INF 519: Foundations and Policy for Information Security
Fall 2017 Syllabus

Instructor	Email	Office	Office Hours	Lecture
Tatyana Ryutov	tryutov@usc.edu	TBD	Fridays 3:30pm–5:30pm	Fri 12:00-3:20pm OHE 100C

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.

Throughout, the course will examine stated 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/fall2017/inf519

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 (DEN student only)

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. No programming will be necessary for this course.

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". The project should be not less than 7 or more than 12 pages in length (not counting appendices or figures). The semester project will be specifically assigned after the applicable foundational concepts have been covered in class. That assignment will include preparation guidelines and the due date.

Office Hours
Fridays 3:30 p.m. – 5:30 p.m. Other hours are by appointment only. Students are advised to make appointments with the professor ahead of time and be specific with the subject matter to be discussed. Students should also be prepared for their appointment by bringing all applicable materials and information.

Grading
Grading method will be relative and on the curve.

Artifact	**Weight**	**Date**
Quizzes	20%	various
Midterm	25%	TBD
Final Exam	30%	December 8
HW Assignments	15%	various
Class Participation	10%	

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, 2003.
(PFL) Security in Computing, Pfleeger, Prentice-Hall, 4th edition, 2006.

Literature:

(BFG) PKI Requirements for a B2B E-Commerce Framework, Roger R. Schell, Rich A Lee and Michael F. Thompson, Black Forest Group, September 13, 2000.

(BIBA) Integrity Considerations for Secure Computer Systems, K. J. Biba, 1977.

(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.

(BRIN) Concepts and Terminology for Computer Security: Donald L. Brinkley and Roger R. Schell, 1995

(CWALL) Dr. David F.C. Brewer and Dr. Michael J. Nash, The Chinese Wall Security Policy, 1989

(EVAL) Schell, Roger R., and Donald L. Brinkley. "Evaluation criteria for trusted systems." Information Security: An Integrated Collection of Essays, ed. Abrams and Jajodia and Podell, IEEE Computer Society Press, Los Alamitos, CA (1995): 137-159.

(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, 25 June 1985, DoD Computer Security Center: Ft. George G. Meade, MD.

(F140) FIPS PUB 140-2, Security Requirements For Cryptographic Modules, NIST, May 25, 2001

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

(HEEL) R.R. Schell, “Computer Security: the Achilles Heel of the Electronic Air Force”, Air University Review, Vol. 30:2, Jan. - Feb., 1979

(HRU) Harrison, Michael A., Walter L. Ruzzo, and Jeffrey D. Ullman. "Protection in operating systems." Communications of the ACM 19.8 (1976): 461-471.

(LAMP) B. Lampson, “Protection,” Proc. Fifth Princeton Symposium on Information Sciences and Systems, Princeton University, March 1971, pp. 437-443, reprinted in Operating Systems Review, 8,1, January 1974, pp. 18 – 24

(RBAC) David Ferraiolo, Richard KuhnRole-Based Access Control, 1992

(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, 1985, Department of Defense Trusted Computer System Evaluation Criteria, Department of Defense 5200.28-STD, Washington, DC.

(TDI) Trusted DBMS Interpretation, National Computer Security Center (18 Nov 1988 Draft)

(TNI) Trusted Network Interpretation. "NCSC-TG 005." National Computer Security Center (1990).

(USEO) Order, Executive. "13526." Classified National Security Information,” December 29 (2009).

Additional References

(AND) Security Engineering: Anderson, Ross, 2001

(MULTICS) The Multics system: an examination of its structure**:** Elliott I Organick, 1972.

(RINGS) A hardware architecture for implementing protection rings, Schroeder, Michael D., and Jerome H. Saltzer, 1972.

(NCSC) Rainbow Series: NCSC TG – 024, Procurement of Trusted Systems: http://en.wikipedia.org/wiki/Rainbow_Series

(THUR) Database and Applications Security: Thuraisingham, Bhavani, 2005.

(INFO) http://www.infosyssec.net/index.html, http://www.infosyssec.com/, One of the most complete web sites

(SANS) http://www.sans.org/reading_room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies_1331

(NIST) http://csrc.nist.gov/groups/SMA/fasp/documents/system_security/System_Security_Plan_Template_01102007.doc

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.

Week	Fri	Topic	Reading
1	8/25	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	BISH CH 1 BRIN p 40-45 HEEL
2	9/1	Introduction to Characteristics of Policy • Building on the foundation of an organizational policy, introduction to the Reference Monitor (RM) Interpreting Reference Monitor Components • How RM can be interpreted for physical controls, introduction its evolution from the Access Matrix concept	BISH CH 2,4 BRIN p 45-59 FPIG LAMP
3	9/8	Formal Security Policy Model Interpretation • Introduce the mathematical basis for a FSPM & distinguish between properties of discretionary and mandatory policy Bell-LaPadula Interpretation for Reference Monitor	BISH CH 5 BRIN p 59-65; 71-76 BLP Sec I&II

		• Describe the formal components of the widely-used BLP model to illustrate bridging between policy and a computer	
4	9/15	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 BLP Sec III p 30-63 TCSEC 4.1.1, 6.1, 6.2, 7.3.2, 7.3.3 BRIN p 76-80
5	9/22	Theoretical Limits on System Security • Review Turing Machine undecidabity, how HRU show general security case is undecidable, and why BLP is decidable result. 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 for segmentation. Hierarchy "Compatibility".	BISH CH3.1, CH3.2, CH15.4 HRU BISH CH6.2 TNI 4.1.1 BIBA Sec I-V BLP p28-29,73
6	9/29	SELinux mandatory labeling 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 CH6.4 BISH CH7 CWALL RBAC
7	10/6	Privacy Policies • Differences and similarities between privacy and confidentiality policies. Privacy in Big Data. Differential privacy. Mid-Term Review • Summary of major topics related to access control, reference monitor and formal security policy models.	PFL CH10
8	10/13	**Midterm** Topic TBD	
9	10/20	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 BRIN p 81 TDI App II TNI App B BRIN p 86-92
10	10/27	TNI Composition of MAID Components • Introduction to a systematic taxonomy of security policy of	TNI A.2.5, B.5-B.8, 4.1.2.2

		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.	BRIN p 65-68 BISH 24
11	11/3	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.	TNI 4.1.2.1 BISH 12,14
12	11/10	Business-Centric Certificates • Business suggestions for addressing shortfalls of PKI and certificate practices in their corporate information policies for secure, pervasive interoperability. Policy for Cryptographic Implementation • Policy considerations for the implementation and use of cryptography, including in certificates for a PKI.	BISH 10.4.2 BISH 14.5 BFG p 1-16-35
13	11/17	System Security Evaluation Policy and Evolution of Security Evaluation Criteria • Historical motivations, goals and structure for security evaluation of a system, and the systematic codification in the TCSEC. Gains and losses for assurance in thirty years of evolution of criteria, with comparisons and contrasts for major instances. Deployment Policy for Trusted Systems • The roles of evaluation, certification and accreditation in policies for deployment of trusted systems	BISH 21.1-21.2.4.3 21.3-21.12 BRIN p 81-86 EVAL ENVI TNI App C
14	11/24	**NO class - Thanksgivings**	
15	12/1	Policy Research Directions • Review notable current research directions in security policies Course Review • Review of the entire course; recall how good policy enables you to decide when you are done building and are ready to start using a secure system.	TBD
	12/8	**Final Examination 11 a.m.-1 p.m.**	

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.

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.