



## **DSCI 519: Foundations and Policy for Information Security**

### **Fall 2022 Syllabus**

<b>Instructor</b>	<b>Email</b>	<b>Office Hours</b>	<b>Lecture</b>
Tatyana Ryutov	<a href="mailto:tryutov@usc.edu">tryutov@usc.edu</a>	<b>TBD</b>	Wednesday 11:00am 2:20pm OHE 100D

#### **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

Artifact	Weight	Date
Quizzes	15%	various
Midterm	20%	October 5
Final Exam	20%	December 7, 11am-1pm

HW Assignments	35%	various
Project	15%	December 4
Class Participation	10%	continuous

### 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.

**PFL** Security in Computing, Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, 2015.

#### Literature:

**BLP** Bell, D. Elliott, and Leonard J. La Padula. Secure computer system: Unified exposition and Multics interpretation. No. MTR-2997-REV-1. MITRE CORP BEDFORD MA, 1976.

**ENVI** Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements -- Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-004-85, DoD Computer Security Center: Ft. George G. Meade, MD, 1985.

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

**FPIGS** Schell, Roger R. "Information security: science, pseudoscience, and flying pigs." Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual. IEEE, 2001.

**LIPN** Steven B. Lipner, "The Birth and Death of the Orange Book", Computer Science, IEEE Annals of the History of Computing, 2015.

**RBAC** R. Sandhu, David F. Ferraiolo, D. Richard Kuhn, "The NIST Model for Role-Based Access Control: Towards a Unified Standard", 2000.

**SANS** Sorchia Diver, "Information Security Policy-A Development Guide for Large and Small Companies", SANS, 2004.

**SHOC** "TCB subsets for incremental evaluation", Shockley, William R., and Roger R. Schell. In

Proceedings of the Third Aerospace Computer Security Conference, Orlando, Florida, pp. 131-139., 1987.

**TCSEC** Department of Defense, Department of Defense Trusted Computer System Evaluation Criteria, Department of Defense 5200.28-STD, 1985.

**TDI** Trusted DBMS Interpretation, National Computer Security Center, 1988.

**TINTO** Mario Tinto, "The Design and Evaluation of INFOSEC Systems", The Computer Security Contribution to the Composition Discussion, 1992.

**TNI** Trusted Network Interpretation. "NCSC-TG 005" National Computer Security Center, 1990.

**USEO** Order, Executive. "13526" Classified National Security Information", 2009.

### 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.

Lec.	Date	Topic	Reading	Other
1	8/24	Course Introduction <ul style="list-style-type: none"><li>Structural overview of the course of study</li><li>Challenge of Security Policy Breaches</li><li>Motivation and definitions. The nature of a witted adversary and the limitations of current cyber security best practice</li></ul>	<b>PFL</b> CH1 <b>BISH</b> CH 1	Lab1
2	8/31	Introduction to characteristics of policy <ul style="list-style-type: none"><li>Building on the foundation of an organizational policy</li><li>Introduction to the Reference Monitor (RM)</li><li>Interpreting RM components</li></ul>	<b>FPIGS</b> <b>TCSEC</b> 6.1 <b>BISH</b> CH 2; CH 4.1-4.4 <b>SANS</b>	HW1
3	9/7	Formal security policy model (FSPM) interpretation <ul style="list-style-type: none"><li>Introduce the mathematical basis for a FSPM &amp; distinguish between properties of discretionary and mandatory policy</li></ul> Bell-LaPadula Interpretation for Reference Monitor <ul style="list-style-type: none"><li>Describe the formal components of the widely-used BLP model to illustrate bridging between policy and a computer <b>Quiz1</b></li></ul>	<b>TCSEC</b> 6.2 <b>BISH</b> CH 5.1-5.3 <b>BLP</b> Sec II pp. 9-25	Lab1 due
4	9/14	U. S. Classified Information policy <ul style="list-style-type: none"><li>Critical examination of an actual organizational policy: the US Government executive order 13526</li></ul> Bell-LaPadula Multics interpretation <ul style="list-style-type: none"><li>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.</li></ul> Introduction of the powerful Basic Security Theorem	<b>USEO</b> <b>TCSEC</b> 4.1 <b>BLP</b> Sec III, pp. 30-63	

5	9/21	<p>Theoretical limits on system security</p> <ul style="list-style-type: none"> <li>Review Turing Machine undecidability, how HRU show general security case is undecidable, and why BLP is decidable result <b>Quiz2</b></li> </ul>	<b>BISH</b> CH 3.1-3.3;	<p><b>HW1</b> due</p> <p>HW2</p>
6	9/28	<p>Biba integrity model</p> <ul style="list-style-type: none"> <li>Introduce problem of formulating an integrity access control. Examine a formal model interpretation for integrity policy, and properties sufficient to preserve information integrity</li> </ul> <p>RM implementation details</p> <ul style="list-style-type: none"> <li>Classic protection rings.</li> </ul> <p>Midterm review</p> <ul style="list-style-type: none"> <li>Summary of major topics related to access control, reference monitor and formal security policy models</li> </ul>	<b>BISH</b> CH 6.1, 6.2	<p>Lab2</p> <p><b>Project</b> <b>proposal</b> due</p>
	10/5	<b>Midterm, TBD</b>		
7	10/12	<p>Lipner and Clark-Wilson integrity models</p> <ul style="list-style-type: none"> <li>Introduce other integrity models, requirements of commercial integrity policies, separation of duty</li> </ul> <p>Hybrid policies</p> <ul style="list-style-type: none"> <li>Security policy can refer equally to confidentiality and integrity. Examine policies that involve conflict of interest, base control on job functions, support creator-based control</li> </ul>	<b>BISH</b> CH 6.3, 6.4; CH 8.1, 8.3, 8.4 <b>RBAC</b>	<p><b>HW2</b> due</p> <p>HW3</p>
8	10/19	<p>Policy composition with TCB subsets</p> <ul style="list-style-type: none"> <li>Allocate subsets of system policy to TCB subsets assigned to totally ordered protection domains</li> </ul> <p>Partitioned TCB for policy composition</p> <ul style="list-style-type: none"> <li>Allocate partitions of system policy to loosely-coupled network components</li> </ul>	<b>SHOC</b> <b>TINTO</b> <b>TDI</b> Appendix II <b>TNI</b> Appendix B p 269-282	<p><b>Lab2</b> due</p> <p>Lab3</p>
9	10/26	<p>TNI composition of MAID components</p> <ul style="list-style-type: none"> <li>Introduction to a systematic taxonomy of security policy of four major policy elements grouped into two classes.</li> </ul> <p>Audit for cyber security</p> <ul style="list-style-type: none"> <li>Compare two divergent views of audit: (1) ad hoc practice that hopes to detect violations and (2) RM based tool to enhance individual accountability <b>Quiz3</b></li> </ul>	<b>TNI</b> p 237-246 <b>BISH</b> CH 25	
10	11/2	<p>Authentication for cyber security</p> <ul style="list-style-type: none"> <li>Authentication as a tool for relating organization policy for access by individuals by binding a RM subject to an identity.</li> </ul> <p>Identification for cyber security</p> <ul style="list-style-type: none"> <li>The role and representation of identities for principals, and how identity is related to the reference monitor. Federated identity.</li> </ul>	<b>PFL</b> CH 2.1, 8.4	<b>HW3</b> due
11	11/9	<p>System security evaluation</p> <ul style="list-style-type: none"> <li>Historical motivations, goals and structure for security</li> </ul>	<b>BISH</b> CH 22.1; 22.2.1-22.2.4.3; 22.7	<b>Lab3</b> due

		evaluation of a system, and the systematic codification in the TCSEC. <ul style="list-style-type: none"> <li>• Common Criteria: an international standard for computer security certification</li> </ul> Deployment Policy for Trusted Systems <ul style="list-style-type: none"> <li>• The roles of evaluation, certification and accreditation in policies for deployment of trusted systems <b>Quiz4</b></li> </ul>	<b>LIPN ENVI</b> p 1-21; Appendix C	
<b>12</b>	11/16	Policy for Cryptographic Implementation <ul style="list-style-type: none"> <li>• Policy considerations for the implementation and use of cryptography</li> </ul>	<b>BISH</b> 22.6.2 – 22.6.5 <b>FIPS</b> 4.1-4.3; 4.6; Appendix C	
	11/23	<b>Thanksgiving break, no class</b>		
<b>13</b>	11/30	Privacy policy Course review	<b>PFL</b> CH 9	
		<b>Final Examination: December 7, 11am-1pm</b>		

### 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](http://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](http://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](http://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](http://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](http://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](http://equity.usc.edu), [titleix.usc.edu](http://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.symlicity.com/care\\_report](http://usc-advocate.symlicity.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](http://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](http://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](http://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](http://dps.usc.edu), [emergency.usc.edu](http://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](http://dps.usc.edu)

Non-emergency assistance or information.

*Office of the Ombuds - (213) 821-9556 (UPC) / (323-442-0382 (HSC)*

[ombuds.usc.edu](http://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.