INF 522: POLICY: THE FOUNDATION OF A SUCCESSFUL INFORMATION ASSURANCE PROGRAM

Mark R. Heckman
mrheckma@usc.edu

Spring 2015 Syllabus

12:30-1:50pm Tue, Thu (3 Units)
Room RTH 217

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 address the nature of human communications, reflecting the awareness of information having value (hence the emergence of policy), possible policy dimensions (expectations), and the means (mechanisms) for actually implementing that policy. This will focus in particular on the identification of information, recognizing that information objects themselves are distinct from the “containers” of those information objects, and markings.

The course will consider the evolution of the user’s expectations, with regard to the information, the information objects and the containers with particular focus on the overall implications of the transition to the digital age. This will examine the implications on policy, including the technology for policy implementation, focusing on the considerations of information objects, encoding schemes, information containers, the technology for “managing” information containers, technology for policy implementation, markings, and communication of information. Additionally this will identify “gains and losses” associated with the evolution of the “age of information”.

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.

This class will be primarily individual study, with weekly assigned readings, several homework assignments, short in-class quizzes, a project, a midterm and a final. Students are also required to perform literature research for each class period.

**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, regular exams and quizzes to reinforce the concepts taught. They will complete a final semester
project to apply and illustrate the concepts in an applied manner.

**Note that a significant portion of the student’s grade comes from class participation. Students are strongly encouraged to come to class with questions about the assigned reading and about current events that relate to cybersecurity.**

There will be no laboratory assignments, and no special computing facility, hardware or software will be necessary for this course.

**Office Hours:** Tuesday 2:00 p.m. – 4:00 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.

**Assignments/Reports:**

Students will be required to complete several homework assignments, which may take several to complete. Students may help each other to understand how to complete the tasks, but all assignments are to be submitted individually and all submissions should reflect each student’s own efforts. See the section on “Academic Integrity” below for further information.

There will be one midterm test and a final exam whose date will be determined by the College. There will be several short in-class quizzes. There will be several homework assignments and one semester project.

It is crucial that students turn in whatever they have on the due date. Assignments may be handed in late only with the consent of the instructor and will be assessed a penalty as follows: 1 day late, 10% penalty; 2 days late, 30% penalty; 3 days late, 60% penalty; 4 or more days, 100% penalty.

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](http://scampus.usc.edu).

**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.

**Class Communication:**

DEN Blackboard at USC will be used for class communication.
Grading Schema:
Final: 30%
Mid-Term: 25%
Quizzes: 15%
Class Participation: 10%
Homework Assignments: 10%
Semester Project: 10%

Total 100%

Grades will range from A through F. The following is the breakdown for grading. This is the nominal breakdown, meaning that the grade awarded will not be less than indicated:

94 - 100 = A    74 - 76 = C
90 - 93 = A-    70 - 73 = C-
87 - 89 = B+    67 - 69 = D+
84 - 86 = B     64 - 66 = D
80 - 83 = B-    60 - 63 = D-
77 - 79 = C+    Below 60 is an F

Books and Readings:

All books, papers or reports will be available to students in one of three ways: 1) in the USC bookstore or other commercial source; 2) via Course Documents that the instructor will provide on DEN Blackboard; and/or 3) via the web.

Required Reading:

Textbook:
(BISH) Computer Security Art and Science: Bishop, Matt, 2003

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


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


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


Additional References


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


(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


(ORAL) http://www.jstor.org/stable/534336

(ORAL2) http://indigenousfoundations.arts.ubc.ca/home/culture/oral-traditions.html


**Class Structure & Schedule:**
Class sequence, dates, topics and guest speakers are subject to change as the semester proceeds. Any revisions will be noted and announced in class.

<table>
<thead>
<tr>
<th>Week/class</th>
<th>Date</th>
<th>Topics Covered</th>
<th>Homework</th>
<th>Assignment*</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a Lec 1</td>
<td>1/13</td>
<td><strong>Course Introduction.</strong> General introduction to class – requirements, schedule, approach, tests, homework, assignments, structural overview of the IA course of study, grading approach, answer questions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1b Lec 2</td>
<td>1/15</td>
<td><strong>Challenge of Security Policy Breaches.</strong> Motivation and definitions. The nature of a witted adversary and the limitations of current cyber security best practice.</td>
<td></td>
<td>BISH CH 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>BRIN p 40-45,68-71 HEEL</td>
</tr>
<tr>
<td>2a Lec 3</td>
<td>1/20</td>
<td><strong>Introduction to Characteristics of Policy.</strong> Building on the foundation of an organizational policy, and an introduction to the Reference Monitor (RM) three key properties. <strong>Interpreting Reference Monitor Components.</strong> How RM can be interpreted for physical controls, and an introduction its evolution from the Access Matrix concept.</td>
<td></td>
<td>BISH CH 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>BRIN p 45-54 FPIG</td>
</tr>
<tr>
<td>2b Lec 4</td>
<td>1/22</td>
<td></td>
<td></td>
<td>BISH CH 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LAMP BRIN p 54-59</td>
</tr>
<tr>
<td>3a Lec 5</td>
<td>1/27</td>
<td><strong>Formal Security Policy Model Interpretation.</strong> Introduce the mathematical basis for a FSPM &amp; distinguish between properties of discretionary and mandatory policy.</td>
<td></td>
<td>BISH CH 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>BRIN p 59-65</td>
</tr>
<tr>
<td>3b Lec 6</td>
<td>1/29</td>
<td><strong>Bell-LaPadula Interpretation for Reference Monitor.</strong> Describe the formal components of the widely-used BLP model to illustrate bridging between policy and a computer.</td>
<td></td>
<td>BLP Sec I&amp;II</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>BRIN p 71-76</td>
</tr>
<tr>
<td>4a Lec 7</td>
<td>2/3</td>
<td><strong>U. S. Classified Information Policy</strong> Critical examination of an actual organizational policy. In particular the US Government executive order 13526.</td>
<td></td>
<td>USEO</td>
</tr>
<tr>
<td>4b Lec 8</td>
<td>2/5</td>
<td><strong>Bell-LaPadula Multics Interpretation</strong> 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.</td>
<td></td>
<td>BLP Sec III</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p 30-47</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>BRIN p 76-80</td>
</tr>
<tr>
<td>#</td>
<td>Lec</td>
<td>Date</td>
<td>Topic</td>
<td>References</td>
</tr>
<tr>
<td>----</td>
<td>-----</td>
<td>------</td>
<td>---------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>5a</td>
<td>Lec 9</td>
<td>2/10</td>
<td>Multics Interpretation of BLP System</td>
<td>BLP Sec III p 47-63, TCSEC 4.1.1, 6.1, 6.2, 7.3.2, 7.3.3, BRIN p 80</td>
</tr>
<tr>
<td>5b</td>
<td>Lec 10</td>
<td>2/12</td>
<td>Theoretical Limits on System Security</td>
<td>BISH p 47-53 HRU</td>
</tr>
<tr>
<td>6a</td>
<td>Lec 11</td>
<td>2/17</td>
<td>Introduction to Integrity Policies</td>
<td>BISH CH6 TNI 4.1.1</td>
</tr>
<tr>
<td>6b</td>
<td>Lec 12</td>
<td>2/19</td>
<td>Integrity Security Policy Problem</td>
<td>BIBA Sec I &amp; II</td>
</tr>
<tr>
<td>7a</td>
<td>Lec 13</td>
<td>2/24</td>
<td>Biba Integrity Policy Interpretations</td>
<td>BIBA Sec III &amp; V</td>
</tr>
<tr>
<td>7b</td>
<td>Lec 14</td>
<td>2/26</td>
<td>RM Implementation Details</td>
<td>BISH 15.4 BISH 5.3 BLP p28-29,73</td>
</tr>
<tr>
<td>8a</td>
<td>Lec 15</td>
<td>3/3</td>
<td>Mid-Term Review</td>
<td>Project Due: Final class Semester Project Description</td>
</tr>
<tr>
<td>8b</td>
<td>Lec 16</td>
<td>3/5</td>
<td>Mid-Term Exam</td>
<td>Closed book in-class exam</td>
</tr>
<tr>
<td>9a</td>
<td>Lec 17</td>
<td>3/10</td>
<td>Policy Composition with TCB Subsets</td>
<td>SHOC BRIN p 81 TDI App II</td>
</tr>
<tr>
<td>9b</td>
<td>Lec 17</td>
<td>3/12</td>
<td>Partitioned TCB for Policy Composition</td>
<td>TNI App B BRIN p 86-92</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3/17</td>
<td>Spring break. No class.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3/19</td>
<td>Spring break. No class.</td>
<td></td>
</tr>
<tr>
<td>Lec</td>
<td>Date</td>
<td>Title</td>
<td>Description</td>
<td>References</td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
<td>----------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>10a</td>
<td>3/24</td>
<td>TNI Composition of MAID Components</td>
<td>Introduction to a systematic taxonomy of security policy of four major policy elements grouped into two classes.</td>
<td>TNI A.2.5, B.5-B.8, BRIN p 65-68</td>
</tr>
<tr>
<td>10b</td>
<td>3/26</td>
<td>Audit for Cyber Security</td>
<td>Compare two divergent views of audit: (1) ad hoc practice that hopes to detect violations and (2) RM based tool to enhance individual accountability.</td>
<td>TNI 4.1.2.2 BISH 24</td>
</tr>
<tr>
<td>11a</td>
<td>3/31</td>
<td>Authentication for Cyber Security</td>
<td>Authentication as a tool for relating organization policy for access by individuals by binding a RM subject to an identity.</td>
<td>TNI 4.1.2.1 BISH 12 BRIN p 65-68</td>
</tr>
<tr>
<td>11b</td>
<td>4/2</td>
<td>Identification for Cyber Security</td>
<td>The role and representation of identities for principals, and how identity is related to the reference monitor.</td>
<td>BISH 14</td>
</tr>
<tr>
<td>12a</td>
<td>4/7</td>
<td>Certificate Policy for Identification</td>
<td>The creation and use of public key certificates as one of the most widely used methods for identification of a principal on the Internet.</td>
<td>BISH 10.4.2 BISH 14.5 BFG p 1-16</td>
</tr>
<tr>
<td>12b</td>
<td>4/9</td>
<td>Business-Centric Certificates</td>
<td>Business suggestions for addressing shortfalls of PKI and certificate practices in their corporate information policies for secure, pervasive interoperability.</td>
<td>BFG p 17-35</td>
</tr>
<tr>
<td>13a</td>
<td>4/14</td>
<td>Policy for Cryptographic Implementation</td>
<td>Policy considerations for the implementation and use of cryptography, including in certificates for a PKI.</td>
<td>F140 1-4.3, 4.6, App C, BRIN p 92-93</td>
</tr>
<tr>
<td>13b</td>
<td>4/16</td>
<td>System Security Evaluation Policy</td>
<td>Historical motivations, goals and structure for security evaluation of a system, and the systematic codification in the TCSEC.</td>
<td>BISH 21.1-21.2.4.3 BRIN p 81-86 EVAL</td>
</tr>
</tbody>
</table>
**Deployment Policy for Trusted Systems**

The roles of evaluation, certification and accreditation in policies for deployment of trusted systems, with TCSEC example for DoD policy.

**Privacy Policies**

Differences and similarities between privacy and confidentiality policies. Privacy in Big Data. Differential privacy.

**Course Review – Policy – The Foundation for Successful Information Assurance**

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.

*Classes end Fri May 1*

**Study days**

5/2-5/5

2-4pm Wed., 5/13

**Final exam**

**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.

**Academic Integrity**

The University, as an instrument of learning, is predicated on the existence of an environment of integrity. As members of the academic community, faculty, students, and administrative officials share the responsibility for maintaining this environment. Faculties have the primary responsibility for establishing and maintaining an atmosphere and attitude of academic integrity such that the enterprise may flourish in an open and honest way. Students share this responsibility for maintaining standards of academic performance and classroom behavior conducive to the learning process. Administrative officials are responsible for the establishment and maintenance of procedures to support and enforce those academic standards. Thus, the entire University community bears the responsibility for maintaining an environment of integrity and for taking appropriate action to sanction individuals involved in any violation. When there is a clear indication that such individuals are unwilling or unable to support these standards, they should not be allowed to remain in the University.” *(Faculty Handbook, 1994:20)*

Examination behavior – any use of external assistance during an examination shall be considered academically dishonest unless expressly permitted by the teacher.

Fabrication – any intentional falsification or invention of data or citation in an academic exercise will be considered a violation of academic integrity.

Plagiarism – the appropriation and subsequent passing off of another’s ideas or words as one’s own. If the words or ideas of another are used, acknowledgment of the original source must be made through recognized referencing practices.

Other Types of Academic Dishonesty – submitting a paper written by or obtained from another, using a paper or essay in more than one class without the teacher’s express permission, obtaining a copy of an examination in advance without the knowledge and consent of the teacher, changing academic records outside of normal procedures and/or petitions, using another person to complete homework assignments or take-home exams without the knowledge or consent of the teacher.

The use of unauthorized material, communication with fellow students for course assignments, or during a mid-term examination, attempting to benefit from work of another student, past or present and similar behavior that defeats the intent of an assignment or mid-term examination, is unacceptable to the University. It is often difficult to distinguish between a culpable act and inadvertent behavior resulting from the nervous tensions accompanying examinations. Where a clear violation has occurred, however, the instructor may disqualify the student’s work as unacceptable and assign a failing mark on the paper.

**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.