DSCI 519: Foundations and Policy for Information Security

Units: 4

FALL 2023

Instructor: Prof. Tatyana Ryutov
Time: 10:00am-1:20pm
Days: Wednesdays
Office: OHE 100D
Contact Info: tryutov@usc.edu
Course website: https://piazza.com/usc/fall2023/dsci519

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. 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.

The course will examine information policies in various contexts, including business, government and technology implementation with an eye to detecting errors, flaws and omissions.

The course focuses on fundamental theory and practice for engineering and operating secure information systems. It addresses challenges of policy formulation, verifiably secure operating system components and secure applications.

Learning Objectives

After successfully completing this course, the students will be able to:

- Understand that a security policy is effectively a definition of security for a computer system
- Understand the need for and the development process of information security policies
- Understand the root causes of security vulnerabilities and why current best practices and ad-on security products fail
- Understand foundational concepts with focus on hard science that goes beyond the search for vulnerabilities in deployed systems and the development of defenses for specific attacks
- Identify key cybersecurity policy frameworks
- Develop an enforceable security policy for an organization
- Critique a security policy for its effectiveness and completeness

Recommended Preparation

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 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

Technological Proficiency and Hardware/Software Required

Students must provide their own laptop. The laptop specifications take into consideration that students will be creating, streaming, and downloading audio and video, communicating using video-conferencing applications, and creating and storing large multimedia files.

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 will partake in oral presentations based on homework and assigned literature readings.

Hours of Instruction

Once weekly for 200 minutes including two 10-minute breaks.

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 Breakdown (preliminary)

Artifact	Weight
Quizzes	15%
Midterm	20%
Final Exam	20%
HW Assignments	35%
Project	15%
Class Participation	10%

Grading Timeline

None of the items in this class are auto graded. Assignments and the exams will typically be graded within 7 days of the due date. Final project deliverables will typically be graded within 5 days of the due date. The class participation grades will typically be graded within 3 days after the end of classes.

Course Homework Submission

Homework submission in electronic form via DEN.

Examination

Both the midterm and the final exam will be two-hour written test administered via the USC DEN. The exams format will be a combination of short answers and essays.

Final exam date and time: refer to the final exam schedule in the USC Schedule of Classes at classes.usc.edu.

The exams can only be taken on the scheduled date and at the scheduled starting time. Accommodations for students with letters from DSP will be provided, though the exam will still need to be taken on the scheduled date and start time. There are no makeup exams. If you miss an exam due to a documented illness or an emergency, official written documentation will need to be submitted to instructor as soon as possible. Approval will be based on the instructor's discretion.

Assignment Submission Policy

Assignments and semester project will be submitted electronically via D2L. Assignments will be accepted after the deadline with the following grade penalties. 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).

Diversity, Equity, and Inclusion (DEI) Statement

Our classroom is a place to expand our knowledge and experiences safely, while being respected and valued. We proactively strive to construct a safe and inclusive learning environment by respecting each other's dignity and privacy. We treat one another fairly and honor each member's experiences, beliefs, perspectives, abilities, and backgrounds, regardless of race, religion, language, immigration status, sexual orientation, gender identification, ability status, socio-economic status, national identity, or any other identity markers.

Disruptive or insulting remarks, gender or racial slurs, or other forms of bullying, intimidation or hate speech and other disrespectful language or behavior will not be tolerated. We welcome your thoughts on how we can improve our learning environment.

Additional Policies

Class notes policy: Notes or recordings made by students based on a university class or lecture may only be made for purposes of individual or group study, or for other noncommercial purposes that reasonably arise from the student's membership in the class or attendance at the university. This restriction also applies to any information distributed, disseminated, or in any way displayed for use in relationship to the class, whether obtained in class, via e-mail or otherwise on the Internet, or via any other medium. Actions in violation of this policy constitute a violation of the Student Conduct Code and may subject an individual or entity to university discipline and/or legal proceedings. Again, it is a violation of USC's Academic Integrity Policies to share course materials with others without permission from the instructor.

Class Participation

Students are expected to actively participate in this course. Participation includes:

- Careful reading and viewing of assigned materials by the date due
- Regular, substantive contributions to discussions and in-class questions
- Active engagement with online content

Course grades for students who do not contribute to the course through active participation will be affected.

Pop out questions (about 6) will be asked during each lecture. Responses will be submitted using Google forms. The students will have 72 hours to submit their responses for each lecture. Failure to submit the responses on time will result in a deduction of the class participation score.

Required Readings

<u>Required Textbooks:</u>

[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] Sorcha Diver, "Information Security Policy-A Development Guide for Large and Small Companies", SANS, 2004.

[SHOC] Shockley, William R., and Roger R. Schell, "TCB subsets for incremental evaluation", 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.

Course Schedule: A Weekly Breakdown

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.

Week	Topic	Reading	Other
8/24 Lec1	Course Introduction • Structural overview of the course of study • Challenge of security policy breaches	**PFL** CH1 **BISH** CH 1	Lab1

	• Motivation and definitions. The nature of a witted adversary and the limitations of current cyber security best practice		
8/31 Lec2	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 **SANS**	HW1
9/7 Lec3	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 **BLP** Sec II pp. 9-25	Lab1 due
9/14 Lec4	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 **BLP** Sec III, pp. 30-63	
9/21 Lec5	Theoretical limits on system security • Review Turing Machine undecidabity, how HRU show general security case is undecidable, and why BLP is decidable result Quiz2	**BISH** CH 3.1-3.3;	HW1 due Lab2
9/28 Lec6	Biba integrity model • Introduce problem of formulating an integrity access control. Examine a formal model interpretation for integrity policy, and properties sufficient to preserve information integrity RM implementation details • Classic protection rings. Midterm review • Summary of major topics related to access control, reference monitor and formal security policy models	**BISH** CH 6.1, 6.2	HW2 Project proposal due
10/5	**Midterm, TBD**		
10/12 Lec7	Lipner and Clark-Wilson integrity models • Introduce other integrity models, requirements of commercial integrity policies, separation of duty Hybrid policies • 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	**BISH** CH 6.3, 6.4; CH 8.1, 8.3, 8.4 **RBAC**	HW3
10/19 Lec8	Policy composition with TCB subsets • Allocate subsets of system policy to TCB subsets assigned to totally ordered protection domains Partitioned TCB for policy composition • Allocate partitions of system policy to loosely-coupled network components	**SHOC** **TINTO** **TDI** Appendix II **TNI** Appendix B p 269-282	Lab2 due Lab3 HW2 due

10/26 Lec9	TNI composition of MAID components • Introduction to a systematic taxonomy of security policy of four major policy elements grouped into two classes. Audit for cyber security • Compare two divergent views of audit: (1) ad hoc practice that hopes to detect violations and (2) RM based tool to enhance individual accountability Quiz3	**TNI** p 237-246 **BISH** CH 25	
11/2 Lec10	Authentication for cyber security • Authentication as a tool for relating organization policy for access by individuals by binding a RM subject to an identity. Identification for cyber security • The role and representation of identities for principals, and how identity is related to the reference monitor. Federated identity.	**PFL** CH 2.1, 8.4	HW3 due
11/9 Lec11	System security evaluation • Historical motivations, goals and structure for security evaluation of a system, and the systematic codification in the TCSEC. • Common Criteria: an international standard for computer security certification Deployment Policy for Trusted Systems • The roles of evaluation, certification and accreditation in policies for deployment of trusted systems Quiz4	**BISH** CH 22.1; 22.2.1-22.2.4.3; 22.7 **LIPN** **ENVI** p 1-21; Appendix C	Lab3 due
11/16 Lec12	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**		
11/30 Lec13	Privacy policy Course review	**PFL** CH 9	
	Final Examination will be held at the University's appointed time.		

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.

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.