CSEC 530/630 Trusted Computing and Trusted Execution

Fall 2023
Location: Golisano Hall (GOL) 70-2750
Time: 11:00 AM - 12:15 PM (Tu/Th)

Instructor: Adam Caulfield
Email: ac7717@rit.edu
Instructor Office Hours: Thursdays 12:15 PM - 1:15 PM
Office Hours Location: Third Floor Conference Room

Contents

1 Course Description

This course covers foundational technologies for establishing trust in modern computing systems, including classic methods (e.g., boot chain-of-trust, secure boot, Trusted Platform Modules - TPMs, exception/privilege levels, and run-time inter-process isolation) and more recent trusted computing architectures such as ARM TrustZone and Intel Secure Guard eXtensions (SGX), which are increasingly popular and widely adopted in both academic research and industry. The course will also include at least four weeks of "special topics" that will touch upon more advanced and research-oriented aspects in the intersection of trusted computing and various realms of digital security & privacy.

2 Activities & Grading Distribution

Grades will be assigned based on a number of activities including in-class quizzes, take-home labs, seminars featuring papers presented by students, and critical reviews of papers presented in the seminars. In addition, an exploratory research project is to be proposed by the students and completed during the semester. Most activities are done in groups, except for Quizzes and seminar critical reviews. The latter two are performed individually. The breakdown of grades per activity is presented in Table 1. A letter grade will be assigned based on the final cumulative grade according to Table 2. Graded activities are detailed below.

Table 1: **Grades' Breakdown**

Area	Number	Total Weight %
Assignments		
Take-home Labs	2	20
Exams		
Quizzes	4	30
Research Seminars		
Paper presentations	1	10
Paper critical reviews	2	5
Participation	1	5
Term Research Project		
Project proposal	1	5
Midterm progress report	1	10
Final paper	1	15
Total		100

Table 2: **Final Letter Grades**

Grade	Letter Grade
93 - 100	A
90 - 93	A-
87 - 90	B+
80 - 87	B
70 - 80	C
60 - 70	D
0 - 60	F

2.1 Quizzes (individually)

The first part of the class is divided in 4 modules:

- Module 1 - Intro. to Trusted Computing and Secure Boot
- Module 2 - Remote Attestation and TPMs
- Module 3 - Runtime Security and ARM TrustZone
- Module 4 - Enclaved Execution Systems and Intel SGX

Exams will be distributed in the form of 4 (quasi-) biweekly short quizzes, one for each module. Each quiz will mostly cover concepts presented within its module (except for cumulative notions and concepts). Quizzes are closed-book, taken in-person, during class.

2.2 Take-Home Lab Assignments (individually)

There will be two self-guided take-home labs covering the basics of setting up and programming ARM TrustZone and Intel SGX. Points will be awarded for finishing lab tasks and answering corresponding questions correctly in a lab report to be submitted on `MyCourses`. Labs are also intended as "beginner guides" to prepare students to work on their final project implementations (see Section 2.4).

- Lab 1: ARM Cortex-A TrustZone (Due on Mid October)
- Lab 2: Intel Software Guard eXtensions (Due on Late October)

2.3 Special Topics

The latter part of the course will cover special/advanced topics in trusted computing. Topics will be determined based on recent developments in the field and student interest. Each special topic will include at least one paper presentation given by a team of students (the exact number of seminars depends on the number of enrolled students). A non-exhaustive list of special topic suggestions include:

- Trusted computing in embedded systems/IoT/CPS.
- New trusted computing architectures (beside TPM, TrustZone, and SGX).
- Attacks on trusted computing architectures.
- Usable security & user-oriented applications of trusted computing.
- Cryptographic protocols using trusted computing and TEEs.
- Trusted computing applications, such as Digital Rigths' Management (DRM), Biometrics, Privacy, etc.

2.3.1 Seminar Presentation (in groups)

Each student team will be responsible for presenting a ≈ 50 minutes seminar about a paper related to one of the special topics. Students are welcome to suggest papers and topics to the instructor. The presented paper should be approved by the instructor at least one week before the presentation. In case students have trouble finding a paper, one will be suggested by the instructor.

2.3.2 Critical Reviews (individually)

Each student must read all presented papers and write critical reviews for 2 papers presented by other students in the research seminars. Critical reviews should be submitted to MyCourses and include at least the following items:

- Title of the paper of choice.
- A paragraph summarizing the paper (in your own words, do not copy-paste the paper abstract!).
- A list of the paper's main strengths (3 or 4 items).
- A list of the paper's main weaknesses (3 or 4 items).
- Detailed discussion of the paper with respect to the following questions:
  - What is the research problem being solved? Why is this problem relevant?
  - What assumptions are made? What is the threat model (adversary's capabilities)?
  - What is the scope of the proposed approach? Does it solve a new problem?
  - What criteria were taken into account for the evaluation of this paper (computational cost, overhead, etc)?

2.3.3 Class participation (rated individually)

Students are expected to attend and participate in discussions during seminars presented by their peers. Participation points will be awarded based on both seminar attendance and participation. Each student is expected to read each paper before its presentation and bring at least one relevant question about the paper to each seminar class.

2.4 Research Project

Each student team is expected to complete a research project related to trusted computing. Acceptable topics can be discussed with the instructor and TA in class and during office hours. The research project should follow (and will be evaluated according to) the following guidelines:

- A 1-page project proposal must be submitted to MyCourses and briefly presented in class by the group. This will be an opportunity to receive feedback from the instructor and classmates on the proposed project.
- A 4-page midterm project report should be submitted to MyCourses. The midterm report should include at least an introduction, a statement about the problem being addressed, a comprehensive review of the related literature, and a plan of action along with the plan's rationale. Successful midterm reports must demonstrate substantial progress since the project proposal submission.
- Teams will be asked to present their final results and are welcome to demo any prototype/implementation (if applicable).
- A written final report describing the project idea, design, implementation, challenges, and results should be delivered by the last lecture. The report should be structured as a typical research paper and contain at least: (1) introduction & motivation; (2) appropriately cited references and a discussion on relevant prior work on the field; (3) clearly discuss the idea rationale; (4) describe any implementation and/or security analysis; (5) report on any experimental results; (6) outline lessons learned, limitations, and potential future directions.
- There is no strictly required format. However, students are encouraged to write their reports using the USENIX template[1]). An appropriately sized report should have about 8 pages in the USENIX format excluding references (or equivalent amount of words in other formats).

[1]USENIX paper template available at: `https://www.usenix.org/conferences/author-resources/paper-templates`

3 Tentative Schedule & Tentative Due Dates

Date	Topic	Deadlines and Remarks
Tu 8/27	Class Overview; Intro. to trust & trusted computing	
Th 8/29	Review: Security and Crypto Basic Building Blocks	
Tu 9/03	Boot Chain of Trust & Intro. to Secure Boot	
Th 9/05	Secure Boot (part 2)	
Tu 9/10	Sec. Boot Limitations & Intro. to Remote Attestation	**1st Quiz (15 min, in class)**
Th 9/12	Discussion on Class Projects	
Tu 9/17	TPM-1: Architecture	
Th 9/19	TPM-2: Operations	
Tu 9/24	TPM-3: TPM-Based Security Services	
Th 9/26	Runtime Security: Privilege Levels, Isolation, MMU	**2nd Quiz (15 min, in class)**
Tu 10/01	TrustZone-1: Architecture	
Th 10/03	TrustZone-2: Operations	**Project proposal deadline**
Tu 10/08	————————	October Break (no class)
Th 10/10	Project Proposal Presentations	
Tu 10/15	TrustZone-3: Security Services	
Th 10/17	SGX-1: Architecture	**3rd Quiz (15 min, in class)**
Tu 10/22	SGX-2: Operations	**Lab 1 Due**
Th 10/24	SGX-3: SGX Services	
Tu 10/29	Special Topics 1	**4th Quiz (15 min, in class)**
Th 10/31	Special Topics 2	**Lab 2 Due**
Tu 11/05	Special Topics 3	
Th 11/07	Special Topics 4	**Midterm project report due**
Tu 11/12	Special Topics 5	
Th 11/14	Special Topics 6	
Tu 11/19	Special Topics 7	
Th 11/21	————————	Thanksgiving Break (no class)
Tu 11/26	Special Topics 8	
Th 11/28	Special Topics 9	
Tu 12/03	Final Project Presentations & Demos (part 1)	**Paper critical reviews due**
Th 12/05	Final Project Presentations & Demos (part 2)	
Tu 12/10	Reading Day (no class)	
Fri 12/13	Final Exams (no class)	**Final project report due**

Table 3: Tentative Class Schedule

NOTE: This schedule is subject to change with reasonable advance notice. Any changes will be announced in class.

4 Large Language Model (LLM) Policy

For any report delivered as part of this class, the usage of LLMs, such as ChatGPT and similar tools, is allowed only for grammatical corrections and improvement of textual presentation. In particular, all ideas as well as intellectual premises or conclusions, must be either authored by the students or cited accordingly. Citations used in reports should refer to official academic sources, such as books and peer-reviewed articles from academic conferences and journals. The use of LLMs to generate any part of a critical review (see Section 2.3.2) is strictly forbidden.

The use of LLMs to assist in take-home lab implementations (see Section 2.2) is allowed. However, it will most likely prove unnecessary and more cumbersome than simply following the lab specifications, which already contain step-by-step instructions.

5 Related Courses

1. Secure and Trusted Systems. Byoungyoung Lee. Purdue University. `https://lifeasageek.github.io/class/cs590-sts/`.
2. Trusted Computing. Sven Bugiel. Saarland University. `https://cms.cispa.saarland/trust18`.
3. Introduction to Trusted Computing. Ariel Segall. MIT. `http://opensecuritytraining.info/IntroToTrustedComputing.html`.

6 Important RIT Deadlines

Please refer to RIT academic calendar for add or drop deadlines. Note: CSEC department policy states that a student has one semester to challenge any grade. After that, grades cannot be challenged.

7 Academic Integrity

Plagiarism or any form of cheating in homework, assignments, or exams is subject to serious academic penalties. This includes violations of the LLM usage policy (see Section 4). As an institution of higher education, RIT expects students to behave honestly and ethically at all times, especially when submitting work for evaluation in conjunction with any course or degree requirement. All students are encouraged to become familiar with RIT's Academic Integrity Policy, Honor Code, and Student Conduct Policy.

RIT's Academic Integrity Policies will be strictly enforced in this class.

8 ADA Statement

RIT is committed to providing reasonable accommodations to students with disabilities. If you would like to request accommodations such as special seating or testing modifications due to a disability, please contact the Disability Services Office. It is located in the Student Alumni Union, Room 1150. the Web site is `http://www.rit.edu/dso`. After you receive accommodation approval, it is imperative that you speak with the instructor so that you can work out whatever arrangement is necessary.

9 Harassment & Discrimination Statement

RIT is committed to providing a safe learning environment, free of harassment and discrimination as articulated in our university policies located on our governance website (`https://www.rit.edu/academicaffairs/policiesmanual/policies/governance`). RIT's policies require faculty to share information about incidents of gender based discrimination and harassment with RIT's Title IX coordinator or deputy coordinators, regardless whether the incidents are stated to them in person or shared by students as part of their coursework.

If you have a concern related to gender-based discrimination and/or harassment and prefer to have a confidential discussion, assistance is available from one of RIT's confidential resources on campus (listed below).

1. The Center for Women & Gender: Campus Center 1760; 585-475-7464; CARES (available 24 hours, 7 days a week). Call or text 585-295-3533.

2. RIT Student Health Center. August Health Center, 1st floor; 585-475-2255.

3. RIT Counseling Center. August Health Center, 2nd floor 2100; 585-475-2261.

4. The Ombuds Office. Student Auxiliary Union 1114; 585-475-7200 or 585-475-2876.

5. The Center for Religious Life. Schmitt Interfaith Center Rm1400; 585-475-2137.

6. NTID Counseling & Academic Advising Services, 2nd Floor Lynden B. Johnson; 585-475-6468, 585-286-4070.

10 Syllabus Updates

Information in the syllabus may be subject to change with reasonable advance notice. Any changes will be announce in class.