DSCI 525: TRUSTED SYSTEM DESIGN, ANALYSIS, AND DEVELOPMENT

Spring 2022 Syllabus

Instructor	Email	Office Hours	Lecture
Tatyana Ryutov	tryutov@usc.edu	Thursday 3-5pm via Zoom In-person by request, PHE 336	Monday 2:00-5:20pm RTH 217

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

Course Resources
Piazza **https://piazza.com/usc/spring2022/dsci525** will be used for posting lecture notes, announcements, assignments, and intra-class communication

- DEN D2L will be used for:
  - posting of grades
  - homework submission
  - quiz submission
  - exam submission

Learning Objectives
Students will have the following learning 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. Virtualization
5. Non-discretionary security representation generality
6. Trusted distribution
7. Hardware root of trust
8. Methods of analysis and evaluation
9. Software engineering practices of secure system development and management
10. Hardware vulnerabilities and techniques for building secure and trusted hardware

Grading

Quizzes	15%
Midterm	20%
Final Exam	20%
HW Assignments	20%
Class Participation	10%
Semester Project	15%

Technological Proficiency and Hardware/Software Required
This course is intended for graduate students typically coming out of computer science, mathematics, computer engineering, or informatics. Background in computer security, computer architecture, operating systems, software development preferred. Recommended previous course of study is DSCI-519.

All key concepts and relevant methodology will be reviewed and introduced throughout the course, however students should be comfortable learning about basics of operating systems and software development.

Required Readings:

REQURED TEXTBOOKS:

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

[OSS] Operating System Security, Trent Jaeger, 2008.

LITERATURE:

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

[CRO] Alexander Crowell, Beng Heng Ng, Earlence Fernandes, Atul Prakash: The Confinement Problem: 40 Years Later. JIPS 9(2): 189-204, 2013.

[PARNAS] D. L. Parnas. "On the Criteria to Be Used in Decomposing Systems into Modules," Communications of the ACM, Vol. 15, No. 12, pp.1053-1058, 1972.

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

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

[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. Covert Storage Channel Analysis: A Worked Example. Proc. National Computer Security Conference, 1990.

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

[PATTERNS] Using Proven Reference Monitor Patterns for Security Evaluation, Mark R. Heckman, and Roger R. Schell, 2016.

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

[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.

[STACK] Smashing the stack for fun and profit, by Aleph One.

[BUF] Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade by Crispin Cowan, Perry Wagle, Calton Pu, Steve Beattie, and Jonathan Walpole.

[LOW] Low-level Software Security by Example by Ulfar Erlingsson, Yves Younan, and Frank Piessen.

[RET] Return-Oriented Programming: Systems, Languages, and Applications by Ryan Roemer, Erik Buchanan, Hovav Shacham, and Stefan Savage.

Supplemental Readings:

[MCGRAW] Software Security: Building Security In, book by Gary McGraw.

[HW] Introduction to Hardware, Security and Trust, book by Mohammad Tehranipoor, Cliff Wang, 2012.

Description and Assessment of Assignments
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. There will be several short in-class quizzes. There will be several homework assignments and one semester project.

Assignment Submission Policy
All assignments are to be submitted individually. Assignments and projects are due on time. There is a substantial grade penalty for late submission. 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

Projected Course Schedule: A Weekly Breakdown
Class sequence, dates, reading assignments, and topics are subject to change as the semester proceeds. Any revisions will be noted and announced in class.

Lectures	Topics	Readings
Lecture 1 1/10	Course introduction, Overview of Trusted Operating System Design and • Security Kernel (SK) approach, • Software engineering practices of secure system development and management	OSS Chapter 1, 2, 4 GAS Chapters 2, 4 EPL FPIGS PATTERNS
1/17	**No lecture, University holiday**	
Lecture 2 1/24	Design of SK modules: information hiding, layering and minimization, Reference	GAS Chapter 5.2, 8 PARNAS GKS

	monitor objects implemented by SK as segmentation	SFG1 Sections 1-4 SFG2 Sections 4.1 and 4.6.13
Lecture 3 1/31	Security kernel layering Designing a security kernel Detailed design principles for secure systems Management of SK rings and labels	GKS LEV FER Sections: 4.2.1.6, 4.2.1.7.3, 6.1, 6.1.1, 8.10, 10.5 SFG1 Sections: 6-6.4 **Quiz 1**
Lecture 4 2/7	Trusted system building techniques, Trusted path, Trusted functions, Kernel implementation strategies	GAS Chapter 10 VMM
Lecture 5 2/14	Alternative approaches • Capability systems • Separation kernels	OSS Chapters 10 and 11.1 OSS Chapter 6.2
2/21	**No lecture, University holiday**	
Lecture 6 2/28	Confinement and covert channels, Covert channel analysis	CRO GAS Chapter 7 FER pages 61-63 FER Sections: 8.6, 8.11, 10.6 **Quiz 2**
Lecture 7 3/7	Synchronization in a trusted system, Secure initialization and configuration	EVC FER Sections: 4.2.1.6, 4.2.1.7.3, 6.1, 6.1.1, 8.10, 10.5
3/14	**No lecture, Spring recess**	
3/21	**Midterm** **Topic TBD**	
Lecture 8 3/28	Security analysis of trusted systems	A1M
Lecture 9 4/4	Low-level, memory-based attacks and defenses	RET, STACK, BUF, LOW **Quiz 3**
Lecture 10 4/11	Secure Software Development Static Analysis, Symbolic Execution, Penetration Testing, Fuzzing	MCGRAW (supplemental)
Lecture 11 4/18	Trusted computing, Trusted Platform Module, Trusted distribution	FER Sections: 2.4, 4.0, 4.1.9, 4.2.1.3.5, 4.2.1.8.2.6, 4.5.1, 4.5.2, 7.8, 8.20, 8.22 **Quiz 4**
Lecture 12 4/25	Hardware security, vulnerabilities, attacks, Hardware Trojans, Techniques for building secure and trusted hardware	HW (supplemental)
Final Exam May 9, 2-4pm		

Synchronous session recording notice

Live class sessions will be recorded and made available to students through D2L. Please remember that USC policy prohibits sharing of any synchronous and asynchronous course content outside of the learning environment. As a student, you are responsible for the appropriate use and handling of these recordings under existing SCampus policies regarding class notes (https://policy.usc.edu/scampus-part-c/). These rules will be strictly enforced, and violations will be met with the appropriate disciplinary sanction.

Learning Experience Evaluations

Learning Experience Evaluations will be completed during the last day of class. This will be your opportunity to provide feedback about your learning experience in the class. This feedback helps the instructor determine whether students are having the intended learning experiences for the class. It is important to remember that the learning process is collaborative and requires significant effort from the instructor, individual students, and the class as a whole. Students should provide a thoughtful assessment of their experience, as well as of their own effort, with comments focused on specific aspects of instruction or the course. Comments on personal characteristics of the instructor are not appropriate and will not be considered. For this feedback to be as comprehensive as possible, all students should complete the evaluation.

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 Part B, Section 11, "Behavior Violating University Standards" policy.usc.edu/scampus-part-b. Other forms of academic dishonesty are equally unacceptable. See additional information in SCampus and university policies on scientific misconduct, policy.usc.edu/scientific-misconduct.

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.

Support Systems

Counseling and Mental Health - (213) 740-9355 – 24/7 on call
studenthealth.usc.edu/counseling
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

National Suicide Prevention Lifeline - 1 (800) 273-8255 – 24/7 on call
suicidepreventionlifeline.org
Free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week.

Relationship and Sexual Violence Prevention Services (RSVP) - (213) 740-9355(WELL), press "0" after hours – 24/7 on call
studenthealth.usc.edu/sexual-assault
Free and confidential therapy services, workshops, and training for situations related to gender-based harm.

Office of Equity and Diversity (OED) - (213) 740-5086 | Title IX – (213) 821-8298
equity.usc.edu, titleix.usc.edu
Information about how to get help or help someone affected by harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants.

Reporting Incidents of Bias or Harassment - (213) 740-5086 or (213) 821-8298
usc-advocate.symplicity.com/care_report
Avenue to report incidents of bias, hate crimes, and microaggressions to the Office of Equity and Diversity |Title IX for appropriate investigation, supportive measures, and response.

The Office of Disability Services and Programs - (213) 740-0776
dsp.usc.edu
Support and accommodations for students with disabilities. Services include assistance in providing readers/notetakers/interpreters, special accommodations for test taking needs, assistance with architectural barriers, assistive technology, and support for individual needs.

USC Campus Support and Intervention - (213) 821-4710
campussupport.usc.edu
Assists students and families in resolving complex personal, financial, and academic issues adversely affecting their success as a student.

Diversity at USC - (213) 740-2101
diversity.usc.edu
Information on events, programs and training, the Provost's Diversity and Inclusion Council, Diversity Liaisons for each academic school, chronology, participation, and various resources for students.

USC Emergency - UPC: (213) 740-4321, HSC: (323) 442-1000 – 24/7 on call
dps.usc.edu, emergency.usc.edu
Emergency assistance and avenue to report a crime. Latest updates regarding safety, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible.

USC Department of Public Safety - UPC: (213) 740-6000, HSC: (323) 442-120 – 24/7 on call
dps.usc.edu
Non-emergency assistance or information.

Office of the Ombuds - (213) 821-9556 (UPC) / (323-442-0382 (HSC)
ombuds.usc.edu
A safe and confidential place to share your USC-related issues with a University Ombuds who will work with you to explore options or paths to manage your concern.