INF529 Security and Privacy for Informatics
Units: 4
Friday’s 12:00 – 3:20PM

Location: T.B.A (class website http://ccss.usc.edu/529)

Instructor: Clifford Neuman
Office: RTH 512 and ISI 1143
Office Hours: T.B.A.
Contact Info: bcn@isi.edu 310-448-8736.

Teaching Assistant: T.B.A.
Office: T.B.A.
Office Hours: T.B.A.
Contact Info: Email, phone number (office, cell), Skype, etc.

IT Help: T.B.A.
Hours of Service:
Contact Info: T.B.A.
Catalogue Description:

INF 529 Security and Privacy in Informatics  Covers societal implications of information privacy and how to design systems to best preserve privacy. Provides a brief overview of security philosophy and technologies for students not specializing in information security. Covers implications of security technologies in law, public policy, and ethics. Discusses theoretical measures for privacy. Covers the technologies that invade privacy, and technical countermeasures.

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.

Learning 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

Prerequisite(s): none
Co-Requisite(s): none
Concurrent Enrollment: none
Recommended Preparation: General familiarity with the use of common internet and mobile applications.

Required Readings and Supplementary Materials

Selections from Matt Bishop, "Introduction to Computer Security"

Additional References

[KERN] If youre not paranoid your crazy, Walter Kern, The Atlantic, November 2015.


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


[Craig] Terence Craig, "Privacy and Big Data"

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

[IoTAT] Internet of Things security is hilariously broken and getting worse, Ars Technia, January 23 2016


[Kor] Privacy Violations Using Microtargeted Ads: A Case Study. A. Korolova
Description and Assessment of Assignments

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.

Grading Breakdown

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Points</th>
<th>% of Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final Exam</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Mid Term Exam</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Quizzes</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Homework</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Class Participation</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>0</td>
<td>100</td>
</tr>
</tbody>
</table>
Assignment Submission Policy
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 College. There will be four quizzes. There will be eight homework assignments and one semester project.

Students are required to collect articles in current professional and trade journals that are relevant to topics in systems analysis and design. The process is particularly important in keeping current with technology and new methodologies. Each class period, students must submit a paper copy of the articles to the instructor at the beginning of class.

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.

Additional Policies

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.

Emergency Preparedness/Course Continuity in a Crisis
In case of a declared emergency if travel to campus is not feasible, USC executive leadership will announce an electronic way for instructors to teach students in their residence halls or homes using a combination of Blackboard, teleconferencing, and other technologies.

Students with Disabilities
Any student requesting academic accommodations based on a disability is required to register with Disability Services and Programs (DSP) each semester. A letter of verification for approved accommodations can be obtained from DSP. Please be sure the letter is delivered to me as early in the semester as possible. Your letter must be specific as to the nature of any accommodations granted. DSP is located in STU 301 and is open 8:30 am to 5:30 pm, Monday through Friday. The telephone number for DSP is (213) 740-0776.
<table>
<thead>
<tr>
<th>Week</th>
<th>Dates</th>
<th>Topics/Daily Activities</th>
<th>Readings and Homework</th>
<th>Deliverable/ Due Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1</td>
<td>Dates</td>
<td>Overview and general landscape for privacy in information technology systems.</td>
<td>Kern</td>
<td></td>
</tr>
<tr>
<td>Week 2</td>
<td>Dates</td>
<td>Personally Identifiable Information: Use and Misuse</td>
<td>PII</td>
<td>HW#1 Due, Quiz1</td>
</tr>
<tr>
<td>Week 3</td>
<td>Dates</td>
<td>Overview of computer security, Technical means of protection.</td>
<td>Bishop CH1, CH23, CH24</td>
<td>HW#2 Due, Quiz 2</td>
</tr>
<tr>
<td>Week 4</td>
<td>Dates</td>
<td>Identification, Authentication, and Audit</td>
<td>Bishop CH11,13,21</td>
<td>HW#3 Due, Quiz 3</td>
</tr>
<tr>
<td>Week 5</td>
<td>Dates</td>
<td>Social Media, Social Networks, and Privacy</td>
<td>Nissenbaum, Levermore, KOR</td>
<td>HW#4 Due, Quiz 4</td>
</tr>
<tr>
<td>Week 6</td>
<td>Dates</td>
<td>Measuring Privacy, Technical Approaches to Preserve Privacy</td>
<td>TOR</td>
<td></td>
</tr>
<tr>
<td>Week 7</td>
<td>Dates</td>
<td>Review for mid-term, Mid-Term Exam</td>
<td>Review of all readings to date</td>
<td>Mid-term exam</td>
</tr>
<tr>
<td>Week 8</td>
<td>Dates</td>
<td>Aggregation, Anonymization, Correlation, and Data Mining</td>
<td>CAS</td>
<td>HW#5 Due, Quiz 5</td>
</tr>
<tr>
<td>Week 9</td>
<td>Dates</td>
<td>Privacy Considerations in Big Data</td>
<td>Craig, Lane</td>
<td>HW#6 Due, Quiz 6</td>
</tr>
<tr>
<td>Week 10</td>
<td>Dates</td>
<td>Privacy and Criminal Procedure, Legal Treatment of Private Data (includes a guest lecture)</td>
<td>Readings to be Assigned in consultation with guest lecturer</td>
<td></td>
</tr>
<tr>
<td>Week 11</td>
<td>Dates</td>
<td>Civil Law and Privacy, Privacy Statements and Abuse, Discovery (includes a guest lecture)</td>
<td>Readings to be Assigned in consultation with guest lecturer</td>
<td>HW#7 Due, Quiz 7</td>
</tr>
<tr>
<td>Week 12</td>
<td>Dates</td>
<td>The international Face of Privacy, Conflicts in International Law (includes a guest lecture)</td>
<td>Readings to be Assigned in consultation with guest lecturer</td>
<td>HW#8 Due, Quiz 8</td>
</tr>
<tr>
<td>Week 13</td>
<td>Dates</td>
<td>Privacy and the Internet of Things</td>
<td>IoTAT</td>
<td>HW#9 Due, Quiz 9</td>
</tr>
<tr>
<td>Week 14</td>
<td>Dates</td>
<td>Privacy in application areas: Payment, Voting, Communication</td>
<td>Sch15</td>
<td>HW#10 Due, Quiz 10</td>
</tr>
<tr>
<td>Week 15</td>
<td>Dates</td>
<td>Review for Final Exam</td>
<td>Review Readings from entire semester</td>
<td></td>
</tr>
</tbody>
</table>
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://adminopsnet.usc.edu/department/department-public-safety. 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.