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

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.

Key Take-Aways from this Course

- To be effective in hardware-oriented security and trust (HOST), you need to become fluent with C programming, hardware description languages (HDL) such as Verilog or VHDL, statistics, networks and manufacturing test practices. This course exposes students to the tools and techniques used in each of these areas.
- 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.

Course Objectives

- **C1:** 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.

- **C2:** 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.
- **C3:** 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.

Specific Course Requirements

Undergraduate courses in C programming and VHDL are recommended. The course leverages SoC integration of software (C) and hardware (VHDL) as the basis for investigating HOST concepts.

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 UNM Learn (help documentation located in "How to Use Learn" link on left course menu).
- Use email - including attaching files, opening files, downloading attachments.
- Open a hyperlink (click on a hyperlink to get to a website or online resource).
- 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.
- Download, annotate, save and upload PDF files.
- Use the in-course web conferencing tool (Collaborate Web Conferencing software).
- Download and install an application or plug in - required for participating in web conferencing sessions.

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: http://online.unm.edu/help/learn/students/
- 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 using the Kaltura Media Tools inside Learn, 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.

Web Conferencing

Web conferencing will be used in this course during the following times and dates: TBD
For the online sessions, you will need:

- A USB headset with microphone. Headsets are widely available at stores that sell electronics, at the UNM Bookstore or online.
- A high-speed internet connection is highly recommended for these sessions. A wireless Internet connection may be used if successfully tested for audio quality prior to web conferencing.
- For UNM Web Conference Technical Help: (505) 277-0857

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

Textbook and Supplemental Materials

Recommended Textbooks:

- "The Hardware Trojan War: Attacks, Myths, and Defenses", Springer, 2017.
- "Fundamentals of IP and SoC Security, Design, Verification, and Debug", Springer, 2017.
- " Hardware Protection through Obfuscation", Springer, 2017.
- "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/

Required Supplementary Materials

- Students will 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 Participation

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 Friday at 11pm.
- Laboratory reports and the Project report must be submitted by Friday, 11pm the week they are assigned.
- The midterm will be a 2-hour timed exam. See details posted in UNM Learn.

Every effort will be made to report grading to students within 1 week of the submission deadline.

Procedures for Completing Coursework

Include:

- Given the compressed format of this course, late or missed work will receive a zero score.
- All exams will be take-home.

- Other policies:

  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.

Expectations for Participation

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. Your previous course work using VHDL necessarily exposed you to CAD tools such as Vivado. However, if you 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:

- Students are expected to learn how to navigate in Learn
- Students are expected to communicate with one another in team projects
- 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

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

Grading Procedures

All homeworks, laboratories and the project are designed to be tied directly to the core material in this course. Becoming efficient at codesign requires hands-on experience, i.e., lecture material is important but most of your learning will occur while designing solutions, testing them through simulation and hardware experiments, and examining how the tools synthesize designs to implementations. Therefore, a large portion of the grade is allocated to labs and projects, as shown below. I can usually return homework, laboratory and exam scores within a week of the submission deadline.

Laboratory Grading Criteria

- 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

The distribution of weights for the exams, laboratories and projects is as follows. Labs are all equally weighted, and scored as exams on a scale from 0 to 100:

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

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

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	Introduction and Cryptography Lab #0
Week 2	Physical Unclonable Functions Lab #1
Week 3	PUF Implementations Lab #2
Week 4	PUF-Based Authentication and Encryption Lab #3
Week 5	Secure Boot, Midterm Lab #4
Week 6	Hardware Trojans Lab #5
Week 7	Side-Channel Attacks and Countermeasures Project
Week 8	Project

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