Hands-on Hardware Security
EEE 6744 Section 1FE2, 2FED, CAMP
Class Periods: Wednesday | Period 8 - 10 (3:00 PM - 6:00 PM)
Location: Online
Academic Term: Fall 2020

Instructor:

Name: Dr. Swarup Bhunia
Email: swarup@ece.ufl.edu
Telephone: 352-392-5989
Office Hours: Thursday 3-4pm or by appointment

Teaching Assistants:

1) Prabuddha Chakraborty (p.chakraborty@ufl.edu)
2) Naren Vikram Raj Masna (nmasna@ufl.edu)
3) Reiner Dizon (reinerdizon@ufl.edu)

Course Description

This course focuses on practical learning of computer hardware security using a hands-on approach. Students will work on a custom-designed hardware platform to understand innards of a computer system and ethically "hack" into it at different levels. They will examine it to understand security vulnerabilities, mount attacks, and implement countermeasures.

Course Pre-Requisites / Co-Requisites

Prerequisite- EEE 5716 (Introduction to Hardware Security). Students who do not meet this requirement need to take permission from the instructor.

Course Objectives

This lab course consists of a set of well-designed hands-on experiments that intends to help students

- Understand the basic concepts of computer system security which integrates network and information security, software security, and hardware security.
- Learn about hardware components of computer systems and understand their security vulnerabilities through hands-on experience
- Learn and design existing solutions against known attacks.
- Learn to ethically hack into hardware and come up with a new attack models and defense mechanisms against them.
- Analyze and validate computer hardware security issues and build secure computer system.

Materials and Supply Fees

No materials or supply fee. Students will be provided hardware kit for experiments free of charge. They are required to return these kits without any damage at the end of the semester.

Required Textbooks and Software

- No textbook required.
- Software: Altera Quartus and Atmel Studio. Students need to install these two software packages for FPGA and Microcontroller programming in their computer.
- The following books serve as reference for concepts explored in this course:
    - S. Bhunia and M. Tehranipoor, "Hardware Security: A Hands-on Learning Approach", 1st Edition, Morgan Kaufmann, 2018.

- M. Tehranipoor and C. Wang (Eds.). "Introduction to Hardware Security and Trust", Springer, ISBN: 978-1-4419-8079-3, 2012.
- Erickson, Jon. "Hacking: The Art of Exploitation." No Starch Press, San Francisco, 2008. ISBN: 1-59327-144-2.
- Huang, Andrew. "Hacking the Xbox: An Introduction to Reverse Engineering." No Starch Press, San Francisco, 2003. ISBN: 1-59327-029-1
- Petzold, Charles. "Code: The Hidden Language of Computer Hardware and Software." Microsoft Press, Redmond, 2000. ISBN: 0-7356-1131-9

Recommended Materials

- Course notes and lab instructions will be posted in course website

Key Concepts

Introduction to computer security issues - information and network, software, hardware securities. Understand information security through data encryption and decryption to protect data and systems. Learn buffer overflow attacks – stack overflow, heap overflow, and array indexing errors. Learn about various attacks on hardware at different levels – from chips to printed circuit boards (PCBs). Learn bus snooping attacks and protection schemes through bus encryption. Learn hardware tampering attacks (e.g. mod-chip attacks) in field. Understand side-channel attacks including fault injection and power analysis attacks, and hardware Trojan attacks of different forms and sizes triggered by rare events. Understand various countermeasures against hardware attacks including hardware authentication. Be able to reverse engineer a printed circuit board (PCB) to figure out how the hardware components function.

Course Structure

Students will be provided with the custom-designed hardware module (called the HaHa board and cables) in the beginning of a class along with a manual on how to use the module. Students will keep the board through the semester and return at the end. This manual will have instructions and examples on how to use this board for different purposes. For each of the 11 experiments in this course, students will receive written instructions (to be uploaded in the course website before the class) on the objective of the experiment, steps to mount an attack or implement a countermeasure, things to observe or demonstrate, and the reporting format. In addition, in the beginning of each new experiment, the instructor will briefly introduce the topic, steps of the experiments, advanced options if any, and expected learning outcomes. The TAs for this course will be available to help with the experiments, as needed.

Course Schedule

Week	Description of Lab Assignment	Important Dates
1	Introduction to Hardware Security Introduction to (1) Buffer Overflow attacks.	Lab 1, Buffer Overflows assigned.
2	Introduction to (2) Information Security: Encryption/Decryption	Lab 1, Buffer Overflows due. Lab 2, Encryption assigned.
3	Introduction to (3) Bus Snooping attacks	Lab 2, Encryption due. Lab 3, Bus Snooping assigned.
4	Introduction to (4) Hardware Trojans I	Lab 3, Bus Snooping due. Lab 4, Hardware Trojan I assigned.
5		
6	Introduction to (5) Hardware Trojans II	Lab 4, Hardware Trojan I due. Lab 5, Hardware Trojan II assigned.
7	Introduction to (6) Reverse Engineering	Lab 5, Hardware Trojan II due. Lab 6, Reverse Engineering assigned.
8		
9	Introduction to (7) Physical Unclonable Function (PUF) and True Random Number Generator (TRNG)	Lab 6, Reverse Engineering due. Lab 7, PUF assigned.

10	Introduction to (8) Physical Tampering of Hardware (i.e. Mod Chip attacks)	Lab 7, PUF due. Lab 8, Mod Chip assigned.
11	Introduction to (9) Side Channel Attacks	Lab 8, Mod Chip due. Lab 9, Side Channel assigned.
12		
13	Introduction to (10) Fault Injection Attack	Lab 9, Side Channel due. Lab 10, Fault Injection assigned.
14		
15	System level attacks (11)	Lab 10, Fault Injection Attack due.
16		
17		Lab 11 report due.

Online Course Recording

Our class sessions may be audio visually recorded for students in the class to refer back and for enrolled students who are unable to attend live. Students who participate with their camera engaged or utilize a profile image are agreeing to have their video or image recorded. If you are unwilling to consent to have your profile or video image recorded, be sure to keep your camera off and do not use a profile image. Likewise, students who un-mute during class and participate orally are agreeing to have their voices recorded. If you are not willing to consent to have your voice recorded during class, you will need to keep your mute button activated and communicate exclusively using the "chat" feature, which allows students to type questions and comments live. The chat will not be recorded or shared. As in all courses, unauthorized recording and unauthorized sharing of recorded materials is prohibited.

F2F Course Policy in Response to COVID-19

We will have face-to-face instructional sessions to accomplish the student learning objectives of this course. In response to COVID-19, the following policies and requirements are in place to maintain your learning environment and to enhance the safety of our in-classroom interactions.

- You are required to wear approved face coverings at all times during class and within buildings. Following and enforcing these policies and requirements are all of our responsibility. Failure to do so will lead to a report to the Office of Student Conduct and Conflict Resolution.
- This course has been assigned a physical classroom with enough capacity to maintain physical distancing (6 feet between individuals) requirements. Please utilize designated seats and maintain appropriate spacing between students. Please do not move desks or stations.
- Sanitizing supplies are available in the classroom if you wish to wipe down your desks prior to sitting down and at the end of the class.
- Follow your instructor's guidance on how to enter and exit the classroom. Practice physical distancing to the extent possible when entering and exiting the classroom.
- If you are experiencing COVID-19 symptoms (Click here for guidance from the CDC on symptoms of coronavirus), please use the UF Health screening system and follow the instructions on whether you are able to attend class. Click here for UF Health guidance on what to do if you have been exposed to or are experiencing Covid-19 symptoms.
- Course materials will be provided to you with an excused absence, and you will be given a reasonable amount of time to make up work. Find more information in the university attendance policies.

Attendance Policy, Class Expectations, and Make-Up Policy

This class will be presented online using Zoom and requires access to a working webcam and stable internet connection. I prefer that students keep their camera on during the class so that I can see you as I would during normal face-to-face classes. Studies show that if we can see each other's faces then we will have more engagement, more student success, and more faculty success. However, this is not a requirement. I understand if on certain days

you can't have your camera on due to internet bandwidth limitations, other family members, health issues, or any other reasons.

Make sure you meet the following criteria. These are essential for you to be able to complete this course successfully.

- **Lab Assignments** – All lab assignments are to be performed as individually. 11 lab assignments will be given throughout the semester.
- **Report Format** – All reports for lab assignments are to be completed by computer - handwritten assignments will not be accepted. One report per student group. A common report format for all assignment will be provided to the students.
- **Late Assignment/Projects** – Late assignment/lab report will receive a penalty of 10% per day, unless excused. No late submission is accepted after one week of the due date.

Excused absences must be in compliance with university policies in the Graduate Catalog (http://gradcatalog.ufl.edu/content.php?catoid=10&navoid=2020#attendance) and require appropriate documentation.

Evaluation of Grades

1. Each lab report needs to clearly describe which student in the team did which parts of the experiment.
2. The lab report also needs to clearly note individual student's contribution to writing the report.
3. All students in a team need to participate in the lab demos.

Your course grade will be based on your overall performance through the entire semester. The relative weights for the final grade are the following:

Assignment	**Total Points**	**Percentage of Final Grade**
Demos and reports for all 11 experiments. Each experiment has equal points.	100 each	100%
		100%

Grading Policy

The following is given as an example only.

Percent	**Grade**	**Grade Points**
90.0 - 100.0	A	4.00
87.0 - 89.9	A-	3.67
84.0 - 86.9	B+	3.33
81.0 – 83.9	B	3.00
78.0 - 80.9	B-	2.67
75.0 - 79.9	C+	2.33
72.0 – 74.9	C	2.00
69.0 - 71.9	C-	1.67
66.0 - 68.9	D+	1.33
63.0 - 65.9	D	1.00
60.0 - 62.9	D-	0.67
0 - 59.9	E	0.00

More information on UF grading policy may be found at:
http://gradcatalog.ufl.edu/content.php?catoid=10&navoid=2020#grades

Students Requiring Accommodations
Students with disabilities who experience learning barriers and would like to request academic accommodations should connect with the disability Resource Center by visiting https://disability.ufl.edu/students/get-started/. It is important for students to share their accommodation letter with their instructor and discuss their access needs, as early as possible in the semester.

Course Evaluation
Students are expected to provide professional and respectful feedback on the quality of instruction in this course by completing course evaluations online via GatorEvals. Guidance on how to give feedback in a professional and respectful manner is available at https://gatorevals.aa.ufl.edu/students/. Students will be notified when the evaluation period opens, and can complete evaluations through the email they receive from GatorEvals, in their Canvas course menu under GatorEvals, or via https://ufl.bluera.com/ufl/. Summaries of course evaluation results are available to students at https://gatorevals.aa.ufl.edu/public-results/.

University Honesty Policy
UF students are bound by The Honor Pledge which states, "We, the members of the University of Florida community, pledge to hold ourselves and our peers to the highest standards of honor and integrity by abiding by the Honor Code. On all work submitted for credit by students at the University of Florida, the following pledge is either required or implied: "On my honor, I have neither given nor received unauthorized aid in doing this assignment." The Honor Code (https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code/) specifies a number of behaviors that are in violation of this code and the possible sanctions. Furthermore, you are obligated to report any condition that facilitates academic misconduct to appropriate personnel. If you have any questions or concerns, please consult with the instructor or TAs in this class.

Commitment to a Safe and Inclusive Learning Environment
The Herbert Wertheim College of Engineering values broad diversity within our community and is committed to individual and group empowerment, inclusion, and the elimination of discrimination. It is expected that every person in this class will treat one another with dignity and respect regardless of gender, sexuality, disability, age, socioeconomic status, ethnicity, race, and culture.

If you feel like your performance in class is being impacted by discrimination or harassment of any kind, please contact your instructor or any of the following:
- Your academic advisor or Graduate Program Coordinator
- Robin Bielling, Director of Human Resources, 352-392-0903, rbielling@eng.ufl.edu
- Curtis Taylor, Associate Dean of Student Affairs, 352-392-2177, taylor@eng.ufl.edu
- Toshikazu Nishida, Associate Dean of Academic Affairs, 352-392-0943, nishida@eng.ufl.edu

Software Use
All faculty, staff, and students of the University are required and expected to obey the laws and legal agreements governing software use. Failure to do so can lead to monetary damages and/or criminal penalties for the individual violator. Because such violations are also against University policies and rules, disciplinary action will be taken as appropriate. We, the members of the University of Florida community, pledge to uphold ourselves and our peers to the highest standards of honesty and integrity.

Student Privacy
There are federal laws protecting your privacy with regards to grades earned in courses and on individual assignments. For more information, please see: https://registrar.ufl.edu/ferpa.html

Campus Resources:

Health and Wellness

U Matter, We Care:
Your well-being is important to the University of Florida. The U Matter, We Care initiative is committed to creating a culture of care on our campus by encouraging members of our community to look out for one another and to reach out for help if a member of our community is in need. If you or a friend is in distress, please contact umatter@ufl.edu so that the U Matter, We Care Team can reach out to the student in distress. A nighttime and weekend crisis counselor is available by phone at 352-392-1575. The U Matter, We Care Team can help connect students to the many other helping resources available including, but not limited to, Victim Advocates, Housing staff, and the Counseling and Wellness Center. Please remember that asking for help is a sign of strength. In case of emergency, call 9-1-1.

Counseling and Wellness Center: http://www.counseling.ufl.edu/cwc, and 392-1575; and the University Police Department: 392-1111 or 9-1-1 for emergencies.

Sexual Discrimination, Harassment, Assault, or Violence
If you or a friend has been subjected to sexual discrimination, sexual harassment, sexual assault, or violence contact the **Office of Title IX Compliance**, located at Yon Hall Room 427, 1908 Stadium Road, (352) 273-1094, title-ix@ufl.edu

Sexual Assault Recovery Services (SARS)
Student Health Care Center, 392-1161.

University Police Department at 392-1111 (or 9-1-1 for emergencies), or http://www.police.ufl.edu/.

Academic Resources

E-learning technical suppor*t*, 352-392-4357 (select option 2) or e-mail to Learning-support@ufl.edu. https://lss.at.ufl.edu/help.shtml.

Career Resource Center, Reitz Union, 392-1601. Career assistance and counseling. https://www.crc.ufl.edu/.

Library Support, http://cms.uflib.ufl.edu/ask. Various ways to receive assistance with respect to using the libraries or finding resources.

Teaching Center, Broward Hall, 392-2010 or 392-6420. General study skills and tutoring. https://teachingcenter.ufl.edu/.

Writing Studio, 302 Tigert Hall*,* 846-1138. Help brainstorming, formatting, and writing papers. https://writing.ufl.edu/writing-studio/.

Student Complaints Campus*:* https://care.dso.ufl.edu.

On-Line Students Complaints*:* http://www.distance.ufl.edu/student-complaint-process.