

## **Hands-on Hardware Security**

**EEE 6744**

**(3 credits)**

***Class Periods:*** Wednesday Period 8 (3:00 PM - 6:00 PM)

***Location:*** MCCB 1108

***Academic Term:*** Fall 2022

### ***Instructor:***

**Name** Dr. Swarup Bhunia

**Email Address** [swarup@ece.ufl.edu](mailto:swarup@ece.ufl.edu)

**Office Phone Number** 352-392-5989

**Office Hours:** Thursday 3-4pm or by appointment

### ***Teaching Assistant/Peer Mentor/Supervised Teaching Student:***

Please contact through the Canvas website

- Pravin Gaikwad ([pravin.gaikwad@ufl.edu](mailto:pravin.gaikwad@ufl.edu)), Benton 327
- Aritra Bhattacharya ([abhattacharyay@ufl.edu](mailto:abhattacharyay@ufl.edu)), Larsen 317

### ***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.

### **Materials and Supply Fees**

None

### **Required Textbooks and Software**

There is no required textbook for the course.

### **Recommended Materials**

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**

<b>Week</b>	<b>Description of Lab Assignment</b>	<b>Important Dates</b>
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.
5		Lab 4, Hardware Trojan I assigned.
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.
8		Lab 6, Reverse Engineering assigned.

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.
12		Lab 9, Side Channel assigned.
13	Introduction to (10) Fault Injection Attacks Advanced options for graduate students.	Lab 9, Side Channel due.
14		Lab 10, Fault Injection assigned.
15	Final lab assignment on system level attack and presentation.	Lab 10, Fault Injection Attack due.
16		
17		Final assignment due.

### **Attendance Policy, Class Expectations, and Make-Up Policy**

Excused absences must be consistent with university policies in the Graduate Catalog (<https://catalog.ufl.edu/graduate/regulations>) and require appropriate documentation. Additional information can be found here: <https://gradcatalog.ufl.edu/graduate/regulations/>

### **Evaluation of Grades**

**\*\*Assessment Guidance from the ECE Graduate Committee:** Course evaluation components should include:

1. At least one component that individually evaluates each student's understanding of course material and ability to apply concepts.
2. At least one evaluation activity that takes place in class.
3. When a project is involved, evaluation rubrics should be explicitly stated.
4. When team work is expected, individual student contribution verification method should be explicitly stated.

*If an in-class exam is administered then 1 and 2 are fulfilled. In the case of a project, a project report that is graded per the stated evaluation rubrics and states which work was done by each student in the project team will address both 3 and 4.*

Assignment	Total Points	Percentage of Final Grade
Homework Sets (10)	100 each	15%
Quizzes (4)	100 each	15%
Midterm Exam	100	30%
Final Exam	100	30%
Review Paper	100	10%
		100%

### **Grading Policy**

The following is given as an example only.

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

**Course Title, Prefix, and Number**  
**Course Instructor and Academic Term**

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:

[UF Graduate Catalog](#)  
[Grades and Grading Policies](#)

### ***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.ua.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.ua.ufl.edu/public-results/>.

### ***In-Class Recording***

Students are allowed to record video or audio of class lectures. However, the purposes for which these recordings may be used are strictly controlled. The only allowable purposes are (1) for personal educational use, (2) in connection with a complaint to the university, or (3) as evidence in, or in preparation for, a criminal or civil proceeding. All other purposes are prohibited. Specifically, students may not publish recorded lectures without the written consent of the instructor.

A “class lecture” is an educational presentation intended to inform or teach enrolled students about a particular subject, including any instructor-led discussions that form part of the presentation, and delivered by any instructor hired or appointed by the University, or by a guest instructor, as part of a University of Florida course. A class lecture does not include lab sessions, student presentations, clinical presentations such as patient history, academic exercises involving solely student participation, assessments (quizzes, tests, exams), field trips, private conversations between students in the class or between a student and the faculty or lecturer during a class session.

Publication without permission of the instructor is prohibited. To “publish” means to share, transmit, circulate, distribute, or provide access to a recording, regardless of format or medium, to another person (or persons), including but not limited to another student within the same class section. Additionally, a recording, or transcript of a recording, is considered published if it is posted on or uploaded to, in whole or in part, any media platform, including but not limited to social media, book, magazine, newspaper, leaflet, or third party note/tutoring services. A student who publishes a recording without written consent may be subject to a civil cause of action instituted by a person injured by the publication and/or discipline under UF Regulation 4.040 Student Honor Code and Student Conduct Code.

### ***University Honesty Policy***

***Course Title, Prefix, and Number***  
***Course Instructor and Academic Term***

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/process/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
- Jennifer Nappo, Director of Human Resources, 352-392-0904, [jpennacc@ufl.edu](mailto:jpennacc@ufl.edu)
- Curtis Taylor, Associate Dean of Student Affairs, 352-392-2177, [taylor@eng.ufl.edu](mailto:taylor@eng.ufl.edu)
- Toshikazu Nishida, Associate Dean of Academic Affairs, 352-392-0943, [nishida@eng.ufl.edu](mailto: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](mailto: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:** <https://counseling.ufl.edu>, 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](mailto: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 support**, 352-392-4357 (select option 2) or e-mail to Learning-support@ufl.edu.

<https://lss.at.ufl.edu/help.shtml>.

**Career Connections Center**, Reitz Union, 392-1601. Career assistance and counseling; <https://career.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://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code/>; <https://care.dso.ufl.edu>.

**On-Line Students Complaints:** <https://distance.ufl.edu/state-authorization-status/#student-complaint>.