INF 525: TRUSTED SYSTEM DESIGN, ANALYSIS, AND DEVELOPMENT

Professor Roger R. Schell
rrschell@usc.edu
Phone: (213) 740-9438
Office: GER 203

Spring 2015 Syllabus

2:00-3:20pm Tue, Thu (3 Units)
Room RTH217

Course Description:

High consequence applications such as those for critical infrastructure require highly reliable, trusted systems to assure the required availability of processing, and to assure the required confidentiality and integrity of information and processing, even if some parts of the system have high exposure to a witted adversary employing subversion. Hardware and software design techniques for these Trusted Systems must evolve and advance as the sophistication of the cyber adversary also advances. This course conveys a methodology for the development of trusted systems using the Reference Monitor concept as a unifying principle. Highly secure Trusted Systems are based on what is called a Security Kernel that incorporates the Reference Validation Mechanism – the hardware and software that implements the Reference Monitor.

Trusted Systems lay at the core of secure systems. A detailed understanding of the design, analysis and implementation of trusted systems is essential for the development of secure information systems. This course provides an overview of computer security to include an analysis of what is computer security, why systems are not secure, and the general concepts and design techniques applicable to the design of hardware and software. It examines in detail the principles of a security architecture, access control, policy and the threat of malicious code; the considerations of trusted system implementation to include hardware security mechanisms, security models, security kernels, and architectural alternatives; the related assurance measures associated with trusted systems to include documentation, formal specification and verification, and testing. That core needs to be sufficiently capable that it can be leveraged by approaches that extend the trusted system, into applications such as databases and into networks and distributed systems.

This course is intended for graduate students typically coming out of computer science, mathematics, computer engineering, or informatics. Students need to be familiar with operating system principles and able to program. Advanced knowledge of computer architecture, theory of computation, and communications networks will be valuable. Students should 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.

This class will be primarily individual study, with weekly assigned readings, homework assignments, one semester project, a midterm examination and a final examination.

Prerequisite: INF 522 – Policy: The Foundation for Successful Information Assurance

Objectives:

Students will have ten learning objectives for the course, and additional technology application objectives:

Learning Objectives:

1. Understand the fundamental issues that motive computer security to include the impediments and the motivating threat strategies such as subversion
2. Understand the technical basis for the development of trust in computer systems
3. Understand the relationship between trust and policy in trusted computer systems, and the pivotal role of a formal security policy model
4. Understand in depth the techniques and approaches for designing trusted technology in computer systems, including information hiding and layering
5. Understand the relationship and dependences between the underlying hardware and the trusted technologies that can be built on that hardware
6. Understand and be able to apply the fundamental design considerations for trusted systems
7. Understand in detail the concepts of the reference monitor and the nature of the root of trust provided by cryptographic attestation.
8. Understand the architectural issues that are essential to the implementation of trusted technology, including implications of hardware segmentation
9. Understand the processes for specification of trusted systems and how that specification relates to the sufficiency of trusted technology.
10. Understand the extension of the trust model into trusted applications

Technology Application Objectives:

1. Synchronization
2. System initialization
3. Protection rings
4. Multiprocessing
5. Virtualization
6. Non-discretionary security representation generality
7. Trusted Distribution
8. Hardware root of trust
9. Methods of analysis and evaluation

Methods of Teaching:

The primary teaching method will be discussion, case studies, lecture, 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 participation in class 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 and highlight weaknesses in grasp and presentation. They will complete a final semester project to apply and illustrate the concepts in an applied manner.

Students will also be given laboratory assignments which they must complete outside class time. These assignments will generally take multiple sessions to complete. Each lab will be guided via a lab workbook. Labs may or may not require a computing facility. If a computing facility is necessary, one will be provided at the USC University Park campus.

Office Hours: Each semester one hour per week will be announced in class as regular office hours. 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 and Examinations:

Students will be required to complete several homework assignments, which may take several hours to complete. All homework assignments are to be prepared and submitted individually; however students may work in groups to understand and discuss the tasks. There is one midterm test and a final exam which 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.

In class exams and quizzes will be closed book, no notes, no crib-sheets, no electronic devices. Exams/quizzes missed due to a verified serious illness will be assigned a grade scaled from other work.

Guidelines and additional information will be developed and provide for the submission of assignments. 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. Since assignments and projects are expected to be turned in by the time specified there is a substantial grade penalty for late submission. It is recommended that students turn in whatever they have on the due date. The penalty for late submission is a cumulative of 10% times number of days late as reflected below:

1 day late: lose 10%
2 days late: lose 30% (10% + 20%)
3 days late: lose 60% (30% + 30%)
4 days or more late not accepted

Semester Project:

The semester project gives each student the opportunity to use and illustrate the concepts from the course in an applied manner in not less than 7 nor more than 15 pages. This course conveys a methodology for the development of trusted systems using the Reference Monitor concept as a unifying principle. Highly secure Trusted Systems are based on what is called a Security Kernel that incorporates the Reference Validation Mechanism (RVM) – the hardware and software that implements the Reference Monitor. Morrie Gasser in his book Building a Secure Computer System says (p. 162), "The first security kernel, developed by MITRE as government sponsored research project to prove the concept, ran on a DEC PDP 11/45." The design for this project is available in the literature. Based on information you gather and review, you are to report your research and analysis of how this early proof of concept developed by Lee Schiller did, and did not, satisfy requirements of the design and development technologies we have studied.

Class Communication:

Desire2Learn 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 including USC library access.

Required Readdings:

TEXTBOOKS:

[GAS] Building A Secure Computer System, by Morrie Gasser, Van Nostrand Reinhold, New York, 1988.

[ORG] The Multics System: An Examination of Its Structure, by Elliot L. Organick, The MIT Press, Cambridge, Massachusetts, 1972.

LITERATURE:

[A1M] "Security Requirements for a Class A1 M-Component", Extracts from Trusted Network Interpretation. "NCSC-TG 005." National Computer Security Center (1990), prepared August 17, 2005.

[AMES] Ames Jr, Stanley R., Morrie Gasser, and Roger R. Schell. "Security kernel design and implementation: An introduction." *Computer* 16.7 (1983): 14-22.

[EVC] Reed, David P., and Rajendra K. Kanodia. "Synchronization with eventcounts and sequencers." Communications of the ACM 22, no. 2 (1979): 115-123.

[GKS] Schell, Roger, Tien F. Tao, and Mark Heckman. "Designing the GEMSOS security kernel for security and performance." *Proceedings of the 8th National Computer Security Conference*. Vol. 30. 1985.

[EPL] Evaluated Product List, Gemini Computers, Incorporated, GTNP Version 1.01, Network Component,M Only, CSC-EPL-94-008, National Security Agency, 6 September 1994.

[LEV] Levin, T. E., Tao, A., & Padilla, S. J. (1990). Covert Storage Channel Analysis: A Worked Example. *Proc. National Computer Security Conference*, 10-19

[MTS] Schell, R.R., and Tao, T.F., Microcomputer-Based Trusted Systems for Communication and Workstation Applications, Proceedings of the 7th DoD/NBS Computer Security Initiative Conference, NBS, Gaithersburg, MD, 24-26 September 1984, pp. 277-290.

[MULT] Bensoussan, Andre, Charles T. Clingen, and Robert C. Daley. "The Multics virtual memory: concepts and design." Communications of the ACM 15.5 (1972): 308-318.

[FER] *Final Evaluation Report, Gemini Computers, Incorporated, Gemini Trusted Network Processor, Version 1.01*, National Computer Security Center, 1995

[SFG1] GTNP Security Features User's Guide, Vol 1, *Introduction to the GEMSOS Security Kernel*, GNT00-SFG01-0005C, April 24, 2003.

[SFG2] GTNP Security Features User's Guide, Vol 2, *Programmer's Guide to the GEMSOS Security Kernel Interface*, GTN00-SFGP2-0008a, June 1, 2004.

[TCSEC] Department of Defense, 1985, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, Washington, DC.

[VMM] Karger, Paul A., Mary Ellen Zurko, Douglas W. Bonin, Andrew H. Mason, and Clifford E. Kahn. "A retrospective on the VAX VMM security kernel." *Software Engineering, IEEE Transactions on* 17, no. 11 (1991): 1147-1165

Course Plan:

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

The class material is covered in the following tentative order. There will typically be 1-3 class periods for each of the following topics:

1. Introduction to Reference Validation Mechanism – the Security Kernel (SK)
2. Overview of security kernel systematic software engineering process
3. Design of SK modules: information hiding, layering and minimization
4. Reference monitor objects implemented by SK as segmentation
5. Security kernel layering
6. Designing a security kernel
7. Trusted system building techniques
8. Kernel implementation strategies
9. Confinement and covert channels
10. Synchronization in a trusted system
11. Secure initialization and configuration
12. Management of SK rings and labels
13. Trusted distribution and Trusted Platform Module
14. Security analysis of trusted systems

Statement on Academic Conduct, Support Systems and Diversity

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://capsnet.usc.edu/department/department-public-safety/online-forms/contact-us. 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.

Diversity

The diversity of the participants in this course is a valuable source of ideas, problem solving strategies, and engineering 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.