CS785004-ST: Trusted Computing & Architecture

Jump to Today Edit

CS 785: Special Topic on Trusted Computing & Architecture

Instructor: Dr. Zephyr Yao (zhihao.yao@njit.edu)

Class time/place: Tuesday 2:30 PM - 5:20 PM, FMH 319

Office hours: Friday 3:30 PM - 4:30 PM, GITC 4317A

Presentation Signup Sheet: https://docs.google.com/spreadsheets/d/1-D8q6kAqKEfXa-aSohQjavqDK3L1RkriOnNTnhFgZX4/edit#gid=0 (https://docs.google.com/spreadsheets/d/1-D8q6kAqKEfXa-aSohQjavqDK3L1RkriOnNTnhFgZX4/edit#gid=0)

Course Goals:

A study of trusted computing basics and design decisions. Review on memory management and operating system access control, and an introduction to microkernel, virtualization, and Trusted Execution Environments (TEEs). Learn the different threat models and security guarantees, and how recent trusted computing solutions work to ensure system security. You are expected to read and code.

Course Policies:

Academic Integrity:

All exams are closed note and closed book. You are expected to independently develop all source code (i.e., you cannot make use of source code found on the internet) for the coding assignments, unless it is approved in writing by teaching staff. If you decide to work on the course project as a group (max 2 people), you must inform the teaching staff. Academic integrity is a shared responsibility within the group. If any member of the group engages in plagiarism (e.g., copying code from the internet), the entire group may be subject to disciplinary measures. That is being said, you must adhere to NJIT Academic Integrity Policy both as an individual and as part of a group.

Knowingly allowing someone to copy your work is considered academic dishonesty. It is important that you do not share your quiz answers to anyone and do not share your course project source code (including posting publicly on GitHub). However, you ARE ALLOWED to engage in discussions related to concepts, ideas, and syntax errors. Sharing or posting course materials on the Internet without permission from the instructor is not allowed.

Academic Integrity is the cornerstone of higher education and is central to the ideals of this course and the university. Cheating is strictly prohibited and devalues the degree that you are working on. As a member of the NJIT community, it is your responsibility to protect your educational investment by knowing and following the academic code of integrity policy that is found at: NJIT Academic Integrity Code.

Please note that it is my professional obligation and responsibility to report any academic misconduct to the Dean of Students Office. Any student found in violation of the code by cheating, plagiarizing or using any online software inappropriately will result in disciplinary action. This may include a failing grade of F, and/or suspension or dismissal from the university. If you have any questions about the code of Academic Integrity, please contact the Dean of Students Office at dos@njit.edu

Respectful Behavior: Treating instructors, peers, and course staff with respect and professionalism. Turning your electronic devices to silent mode during classes and exams.

Attendance: You are strongly encouraged to attend all classes. If you miss a class, it is your responsibility to catch up on missed material. If you have a documented emergency, you must send your request directly to NJIT Dean of Students as soon as possible. See instructions at, **https://www.njit.edu/dos/student-absence-verification (https://www.njit.edu/dos/student-absence-verification)** . **Do not send your documentation to the teaching staff.** After the Dean of Students approves your request, you may take a make-up exam. If you miss an exam without approval from the Dean of Students, you will receive no credit for the missed exam. The lowest two in-class quiz scores will be dropped, so you do not need to inform the teaching staff if you are going to miss an in-class quiz. There are no make-up quizzes.

If you need any accessibility accommodation, you should contact NJIT Office of Accessibility Resources and Services. Their contact information is listed at, **https://www.njit.edu/accessibility/accommodations-and-support-services (https://www.njit.edu/accessibility/accommodations-and-support-services)** .

Canvas: Regularly check Canvas for updates and announcements. This syllabus and schedule are subject to change. It is the student's responsibility to stay informed about any changes or additional information posted by the instructor.

Grading (total 100 pts):

Paper presentations: 30 pts

Paper summaries & Participation: 30 pts

Course project: 40 pts

Letter grades are translated as follow,

A 90% and above

B+ 85% and above

B 80% and above

C+ 75% and above

C 70% and above

F otherwise

Paper summaries

- Each presentation is conducted by an individual student.
- Sign up for a presentation on Google Sheet, **https://docs.google.com/spreadsheets/d/1-D8q6kAqKEfXa-aSohQjavqDK3L1RkriOnNTnhFgZX4/edit?usp=sharing** **(https://docs.google.com/spreadsheets/d/1-D8q6kAqKEfXa-aSohQjavqDK3L1RkriOnNTnhFgZX4/edit?usp=sharing)**
- Each presentation should last for at least 40 minutes, followed by a 10-minute Q&A session.
- Paper Selection: Assigned papers, but approval may be sought for presenting a paper of choice. Inform the instructor at least 2 weeks prior to your presentation if you would like to present a paper of your choice, so that the other students can be informed of the change.
- Presentation grades will be based on the quality of the presentation and the students' understanding of the paper content.
- Each student is required to present at least one paper. However, you have the option to volunteer for additional presentations. Your paper presentation score will be based on the highest performance among all your presentations.
- Grading criteria for presentation is listed below: high-level idea grasp (20%), correctness in paper's design and implementation (20%), presentation of evaluation (20%), presentation of related work (20%), response to questions (20%). These criteria applies to your project presentation as well.

Paper Summaries

- Submit a hardcopy summary before the class starts weekly, accompanying the paper presentation. Using AI to generate paper summaries is not allowed.
- Content: One-page summary with at least 3 thoughtful questions.

Course project

See details at Canvas Page: Course Project

Schedule

Week 1: January 16 System security overview

Week 2: January 23 Cryptography basics and TPM

Week 3: January 30 Virtual Machine 1 - Overview

Week 4: February 6 Virtual Machine 2 - Secure VM

Week 5: February 13 Virtual Machine 3 - I/O virtualization

Week 6: February 20 Microkernel-based trusted computing

Week 7: February 27 TBD

Week 8: March 5 Secure language-based trusted computing

Week 9: March 12 (Spring Recess, no class)

Week 10: March 19 Intel SGX overview

Week 11: March 26 ARM TrustZone overview

Week 12: April 2 Speculative execution and side-channel attacks

Week 13: April 9 Hardware-isolated trusted computing

Week 14: April 16 Confidential computing in AI and ML

Week 15: April 23 Final project presentations

Week 16: April 30 Final project presentations

Presentation and paper reading will be based on the weekly schedule below.

https://docs.google.com/spreadsheets/d/1-D8q6kAqKEfXa-aSohQjavqDK3L1RkriOnNTnhFgZX4/edit#gid=0 (https://docs.google.com/spreadsheets/d/1-D8q6kAqKEfXa-aSohQjavqDK3L1RkriOnNTnhFgZX4/edit#gid=0)

	Date	Paper	Link
Week 1	January 16	N/A	
Week 2	January 23	Trusted Platform Module as an Enabler for Security in Cloud Computing	https://ieeexplore.ieee.org/abstract/document/5931361 (https://ieeexplore.ieee.org/abstract/document/5931361)
Week 3	January 30	Xen and the art of virtualization	https://dl.acm.org/doi/10.1145/945445.945462 (https://dl.acm.org/doi/10.1145/945445.945462)
Week 4	February 6	The Turtles Project: Design and Implementation of Nested Virtualization	https://www.usenix.org/legacy/events/osdi10/tech/full_papers/Ben-Yehuda.pdf (https://www.usenix.org/legacy/events/osdi10/tech/full_papers/Ben-Yehuda.pdf)
Week 5	February 13	Sugar: Secure GPU acceleration in web browsers	https://dl.acm.org/doi/pdf/10.1145/3296957.3173186 (https://dl.acm.org/doi/pdf/10.1145/3296957.3173186)
Week 6	February 20	seL4: Formal Verification of an OS Kernel	http://web1.cs.columbia.edu/~junfeng/09fa-e6998/papers/sel4.pdf (http://web1.cs.columbia.edu/~junfeng/09fa-e6998/papers/sel4.pdf)
Week 7	February 27	TBD	
Week 8	March 5	Theseus: an Experiment in OS Structure and State Management	https://www.usenix.org/system/files/osdi20-boos.pdf (https://www.usenix.org/system/files/osdi20-boos.pdf)
Week 9	March 12	- SPRING RECESS -	
Week 10	March 19	Innovative Instructions and Software Model for Isolated Execution	https://dl.acm.org/doi/10.1145/2487726.2488368 (https://dl.acm.org/doi/10.1145/2487726.2488368)
		AdAttester:	

Week 11	March 26	Secure Online Mobile Advertisement Attestation Using TrustZone	https://dl.acm.org/doi/10.1145/2742647.2742676 (https://dl.acm.org/doi/10.1145/2742647.2742676)
Week 12	April 2	Spectre Attacks: Exploiting Speculative Execution	https://ieeexplore.ieee.org/document/8835233 (https://ieeexplore.ieee.org/document/8835233)
Week 13	April 9	Minimizing a Smartphone's TCB for Security-Critical Programs with Exclusively-Used, Physically-Isolated, Statically-Partitioned Hardware	https://dl.acm.org/doi/pdf/10.1145/3581791.3596864 (https://dl.acm.org/doi/pdf/10.1145/3581791.3596864)
Week 14	April 16	SGXIO: Generic Trusted I/O Path for Intel SGX	https://dl.acm.org/doi/10.1145/3029806.3029822 (https://dl.acm.org/doi/10.1145/3029806.3029822)
Week 15	April 23	- PROJECT PRESENTATION -	
Week 16	April 30	- PROJECT PRESENTATION -	

Course Summary:

Date	Details	Due
	Course evaluation (https://njit.instructure.com/courses/33911/assignments/416973)	
	Paper discussion (https://njit.instructure.com/courses/33911/assignments/416931)	

[Paper summary](https://njit.instructure.com/courses/33911/assignments/416881)
(https://njit.instructure.com/courses/33911/assignments/416881)

[Presentation 1](https://njit.instructure.com/courses/33911/assignments/416878)
(https://njit.instructure.com/courses/33911/assignments/416878)

[Presentation 2 (optional)](https://njit.instructure.com/courses/33911/assignments/416934)
(https://njit.instructure.com/courses/33911/assignments/416934)

[Project submission](https://njit.instructure.com/courses/33911/assignments/416879)
(https://njit.instructure.com/courses/33911/assignments/416879)