ECE 4156 Course Syllabus

Course Number: **ECE 4156 A**
Course Title: **Hardware-Oriented Security and Trust**
Credits: **3 lecture hours = 3 credit hours total**
Semester: **Spring 2027**
Instructor: **Assoc. Prof. Vincent John Mooney III**

Prerequisites: ECE 3020 Mathematical Foundations of Computer Engineering *or* ECE 3058 Architecture, Systems, Concurrency & Energy in Computation *or* ECE 3170 Cryptographic Hardware for Embedded Systems

Required course material:
(Books) Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography*, 5th printing, CRC Press, 1996, and Jonathan Katz & Yehuda Lindel, *Introduction to Modern Cryptography*, 3rd edition, CRC Press, 2020
(Lecture Notes) To be distributed via a course website

Topical Outline
Module 1: Advanced Authentication
- Message Authentication Codes (MAC)
- Entropy & randomness
- Multi-party authentication

Module 2: Modern Cryptography
- Data privacy
- Indistinguishability
- Encryption modes
- Secret sharing
- AES, ECC and SHA

Module 3: Physically Unclonable Functions (PUFs)
- PUF construction classes
- PUF entropy sources
- PUF metrics & attacks including machine learning
- Practical considerations including current status

Module 4: Hardware and Software Vulnerabilities
- Common weakness enumerations
- Secure boot
- Timing Attacks
- Countermeasures in hardware

Module 5: Hardware Attacks
- Reverse engineering
- Advanced Hardware Trojans (HTs)

Evaluation Criteria: The course will have midterm exam(s), a final exam and frequent homeworks/labs. Labs will be based on VHDL and associated digital design (e.g., Synopsys Design Compiler) and simulation tools. This class may be taught in one section with both graduate students as well as undergraduates; to distinguish course expectations, graduate students will have to answer an additional question on an

advanced topic on homeworks and exams. For example, for an exam with five questions, the instructions will indicate that the fifth question is more advanced and should only be answered by students enrolled in the graduate section of the course. A typical breakdown of the percentage of the final grade for each component is 15% for homeworks, 20% for labs, 15% for each midterm (two total), and 35% for the final. Please note that in future semesters these percentages may vary but will always add up to 100%. The initial typical grading curve of 90% and above is an A, 80-89% B, 70-79% C, 60-69% D and below 60% is an F will be modified to remain or become more lenient after each exam. For example, after the first midterm exam the curve could be moved to 89% and above is an A, 80-88% B, 70-79% C, 58-69% D and below 58% is an F. Once moved, the curve will never move back up, e.g., if a B is moved to be 79-88% is a B then the curve will never go back up to 80-89% is a B.

Mode of Instruction for Spring 2027: The course will be taught in person with reasonable effort made to also provide lectures live on-line (synchronous) as well as recorded for later viewing (asynchronous). However, the on-line and recorded options are not guaranteed to always be available (100% of the time). In order to make time in class to go over homework questions, some (approximately 25%) of the lectures maybe be prerecorded while the rest of the lectures will be provided live in person, i.e., during the posted class meeting times in the official classroom. Class time will also be used to go over practice problems, e.g., old exams, to help prepare for the midterms and the final. For classes delivered live in the classroom while simultaneously broadcasting (e.g., using Zoom or Teams) and recording the lectures, typically a recording of each synchronous class (regardless of content, i.e., including both lecture material as well as problem solving sessions) will be made available in the Media Gallery on Canvas within 24 hours after each class. Typically Kaltura Capture is used to record class, but broadcast software (e.g., Zoom or Teams) may also be used. Due to ongoing concerns about viruses and other forms of communicable diseases, it is anticipated that not all students will want to attend all classes live in person. Therefore, other than for exams and to pick up the hardware (an FPGA board) to be loaned out for labs, in-person class attendance will not be required for this class, but it will be highly encouraged subject to health considerations. Class attendance will be required for all exams (midterms and the final); remote taking of exams will not be provided. Any medical or other emergency situation is covered by Attendance & Absences below.

Learning Objectives: This course aims to teach students the following:

1. Describe vulnerabilities in hardware and low-level software (e.g., firmware) which may be exploitable by malicious hackers.
2. Explain the concepts of randomness and entropy in the context of VLSI hardware which is difficult to duplicate or clone.
3. Describe and utilize important cryptographic principles such as authentication and message encoding for secrecy and privacy.
4. Identify and analyze attacks specific to semiconductor chip fabrication including advanced hardware Trojans.

Learning Outcomes: Upon successful completion of this course, students will have achieved the following:

1. Develop the ability to both identify and mitigate vulnerabilities in hardware and low-level software including firmware.
2. Develop analysis and evaluation skills with respect to entropy and randomness in electronics hardware.
3. Develop and apply important cryptographic techniques including modern authentication and encryption.
4. Evaluate and investigate VLSI semiconductor specific malicious attacks including hardware Trojans.

Attendance & Absences: Students with medical, family or other critical emergencies should contact the Office of the Dean of Students. Students should familiarize themselves with http://www.catalog.gatech.edu/rules/4/. To the extent possible, students should communicate excused absences in advance; when not possible, students shall communicate their excused absences as soon after the emergency as can reasonably be expected for the situation. Late assignments will not be accepted for credit without an excused absence. Missed exams will be handled on a case-by-case basis typically in close coordination and cooperation with the Office of the Dean of Students.

As noted above under Mode of Instruction, in-person class attendance is only required for exams and to pick up the FPGA hardware used for labs. The aim is to provide the majority of lectures in a remote fashion duplicating (albeit imperfectly) the classroom instruction. However, please note that while 100% reliable internet cannot be guaranteed, Kaltura Capture runs locally and records all class material regardless of periodic internet connectivity problems. In other words, subject to software and/or hardware problems (such as a microphone malfunction), all class content will be available and uploaded for students to view after the fact. Students who choose to attend remotely and miss portions of class due to internet connectivity and other similar issues are responsible for viewing the lecture recording of any material missed. Students are responsible for all class content.

Honor Code: Students are expected to hold the highest ethical standards not only for this class but also for the rest of their professional careers. Hardware security is a very serious topic and is critical to ensuring privacy, confidentiality and a healthy society. However, ethics in this course start and end in the human person. The Georgia Tech Honor Code http://www.policylibrary.gatech.edu/student-affairs/academic-honor-code http://catalog.gatech.edu/rules/18/ holds in all of its parts. When there is reasonably clear evidence of a violation, a referral to the Office of the Dean of Students will occur, and all hearings and other resulting procedures will be followed to completion.

Office of Disability Services: Students who are registered with the Office of Disability Services (ODS) shall provide appropriate forms and paperwork in person to the course instructor. If you think you may have learning needs, feel free to contact the Office of Disability Services at (404) 894-2563 or https://disabilityservices.gatech.edu/. An accommodation letter must be obtained from ODS in order to receive accommodations.