Course Description
Security policy has been defined as the set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. A policy identifies what information is to be protected, why it is to be protected, and who (and under what circumstances) may have what form of access to that information. The policy lays out the business case for the information protection. It is the basis for all protection measures. Ultimately the protection implementation must be traceable to the policy and the policy must be traceable to the implementation. If such traceability fails usually something breaks and the information is either not adequately protected or the implemented system contains superfluous components. Policy is the basis for the consideration of composition.

The course will examine information policies in various contexts, including business, government and technology implementation (e.g., cryptographic devices) with an eye to detecting errors, flaws and omissions. The intent is to develop, for those policies that survive careful scrutiny, high level architectural considerations for the possible systems implementations.

It is recommended that students have some background in computer security, or a strong willingness to learn. Recommended previous courses of studies include computer science, electrical engineering, computer engineering, management information systems, and/or mathematics. Students should have a solid background in at least operating systems, computer architecture, digital networking, elementary/introductory abstract algebra, and theory of computation/non-computability.

Course Website: https://piazza.com/usc/fall2022/dsci519

Course Resources
Piazza will be used for lectures, announcements, assignments, and intra-class communication
DEN D2L will be used for:
- posting of grades
- homework submission
- quiz submission
- exam submission
Course Objectives
This course has five primary learning objectives for students. Success in this course will largely depend on mastery of these objectives:

1. Understand that the focus is on the protection of information in digital form reflecting an organizational information security policy for persons accessing information, applying cyber security concepts and terminology from the literature.

2. Understand that information assurance is based on confirmation that the policy for a trusted system is enforced in the face of not only natural events but also in the face of a witted adversary for whom subversion may be the attack tool of choice.

3. Be thoroughly familiar with the reference monitor abstraction of system security, as well as with the associated common mathematical models and techniques for their implementation interpretation and objective evaluation.

4. Recognize that some policies do not require sophisticated implementation solutions, while others cannot be implemented within the capabilities of existing information technology or even fundamental limits of the theory of computation.

5. Understand the problem of “composition” and how policy formulation and policy implementation may contribute to, or alternatively inhibit the successful composition of information technology systems.

Methods of Teaching
The primary teaching method will be lectures, discussion, case studies, and possibly guest speakers and demonstrations. Students are expected to perform directed self-learning outside of class, which encompasses, among other things, a considerable amount of literature 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 and exams to reinforce the concepts taught. They will complete a final semester project to apply and illustrate the concepts in an applied manner.

There will be several quizzes, homework assignments, and laboratory assignments.

Semester Project
The semester project gives each student the opportunity to apply the concepts from the course in a similar manner as they would in “the real world”.

Grading

<table>
<thead>
<tr>
<th>Artifact</th>
<th>Weight</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quizzes</td>
<td>15%</td>
<td>various</td>
</tr>
<tr>
<td>Midterm</td>
<td>20%</td>
<td>October 5</td>
</tr>
<tr>
<td>Final Exam</td>
<td>20%</td>
<td>December 7, 11am-1pm</td>
</tr>
<tr>
<td>HW Assignments</td>
<td>35%</td>
<td>various</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------</td>
<td>---------------</td>
</tr>
<tr>
<td>Project</td>
<td>15%</td>
<td>November 30</td>
</tr>
<tr>
<td>Class Participation</td>
<td>10%</td>
<td>continuous</td>
</tr>
</tbody>
</table>

**Course Homework Submission**

Homework submission in electronic form via DEN.

**Late Policy**

Cumulative of 10% times number of days late
- 1 day late: lose 10%
- 2 days late: lose 30% (10% + 20%)
- 3 days late: lose 60% (30% + 30%)

Greater than 4 days late not accepted.

No personal emergencies will be entertained (with the exception of the USC granted emergencies, in which case official documents need to be shown).

**Required Reading**

**Required Textbooks:**

- **BISH** Computer Security Art and Science: Bishop, Matt, 2018.

**Literature:**

- **FIPS** FIPS PUB 140-3, Security Requirements For Cryptographic Modules, NIST, 2019.


Projected Schedule
Class sequence, dates, reading assignments, and topics are subject to change as the semester proceeds. Any revisions will be noted and announced in class and posted on the class website.

<table>
<thead>
<tr>
<th>Lec.</th>
<th>Date</th>
<th>Topic</th>
<th>Reading</th>
<th>Other</th>
</tr>
</thead>
</table>
| 1    | 8/24 | Course Introduction  
- Structural overview of the course of study  
- Challenge of Security Policy Breaches  
- Motivation and definitions. The nature of a witted adversary and the limitations of current cyber security best practice | PFL CH1  
BISH CH 1 | Lab1 |
| 2    | 8/31 | Introduction to characteristics of policy  
- Building on the foundation of an organizational policy  
- Introduction to the Reference Monitor (RM)  
- Interpreting RM components | FPIGS  
TCSEC 6.1  
BISH CH 2;  
CH 4.1-4.4 | HW1 |
| 3    | 9/7  | Formal security policy model (FSPM) interpretation  
- Introduce the mathematical basis for a FSPM & distinguish between properties of discretionary and mandatory policy  
Bell-LaPadula Interpretation for Reference Monitor  
- Describe the formal components of the widely-used BLP model to illustrate bridging between policy and a computer Quiz1 | TCSEC 6.2  
BISH CH 5.1-5.3 | Lab1 due |
| 4    | 9/14 | U. S. Classified Information policy  
- Critical examination of an actual organizational policy: the US Government executive order 13526  
Bell-LaPadula Multics interpretation  
- Careful mapping of sets in the BLP model system state definition, and its access modes, to the hardware and software of the commercial Multics computer. Introduction of the powerful Basic Security Theorem | USEO  
TCSEC 4.1 | |
| 5    | 9/21 | Theoretical limits on system security  
- Review Turing Machine undecidability, how HRU show general security case is undecidable, and why BLP is decidable result Quiz2 | BISH CH 3.1-3.3;  
HW1 due | |
| 6    | 9/28 | Biba integrity model  
- Introduce problem of formulating an integrity access | BISH CH 6.1, 6.2 | Lab2 |
<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topics</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>Project proposal due</td>
</tr>
<tr>
<td>2</td>
<td>10/5</td>
<td>Midterm, TBD</td>
<td>HW2 due</td>
</tr>
<tr>
<td>3</td>
<td>10/12</td>
<td>Lipner and Clark-Wilson integrity models</td>
<td>HW3 due</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Introduce other integrity models, requirements of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>commercial integrity policies, separation of duty</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security policy can refer equally to confidentiality and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>integrity. Examine policies that involve conflict of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>interest, base control on job functions, support creator-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>based control</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>10/19</td>
<td>Policy composition with TCB subsets</td>
<td>Lab2 due</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Allocate subsets of system policy to TCB subsets</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>assigned to totally ordered protection domains</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Partitioned TCB for policy composition</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Allocate partitions of system policy to loosely-coupled</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>network components</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10/26</td>
<td>TNI composition of MAID components</td>
<td>Lab3 due</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Introduction to a systematic taxonomy of security policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>of four major policy elements grouped into two classes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Audit for cyber security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Compare two divergent views of audit: (1) ad hoc</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>practice that hopes to detect violations and (2) RM based</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>tool to enhance individual accountability Quiz3</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>11/2</td>
<td>Authentication for cyber security</td>
<td>HW3 due</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Authentication as a tool for relating organization policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>for access by individuals by binding a RM subject to an</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>identity.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identification for cyber security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The role and representation of identities for principals,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>and how identity is related to the reference monitor.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Federated identity.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>11/9</td>
<td>System security evaluation</td>
<td>Lab3 due</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Historical motivations, goals and structure for security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>evaluation of a system, and the systematic codification in</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the TCSEC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Common Criteria: an international standard for computer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>security certification</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deployment Policy for Trusted Systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The roles of evaluation, certification and accreditation in</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policies for deployment of trusted systems Quiz4</td>
<td></td>
</tr>
</tbody>
</table>
Policy for Cryptographic Implementation

- Policy considerations for the implementation and use of cryptography

BISH 22.6.2 – 22.6.5
FIPS 4.1-4.3; 4.6;
Appendix C

11/23 Thanksgiving break, no class

13 11/30 Privacy policy
Course review

PFL CH 9 Project due

Final Examination: December 7, 11am-1pm

Synchronous session recording notice
Live class sessions will be recorded and made available to students through Blackboard (including transcriptions). Please remember that USC policy prohibits sharing of any synchronous and asynchronous course content outside of the learning environment. As a student, you are responsible for the appropriate use and handling of these recordings under existing SCampus policies regarding class notes (https://policy.usc.edu/scampus-part-c/). These rules will be strictly enforced, and violations will be met with the appropriate disciplinary sanction.

Going back to Campus
Although we are starting the semester with online instruction only, conditions may improve. In such case, courses listed as hybrid will give opportunity to students to attend class in person. This will happen only by following the strictest health guidelines and safety protocols. These are listed in the Trojans Return page. Please take the time to read this ahead so that you are prepared in case it is possible to return to in-person instruction.

Learning Experience Evaluations
Learning Experience Evaluations will be completed during the last day of class. This will be your opportunity to provide feedback about your learning experience in the class. This feedback helps the instructor determine whether students are having the intended learning experiences for the class. It is important to remember that the learning process is collaborative and requires significant effort from the instructor, individual students, and the class as a whole. Students should provide a thoughtful assessment of their experience, as well as of their own effort, with comments focused on specific aspects of instruction or the course. Comments on personal characteristics of the instructor are not appropriate and will not be considered. For this feedback to be as comprehensive as possible, all students should complete the evaluation.

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 Part B, Section 11, “Behavior Violating University Standards” policy.usc.edu/scampus-part-b. Other forms of academic dishonesty are equally unacceptable. See additional information in SCampus and university policies on scientific misconduct, policy.usc.edu/scientific-misconduct.

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.

Support Systems

Counseling and Mental Health - (213) 740-9355 – 24/7 on call
studenthealth.usc.edu/counseling
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

National Suicide Prevention Lifeline - 1 (800) 273-8255 – 24/7 on call
suicidepreventionlifeline.org
Free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week.

Relationship and Sexual Violence Prevention Services (RSVP) - (213) 740-9355(WELL), press “0” after hours – 24/7 on call
studenthealth.usc.edu/sexual-assault
Free and confidential therapy services, workshops, and training for situations related to gender-based harm.

Office of Equity and Diversity (OED) - (213) 740-5086 | Title IX – (213) 821-8298
equity.usc.edu, titleix.usc.edu
Information about how to get help or help someone affected by harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants.

Reporting Incidents of Bias or Harassment - (213) 740-5086 or (213) 821-8298
usc-advocate.symplicity.com/care_report
Avenue to report incidents of bias, hate crimes, and microaggressions to the Office of Equity and Diversity |Title IX for appropriate investigation, supportive measures, and response.

The Office of Disability Services and Programs - (213) 740-0776
dsp.usc.edu
Support and accommodations for students with disabilities. Services include assistance in providing readers/notetakers/interpreters, special accommodations for test taking needs, assistance with architectural barriers, assistive technology, and support for individual needs.

USC Campus Support and Intervention - (213) 821-4710
campussupport.usc.edu
Assists students and families in resolving complex personal, financial, and academic issues adversely affecting their success as a student.

Diversity at USC - (213) 740-2101
diversity.usc.edu
Information on events, programs and training, the Provost’s Diversity and Inclusion Council, Diversity Liaisons for each academic school, chronology, participation, and various resources for students.

USC Emergency - UPC: (213) 740-4321, HSC: (323) 442-1000 – 24/7 on call
dps.usc.edu, emergency.usc.edu
Emergency assistance and avenue to report a crime. Latest updates regarding safety, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible.

USC Department of Public Safety - UPC: (213) 740-6000, HSC: (323) 442-120 – 24/7 on call
dps.usc.edu
Non-emergency assistance or information.

Office of the Ombuds - (213) 821-9556 (UPC) / (323-442-0382 (HSC)
ombuds.usc.edu
A safe and confidential place to share your USC-related issues with a University Ombuds who will work with you to explore options or paths to manage your concern.