SRA 221: Fundamentals of Information Security

Spring 2017 - 3 Credits

Course Prerequisite: IST 110 & CMPSC 101 (Or IST 297D)
Section 003
Class Time and Room: M W F 1:25 PM – 2:15 PM
Professor: Dr. Stan Aungst, B.A., B.A., M.A., M.B.A., Ph.D.
sga103@psu.edu
Office Hours – Friday 1:30pm-2:30pm & by appointment

Teaching Assistant: 
Office Hours – By appointment

Office Hours –TBD

A detailed schedule of this course will be posted in a separate document on Angel (Which will include but is not limited to, lecture schedule, due dates, quiz dates, labs, etc.). This is subject to change and it is your responsibility to stay up to date with the schedule.

Course Description:

This course provides a basic understanding of the fundamentals of information security. This includes an introduction to security architectures, threats, worms and viruses, physical security, access control, multifactor authentication, and designing secure applications for mobile devices and remote access (E2E security is emphasized).

Students will also be introduced to the basic topics and principles of information security, general security concepts, risk management, and other interrelated methods of information security. These include such things as the impact of physical security on network security control and wireless security operations in business, government and information warfare (Cyberwars). Also standards (IEEE, NIST, FIPS, Suite B compliance recommended by NSA.) protocols, hacks/cracks, malware/defense, Intrusion Detection Systems (IDS, host and network), trusted systems, and cryptography including public key infrastructure (PKI) and digital signatures, encryption algorithms (RSA and ECC) and their performance metrics will be discussed and measured.
Students will also be introduced to disaster recovery plans, business continuity and organizational policies, and the social and legal issues of information security. Finally, time permitting and student interest being present, secure RFID’s or Passport security architectures and methods will be introduced to the students.

This course has a required separate laboratory (hands-on) component which will reinforce the concepts taught in the lectures and assist the teams for completing their required project.

**Course Texts:**

Required:


Recommended reading and a more technical intermediate text:

- **Practical Cryptography**, Niels Ferguson, Bruce Schneier, 2003

**Course Objectives:**

- Understand basic security concepts, security architectures, models, and methods of information security.
- Develop an understanding of information security in relationship to computer operating systems, wired and wireless networks, information systems, and applications including mobility.
- Gain a familiarity with prevalent cyber-attacks and defenses.
- Gain an understanding of protocols and standards and their importance.
- Develop a basic understanding of cryptography, its history and significance, and the cryptographic architectures that are utilized in the government, the military, and industrial settings.
- Real world Hybrid Computing Implementations.
- Develop an understanding of security policies and the associated security management issues including physical security.
- Develop an understanding of the social and legal issues of security and privacy.
- Awareness of current and future trends in information and cyber security.

**Course Methodology:**

I hear and I forgot
I see and I remember
I do and I understand
Kung Fu Tzu (Confucius)

This course will incorporate collaborative and action-learning experiences virtually and in a computer lab. In addition, emphasis will be placed on developing and practicing writing and speaking skills through application of the concepts that define the course. Additional information will be found in a separate lab document.

A combination of hands-on exercises (lab assignments), quizzes, group projects (report and presentation), and class participation will be used for evaluation. Individual, team assignments, and a peer review at the end of the semester will form part of the basis for evaluation.

Guest Speakers on their particular areas of expertise will be presented to the class to enrich the student’s knowledge. This will also give the students the opportunity to ask questions to practitioners in the field of Security and Communications.

The success of the learning endeavor rests on several factors which include the level of direct involvement on the part of the student. It takes more than sporadic and passive attendance at a lecture to learn a technical complex subject. To truly learn and understand all of the elements of a complex issue, it requires exploration that comes from intimate involvement with the material.

Computer Security is a complex subject with many composite domains, overlapping principles, and highly specific, detailed technical aspects. Developing skilled professionals in computer security requires that several components be addressed, namely technical and principal-based knowledge coupled with practical experience.

**Grading and Calendar of Events**

N.B. A major component of the course will be several hands-on exercises, quizzes, and a final team-based written and orally presented project. This course will incorporate collaborative and action-learning (computer lab) experiences wherever appropriate. Emphases will be placed on developing and practicing writing and speaking skills through application of the concepts, theories and technologies that define the course.

**Grading**

<table>
<thead>
<tr>
<th>Category</th>
<th>Point Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attendance</td>
<td>60 Points</td>
</tr>
</tbody>
</table>
Quizzes (5, lowest dropped)  20 each x 5 = 100 points
Monster Quiz on Cryptography (Not dropped)  50 points
The Athens Affair  100 points
Labs  10 each x 6 = 60 points
Team Project (Oral)  50 points
Team Project (Written)  150 points

TOTAL Points Possible  570 points

Letter Grading

<table>
<thead>
<tr>
<th>Score Range</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>94-100</td>
<td>A</td>
</tr>
<tr>
<td>90-93</td>
<td>A-</td>
</tr>
<tr>
<td>87-89</td>
<td>B+</td>
</tr>
<tr>
<td>84-86</td>
<td>B</td>
</tr>
<tr>
<td>80-83</td>
<td>B-</td>
</tr>
<tr>
<td>77-79</td>
<td>C+</td>
</tr>
<tr>
<td>70-76</td>
<td>C</td>
</tr>
<tr>
<td>60-69</td>
<td>D</td>
</tr>
<tr>
<td>Below 60</td>
<td>F</td>
</tr>
</tbody>
</table>

Late Work/Missed Quizzes

Late work will only be accepted for full credit if there is either,
A.) Prior approval from the Professor or TA.
B.) A medical document is provided from UHS.

Otherwise late work will only be worth up to half credit and is due 48 hours from the original due date.

Note - **It is your responsibility** to check to make sure submissions were successful. This includes making sure attachments are submitted and ensuring the submission is in the posted drop box. To reduce risk of a submission failing, ensure you are using an angel supported browser.

There will be no makeup quizzes/exams unless there is either,
A.) Prior approval from the Professor or TA.
B.) A medical document is provided from UHS.

Attendance
Attendance for this class will be tracked and count towards your final grade. Attendance will be recorded by putting in the pin under the ANGEL resources tab. The pin will be provided in class and is not to be shared with anyone. Any sharing of the pin will result in an academic integrity violation. You will be provided three unexcused days in the semester, which will not negatively affect your grade. Any unexcused absences after the third will deduct 2 points from your attendance grade. The professor or the TA must approve excused absences prior to the start of class.

**Project Overview**

SRA 221 Overall Project Requirements are included in a separate document (Summary and Detailed)

A Team Contract will be signed after the drop period to ensure team integrity and responsibilities for the Team Project requirement and deliverables.

**Project Deliverables**

Project Proposal (Due during the Third Week of Class) Give to TAs before starting your project. For this proposal, each team needs to research possible communication applications that can be implemented in the given time constraint of the semester. The purpose of this activity is for students to gain experience working with open source technologies and researching vulnerabilities that exist within various implementations. Must be submitted any time after the third week of the semester.

It is the team’s responsibility to provide the client with detailed summary of the solution including, but not limited to, initial requirements documentation, memorandum of understanding, detailed setup instructions, and value and risk analysis of the implementation. Additionally, a proposal, setup summary, and security plan for the chosen application should be included. Students will also have to prove to the client that their solution is secure and the information is being encrypted when it is transmitted. The following outlines the information that will need to be compiled and submitted for the final project documentation. The final version of all the documents will be due the last week of class unless otherwise noted. Drafts will be collected and then returned with feedback on most documents. (In addition see project document).

**Preliminary Research**
In order to accomplish this project, it is necessary for each team to gain experience on various secure communication technologies. Therefore, through the semester the labs will be designed to give teams hands on experience with these technologies so that they are better prepared for the final project.

Lab Overview

Lab reports will be due online within a drop box on Angel. Each lab will be setup in a way that will provide students with references and examples so that they can use that knowledge to solve the problems that need to be resolved for the lab. Contact the TAs for assistance with the labs.

Labs, Dates, and Content will be announced and posted on Angel by TAs.

Please note: We will do our best to coordinate Labs to correspond with Lectures. This does not always occur because of technical problems with Virtual Labs.

Academic Integrity

According to the Penn State Principles and University Code of Conduct: Academic integrity is a basic guiding principle for all academic activity at Penn State University, allowing the pursuit of scholarly activity in an open, honest, and responsible manner. In according with the University’s Code of Conduct, you must not engage in or tolerate academic dishonesty. This includes, but is not limited to cheating, plagiarism, fabrication of information or citations, facilitating acts of academic dishonesty by others, unauthorized possession of examinations, submitting work of another person, or work previously used without informing the instructor, or tampering with the academic work of other students. Any violation of academic integrity will be investigated, and where warranted, punitive action will be taken. For every incident when a penalty of any kind is assessed, a report must be filed. This form is used for both undergraduate and graduate courses. This report must be signed by both the instructor and the student, and then submitted to the Academic Dean.

Bottom line – Cheating will not be tolerated. Including Plagiarism. Do your own work. Cheating will be reported immediately to academic integrity.

Affirmative Action & Sexual Harassment
The Pennsylvania State University is committed to a policy that all persons shall have equal access to programs, facilities, admission, and employment without regard to personal characteristics not related to ability, performance, or qualifications as determined by University policy or by Commonwealth or Federal authorities. Penn State does not discriminate against any person because of age, ancestry, color, disability or handicap, national origin, race, religious creed, gender, sexual orientation, or veteran status. Direct all inquiries to the Affirmative Action Office, 211 Willard Building.

**Americans with Disabilities Act**

IST welcomes persons with disabilities to all of its classes, programs, and events. If you need accommodations, or have questions about access to buildings where IST activities are held, please contact us in advance of your participation or visit. If you need assistance during a class, program, or event, please contact the member of our staff or faculty in charge.

**An Invitation to Students with Learning Disabilities**

It is Penn State’s policy to not discriminate against qualified students with documented disabilities in its educational programs. If you have a disability-related need for modifications in your testing or learning situation, your instructor should be notified during the first week of classes so that your needs can be accommodated. You will be asked to present documentation from the Office of Disability Services (located in 116 Bouclé Building, 863-1807) that describes the nature of your disability and the recommended remedy. You may refer to the Nondiscrimination Policy in the Student Guide to University Policies and Rules.

**Computer Use**

The students are expected to comply with PSU Policy AD20, Computer and Network Security.