Applied Information Security
IST 522 – Spring 2009

Instructor

Joseph V. Giordano

Office:	N/A
Office Hours:	Schedule by LMS email for appointment
Phone:	(315) 733-4818
Email:	Use LMS exclusively

Course Meeting Time & Place

This is an on-line course. On-line discussions are asynchronous in this course.

Prerequisites

This course requires fundamental knowledge of information systems and information systems security. Enrolled students are expected to acquire basic knowledge in computer hardware, information systems and network prior to attending this course. The prerequisite includes IST 623/423: Introduction of Information Security, unless pre-approved by the instructor.

Course Description

The objective of this course aims at exploring threat phenomenon, security techniques and advanced information security applications in the context of computer forensics. An organization not only needs to proactively understand different types of threats, and adopt techniques and applications in defending its information assets, but should also be sensitive to preserving digital evidence when a cyber crime occurs. By successfully completing this course, students will gain knowledge in the following subject areas: cyber warfare, cyber terrorism, human threats, technological threats (such as phishing, spamming, etc.), digital forensics for mobile devices, host security, non-host security techniques (such as steganography, Digital Rights Management, and biometrics), network security, e-commerce security, wireless security, peer-to-peer (P2P), grid security, and the social responsibilities of information security professionals.

Quizzes and lab exercises will be given throughout this course. In addition to the labs and hands-on exercises found in the required textbook, we will adopt the labs that were originally designed by Sonia Glumich of the Air Force Research Laboratory. The lab book can be found under Course Content on WebCT.

Textbooks and Readings

Required Textbook:

- Volonino, L., Anzaldua, R., and Godwin, J. (2007). *Computer Forensics: Principles and Practices*. Prentice Hall. ISBN-10: 0-131-54727-5.

Assignments & Grading

Your course grade depends on the following activities:

ACTIVITIES	POINTS
Weekly Threaded Discussions	10 points
Quizzes (Three, worth 10 points each)	30 points
Labs (Four, worth 10 points each)	40 points
Final Research Paper/Lab/Exam (Notify me of your choice)	20 points
TOTAL	**100 POINTS**

Attendance, Class Participation, & Group Projects

- Students are expected to submit all assignments before or on the due date. Late submission is allowed up to one week but with a penalty up to 5% per day.

- Students should turn in a Word file of their assignments (reflective paper, extended abstract, research paper, etc.). Please submit your assignments to the instructor via e-mail with the Learning Management System (LMS) of the School of Information Studies at Syracuse University before the deadline.

- Students can continue threaded discussions after the deadline, but the instructor will take only those inputs posted before the deadline for grading.

- The lab exercises are group assignments. Groups should be formed during the first two weeks of on-line discussions.

- For the individual research project, each student is required to write a research paper on a topic of their choosing. Each student is required to submit a research proposal, an extended abstract, and the final research paper on the due dates.

Descriptions and Formats of Major Course Deliverables

Threaded Discussions:

- There will be weekly threaded discussions. Discuss, describe and analyze major topic areas in applied information security. The quality of your discussions and contributions are measured and evaluated. Strong weekly participation is encouraged. The quality of your discussions will be tallied up at the end of the semester and will be worth up to 10 points of your final grade. I may decide to assign discussion leadership duties to new students each week. It will be your duty to start the discussion by coming up with relevant points and issues that need to be looked at.

Quizzes:

- Three quizzes are given throughout the semester. Each quiz will be worth ten points. You are expected to work on your own. Quizzes shall be taken and are graded on the LMS. Deadlines for each quiz are tentatively scheduled by midnight Saturday of the test-week.

Lab Work:

- Students will perform the lab or hands-on exercise, record the lab results and findings, and discuss their methodology, interpretation and implication of the lab work. **Option: Labs can be worked in groups.**

Research Project:

- A security topic will be selected by each individual (You can propose a topic for the paper or if you want I can provide you with a list of suggested topics).
- Extended Abstract:
  - Describe your research plans.
  - Less than 3 pages, double-spaced, 12-font size, 1 inch margins, Times New Roman.
  - Include abstract (less than 300 words), brief description of sections/subsections (e.g., related work, problems, your new approaches, future work, conclusions, etc.), and references (at least five references from published journals or conference proceedings).
- Final Paper:
  - ⌖10 pages, double-spaced, 12-font size, 1 inch margins, Times New Roman. APA or MLA citations.
  - Include abstract (less than 300 words), full description of sections/subsection, and references.

In lieu of the Final Research Paper, students can either work on another hands-on Lab or take a Comprehensive Final Examination. (Note: permission of the instructor is required.)

Course Calendar

WEEK	TOPICS	READINGS/ASSIGNMENTS
1 12 Jan	Forensic Evidence and Crime Investigation	Chap 1
2 19 Jan	Digital Detective Work	Chap 2 LAB #1 (Exercise 2.1)
3 26 Jan	Tools, Environments, Etc…	Chap 3 QUIZ #1
4 2 Feb	Policies and Procedures	Chap 4
5 9 Feb	Data, PDA, and Cell Phone Forensics	Chap 5
6 16 Feb	Operating Systems and Data Transmission Basics for Digital Investigations	Chap 6 QUIZ #2
7 23 Feb	Investigating Windows, Linux and Graphics Files	Chap 7
8 2 Mar	E-Mail and Web Mail Forensics	Chap 8 LAB #2 (Project 8.3)
9 16 Mar	Internet and Network Forensics and Intrusion Detection	Chap 9 LAB #3 (Project 9.1)
10 23 Mar	Tracking Down Thos Who Intend to Do Harm	Chap 10
11 30 Mar	Fraud and Forensic Accounting	Chap 11 QUIZ #3

12 6 Apr	**Steganography, Message Digests and Digital Investigations**	**LAB #4**
13 13 Apr	**Biometrics and Insider Threat**	
14 20 Apr	**Wireless, P2P and E-Commerce Security**	
15 27-28 Apr	**Spam**	
FINALS 30 Apr – 6 May	**Final Research Paper, Lab, or Comprehensive Exam**	

Academic Integrity

The academic community of Syracuse University and of the School of Information Studies requires the highest standards of professional ethics and personal integrity from all members of the community. Violations of these standards are violations of a mutual obligation characterized by trust, honesty, and personal honor. As a community, we commit ourselves to standards of academic conduct, impose sanctions against those who violate these standards, and keep appropriate records of violations. The academic integrity statement can be found at:

http://supolicies.syr.edu/ethics/acad_integrity.htm

Student with Disabilities

In compliance with section 504 of the Americans with Disabilities Act (ADA), Syracuse University is committed to ensure that "no otherwise qualified individual with a disability…shall, solely by reason of disability, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or

activity…" If you feel that you are a student who may need academic accommodations due to a disability, you should immediately register with the Office of Disability Services (ODS) at 804 University Avenue, Room 308 3rd Floor, 315.443.4498 or 315.443.1371 (TTD only). ODS is the Syracuse University office that authorizes special accommodations for students with disabilities.