff, and not me.

**ACCESSIBILITY**
Fort Hays State University will ensure that no qualified person with a disability is denied the benefits of, excluded from participation in, or otherwise subjected to discrimination because of inaccessibility of education programs and activities operated by Fort Hays State University. To obtain information as to the existence and location of services, activities, and facilities that are accessible to persons with disabilities, contact the Director of Affirmative Action.

ACADEMIC HONESTY
Membership in the FHSU learning community imposes upon the student a variety of commitments, obligations and responsibilities. It is the policy of FHSU to impose sanctions on students who misrepresent their academic work. Classroom instructors will select appropriate sanctions or other designated persons consistent with the seriousness of the violation and related considerations.

Examples of academic dishonesty include but are not limited to: (1) Plagiarism, taking someone else’s intellectual work and presenting it as one’s own (which covers published and unpublished sources). Using another’s term paper as one’s own; handing in a paper purchased from an individual or agency; submitting papers from living group, club or organization files; or using another’s computer program or document are all examples of plagiarism. Standards of attribution and acknowledgment of literary indebtedness are set by each discipline. In political science, students must cite all work from which they take any recognizable length of work, including but not limited to phrases, sentences, and data. Students should consult with their department or with recognized handbooks in their field if in doubt. (2) Cheating is unacceptable in any form. Examples include consultation of books, library materials or notes during tests without the instructor’s permission; use of crib sheets or hidden notes; intentional observation of another student’s test; receipt of a copy of an exam or questions or answers from an exam to be given or in progress; substitution of another person for the student on an exam or another graded activity; deliberate falsification of lab results; submission of falsified data; alteration of exams or other academic exercises; and collaboration on projects where collaboration is forbidden. (3) Falsification, forgery or alteration of any documents pertaining to assignments and examinations. (4) Students who (cooperate or in other ways promote) participate in promoting cheating or plagiarism by others (or who take credit for the work of others) will also be in violation of this policy.

Students participating in any violation of this policy must accept the consequences of their actions. Classroom instructors and/or university review/appeals committees and administrators will assess the sanctions for violation of this policy. The seriousness of the violation will dictate the severity of the sanction imposed.

Academic sanctions may include but not be limited to any of the following: (a) verbal or written warning; (b) lowering of grade for assignment/activity; (c) lowering of term grade; (d) failure of class assignment. Administrative sanctions may include but not be limited to either of the following: (a) suspension from the University; (b) dismissal from the University I take academic
honesty as the bedrock of collegiate work, and I will not accept cheating in any way, shape, or form. My personal policy is to give students grades of “U” (unsatisfactory, or fail) for both the assignment AND the course. Any incident of plagiarism is subject to the perpetrator’s immediately removal from class and failure.
Tentative Course Schedule:

**Week One** - Overview of Information Systems Security, CISSP and the ten domains of the Common Body of Knowledge.

**Week Two** - Security trends to include its evolution as related to computing; information warfare; the layered approach to security; and politics that affect security.

**Week Three** - Security management practices to include management responsibilities; security principles; risk management and analysis; security roles; and personnel security issues.

**Week Four** - Access Control including identification methods and technologies; biometrics; authentication methods, models and technologies; accountability, monitoring and auditing practices; and possible threats to access control practices and technologies. First quiz.

**Week Five** - Security models and architecture including trusted computing base and security mechanisms; components within an operating system; security models used in software development; security criterion and ratings; and certification and accreditation processes.

**Week Six** - Physical Security to include administrative, technical and physical controls; facility location, construction and management; physical security risks, threats and countermeasures; electrical issues and countermeasures; fire prevention, detection and suppression; and authenticating individuals and intrusion detection.

**Week Seven** - Telecommunications and networking security to include OSI model, TCP/IP and other protocols; LAN, WAN and MAN technologies; cabling and data transmission types; network devices and services, intranets and extranets; telecommunication protocols and devices; remote access methods and technologies; and wireless technologies. Second quiz.

**Week Eight** - Midterm exam

**Week Nine** - Security paper information, discussion and topics posted.

**Week Ten** - Cryptography including its history; components and their relationships; government involvement; symmetric and asymmetric key cryptosystems; public key infrastructure; hashing algorithms; and types of attacks on cryptosystems.

**Week Eleven** – Disaster recovery and business continuity to include business impact analysis; operational and financial impact analysis; Contingency planning requirements; disaster and contingency plans; and backup and off-site facilities.

**Week Twelve** - Law, Investigation, and ethics including ethics pertaining to security professionals and best practices; computer crime and laws; motivations and profiles of attackers; computer crime investigation process and evidence collection; incident-handling procedures; and laws and acts in effect to fight computer crime.
**Week Thirteen** – Application and system development to include different types of software controls and implementation; database concepts and security issues; data warehousing and mining; software life cycle development processes; change control concepts; object-oriented programming components; and expert systems and artificial intelligence. Third quiz.

**Week Fourteen** – Operations security to include administrative management responsibilities; product evaluation and operational assurance; trusted recovery states; e-mail security; and threats to operational security.

**Week Fifteen** – Security policies, information systems security update and related information/links.

**Week Sixteen** – Fourth quiz. Security paper due.

**Week Seventeen** – Final Exam

**Online Resources:**
please refer to https://sites.google.com/site/professorjiang/ia-links.