USCSchool Name

INF523 Computer Systems Assurance

Units: 4

3 Hour Lecture, plus 1 hour case study discussion

Location: Physical address and/or course-related URLs, etc.

Instructor:
Office:
Office Hours:

Contact Info: Email, phone number (office, cell), Skype, etc.

Teaching Assistant:
Office: Physical or virtual address
Office Hours:
Contact Info: Email, phone number (office, cell), Skype, etc.

IT Help: Group to contact for technological services, if applicable.
Hours of Service:
Contact Info: Email, phone number (office, cell), Skype, etc.

Course Description

All of us have experienced at one time or another the disquieting circumstance of having an information system upon which we depend (to one degree or another) behave in some unanticipated fashion. With the addition of networking and ubiquitous communications the problem has become more extensive and subtle. Just park all your data in the “cloud” and it will always be there for you to use. How do you know it will “always be there for you to use”? Generally how do we know that any of these all-encompassing services will always be there? The notion of how do you know is expressed in many fields of endeavor, and particularly in the digital domain as Assurance. For the purposes of this course, Assurance is defined as “the basis for believing an information system will behave as expected”.

The extent to which one can believe that a particular system will behave as expected has been one of the major challenges in fielding “secure” information systems. There are too many areas that can hide bugs, errors, design flaws, implementation errors, undocumented assumptions and the like, for any exhaustive approach to assurance to be effective. Consequently there has emerged a somewhat undisciplined if not chaotic approach(s) to assurance. This course will survey these approaches and analyze strengths, weaknesses, and shortcomings toward solving the challenge of fielding “secure information systems” that are fit for purpose.

This course revisits the ideas intended to be captured and enabled by assurance. It reviews the initial introduction of the concept in the computer / information security discipline; studies the evolution of the thinking; examines the multiple attempts to codify assurance; examines the current trajectory of assurance with regard to modern IT systems acquisition; addresses assurance with regard to the whole lifecycle and logistics process(s); addresses assurance with regard to hardware, assurance with regard to software, change control and systems management.

It turns out that assurance has been a major challenge from the beginning of the development of “secure” systems. In some perspectives we have achieved observable improvement. In other areas we cannot tell and in others we have clearly lost ground.

It is recommended that students have some background in computer security, or a strong willingness to learn. Recommended previous courses of study include computer science, electrical engineering, computer engineering, management information systems, and/or mathematics.

This class will be primarily individual study, with weekly assigned readings, approximately seven homework assignments, four quizzes, one group project, a midterm and a final. In addition to the foundational material, case studies of assurance in illustrative real systems will be covered in lecture. In a weekly discussion section

In a separate discussion section which meets as part of the class, students will be guided by the instructor in preparation for presentation of a group project that involves creation of a case study on assurance for a particular class of system such as cloud services, mobile payments, file storage.

Learning Objectives

Students will be given the opportunity to examine the source material for the original motivation and introduction of assurance into the vernacular and analysis of information security. They will follow the motivation and evolution of the concepts of assurance through the codification of assurance to its subsequent dilution and disassociation as is captured in today's common criteria. Students will examine mechanisms and processes that support / subtract from the assurance argument. Students will have the opportunity to study the relationship between assurance and risk management.

Methods of Teaching:

The primary teaching method will be discussion, case studies, 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 are to 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, complete regular exams to reinforce the concepts taught and highlight weaknesses in grasp and presentation, complete assigned projects to apply and illustrate the concepts (through demonstrations or class projects). In groups, students will prepare a case study on assurance in a relevant current day system.

There will be one mid-term exam and a final examination, along with four quizzes.

Students will be required to complete approximately seven homework assignments, which should average approximately ten hours to finish.

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

Prerequisite(s): Informatics 519
Co-Requisite (s): None
Concurrent Enrollment: None

Required Readings and Supplementary Materials

All books, papers or reports will be available to students in one of three ways: 1) in the USC bookstore; 2) through posting of materials in desire 2 learn, or 3) via the web.

Books:

BISHOP, Matt Bishop, *Computer Security: Art and Science*, Addison-Wesley, 2002.

WARE, "Security Controls for Computer Systems"(The Ware Report), Rand Corporation, February 11, 1970.

ANDERSON, “Computer Security Technology Planning Study” (The Anderson Report) ESD-TR-73-51, Vol. ll, James P. Anderson and Company, October 1972.

TDI Trusted Database interpretation of the TCSEC

Rainbow Series: The Orange Book
Federal criteria
German Green Book
Common Criteria
Goldman’s Paper GPALS

Description and Assessment of Assignments

The following assignments are representative of those which will be assigned. The specific of the assignment will vary from semester to semester.

Homework Assignment #1:

- Scope: Assurance Models in the Commercial Sector
- Objective: To understand the principles of assurance and how this applies to organizational decision making and information security
- Tasks: Complete a 10 page report on the following topic: find worked examples of assurance applied to commercial products. You must find at least five examples, and ascertain to what extent they have common characteristics.

Homework Assignment #2:

- Scope: Assurance and the Product Life Cycle
- Objective: To understand the dynamics and principles of assurance as it relates to a product’s life cycle and subsequently organizational planning
- Tasks: Complete a 10 page report: explaining how assurance is established across the product life cycle.

Homework Assignment #3:

- Scope: Assurance Models in the Commercial and Computational Spaces
- Objective: To understand the similarities and differences between assurance models in the commercial space and in the digital domain.
- Tasks: Complete a 10 page report on: (what are the) similarities and differences between assurance in the commercial sector and the virtual/computational domain? Provide examples of each type.

Homework Assignment #4:

- Scope: Assurance and Risk
- Objective: To understand the principles and relationship between assurance and risk, and the relationship to information security
- Tasks: Complete a 10 page report on (what is) the relationship between assurance and risk? How does the relationship change in the face of an evolving threat?

Homework Assignment #5:

- Scope: Notion of Greater Assurance
- Objective: To understand the meaning of "greater assurance" in both the physical and cyber world, and how to apply this to information security
- Tasks: Complete a 10 page report on: does the notion of greater assurance have any validity? Justify your answer, and if "yes", give examples and explain.

Homework Assignment #6:

- Scope: Coupling Features with Assurance
- Objective: To understand the notion of coupling features with assurance, both in philosophy and practice, and as applied to solving information security challenges
- Tasks: Complete a 10 page report on: (what is) the underlying philosophy coupling features with assurance? And if that coupling is abandoned, what can go wrong?

Homework Assignment #7:

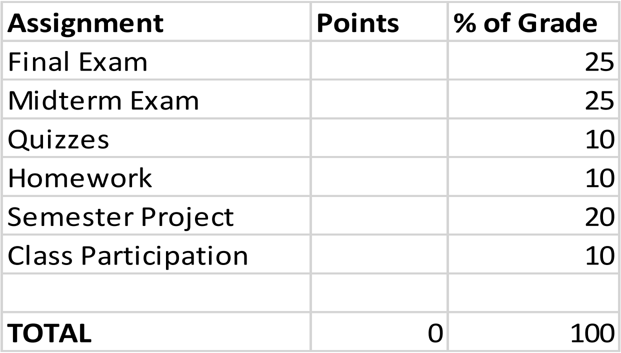
- Scope: Assurance and Common Criteria
- Objective: To understand the principles of assurance as described in the common criteria and understand how this matters in information security.
- Tasks: Complete a 10 page report on: the common criteria speaks of assurance packages, how is a common criteria assurance package reconciled with threat, risk and operations?

Semester Project:

This project is a group project. Students will prepare a case study on assurance in a currently relevant application domain such as cloud computing, mobile payments, distributed file storage, etc. The topic will be approved by the instructor before students begin the project.

Grading Breakdown

How will students be graded overall, including the assignments detailed above. Participation should be no more than 15%, unless justified for a higher amount. All must total 100%.



Assignment	Points	% of Grade
Final Exam		25
Midterm Exam		25
Quizzes		10
Homework		10
Semester Project		20
Class Participation		10
TOTAL	0	100

Assignment Submission Policy

All homework assignments are to be submitted individually; however students may work in groups to complete the tasks. There is one midterm test and a final exam which date will be determined by the College. There will be four quizzes. There will be seven homework assignments and one semester project.

Guidelines and additional information will be developed, which will provide a common vernacular for the assignments. It is crucial that students turn in whatever they have on the due date. NO assignment will be accepted late. 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.

Additional Policies

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.

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.

Course Schedule: A Weekly Breakdown

Week/ class	Date	Topics Covered	Home work	Assignment
1a		General introduction to class – requirements, schedule, approach, tests, homework, standing assignments, structural overview of the IA course of study, grading approach, answer questions.		
1b		Start Genesis of assurance. Genesis of assurance	HW#1 Due:	
2a		So what is assurance and why do we need / use / have assurance (no way to prove the absence of a negative behavior, cannot prove the absence of a flaw) Working examples: consumer reports, Underwriters Lab, Good House Keeping, EBay seller's ratings.		Read the Ware Report Read the Anderson Report
2b		What is the purpose of these and other such actions? What sort of things do / do not constitute assurance A definition of assurance		In Class Quiz
3a		Assurance in everyday life Are product guarantees a sort of assurance or something else? Does assurance have scope (yes)	HW#2 Due:	
3b		Is testing a form of assurance? Why / why not is testing sufficient?		Last day to drop class is
4a		Emergence of assurance in the information technology. IA discipline		Read Pete and Brian Read BISHOP 18 Read the Orange Book.
4b		The idea of mechanism versus process / evidence	HW#3 Due:	Cont, Orange Book
5a		Considerations / complexities re assurance		Read the TNI

		Coupling of Features and Assurance. Does it make sense to invest in high assurance for a fundamentally weak component / service?		READ BISHOP 19
5b		Does assurance have scale? Evaluation by parts, Balanced assurance The binding of assurance to perceived threat / extend of “harms way” The composition problem		Read the TDI READ BISHOP 20
6a		Examination of a actual Final Evaluation Report: Assurance argument.		Read the FER for the STX 200
6b		Assurance in process: The Capability Maturity Model. The problem is the CMM does not of itself specify a process	HW#4 Due:	In Class Quiz #2 Read CMM READ BISHOP 21
7a		More assurance in process GPALS. GPALS is a process (actually a nest of processes) that map to CMM		Read GPALS 1&2
7b		The evolution of assurance in criteria Revisit the Orange Book / Red Book and the Integrity interpretation		Read the German Green Book
8a		The Political / Economic climate and motivations. Break into the EPL. The decoupling of features and assurance The German Green Book (Christian Jahall		READ FEDERAL CRITERIA READ TINTO
8b		The cascading of new Criteria and national schemes Everybody wanted into the act. Evaluation shopping Competing “lists” The Brits criteria, and France and Canada		Read the Federal Criteria
9a		Review		Review Mid-Term
9b		Mid Term Exam		
10a		The revision of the OB and the treatment of Assurance The Federal Criteria	HW#5 Due:	

		Examine the positioning of assurance. What has happened to assurance through this evolution.		
10b		Change of Ownership of the Criteria – transfer from NCSC to NIST Harmonization of the Criteria.		Read the Common Criteria
11a		The Common Criteria	HW#6 Due:	In Class Quiz #3
11b		The organization of Assurance in The CC		READ CC
12a		How does it actually work?		
12b		Examination of the various national schemes		
13a		Examination of an actual CC evaluation report: Assurance argument	HW#7 Due:	Cf cc evaluated product list
13b		What seems to be missing in the current assurance paradigm?		
14		Remaining problems		In Class Quiz #4
15a		National Mandates WRT the CC		Read NSTICC 11
15b		How might assurance be extended to Secure systems engineering		Semester Project Case Studies Due
16		*The final exam will be held as indicated in the online schedule of classes.*		

Statement on Academic Conduct and Support Systems

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.