Hands-on Hardware Security
EEE 6744
(3 credits)
Class Periods: Wednesday Period 8 (3:00 PM - 6:00 PM)
Location: TBD
Academic Term: Fall 2019

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) Shuo Yang (sy@ufl.edu)
2) Abdulrahman Alaql (alaql89@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)

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.

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. For EDGE students, video recording of this introductory lecture (15 min) will be posted in Canvas. We do not need an EDGE class room for recording 11 of these this short (15 min) videos. The TAs for this course will be available to help in-campus students in the lab and EDGE students via Skype with the experiments, as needed.

Recommended Textbooks and Software

There is no required textbook for the course. The following books serve as reference for concepts explored in this course:

i. S. Bhunia and M. Tehranipoor, "Hardware Security: A Hands-on Learning Approach", 1st Edition, Morgan Kaufmann, 2018.
ii. M. Tehranipoor and C. Wang (Eds.). "Introduction to Hardware Security and Trust", Springer, ISBN: 978-1-4419-8079-3, 2012.
iii. Erickson, Jon. "Hacking: The Art of Exploitation." No Starch Press, San Francisco, 2008. ISBN: 1-59327-144-2.
iv. Huang, Andrew. "Hacking the Xbox: An Introduction to Reverse Engineering." No Starch Press, San Francisco, 2003. ISBN: 1-59327-029-1
v. Petzold, Charles. "Code: The Hidden Language of Computer Hardware and Software." Microsoft Press, Redmond, 2000. ISBN: 0-7356-1131-9
vi. The course will use the Facebook "Hardware Security" Group created by Dr. Bhunia for sharing and discussing new developments in hardware security.
vii. Software: Altera Quartus and Atmel Studio

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 Advanced options for graduate students.	Lab 4, Hardware Trojan I due. Lab 5, Hardware Trojan II assigned.
7	Introduction to (6) Reverse Engineering Advanced options for graduate students.	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) Advanced options for graduate students.	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 Advanced options for graduate students.	Lab 8, Mod Chip due. Lab 9, Side Channel assigned.
12		
13	Introduction to (10) Fault Injection Attacks Advanced options for graduate students.	Lab 9, Side Channel due. Lab 10, Fault Injection assigned.
14		
15	Final Project presentation: ***"Can You Hack It?"***	Lab 10, Fault Injection Attack due.
16		
17	More detailed report for graduate students.	Final Project due.

Attendance Policy, Class Expectations, and Make-Up Policy

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. 10 lab assignments will be given throughout the semester and one grand project ***"Can You Hack It?"*** will be assigned after completing all lab experiments. For graduate students, there will be advanced options for select experiments. These options will be described in the lab instructions.
- **Report Format** – All reports for lab assignments are to be completed by computer - handwritten assignments will not be accepted. One report per student. 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.
- **Exams and Make-up Exam** – There will be 2 quizzes throughout the semester. Make-up exams and quizzes are only offered to students with excused absences.

Excused absences are consistent with university policies in the undergraduate catalog (https://catalog.ufl.edu/ugrad/current/regulations/info/attendance.aspx) and require appropriate documentation.

Evaluation of Grades

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

- Demo and Reports for all Lab Assignments 60%
- 2 Quizzes 10%
- Final Project (Demo + Report) 30%

Grading Policy

Percent	Grade	Grade Points
93.4 - 100	A	4.00
90.0 - 93.3	A-	3.67
86.7 - 89.9	B+	3.33
83.4 - 86.6	B	3.00
80.0 - 83.3	B-	2.67
76.7 - 79.9	C+	2.33
73.4 - 76.6	C	2.00
70.0 - 73.3	C-	1.67
66.7 - 69.9	D+	1.33
63.4 - 66.6	D	1.00
60.0 - 63.3	D-	0.67
0 - 59.9	E	0.00

More information on UF grading policy may be found at:
https://catalog.ufl.edu/ugrad/current/regulations/info/grades.aspx

Students Requiring Accommodations

Students with disabilities requesting accommodations should first register with the Disability Resource Center (352-392-8565, https://www.dso.ufl.edu/drc) by providing appropriate documentation. Once registered, students will receive an accommodation letter which must be presented to the instructor when requesting accommodation. Students with disabilities should follow this procedure as early as possible in the semester.

Course Evaluation

Students are expected to provide feedback on the quality of instruction in this course by completing online evaluations at https://evaluations.ufl.edu/evals. Evaluations are typically open during the last two or three weeks of the semester, but students will be given specific times when they are open. Summary results of these assessments are available to students at https://evaluations.ufl.edu/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://www.dso.ufl.edu/sccr/process/student-conduct-honor-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.

Campus Resources:

Health and Wellness

U Matter, We Care:
If you or a friend is in distress, please contact umatter@ufl.edu or 352 392-1575 so that a team member can reach out to the student.

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 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 support, 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://www.dso.ufl.edu/documents/UF_Complaints_policy.pdf.

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