INF 523: ASSURANCE IN CYBERSPACE AS APPLIED TO INFORMATION SECURITY

Mark R. Heckman
mrheckma@usc.edu

Spring 2015 Syllabus

6:40-9:20pm Wednesday (3 Units)
Room OHE 120

Instructor's Office Hours:

Wed. 3-4pm and by appointment.

Teaching Assistant: TBA

Office:
Office Hours:
Contact Info:

IT Help:

Hours of Service:
Contact Info:

Catalogue Description:

INF 523 Assurance in Cyberspace Applied to Information Security (3) Assurance as the basis for believing an information system will behave as expected. Approaches to assurance for fielding secure information systems that are fit for purpose. Recommended preparation: Prior degree in computer science, electrical engineering, computer engineering, management information systems, and/or mathematics. Some background in computer security preferred.

Expanded Course Description:

The definition of security for a system is given by the security policy. A system is "secure" only insofar as it correctly implements the security policy. But flaws in a system's design and implementation may create vulnerabilities that allow an attacker to violate that policy, and the complexity of computer systems make it difficult to verify that a system's design and implementation are free of flaws. In fact, the current state-of-the-art in system development is incapable of "proving" that a system of more than trivial complexity is secure.

Because absolute proof about the security of a system is (at least with current technology) unobtainable, a system's "assurance case" – the argument that the system correctly implements the security policy – is formed from a body of supporting evidence generated at different stages of the system lifecycle. This course will explore different techniques and methods for creating the assurance case.

Course Objectives:

Students will develop the following abilities:

- To *identify* stages in the system lifecycle where flaws may be introduced into a system
- To *describe* methods and techniques for creating an assurance argument
- To *evaluate* the strengths and weaknesses in each of the methods and techniques
- To *balance* costs with benefits of applying each method and technique based on an assessment of risk
- To *create* an assurance argument using the body of evidence generated at different stages in a system's lifecycle

Methods of Teaching:

The course will be primarily individual study, with weekly assigned readings, several homework assignments, short in-class quizzes, a project, a midterm and a final. Students may also be required to perform literature research.

Some of the homework assignments will require the use of special software. A virtual machine image will be provided that students can download and run on their own systems.

Assignments/Reports:

Students will be required to complete several homework and lab assignments. 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.

It is important that students turn in assignments 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 incomplete grade will be granted only under the conditions called out in the student handbook, *SCAMPUS*, which is available online, http://scampus.usc.edu.

Class Communication:

DEN Blackboard at USC will be used for class communication.

Grading Schema:
Final: 30%
Mid-Term: 25%
Quizzes: 10%
Homework Assignments: 25%
Class Participation: 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:

All reading listed in the class schedule (below) is required. The “Bishop book” (Computer Security Art and Science: Bishop, Matt, 2003) is the textbook used in first semester INF Cybersecurity courses.

Additional References

TBA

Class Structure & Schedule:

Class sequence, dates, topics and other scheduled items are subject to change as the semester proceeds. Any revisions will be noted and announced in class.

Week	Date	Topics Covered	Homework	Reading
1	Jan 14	**Course Introduction.** General introduction to class – requirements, schedule, approach, exams, homework, labs, structural overview of the course of study, grading approach, answer questions. **What is Assurance?** System lifecycle. The assurance argument. Types of evidence collectable at each stage of the lifecycle.		Bishop book, Chapter 18, "Introduction to Assurance" Introduction to the Secure Software Development Lifecycle (http://resources.infosecinstitute.com/intro-secure-software-development-life-cycle/)
2	Jan 21	**Measuring Security.** Security metrics and their applicability to assurance. **Security Risk Assessment.** Rationale for, and methods of, identifying and quantifying risks to an organization's information assets in order to allocate resources to increase assurance.		ISACA - How Can Security Be Measured? (http://www.isaca.org/Journal/Past-Issues/2005/Volume-2/Documents/jpdf052-how-can-security.pdf) ISACA - Performing a Security Risk Assessment (http://www.isaca.org/Journal/Past-Issues/2010/Volume-1/Documents/1001-performing-a-security.pdf)

3	Jan 28	**Assurance Requirements in Evaluation Criteria.** Assurance requirements at different evaluation levels. **Capability Maturity Models**. An approach for assessing the capability of a vendor to produce a secure system. **Microsoft's SDLC.** A contemporary, real-world assurance process at a major software company.		TCSEC, pp. 10, 50-53, 62-63, 67-68, 77-79 CC Part 3, pp. 15-17, 44-45 SSE-CMM/ISO 21827 Capability Maturity Model (http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html - search for "ISO 21827") Build Security In Maturity Model (BSIMM) (http://www.bsimm.com/) Microsoft Security Development Lifecycle (http://www.microsoft.com/security/sdl/default.aspx)
4	Feb 4	**Threat Modeling.** Methods of identifying threats and countermeasures.	Threat modelling	Attack Trees (https://www.schneier.com/paper-attacktrees-ddj-ft.html) Foundations of Attack–Defense Trees (http://satoss.uni.lu/members/barbara/papers/adt.pdf) A Requires/Provides Model for Computer Attacks (http://seclab.cs.ucdavis.edu/papers/NP2000-rev.pdf) Uncover Security Design Flaws Using the STRIDE Approach (http://msdn.microsoft.com/en-us/magazine/cc163519.aspx)

5	Feb 11	**Modularization and Layering**. System design using abstraction, encapsulation and information hiding. Separation of interface from implementation.		D.L. Parnas, *On the Criteria To Be Used in Decomposing Systems into Modules,* 1972 Daniel Hoffman, *On Criteria for Module Interfaces*, 1990 Paul Karger, et. al., *A VMM security kernel for the VAX architecture*, 1990 – Section 3.7 Final Evaluation Report, Gemini Trusted Network Processor, 1995 – Section 4.2

6	Feb 18	**Secure Programming.** Common flaws in software. Software development practices to help prevent vulnerabilities. Programming language features that aid in developing secure software. Bug tracking.		Bishop book, Chapter 23, “Vulnerability Analysis”, pp. 660-685 (vulnerability classification) IEEE – Avoiding the top 10 Software Security Design Flaws (http://cybersecurity.ieee.org/images/files/images/pdf/CybersecurityInitiative-online.pdf) [Skim] CERT Top 10 Secure Coding Practices (https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices) [Skim] Common Weakness Enumeration (http://cwe.mitre.org/) [Skim] OWASP Top 10 2013 (http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf) [Skim] SANS Top 25 Software Errors (https://www.sans.org/top25-software-errors/)

7	Feb 25	**Security Testing.** Types of testing, including static, dynamic, vulnerability scanning, and penetration testing.	Security testing tools	*Analysis Techniques for Information Security*, pp. 5-10 (static testing) Nathaniel Ayewah, David Hovemeyer, J. David Morgenthaler, John Penix, William Pugh, *Using static analysis to find bugs*, IEEE Software, vol. 25, no. 5, pp. 22–29, Sep./Oct. 2008 P. Oehlert, *Violating assumptions with fuzzing*, 2005 (fuzzing/dynamic testing) Jose Fonseca, et. al., *Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks*, 2007 (vulnerability scanning) Bishop book, Chapter 23, "Vulnerability Analysis", pp. 645-660 (penetration testing)
8	Mar 4	**Mid-Term Review** Review of major topics covered to this point.		
9	Mar 11	***Mid-Term Exam*** Closed book, in-class exam		
10	Mar 18	**Spring break. No class.**		
11	Mar 25	**Covert Channel Analysis**. Methods for detecting covert storage and timing channels.		Richard A. Kemmerer, *Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels*, 1983 Steven Gianvecchio and Haining Wang, *An Entropy-Based Approach to Detecting Covert Timing Channels*, 2011

12	Apr 1	**Secure Operation.** Secure distribution, configuration, maintenance, and disposal. System audit and integrity monitoring.		Gene H. Kim, The Design and Implementation of Tripwire: A File System Integrity Checker, 1993
13	Apr 8	**Introduction to Formal Methods.** Mathematical techniques for "proving" the security of a system. Propositional, first-order, and higher-order logics.	Basic proofs	Introduction to Logic, chapters 2, 3, 6, 7 (http://logic.stanford.edu/intrologic/chapters/cover.html)
14	Apr 15	**Formal Specifications and Proofs.** Formally specifying policies and systems in mathematical language. Showing the correspondence between system and policy.	Write a formal spec	
15	Apr 22	**Introduction to PVS Theorem Prover.** Introduction to writing formal specifications and doing proofs using PVS.	PVS proofs	
16	Apr 29	**Final Review.** Summary of major topics covered in the class.		
	May 1	*Classes End*		
		Study Days		
7-9 p.m.	Wed. May 6	***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)

Academic dishonesty includes: (Faculty Handbook, 1994: 21-22)
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.

Statement of Diversity
The diversity of the participants in this course is a valuable source of ideas, problem solving strategies, and creativity. I encourage and support the efforts of all of our students to contribute freely and enthusiastically. We are members of an academic community where it is our shared responsibility to cultivate a climate where all students and individuals are valued and where both they and their ideas are treated with respect, regardless of their differences, visible or invisible.