GRADUATE COURSE SYLLABUS

Introduction to Information Security (IST623)

Course Author: Dr. Joon S. Park, PhD.
Office: 334 Hinds Hall
Phone: (315) 443-6887
Email: jspark@syr.edu

Live Session Instructor: Benson M. Poikayil
Email: bpoikayi@syr.edu

Course Description

This 3-credit undergraduate course (IST623 Introduction to Information Security) is intended to teach fundamental elements in information security and introduce the key areas of security challenges, countermeasures, and real-life examples. The course will focus on a comprehensive understanding of information security rather than a specific security area. Topics include security properties, vulnerabilities, cryptography, security policies, access control, authentication, firewalls, wireless security, Internet security protocols, security management, security evaluation, and case studies. Students will also have hands-on experiences in information security through online labs.

Prerequisite / Co-requisite:
None

Credits:
3 credits

Learning Objectives

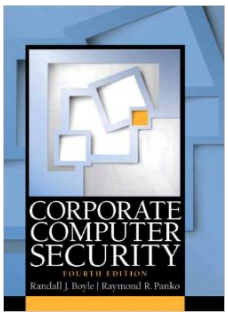
After taking this course, the students will understand the comprehensive aspect of information security and be able to:

- Explain the fundamental security properties, challenges, countermeasures, and real-life examples.
- Describe the key concepts, technical elements, and their tradeoffs in cryptography, access control, authentication, wireless security, firewalls, Internet security protocols.
- Explain in-depth security knowledge and skills in the security case studies that they selected.
- Demonstrate the hands-on ability in host protection, cryptography, secure communication, and network security analysis, using various security services and tools.
- Exhibit the ability in research, presentation, and Q&A discussion about information security.
- Begin to develop specialty on a specific area of information security in their further study and career preparation, extending the knowledge and skills learned from this course.

Course Materials

This introductory course in information security is intended to teach the comprehensive concepts and core elements in the area. Therefore, there is no single book that covers all the topics of the course. We will use the lecture materials developed by Dr. Park for this course and the textbook along with additional resources.

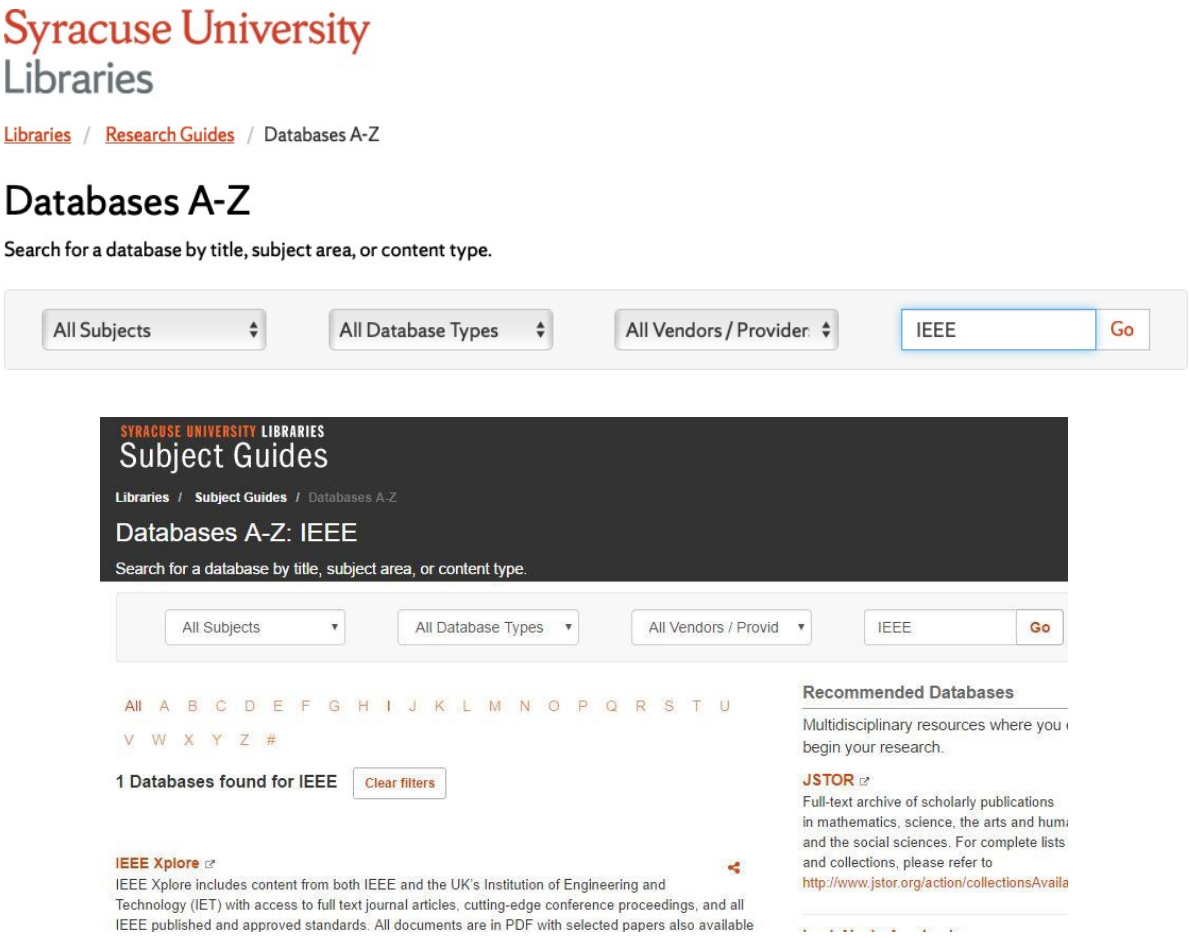
- Textbook
  - Corporate Computer Security (4th Edition)
    Authors: Randall Boyle and Raymond Panko
    ISBN-13: 978-0133545197
    ISBN-10: 0133545199
    Available through the Syracuse University Bookstore and other online bookstores.
  - In addition to the lecture slides and the textbook, additional class materials may be posted within the course LMS.



- Online labs
  - Each student is required to purchase the lab access code in order to conduct the online labs throughout the course. Cost: $60, ISBN: **9781284193077**.
  - For ordering and access, please refer to the instruction posted within the course LMS.
  - You will be required to provide the Course ID **8B726D** for the process.
  - Once you log in the lab environment, you can use the online labs for this course anytime.

- Recommended search engines for research articles
  - ACM Digital Library
  - IEEE Xplore
  - CiteSeer (http://citeseer.ist.psu.edu/)

- Note: In order to access the digital libraries with the university's license, your access should start from Syracuse University Libraries (http://library.syr.edu/). You may need to select Databases under the Search field and find/select a specific database (e.g., ACM Digital Library or IEEE Xplore) first. I entered "IEEE" and found "IEEE Xplore" in the example screen below.) If your current machine does not use an SU IP (say, you are using a home machine), you will be asked to log in with your SU NetID. Then, you can use the database for your search.



Course Requirements, Deliverables and Expectations

Activities	Points	Weight
Assignments	#1—Short Biography: 4 points #2—BLP Analysis: 5 points #3—SKC vs. PKC: 6 points #4—IPsec Modes: 7 points #5—P/F Firewalls vs. Proxy: 8 points	30%
Hands-on Labs	#1: 5 points #2: 7 points #3: 8 points	20%
	Bonus Lab (Optional): 3 points	
Case Study (Group)	Presentation: 20 points TME: 10 points	30%
Class Participation	20 points	20%
Total		100%

Working Groups: Through the group activities in the course, all the students will have valuable experience working with group members for their case studies. The quality outcomes of the group activities can be counted for part of your professional career development. Typically, working groups will be formed in the second week of the course. Each team typically includes three to five students, with four being the ideal number.

Assignments (Individual): Each student has a total of 5 assignments that they are required to submit for this course. Three of these are setup as discussions and two are report submissions. Assignment information and deadlines can be found within the Assignment section on LMS.

Hands-on Labs (individual): Each student will conduct hands-on labs in the online lab environment based on the class contents. Lab instruction can be found within the LMS Toolbox. Each student is required to submit the lab report after each lab. Deadlines for each lab report can be found within the Assignment section on LMS.

Class Participation (Individual): Students are expected to complete the asynchronous coursework before the live session. When you have reviewed the weekly session within the coursework, you should check the **Mark As Complete** button in the upper right corner of the page. Each student will need to participate in weekly discussions about current events related to cyber security within the Wall on 2U. You can briefly discuss about some recent news, security related article you found interesting, or even about something you learned from a class session/readings during the course. Students are also expected to attend all the synchronous/live sessions and participate in discussions. These activities will be tracked on LMS and factored into the student grade.

Case Study (Group): Each group is required to choose a research topic and present its research outcomes to the class in Week#9 Live Session.

- The topic can be in all aspects of security/privacy-related specific cases. For instance, topics of interest may include, but are not limited to, major security breaches or critical security vulnerabilities that occurred in the last 3 years, security tools analysis, study of threat groups, and other security/privacy related cases.
- At the end of the course, each group is required to present its final research outcomes to the class and facilitate the Q&A session about the topic (about 25-30 minutes per group including Q&A).
- Each presentation should cover the key points of the chosen topic, lessons learned, and at least five references (e.g., published news, journal articles, conference proceedings, online resources, etc.) relevant to the topic, providing the URL, PDF, or other reference information.
- Each group is required to post their presentation materials (e.g., slides, URL links, video/audio clips, etc.) to the course LMS within the assignment section 24 hours

before the live class presentation day so that the other students can preview them before the class. No other submission is required.

TME (individual): Group work needs a team effort by the members. Each member is required to contribute individually to a whole. To encourage each member's active participation in the group activities and produce a fair grading result, **each student** is required to submit his/her TME (Team Member Evaluation) at the end of the semester, considering self/peer contribution to the group work throughout the semester. TME is an individual evaluation. The instructor will take your TME very seriously for grading each student's group work. You must not share your TME with others. The TME form and the rubric will be available within the course LMS. I would like to urge you to start working with your group members for the group activities as soon as possible so that each member can spend sufficient time on his/her contribution to the team.

Grading

Grades	Grade points /credit	Total Points Earned
A	4.000	90-100
A-	3.667	85-89
B+	3.333	80-84
B	3.000	75-79
B-	2.667	70-74
C+	2.333	65-69
C	2.000	60-64
C-	1.667	55-59
F	0	Below 55

University Attendance Policy

Attendance in classes is expected in all courses at Syracuse University. Students are expected to arrive on campus in time to attend the first meeting of all classes for which they are registered. Students who do not attend classes starting with the first scheduled meeting may be academically withdrawn as not making progress toward degree by failure to attend. Instructors set course-specific policies for absences from scheduled class meetings in their syllabi.

It is a federal requirement that students who do not attend or cease to attend a class to be reported at the time of determination by the faculty. Faculty should use "ESPR" and "MSPR" in Orange Success to alert the Office of the Registrar and the Office of Financial Aid. A grade of NA is posted to any student for whom the Never Attended flag is raised in Orange SUccess. More information regarding Orange SUccess can be found here, at: http://orangesuccess.syr.edu/getting-started-2/
Students should also review the University's religious observance policy and make the

required arrangements at the beginning of each semester

Course Policies

Notification of changes

All class announcements, changes to the syllabus or class schedule will be done through 2U Wall. Additionally, most of the course assignments are done through 2U as well. It is your responsibility to check for updates regularly.

Acknowledgement

This class will provide you with knowledge related to computer security and its associated vulnerabilities. Please be aware that the intent of this class is to give you an understanding about computer security and how it works in the corporate environment. There are many local, state and federal laws that prohibit the unauthorized access of another an electronic device. Failing this class because you hack into someone's computer could be the least of your concerns.

Assignment Submission

Please submit assignments as directed. All the assignments should be submitted through Wall as Microsoft Word documents. E-mail attachments and hard copies will not be accepted. Assignments should be prepared in a professional manner according to the submission guidelines and with correct spelling and grammar.

Late Submission

Considering the real-world constraints and professional responsibilities at work, students are required to submit all the assignments before or on the due date. The deadlines are firm. Late submissions will not be accepted.

Make-up Condition

Make-up assignments will only be allowed if the student can provide a formal documentation through the corresponding office. If you are having problems in keeping up with the class, you should contact the instructor immediately so that appropriate arrangements can be made as soon as possible.

Class Participation

Real-world professionals are expected to attend and participate in all meetings that are concerned with the work. Therefore, weekly Live Session attendance with **your full video connection is required**. Live session participation with Audio-only or video-paused (no streaming) may negatively affect your point. If you arrive late or leave early, you will be marked absent. Your active and constructive involvement with the asynchronous content and live class sessions will help to ensure that you receive the most benefit from this class.

Non-attendance in class for part of the semester will be reflected in a decrease in this grade (and most likely in other grades as well). There are no excused absences unless documented by the university.

Course Evaluations

There will be an end of course evaluation for you to complete this term. This evaluation will be conducted online and is entirely anonymous. You will receive an official notification in your email account with the evaluation website link and your passcode. Please take the time and fill out this evaluation as your feedback and support of this assessment effort is very much appreciated. The school carefully reviews ratings and comments that you submit, and these factor into decisions about course, program and instructor development.

Syracuse University Policies

Students should review the University's policies regarding: Diversity and Disability https://www.syracuse.edu/life/accessibility-diversity/; the Religious Observances Notification and Policy- http://supolicies.syr.edu/studs/religious_observance.htm; and Orange SUccess - http://orangesuccess.syr.edu/getting-started-2/

Disability-Related Accommodations

Syracuse University values diversity and inclusion; we are committed to a climate of mutual respect and full participation. There may be aspects of the instruction or design of this course that result in barriers to your inclusion and full participation in this course. I invite any student to meet with me to discuss strategies and/or accommodations (academic adjustments) that may be essential to your success and to collaborate with the Office of Disability Services (ODS) in this process.

If you would like to discuss disability-accommodations or register with ODS, please visit their website at http://disabilityservices.syr.edu./ Please call (315) 443-4498 or email disabilityservices@syr.edu for more detailed information.

ODS is responsible for coordinating disability-related academic accommodations and will work with the student to develop an access plan. Since academic accommodations may require early planning and generally are not provided retroactively, please contact ODS as soon as possible to begin this process.

Academic Integrity Policy

Syracuse University's Academic Integrity Policy reflects the high value that we, as a university community, place on honesty in academic work. The policy defines our expectations for academic honesty and holds students accountable for the integrity of all work they submit. Students should understand that it is their responsibility to learn about course-specific expectations, as well as about university-wide academic integrity expectations. The policy governs appropriate citation and use of sources, the integrity of work submitted in exams and assignments, and the veracity of signatures on attendance

sheets and other verification of participation in class activities. The policy also prohibits students from submitting the same work in more than one class without receiving written authorization in advance from both instructors. Under the policy, students found in violation are subject to grade sanctions determined by the course instructor and non-grade sanctions determined by the School or College where the course is offered as described in the Violation and Sanction Classification Rubric. SU students are required to read an online summary of the University's academic integrity expectations and provide an electronic signature agreeing to abide by them twice a year during pre-term check-in on MySlice.

Educational Use of Student Work

Student work prepared for University courses in any media may be used for educational purposes, if the course syllabus makes clear that such use may occur. You grant permission to have your work used in this manner by registering for, and by continuing to be enrolled in, courses where such use of student work is announced in the course syllabus. I intend to use academic work that you complete this semester for educational purposes in this course during this semester. Your registration and continued enrollment constitute your permission. I intend to use academic work that you complete this semester in subsequent semesters for educational purposes.

University Enrollment Policy

Only officially registered students are allowed in this course. University policy prohibits students from attending, being evaluated, auditing, or participating in regular semester courses without being officially enrolled.

Schedule Change

The course schedule is a plan, which may be changed.

Course Schedule:

PLEASE NOTE – Class schedule maybe subject to change. Change will be announced in class and on LMS.

Week No.	Topics	Class Activities/Assignments	Readings	Assignments Due*
#1 Oct 6th	Course Overview and Syllabus Introduction (Security Properties, Security Trends)	Ice Breaker Assignment #1 (Short Biography)	Lecture Materials Textbook: Chap.1.1–1.3	**Assignment #1(Short Bio)** **Due: Oct 10th**
#2 Oct 13th	Security Policies (Security Policy Levels,Principles, Examples, Security vs. Privacy)	Form ResearchGroups	Textbook: Chap.2.5-2.7	
#3 Oct 20th	Security Models (Access Control Models, BLP Rules,RBAC Concepts)	Assignment #2 (BLP Analysis)	Lecture Materials Textbook: Chap.5.1, 5.7	
#4 Oct 27th	Secret Key Cryptography (Operational Scheme,Basic Algorithms, Attack Analysis)	Lab #1 – Host Protection Research Proposal (5mins)	Lecture Materials Textbook: Chap. 3.1–3.2	**Assignment #2**
#5 Nov 3rd	Public Key Cryptography (Operational Schemes,Number Theory, BasicAlgorithms, Digital Hashes, Digital Certificates)	Assignment #3(SKC vs. PKC)	Lecture Materials Textbook: Chap.3.6–3.7	**Lab #1 Report**
#6 Nov 10th	Authentication (Passwords, One-Time Passwords, Biometrics, Cryptographic Techniques, Kerberos)	Lab #2 – Cryptography	Lecture Materials Textbook: Chap.5.3–5.6	**Assignment #3**

#7 Nov 17th	Internet Security Protocols (SSL/TLS, IP Tunneling, IPsec)	Assignment #4 (IPsec Modes) Bonus Lab	Lecture Materials Textbook: Chap. 3.10–3.11	**Lab #2 report**
Nov 24th	Thanksgiving Break			
#8 Dec 1st	Security in WirelessNetworks (WirelessNetwork Attacks, Wireless Security Protocols, Comparison)	Lab #3 – Network Security Analysis	Lecture Materials Textbook: Chap. 4.6	**Assignment #4** **Bonus Lab Report**
#9 Dec 8th	Case Study Dissemination	Case Study Q&A	Group Presentations	**Each Group's Presentation Materials - Due 24 hours before class** **Lab #3 report**
#10 Dec 15th	Firewalls (Packet Filtering Firewalls,Proxy) and Course wrap up	Assignment #5 (P/F Firewalls vs.Proxy) Final Submissions Course Evaluation	Lecture Materials Textbook: Chap. 6.1–6.3, 6.5	**Assignment #5** **TME**