INF 429: SECURITY AND PRIVACY

Clifford Neuman
bcn@isi.edu

Fall 2017 Syllabus

Time, Days(s) (3 Units)
Room XXX

Instructor's Office Hours:

Day, time room. Other times by appointment.

Teaching Assistant:

Office:
Office Hours:
Contact Info:

IT Help:

Hours of Service:
Contact Info:

Catalogue Description:

INF 429 Security and Privacy (3) Basic concepts in information security and privacy; Implications security and privacy breaches; Security and privacy policies, threats, and protection mechanisms; Security and privacy laws, regulations, and ethics.

Expanded Course Description:

Much of the information managed in computer systems is sensitive and private The ability of an organization to meaningfully collect, store, and use information requires confidence on the part of all organizational stakeholders that the information will be secure: accessible when needed and safe from tampering and compromise. Thus, the security and privacy of information – its confidentiality, integrity, and availability – must be a major consideration in the application of informatics to human communication.

The laws, rules, and expectations of the societies in which an organization operates, and the goals and practices of the organization itself, determine how the organization will manage, protect, and distribute information. They provide the basis for the organization's security and privacy policy. The policy identifies what information is to be protected, why it must be protected, and who (and under what circumstances) may have access to that information. Security and privacy policies, and threats to the enforcement of those policies, ultimately determine the specific measures implemented to protect the

information. Those measures must protect not just the information, but also the system components used to store, process, and transmit the information.

This course covers fundamental problems and principles in the security and privacy information in an interconnected world. Because information processing systems today are overwhelmingly digital, this course places special emphasis on security and privacy in digital systems. The course touches on legal and ethical aspects of security and privacy, security and privacy policies and models, threats to security and privacy, and technical mechanisms for security and privacy enforcement in digital systems. **Case studies based on recent events will be used as much as possible to illuminate the real-world impact of each of the topics covered by the course**.

This class is lecture based augmented by weekly assigned readings, several homework assignments, short in-class quizzes, a project, a midterm and a final.

Course Objectives:

Students will develop the following abilities:

- To *recognize* types of information that have value and that must be protected
- To *describe* current cultural, legal, and ethical concerns about security and privacy in different parts of the world
- To *evaluate* security and privacy needs across organizations and to *synthesize* a security and privacy policy
- To *identify* security and privacy threats to the organization's policy
- To *apply* basic security and privacy controls to enforce the organization's policy

Methods of Teaching:

The primary teaching method will be lectures, discussion, case studies, guest speakers and demonstrations. Students are expected to perform directed self-learning outside of class through literature and case-study review. In addition, students may partake in oral presentations based on homework and assigned literature readings.

The students are expected to take an active role in the course. Students will attend lectures and actively participate in the classroom. They will complete homework, regular exams and quizzes to reinforce the concepts taught and highlight weaknesses in grasp and presentation. They will complete a final semester project to apply and illustrate the concepts in an applied manner.

There will be no laboratory assignments, and no special computing facility, hardware or software will be necessary for this course.

Assignments/Reports:

Students will be required to complete ten homework assignments, which may take 4-6 hours to complete. All homework assignments are to be submitted individually; however students may work in groups to complete the tasks. There is one midterm test and a final exam which date will be determined by the Schedule of Classes. There will be 11 short in-class quizzes. There will be one semester project.

Guidelines and additional information will be developed which will provide a common vernacular for the assignments. It is crucial that students turn in whatever they have on the due date. NO assignment will be accepted late. An incompletes grade will be granted only under the conditions called out in the student handbook, *SCAMPUS*, which is available online, http://scampus.usc.edu.

Semester Project:

The semester project gives each student the opportunity to use and illustrate the concepts from the course in an applied manner in not less than 7 nor more than 15 pages, and will be assigned after the applicable foundational concepts have been covered in class. That assignment will include preparation guidelines and due date.

The project will be for each student to create a privacy and security plan for sensitive information acquired and managed by a large organization. Students will be required to write a plan that satisfies the following requirements:

1. Identify sensitive information acquired and managed by the organization and the legal, regulatory, and social requirements and restrictions on the security and privacy of that data;
2. Write a privacy and security policy for the organization that can be traced to the requirements;
3. Identify threats to that policy; and
4. Describe security controls that could be used to mitigate the threats.

Class Communication:

DEN Blackboard at USC will be used for class communication.

Grading Schema:
Final: 30%
Mid-Term: 25%
Quizzes: 15%
Class Participation: 10%
Homework Assignments: 10%
Semester Project: 10%

Total 100%

The record of class participation is kept by the TA; DEN remote students are made aware

of what is expected of them regarding participation.

Grades will range from A through F. The following is the breakdown for grading. This is the nominal breakdown, meaning that the grade awarded will not be less than indicated:

94 - 100 = A 74 - 76 = C
90 - 93 = A - 70 - 73 = C-
87 - 89 = B+ 67 - 69 = D+
84 - 86 = B 64 - 66 = D
80 - 83 = B- 60 - 63 = D-
77 - 79 = C+ Below 60 is an F

Return of Course Assignments
Returned paperwork, unclaimed by a student, will be discarded after a year and hence, will not be available should a grade appeal be pursued following receipt of his/her grade

Books and Readings:

All books, papers or reports will be available to students in one of three ways: 1) in the USC bookstore or other commercial source; 2) via Course Documents that the instructor will provide on DEN Blackboard; and/or 3) via the web.

Required Reading:

William Stallings, "Computer Security: Principles and Practice

Additional References

Saul Levemore, "The Offensive Internet: Speech, Privacy, and Reputation"

Terence Craig, "Privacy and Big Data"

Julia Lane, "Privacy, Big Data, and the Public Good: Frameworks for Engagement"

Class Structure & Schedule:

Class sequence, dates, topics and guest speakers are subject to change as the semester proceeds. Any revisions will be noted and announced in class.

Week	Date	Topics Covered	Homework	Reading
1		**Course Introduction.** General introduction to class – requirements, schedule, approach, tests,		Stallings 1

		homework, assignments, structural overview of the course of study, grading approach, answer questions. **What is Security and Privacy?** The value of information; Need to protect information; Different roles of technology, law, policy, and ethics.		
2		**Laws, social mores, and ethics**. Sources of security and privacy policies. Cultural differences with respect to security and privacy. Special difficulties concerning policies that must satisfy international requirements. Tradeoff between security and usability. Social and behavioral considerations.	HW #1 Due Quiz #1	
3		**Security and privacy policies.** Synthesis of policies from laws, social mores, organization goals, and ethics. Derivation of formal policies from human-language policies.	HW#2 Due Quiz #2	Stalling 4 Stallings 5
4		**Risks in security and privacy**. Including identity theft, stalking, online victimization, surveillance. **General threats to security and privacy**. Threat actors – hackers, organized crime, and nation states. Motivations, techniques (e.g., "phishing"), attack vectors, tools.	HW #3 Due Quiz #3	
5		**Threats specific to big data.** Security and privacy threats in the "cloud" and other shared computing utilities. Velocity, volume, and variety. Inference and aggregation.	HW #4 Due Quiz #4	
6		**Mid-Term Review** Summary of major topics covered to this point. Introduction of semester project.	Semester project assigned Quiz #5	
7		**Mid-Term Exam** Closed book in-class exam		

8		**Fundamental principles of security and privacy in digital systems.** Basic abstract components of a secure system: subjects, objects, access permission database, authentication, and audit. Least privilege. System assurance.	HW #5 Due Quiz #6	Stalling 10
9		**Deriving security and privacy requirements.** Using the formal security and privacy policy to derive specific technical requirements. Components of security architecture.	HW #6 Due Quiz #7	
10		**Introduction to cryptography**. Cryptosystems and ciphers. Importance of key management. Strengths and weaknesses of encryption.	HW #7 Due Quiz #8	Stallings 2 Stallings 19 Stallings 20
11		**Identification and authentication**. Common mechanisms. Advantages and disadvantages of specific mechanisms, such as passwords, pass-phrases, fingerprints and other biometrics, and multi-factor authentication. Access control lists. Authorization mechanisms to protect information while still permitting information sharing.	HW #8 Due Quiz #9	Stallings 3
12		**Network and mobile security**. Basic concepts and mechanisms of network security. Firewalls, VPNs, etc. E-commerce security mechanisms. Special problems with security and privacy of mobile devices.	HW #9 Due Quiz #10	Stallings 21 Stallings 22 Stallings 9
13		**Types of attacks and vulnerability analysis**. Malicious code. Advanced persistent threats. Antivirus, intrusion detection, and other ways to recognize attacks. Sensitivity vs. false positive problem.	HW #10 Due Quiz #11	
14		Risk management, physical security, audit, compliance and governance.		Stallings 13 Stallings 15 Stallings 16

15		**Final Review.** Summary of major topics covered in the class.		
		Classes End		
		Study Days		
		Final Exam		
		Semester ends		

Statement on Academic Conduct and Support Systems

Academic Conduct

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in *SCampus* in Section 11, *Behavior Violating University Standards* https://scampus.usc.edu/1100-behavior-violating-university-standards-and-appropriate-sanctions. Other forms of academic dishonesty are equally unacceptable. See additional information in *SCampus* and university policies on scientific misconduct, http://policy.usc.edu/scientific-misconduct.

Discrimination, sexual assault, and harassment are not tolerated by the university. You are encouraged to report any incidents to the *Office of Equity and Diversity* http://equity.usc.edu or to the *Department of Public Safety* http://capsnet.usc.edu/department/department-public-safety/online-forms/contact-us. This is important for the safety of the whole USC community. Another member of the university community – such as a friend, classmate, advisor, or faculty member – can help initiate the report, or can initiate the report on behalf of another person. *The Center for Women and Men* http://www.usc.edu/student-affairs/cwm/ provides 24/7 confidential support, and the sexual assault resource center webpage http://sarc.usc.edu describes reporting options and other resources.

Support Systems

A number of USC's schools provide support for students who need help with scholarly writing. Check with your advisor or program staff to find out more. Students whose primary language is not English should check with the *American Language Institute* http://dornsife.usc.edu/ali, which sponsors courses and workshops specifically for international graduate students. *The Office of Disability Services and Programs* http://sait.usc.edu/academicsupport/centerprograms/dsp/home_index.html provides certification for students with disabilities and helps arrange the relevant accommodations. If an officially declared emergency makes travel to campus infeasible, *USC Emergency Information* *http://emergency.usc.edu* will provide safety and other updates, including ways in which instruction will be continued by means of blackboard, teleconferencing, and other technology.