Cover Sheet: Request 10616

EEL4876 Intro to Hardware Security and Trust

Info

Process	Course|New|Ugrad/Pro
Status	Pending
Submitter	Edvardsson, Laurie laurie@ece.ufl.edu
Created	12/9/2015 12:04:25 PM
Updated	2/9/2016 1:18:14 PM
Description	Fundamentals of hardware security and trust for integrated circuits. Cryptographic hardware, invasive and non-invasive attacks, side-channel attacks, physically unclonable functions (PUFs), true random number generation (TRNG). watermarking of Intellectual Property (IP) blocks, FPGA security, counterfeit detection, hardware Trojan detection and prevention in IP cores and integrated circuits.

Actions

Step	Status	Group	User	Comment	Updated
Department	Approved	ENG - Electrical and Computer Engineering 011905000	Fox, Robert M		1/4/2016
No document changes					
College	Approved	ENG - College of Engineering	Caple, Elizabeth		1/21/2016
No document changes					
University Curriculum Committee	Comment	PV - University Curriculum Committee (UCC)	Case, Brandon	Added to February agenda	1/22/2016
No document changes					
University Curriculum Committee	Pending	PV - University Curriculum Committee (UCC)			1/22/2016
No document changes					
Statewide Course Numbering System					
No document changes					
Office of the Registrar					
No document changes					
Student Academic Support System					
No document changes					
Catalog					
No document changes					
College Notified					
No document changes					

Course|New for request 10616

Info

Request: EEL4876 Intro to Hardware Security and Trust
Submitter: Edvardsson, Laurie laurie@ece.ufl.edu
Created: 2/9/2016 10:40:23 AM
Form version: 2

Responses

Recommended Prefix: EEL
Course Level : 4
Number : 876
Lab Code : None
Course Title: Introduction to Hardware Security and Trust
Transcript Title: Intro HW Secur/Trust
Effective Term : Fall
Effective Year: 2016
Rotating Topic?: No
Amount of Credit: 3
Repeatable Credit?: No
S/U Only?: No
Contact Type : Regularly Scheduled
Degree Type: Baccalaureate
Weekly Contact Hours : 003
Category of Instruction : Joint (Ugrad/Grad)
Delivery Method(s): On-Campus
Course Description : Fundamentals of hardware security and trust for integrated circuits. Cryptographic hardware, invasive and non-invasive attacks, side-channel attacks, physically unclonable functions (PUFs), true random number generation (TRNG). watermarking of Intellectual Property (IP) blocks, FPGA security, counterfeit detection, hardware Trojan detection and prevention in IP cores and integrated circuits.
Prerequisites : EEL 4712C(C)
Co-requisites : None
Rationale and Placement in Curriculum : This technical elective is being offered by new faculty hires in the area of cybersecurity as it relates to computer hardware.
Course Objectives : The student will be able to describe the state-of-the-art security methods and devices; identify attacks and design countermeasures against them; identify and isolate hardware Trojans; create the integration of security as a design metric; protect the design of intellectual property against piracy and tampering.
Course Textbook(s) and/or Other Assigned Reading: Title: Introduction to Security and Trust
Author: Tehranipoor and Wang
Publication date and edition: Springer, 2011
ISBN number: 978-1441980793
Software: Xilinx ISE package and Synopsys Verilog simulation package
Hardware: Avnet Spartan-6LX9 MicroBoard

Weekly Schedule of Topics : Week 1 - Syllabus, Ethics, Introduction to hardware security and trust, Emerging applications and the new threats
Week 2 – Introduction to Cryptography
Week 3 - Basics of VLSI Design and Test
Week 4 - Security Based on Physically Unclonability and Disorder
Week 5 - Hardware Metering; Watermarking of HWIPs
Week 6 - Physical Attacks and Tamper resistance
Week 7 – Side Channel Attacks and Countermeasures, Countermeasures for Embedded

Microcontrollers
Week 8 – Fault Injection Attacks; Security in Embedded Systems
Week 9 – Security for RFID Tags; Hardware Trojans: IC Trust (Taxonomy & Detection)
Week 10 – Hardware Trojans: IP Trust (Detection)
Week 11 - Design for Hardware Trust
Week 12 - Protecting against Scan-based Side Channel Attacks
Week 13 - Counterfeit Detection and Avoidance
Weeks 14-16 - Student presentations

Grading Scheme : 50% midterm and final exams
20% Project Demonstration
20% Assignments
10% Oral Presentation

Instructor(s) : Dr. Domenic Forte, Dr. Swarup Bhunia, Dr. Mark Tehranipoor

EEL 4876 Introduction to Hardware Security and Trust

1. Catalog Description – (3 credits) Fundamentals of hardware security and trust for integrated circuits. Cryptographic hardware, invasive and non-invasive attacks, side-channel attacks, physically unclonable functions (PUFs), true random number generation (TRNG). watermarking of Intellectual Property (IP) blocks, FPGA security, counterfeit detection, hardware Trojan detection and prevention in IP cores and integrated circuits.

2. Pre-requisites – EEL 4712C

3. Course Objectives – The student will be able to describe the state-of-the-art security methods and devices; identify attacks and design countermeasures against them; identify and isolate hardware Trojans; create the integration of security as a design metric; protect the design of intellectual property against piracy and tampering.

4. Contribution of course to meeting the professional component (ABET only – undergraduate courses) – 3 hours of Engineering Science

5. Relationship of course to program outcomes (ABET only undergraduate courses) – a, f, i, j, k

6. Instructor – Dr. Domenic Forte
    a. Office location: 339E Larsen
    b. Telephone: 392-1525
    c. E-mail address: dforte@ece.ufl.edu
    d. Class Web site: http://dforte.ece.ufl.edu
    e. Office hours: TBD

    Instructor – Dr. Swarup Bhunia
    a. Office location: 336A Larsen
    b. Telephone: 392-5989
    c. E-mail address: dforte@ece.ufl.edu
    d. Class Web site: http://dforte.ece.ufl.edu
    e. Office hours: TBD

    Instructor – Dr. Mark Tehranipoor
    a. Office location: 25 Benton
    b. Telephone: 392-1525
    c. E-mail address: dforte@ece.ufl.edu
    d. Class Web site: http://dforte.ece.ufl.edu
    e. Office hours: TBD

7. Teaching Assistant - TBD
    a. Office location:
    b. Telephone:
    c. E-mail address:

d. Office hours:

8. Meeting Times and Location – Monday, Wednesday Friday, 3rd period, 339 Larsen

9. Class/laboratory schedule – 3 class periods each week consisting of 50 minutes each

10. Material and Supply Fees - None

11. Textbooks and Software Required -
    a. Title: Introduction to Security and Trust
    b. Author: Tehranipoor and Wang
    c. Publication date and edition: Springer, 2011
    d. ISBN number: 978-1441980793
    e. Software: Xilinx ISE package and Synopsys Verilog simulation package
    f. Hardware: Avnet Spartan-6LX9 MicroBoard per team of 3 students. Students should check with the instructor before purchasing the board.

12. Recommended Reading -

Reading

- 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 (WS)
- The Hunt for the Kill Switch
- Hardware Trojan (computing)
- Defense Science Board Task Force On High Performance Microchip Supply
- Old Trick Threatens the Newest Weapons
- A Survey of Hardware Trojan taxonomy and Detection
- Detecting malicious inclusions in secure hardware: Challenges and Solutions
- FPGA Design Security Bibliography
- Supergeek pulls off 'near impossible' crypto chip hack
- Security through obscurity
- Trust-Hub

Videos

- What's inside a microchip? http://www.youtube.com/watch?v=GdqbLmdKgw4
- Zoom Into a Microchip http://www.youtube.com/watch?v=Fxv3JoS1uY8
- Public Key Cryptography: RSA Encryption: http://www.youtube.com/watch?v=wXB-V_Keiu8

- Counterfeit Electronics Could Be Dangerous, Funding Nefarious People http://www.youtube.com/watch?v=dbZiUe6guxc
- How Computers and Electronics Are Recycled http://www.youtube.com/watch?v=Iw4g6H7alvo
- Counterfeit Electronic Components Process http://www.youtube.com/watch?v=5vN_7NJ4qYA
- Counterfeit Inspection http://www.youtube.com/watch?v=MbQUvu2LN6o
- Gold from waste circuit electronics http://www.youtube.com/watch?v=ZkhOuNvkuu8
- Tarnovsky Deconstruct Processor https://www.youtube.com/watch?v=w7PT0nrK2BE

13. Course Outline –
    a) Week 1 - Syllabus, Ethics, Introduction to hardware security and trust, Emerging applications and the new threats
    b) Week 2 – Introduction to Cryptography
    c) Week 3 - Basics of VLSI Design and Test
    d) Week 4 - Security Based on Physically Unclonability and Disorder
    e) Week 5 - Hardware Metering; Watermarking of HWIPs
    f) Week 6 - Physical Attacks and Tamper resistance
    g) Week 7 – Side Channel Attacks and Countermeasures, Countermeasures for Embedded Microcontrollers
    h) Week 8 – Fault Injection Attacks; Security in Embedded Systems
    i) Week 9 – Security for RFID Tags; Hardware Trojans: IC Trust (Taxonomy & Detection)
    j) Week 10 – Hardware Trojans: IP Trust (Detection)
    k) Week 11 - Design for Hardware Trust
    l) Week 12 - Protecting against Scan-based Side Channel Attacks
    m) Week 13 - Counterfeit Detection and Avoidance
    n) Weeks 14-16 - Student presentations

14. Attendance and Expectations - Cell phones and other electronic devices are to be silenced. No text messaging during class or exams.

    The course is comprised of weekly lectures, 3-4 modules, student presentation module, and a final project.

    Students must submit ***individual*** work ***individually*** on each module and as a team of 3 on final project. You are encouraged to work together on homework assignments and share ideas on lab assignments. However, you are not allowed to copy or duplicate any lab material (code, drawings, etc.) from another student. This work will be considered cheating and will be dealt with in a severe manner. See Section 18 on Honesty Policy.

The final project will require implementation of a hardware security primitive or attack on an FGPA based on a detailed specification given to the teams. Students will prepare a presentation and demonstration for the project.

It is the student's responsibility to return all FGPA boards by the time of project demonstration.

Requirements for class attendance and make-up exams, assignments, and other work in this course are consistent with university policies that can be found in the online catalog at: https://catalog.ufl.edu/ugrad/current/regulations/info/attendance.aspx

15. Grading –

50%	midterm and final exams
20%	Project Demonstration
20%	Assignments
10%	Oral Presentation

The requirements differ between the graduate and undergraduate students based on grading methods, homework assignments, and final project.

Undergraduates: The undergraduate students are given homework assignments from the textbook, and they are only required to give an oral presentation and demonstration of the project.

Graduates: The graduate students are given a more challenging homework questions, final project and they are expected to give a detailed project report.

16. Grading Scale –

A	A-	B+	B	B-	C+	C	C-	D+	D	D-	E
93-100	90-92	87-89	83-86	80-82	77-79	73-76	70-72	67-69	63-66	60-62	0-59

"A C- will not be a qualifying grade for critical tracking courses. In order to graduate, students must have an overall GPA and an upper-division GPA of 2.0 or better (C or better)." Note: a C- average is equivalent to a GPA of 1.67, and therefore, it does not satisfy this graduation requirement. For more information on grades and grading policies, please visit: https://catalog.ufl.edu/ugrad/current/regulations/info/grades.aspx

17. Make-Up Exam Policy – If you have a University-approved excuse and arrange for it in advance, or in case of documented emergency, a make-up exam will be allowed and arrangements can be made for making up missed work. University attendance policies can be found at:
https://catalog.ufl.edu/ugrad/current/regulations/info/attendance.aspx

Otherwise, make-up exams will be considered only in extraordinary cases, and must be taken before the scheduled exam. The student must submit a written petition to the instructor two weeks prior to the scheduled exam and the instructor must approve the petition.

18. 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 (http://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.

19. Accommodation for Students with Disabilities – Students requesting classroom accommodation must first register with the Dean of Students Office. That office will provide documentation to the student who must then provide this documentation to the course instructor when requesting accommodation.

20. UF Counseling Services – Resources are available on-campus for students having personal problems or lacking clear career and academic goals. The resources include:
    - UF Counseling & Wellness Center, psychological and psychiatric services, 3190 Radio Rd, 392-1575, online: http://www.counseling.ufl.edu/cwc/Default.aspx,
    - Career Resource Center, Reitz Union, career and job search services, 392-1601.
    - University Police Department, 392-1111 or 911 for emergencies

21. Software Use – All faculty, staff and student 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.

22. Course Evaluation – Students are expected to provide feedback on the quality of instruction in this course based on 10 criteria. These evaluations are conducted online at: https://evaluations.ufl.edu. 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.