Introduction to Hardware Security (CMPE-361)

Department of Computer Engineering
Rochester Institute of Technology
Fall 2241

Instructor:	Dr. Michael Zuzak
Office:	GLE-3445
Office Hours:	Monday, 1:00 PM – 2:00 PM *(Tentative)*
	Wednesday, 11:00 AM – 12:00 PM *(Tentative)*
Contact:	mjzeec@rit.edu, (585) 475-2312
Class Time/Location:	Class—MW, 3:00-4:15 PM, Sustainability Inst (SUS)-3160
	Lab—F, 10:00-11:50 PM, James E Gleason Hall (GLE)-3410
Teaching Assistants:	Chris Nokes (crn2267@g.rit.edu)
	Michael Oldziej (mo3047@g.rit.edu)
Lab Manager:	Mr. Sean Cain (srceec@rit.edu, GLE-3411)

The objective of this course is to build the knowledge and skills necessary to design, evaluate, and implement secure hardware systems. Course topics will span the fundamentals of hardware security and trust, which may include security principles and properties, encryption/decryption, side-channel attacks, hardware manufacture and test, physically uncloneable functions (PUF), true random number generation, hardware trojan detection, secure system design, and trusted execution environments. Laboratory assignments and projects facilitate the hands-on learning of course topics including cryptographic hardware design, side-channel attacks, integrated circuit test and verification, PUFs, true random number generation, and secure system design using a field programmable gate array (FPGA) and an embedded processor as an implementation platform.

PREREQUISITES:

Following are the required prerequisite courses:

- CMPE-250 or equivalent
- CMPE-260 or equivalent

OPTIONAL RESOURCES:

- S. Bhunia and M. Tehranipoor, Hardware Security: A Hand-on Training Approach, Morgan Kauffman, 2018
- M. Tehranipoor and C. Wang (Eds.), Introduction to Hardware Security and Trust, Springer, 2011
- Mihir Bellare and Phil Rogaway, Introduction to Modern Cryptography

- Ross J. Anderson. Security Engineering: A guide to building dependable distributed systems. John Wiley and Sons, 2001
- Matt Bishop, Computer Security: Art and Science, Addison-Wesley, 2003
- William Stallings. Cryptography and Network Security, Fourth edition, 2007
- NSF Trust-Hub (https://trust-hub.org)

GRADING

Labs:	45%
Projects:	30%
Mini Quizzes:	10%
Homework:	15%

A	>= 90%
A-	88%-89%
B+	85%-87%
B	80%-84%
B-	78%-79%
C+	75%-77%
C	70%-74%
C-	68%-69%
D	60%-67%
F	<60%

Reference material, class notes, homework, and lab assignments will be posted on mycourses (http://mycourses.rit.edu). All updates relevant to the course will be communicated through mycourses. Students are responsible for any announcements sent to email addresses used in mycourses.

LABS AND PROJECT

This course emphasizes hands-on hardware security. Therefore, students will be spending a significant amount of the course time in labs for a complete learning experience. The guidelines for writing lab reports will be posted on mycourses. Labs must be turned in by the due date at the beginning of the lab section to receive full credit. For each delayed day, there will be a 10% deduction in the lab grade. Students are expected to work independently on labs. Collaboration is permitted only when instructed.

MINI QUIZZES

There will be a quiz roughly each week to check students' understanding of lectures, assigned readings, and homework questions. Quizzes will usually be given at the beginning of class.

HOMEWORK

Homework is due at the beginning of the class on the due date. Late submissions will lose 10% per day late.

COURSE TOPICS

This course will cover the following topics:

- Security principles (security, privacy, trust, reliability, testability)
- Cryptography (encryption/decryption)
- Attacker models and common hardware attacks
- Security properties (Confidentiality, Availability, Authorization, Integrity, Provenance, Indistinguishability)
- Side-Channel Attacks (power, timing, template)
- Hardware test and verification (design-for-test/trust)
- Secure and trustworthy hardware manufacturing practices
- Hardware Trojan detection and mitigation
- Physically uncloneable functions and true random number generation
- Secure system design and trusted execution environments

ABET STUDENT OUTCOMES

Engineering Design: an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors

- Develop and evaluate a hardware system based on a design and security specification
- Write and assess a threat model for a hardware system

Experiments and Data: an ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions

- Measure and analyze power consumption to perform power side-channel attacks on AES

Independent Learning: an ability to acquire and apply new knowledge as needed, using appropriate learning strategies

- Develop and document a methodology to test arbitrary hardware for malicious circuitry

COURSE OUTCOMES

Upon successful completion of the course, students will be able to

- Transform design requirements into formal attacker models.
- Specify relevant hardware security techniques to protect against common attackers.
- Design hardware systems incorporating security, privacy, and trust protections against a known attacker model.
- Evaluate the security properties of hardware systems.
- Assess security, privacy, and trust vulnerabilities in hardware/software systems and design attacks to exploit these vulnerabilities.

<u>TENTATIVE</u> SCHEDULE

Week	Topics	Labs
1	Syllabus and Course Introduction	Lab 1 – Lab Equipment Setup and Power Analysis Attacks
	Introduction to Hardware Security and Trust	
2	Introduction to Cryptography - 1	Lab 2 – Differential Power Analysis Attacks on AES
	Introduction to Cryptography - 2	
3	Basics of VLSI Design and Test	
	Introduction to Side-Channel Attacks	
4	Power Side-Channel Attacks - 1	Lab 3 – Correlation Power Analysis
	Power Side-Channel Attacks - 2	
5	Covert Channel Attacks	Lab 4 – Correlation Power Analysis Attack on AES
	Introduction to IP Theft and Reverse Engineering	
6	Hardware Trojans and Integrated Circuit Testing - 1	Slack/TBD
	Hardware Trojans and Integrated Circuit Testing - 2	
7	Project Introduction	Project 1 – Hardware Trojan Detection
	TBD	
8	Integrated Circuit Watermarking	
	Counterfeit Detection and Avoidance – 1	
9	Counterfeit Detection and Avoidance - 2	
	Invasive/Non-Invasive Physical Attacks	
10	Project 1 Presentations	Lab 5 - Voltage Glitch for Password Bypass
	Physical Attacks, Reverse Engineering, and Fault Injection - 1	
11	Physical Attacks, Reverse Engineering, and Fault Injection - 2	Lab 6 – PUFs on FPGAs
	PUFs and TRNG – 1	
12	PUFs and TRNG – 2	
	Trusted Execution Environments – 1	
13	Trusted Execution Environments – 2	Project 2 – Secure System Design
	Project Introduction	
14	Security Policies and Access Control	
	Emerging Technologies and Topics – 1	
15	Emerging Technologies and Topics – 2	
	TBD	
16	Final Presentations/Projects	Finals Week – No Lab

ACCOMODATIONS FOR DISABILITIES

"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 website is www.rit.edu/dso. After you receive accommodation approval, it is imperative that you see me during office hours so that we can work out whatever arrangement is necessary."

KGCOE ACADEMIC HONESTY POLICY (Derived from section D8.0 of the Institute Policies and Procedures Manual)

As a university, RIT is committed to the pursuit of knowledge and the free exchange of ideas. In such an intellectual climate it is fundamentally imperative that all members of this academic community behave in the highest ethical fashion possible in the manner by which they produce, share, and exchange this information. In the case of students, Academic Honesty demands that at all times student work be the work of that individual student, and that any information that a student uses in a work submitted for evaluation be properly documented. Any violation of these basic standards constitutes a breach of Academic Honesty and hence becomes Academic Dishonesty.

HONOR PRINCIPLES

"RIT Engineering faculty, staff and students are truthful and honorable, and do not tolerate lying, cheating, stealing, or plagiarism." All members of our community are expected to abide by these principles and to embrace the spirit they represent. We each have a responsibility to address any unethical behavior we observe; either through direct discussion with the offending party, or by discussion with an appropriate faculty or staff member. Allowing unethical behavior to continue unchallenged is not acceptable.

ACADEMIC DISHONESTY

Academic Dishonesty falls into three basic areas: cheating, duplicate submission and plagiarism.

1. Cheating

Cheating is any fraudulent or deceptive academic act, including falsifying of data, possessing, providing, or using unapproved materials, sources, or tools for a work submitted for faculty evaluation.

2. Duplicate Submission

Duplicate submission is the submitting of the same or similar work for credit in more than one course without prior approval of the instructors for those courses. (If the courses are taken in separate quarters, only the permission of the second instructor is required.) Similar rules apply for prior work done on coop.

3. Plagiarism

Plagiarism is the representation of others' ideas as one's own without giving proper credit to the original author or authors. Plagiarism occurs when a student copies direct phrases from a text (e.g. books, journals, internet), or paraphrases or summarizes those ideas without attribution. This also applies to group effort on work submitted for faculty evaluation.

CONSEQUENCES OF ACADEMIC DISHONESTY

Any act of Academic Dishonesty will incur the following consequences. After notifying and presenting the student with evidence of such misconduct, the instructor has the full prerogative to assign a lower grade, including an "F" for the offense itself or for the entire course. If after careful review of the evidence, the instructor decides that the student's actions are indeed misconduct and warrant a penalty, the instructor will add a letter to the student's file in his or her home department (copy to the student, Department Head and the Dean) documenting the offense. Depending on the seriousness of the offense, the student may also be brought before the Academic Conduct Committee of the College in which the offense occurred, and may face academic suspension or dismissal from the Institute. The student has the right to appeal any disciplinary action as described in section D17.0 "Academic Conduct and Appeals Procedures" and D18.0 "RIT Student Conduct Process" of the Institute Policies and Procedures Manual. This KGCOE policy is intended to apply to all academic pursuits at RIT, including courses taken outside of the KGCOE (with additional adherence to the policies of the relevant academic unit).