Course ID: ECE 525 Hardware-Oriented Security and Trust
Professor Jim Plusquellic
jplusq@unm.edu
ECE 236C, 12pm to 1pm, Mon. and Wed.
http://ece-research.unm.edu/jimp

Department Information
Electrical and Computer Engineering Bldg
MSC01 1100
1 University of New Mexico
ECE Bldg., Room 125
Albuquerque, NM 87131-0001
Phone: 505-277-2436

Program Information
Undergraduate Academic Advisor: Elias
Office: ECE Building Room 115
Phone: (505) 277-1435

Course Description
This course investigates recent technology developments for the design and evaluation of secure and trustworthy hardware. Hardware security and trust techniques are required to ensure that chips remains secure and trustworthy during its entire lifecycle from design to manufacturing, deployment, service and retirement. The following topics are covered in this course as well as their application to the Internet-of-Things (IoT), autonomous cars, smart homes, smart grid, factory automation, smart infrastructure and cloud computing.

- Hardware security primitives, including Physical Unclonable Functions (PUFs), are investigated that are capable of generating unique, unclonable chip identifiers and secret bitstrings. Internal chip-generated secrets can be used to detect counterfeiting, for implementing intellectual property licensing and metering schemes, and to provide a root-of-trust for secure boot and for authentication and encryption between Internet-of-Things (IoT) devices.
- Techniques are discussed that are designed to detect Hardware Trojans inserted by adversaries to provide 'back-doors' and 'kill switches' in chips.
- Circuit design techniques are investigated that can protect chips against unauthorized extraction of private information within chips using Side-Channel attacks.
- Circuit obfuscation methods are discussed that prevent black-market cloning, reverse engineering and intellectual property theft.

Course Goals

- Hardware-Oriented Security and Trust (HOST) is focused on the design, implementation and deployment of secure and trustworthy hardware platforms, including chips, boards and systems. In order to design secure and trustworthy chips and systems, one must first have a broad knowledge of the vulnerabilities, of security and trust primitives and techniques, and of statistical tools and techniques. This course exposes students to all of these HOST aspects as well as to state-of-the-art countermeasures.
- There are many vulnerabilities in hardware and software systems, and the overall security and trust of a system is only as strong as its weakest link. This course provides a comprehensive survey of state-of-the-art technology and practices.

- News stories related to security breaches are published frequently, revealing the nature of the game between adversaries armed with new capabilities and attack mechanisms and an ever changing suite of countermeasures introduced by trusted authorities to thwart such attacks. To be effective, you will need to have an on-going, regular interaction with the commercial and academic communities. This course provides the background for students to succeed in HOST-based careers.
- Hardware-based security and trust intersects with software-based security, but is distinct in many ways. A simulation-based approach used in software security to learning HOST concepts is not as effective as a hands-on experimental-based approach. In fact, several important topics within HOST cannot be fully explored using modeling and simulation, e.g., PUFs and side-channel methods for extracting information and detecting hardware Trojans are heavily impacted by poorly modeled within-die process variations. This course takes a hardware-based, hands-on approach to learning, exposing students to FPGAs, test and measurement equipment, and live network communication protocols.
- An important component of Computer Engineering is becoming fluent with computer-aided design (CAD) tools, such as Xilinx Vivado and Cadence Virtuoso. The laboratories and project expose students to FPGA hardware synthesis tools and SoC tool flows that integrate custom hardware with C programs running on embedded microprocessors.

NOTE This is a laboratory/project based course. Most of your learning will take place as you complete the laboratory and project assignments. The lecture material is supplemental to your learning, i.e., you should become familiar with the tools and techniques described in the lecture material, assimilate and apply those techniques as needed to complete the laboratory and project assignments. This is a graduate course and therefore, I will expect you to evaluate the problems, decide on which tools/techniques are relevant and useful for the task, and then adapt and apply them to derive a solution.

Course Objectives/Learning Outcomes

- **C1 (Crytographic Algorithms):** Describe the algorithms and security properties of modern cryptographic algorithms including secure hash, encryption and key exchange mechanisms.
- **C2 (Hardware Security and Trust Primitives and Methods):** Define the emerging set of hardware security and trust primitives and describe the underlying principles on which they are based for detecting and preventing adversarial attacks.
- **C3 (Mathematical and Statistical Methods for Assessing Security Properties):** Describe and apply mathematical and statistical methods to evaluate the security properties of hardware security and trust primitives and methods.
- **C4 (CAD Tools):** Demonstrate the ability to apply hardware security and trust primitives and techniques to an actual internet-of-things (IoT) application scenario using an FPGA SoC architecture.

Technical Goals

- An important component of Computer Engineering is becoming fluent with Computer-Aided Design tools, such as Xilinx Vivado and Cadence Virtuoso. This course will introduce you to Vivado, which will be used in combination with the C programming language.
- Hardware-oriented security and trust is focused on the design and implementation of secure and trusted chips and systems. A key skill to building secure and trusted systems is first understanding adversarial attack mechanisms and system vulnerabilities and then choosing the

appropriate countermeasures. This course will provide students with tools, techniques and a theoretical basis for building systems that are highly resilient to a well financed, highly capable adversary.
- Proficiency in building systems that are secure and trustworthy requires a broad knowledge of the design, fabrication and operational behavior of microelectronic systems, including complex CAD tool flows, manufacturing process variations and testing processes, information leakage in side-channel signals and electromagnetic emissions, temperature-voltage sensitivity, statistical assessment techniques and machine learning classification algorithms. This course will provide instruction on these concepts and on the use of commercial CAD tools and hardware systems, which define the basis of modern IoT systems and applications.

Specific Course Requirements

An undergraduate course in C programming is highly recommended, as well as experience with FPGAs.

Technical Skills

In order to participate and succeed in this class, you will need to be able to perform the following basic technical tasks:
- Use Canvas.
- Use email, including attaching files, opening files, downloading attachments and open a hyperlink.
- Use a word processor to create homework, laboratory and project reports. NOTE: YOU MUST ONLY SUBMIT TXT and/or PDF files. WORD, EXCEL or other types of word processing formats will NOT be accepted.
- Create and upload PDF files.
- Work within a Linux operating system environment, e.g., have knowledge of basic commands including file and directory operations, of software for editing files, of networking concepts, e.g., setting static IPs, configuring routers, etc.
- Have experience with writing, compiling and debugging C programs.
- Install and use computer-aided design (CAD) tools.
- Connect, configure and carry out hardware demonstrations on FPGAs, e.g., powering up an FPGA board, connecting ethernet and USB cables to computers and routers, running serial and network communication and file transfer programs.

Supplemental documentation is provided for computer management tasks

Course Requirements

Students are expected to view the video lectures covering the technical topics, take the quizzes and complete the reading, laboratory and project assignments. This course includes one mid-term exam. There is no final exam, instead students are expected to complete a final project and perform a hardware demonstration.

Technical Requirements

Computer
- A high speed Internet connection is highly recommended.
- Supported browsers include: Internet Explorer, Firefox, and Safari. Detailed Supported Browsers and Operating Systems.

- Any computer capable of running a recently updated web browser should be sufficient to access your online course. However, bear in mind that processor speed, amount of RAM and Internet connection speed can greatly affect performance. Many locations offer free high-speed Internet access including UNM's Computer Pods.
- For watching the course videos, be sure you have downloaded and installed the latest version of Java, Flash, and Mozilla Firefox. They may not come preloaded.
- Microsoft Office products are available free for all UNM students (more information on the UNM IT Software Distribution and Downloads page: http://it.unm.edu/software/index.html)

For UNM Learn Technical Support: (505) 277-0857 (24/7) or use the "Create a Support Ticket" link in your course.

Textbook and Supplemental Materials

Recommended Textbooks and Book Chapters:

- "The Hardware Trojan War: Attacks, Myths, and Defenses", Chapter 10, "Detecting Hardware Trojans using Delay Analysis", Springer, 2017 (provided on course webpage).
- "Fundamentals of IP and SoC Security, Design, Verification, and Debug", Chapter 6, "PUF-Based Authentication", Springer, 2017 (provided on course webpage).
- "Physically Unclonable Functions: Constructions, Properties and Applications", Roel Maes, Springer, SBN 978-3-642-41394-0, ISBN 978-3-642-41395-7 (eBook)
- "Handbook of Applied Cryptography", A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, http://cacr.uwaterloo.ca/hac/ (freely available for downloading).

Required Supplementary Materials

- Students may be required to setup an account with Xilinx (www.xilinx.com) as a mechanism to download the Vivado software tool. A free license will be provided by Xilinx.
- Students may be required to buy an FPGA board (at an academic discount price) as covered in the laboratory introductory video(s).

Coursework and Deadlines

Weekly Schedule

- Each module will be covered in 1 week, e.g., Module 1 in week 1, etc.
- All screen casts will be followed by a quiz. Quizzes corresponding to a module MUST be completed in order, and by Sunday at 11pm.
- Laboratory reports and the project report must be submitted by Sunday, by 11pm the week they are assigned.
- The midterm will be a 2-hour timed exam.

Every effort will be made to answer student questions within 2 days, and to report grading to students within 1 week of the submission deadline.

Class Effort and Expectations

Please plan on devoting approx. 15 hour per week to cover the lecture material, participate in discussions and to do the homework, laboratories and project. You have likely been exposed to the C programming language and CAD tools such as Vivado in previous courses. However, if your experience is limited, please plan on spending additional time beyond the 15 hours per week. This course is 8 weeks long and therefore, runs at twice the pace of a regular course. Therefore, 15

hours may sound like a lot but we'll need to cover 16 weeks of material in 8 short weeks. Other requirements to consider:

- PLEASE NOTE THAT ALL ASSIGNMENTS WILL BE POSTED TO THE FOLLOWING WEBSITE:
  http://ece-research.unm.edu/jimp/HOST/index.html
  UNM's learning website is supplemental to this course.
- Students are expected to communicate with one another on laboratory and project assignments.
- Students are expected to keep abreast of course announcements.
- Students are expected to use the Learn course email as opposed to a personal email address.
- Students are expected to keep instructor informed of class related problems, or problems that may prevent the student from full participation.
- Students are expected to address technical problems immediately.
- Students are expected to observe course netiquette at all times.

Grading Procedures

All homeworks, laboratories and the project are designed to be tied directly to the core material in this course. Becoming efficient at hardware-oriented security and trust requires hands-on experience, i.e., a significant component to your learning experience will occur while designing solutions and testing them through hardware experiments. Therefore, a significant portion of the grade is allocated to labs and projects, as shown below. All exams will be take-home.

Grading Policy

I will accept late work but please submit your initial attempt by the indicated times. Late work will be automatically be assigned half-credit if submitted after the deadline, so turn in whatever you can before the deadline. Also, all the work in this class is cumulative so if you fall behind, it will be very hard for you to catch up.

If you anticipate difficulty in meeting a deadline, you need to notify me at least 1 day in advance of the deadline and be prepared to provide evidence explaining why you will be late.

All written work needs to be submitted online. If you have difficulty using a tool to complete work, use the "Create a Support Ticket" link in the Course Menu and immediately notify me of your difficulties.

Grading Distribution and Description

The distribution of weights for the exams, laboratories and projects is as follows:

Midterm	30%
Laboratories	30%
Project	30%
Participation (5%) and Quizzes (5%)	10%

Midterm Exam: The mid-term exam consists entirely of short answer types of questions. A sample exam is provided to enable students to be prepared for the type of questions they will be

expected to answer. Your written answers will be assessed according to the level of understanding that you have of the subject matter, i.e., primarily on the correctness of your answer, but also on the conciseness of your answer. Focus on answering the question and avoid writing 'everything you know' about the topic. The exam is designed to give you enough time to write concise answers to the questions.

Laboratories: Students purchase an FPGA board at the beginning of the course and work through a series of laboratories to become familiar with working with FPGAs using computer-aided design tools, e.g., Xilinx Vivado. There are 6 laboratories beginning with installation instructions of Vivado and statistical testing methods of bitstrings, through an implementation of a physical unclonable function. The laboratory reports are graded according to the rubrics defined below.

Project: Students will work in groups of two to implement an PUF-based authentication protocol, which builds on work carried out in the laboratories. The authentication protocol is implemented using FPGA boards internet-connected to a server. Students develop and debug a C program that implements the protocol and interfaces to the PUF implementation (the PUF implementation is supplied to the students). A project hardware demonstration and a project report are used to assess the quality and completeness of the students' protocol implementation. The project report is graded according to the rubrics defined below.

Discussions: Every module will include a 'Questions' discussion forum. Students are expected to participate actively in discussions by asking and answering questions that other students or the instructor posts. Participation in question and answer discussion forums represent the main component of the 'Participation' component of your grade. At least one post which asks a question, provides a comment or an answer to another student's question is required from each student in each of the 8 modules in order to receive 3% of the 5% allocated for participation. Student engagement will be monitored by the instructor and exceptional interaction will be rewarded with full credit of 5%.

Participation: Tracking Course Activity UNM Learn automatically records all students' activities including: your first and last access to the course, the pages that you have accessed, the number of discussion messages that you have read and sent, discussion text and posted discussion topics. This data can be accessed by the instructor to evaluate class participation and to identify students having difficulty.

Summary of Course Work: There are a total of 6 laboratories each assigned a maximum of 10 points. Each laboratory is considered an 'Assignment' and requires a laboratory report. You are also expected to participate in all 8 discussion forums, one within each of the 8 modules. The midterm and final project are also components of the required work in this course.

No incompletes will be given, except as required by university policy for truly exceptional circumstances.

Cheating at any time in this course will cause you to fail the course. Cheating is defined in the standard way as copying assignments from others and acts of plagiarism, **but also includes using ChatGPT for any part of any assignment, project, exam or discussion board conversation**. I reserve the right to call you into my office at any point to ask you to explain your work in words. If you are not able to do so, I will report an incident of cheating to UNM authorities.

For a complete description of academic dishonesty, refer to the UNM Student Handbook.

Laboratory and Project Rubrics

- 20% Description
  Does the report minimally include the following components: title, introduction to the lab that describes the problem to be solved, a body section that shows how the problem was solved (with schematic and supporting waveforms, if needed), and concluding remarks on the results and the student's experience?
- 20% Correctness
  Is the problem solved correctly?
- 20% Completeness
  Are all the steps needed to solve the problem explicitly shown. For example, are the schematic diagram and the boolean equations given? Is the code given? Are the waveforms given? Are there comments in the Verilog code? Depending on the requirements given in the lab description, some of these components are not needed.
- 20% Clarity/Conciseness
  Are the description and results clearly and concisely presented or is there unnecessary clutter or redundancy?
- 20% Quality of write-up
  Is the lab report easy to read? Are the figures, plots, etc. neatly and professionally presented, i.e., in electronic form with arrows and text explaining the important features? Is the information on the title page complete, with a meaningful title and the student's name.

Grading Scale

A+	(97-100)
A	(93-96)
A-	(90-92)
B+	(87-89)
B	(83-86)
B-	(80-82)
C+	(77-79)
C	(73-76)
C-	(70-72)
D+	(67-69)
D	(63-66)
D-	(60-62)
F	(0-59)

Schedule of Activities

Week(1): Introduction and Cryptography
Week(2): Physical Unclonable Functions
Week(3): PUF Implementations
Week(4): PUF-Based Authentication
Week(5): Secure Boot
Week(6): Hardware Trojans
Week(7): Side Channel Attacks and CounterMeasures

Week(8): Project

Netiquette

- In following with the UNM Student Handbook, all students will show respect to their fellow students and instructor when interacting in this course. Take Netiquette suggestions seriously. Flaming is considered a serious violation and will be dealt with promptly. Postings that do not reflect respect will be taken down immediately.
- This course encourages different perspectives related to such factors as gender, race, nationality, ethnicity, sexual orientation, religion, and other relevant cultural identities. The course seeks to foster understanding and inclusiveness related to such diverse perspectives and ways of communicating.
- Link to Netiquette document: http://online.unm.edu/help/learn/students/pdf/discussion-netiquette.pdf

UNM Policies

Title IX: Gender Discrimination

In an effort to meet obligations under Title IX, UNM faculty, Teaching Assistants, and Graduate Assistants are considered "responsible employees" by the Department of Education (see page 15 - http://www2.ed.gov/about/offices/list/ocr/docs/qa-201404-title-ix.pdf). This designation requires that any report of gender discrimination which includes sexual harassment, sexual misconduct and sexual violence made to a faculty member, TA, or GA must be reported to the Title IX Coordinator at the Office of Equal Opportunity (oeo.unm.edu). For more information on the campus policy regarding sexual misconduct, see: https://policy.unm.edu/university-policies/2000/2740.html

Copyright Issues

All materials in this course fall under copyright laws and should not be downloaded, distributed, or used by students for any purpose outside this course.

Accessibility

The American with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodations of their disabilities. If you have a disability requiring accommodation, please contact the UNM Accessibility Resource Center in 2021 Mesa Vista Hall at 277-3506 or http://as2.unm.edu/index.html. Information about your disability is confidential.

- Blackboard's Accessibility statement: http://www.blackboard.com/accessibility.aspx

Academic Misconduct

You should be familiar with UNM's Policy on Academic Dishonesty and the Student Code of Conduct (http://pathfinder.unm.edu/code-of-conduct.html) which outline academic misconduct defined as plagiarism, cheating, fabrication, or facilitating any such act.

Drop Policy

UNM Policies: This course falls under all UNM policies for last day to drop courses, etc. Please see http://www.unm.edu/studentinfo.html or the UNM Course Catalog for information on UNM

services and policies. Please see the UNM academic calendar for course dates, the last day to drop courses without penalty, and for financial disenrollment dates.

UNM Resources

CAPS Tutoring Services http://caps.unm.edu/programs/online-tutoring/
CAPS is a free-of-charge educational assistance program available to UNM students enrolled in classes. Online services include the Online Writing Lab, Chatting with or asking a question of a Tutor.

Embedded Tutor - if this course has a tutor assigned, substitute the following:
This course has tutoring services incorporated into the course. Please see the "CAPS Tutor" link in the course menu on the left for more details.

UNM Libraries http://library.unm.edu

Student Health & Counseling (SHAC) Online Services
http://online.unm.edu/help/learn/support/shac

Tentative Course Outline:

Date	Lecture
Week 1&2	Introduction and Cryptography Lab #0
Week 3&4	Physical Unclonable Functions Lab #1
Week 5&6	PUF Implementations Lab #2
Week 7&8	PUF-Based Authentication and Encryption Lab #3
Week 9&10	Secure Boot, Midterm Lab #4
Week 11&12	Hardware Trojans Lab #5
Week 12&14	Side-Channel Attacks and Countermeasures Project
Week 15&16	Project

Changes/Additions to this schedule will be posted as needed throughout the term