Department of Electrical Engineering and Computer Science, The University of Tennessee
ECE 459/559 – Secure and Trustworthy Computer Hardware Design, Spring 2016

The prevalence of modern computing systems provide many benefits but also come with a wide variety of new and challenging security and privacy concerns. Additional security issues arise from the globalization of computer hardware design and manufacture where a wide variety of parties are involved in the development of modern computer systems. Thus, trust and security are necessary through the full lifecycle of any computer system, from design to fabrication to deployment and use. Reliable design flows are first required to guarantee the production of trustworthy designs that protect against threats such as tampering and information leakage. Protections must also be put in place to mitigate issues through the development cycle of a computer system where malicious design modifications (i.e. hardware Trojans) and counterfeiting may be possible.

This course provides an in-depth introduction to a range of developments for the design of secure and trustworthy computer hardware. Topics covered include physical and invasive attack models, SCA attacks, physical unclonable functions, hardware-based random number generators, watermarking of intellectual property (IP) blocks, FPGA security, passive and active metering for piracy prevention, and hardware Trojan detection and isolation.

Teaching Staff
Professor: Garrett S. Rose: garose@utk.edu, 865-974-3132, **MK308**

Schedule
Lecture: MWF 10:10 am – 11:00 am **MK525**
Lab assignments: To be completed as individual homework assignments

Office Hours
Professor Rose: MW 2:00pm – 3:30pm; F 1:00pm – 2:00pm

Suggested Text (not required)
M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*, Springer, 2011.

Additional Reading
Academic papers and other relevant literature to be provided as needed

Grading

Labs/Homework:	15%
Quizzes/Participation:	10%
Mid-Term:	20%
Final Project:	35%
Final Exam:	20%

Assignment Policy
Lab assignments and homework are individual assignments to be completed on your own time – the professor will be available to help. Completed lab assignments must be verified and reports signed by the *before* class on the due date. All homework and lab assignments are to be handed in at beginning of class on due date unless told otherwise. ***If there is a reasonable excuse, you will get one week after original due date to submit only if you notify the professor first***. One week after due date, solutions to homework assignments will be posted on Blackboard and no excuses will be accepted for late assignments. In *extreme* situations, you may be accommodated by other substitute assignments (alternate homework, extra credit, etc.).

Academic Integrity
All homework and lab assignments to be turned in for credit must be each student's own work. Students can discuss problems and general ideas but any code or other deliverable must be written independently by each student.

Pop quizzes and in-class activities may be given from time to time during the class lecture period. Some in-class activities may allow for or even require collaboration with other students. Quizzes and in-class activities will be graded as part of "Quizzes/Participation." ***Quizzes and both exams will be closed-book with no discussion allowed***. Any violations can result in a zero on the given quiz or exam.

Electronic Devices
Laptops, smartphones, tablets and other electronic devices are allowed during lectures in as much as such devices are used with discretion and proper respect is given to the professor and other students. If the use of any electronic device is found to be a distraction then said device must be turned off and put away immediately.

A major component of this course consists of learning to code with VHDL. As such, some in-class activities may benefit from the use of a laptop or tablet. However, no activity will be given which requires the use of such devices.

Project Expectations
A major component of this course is a group project where students will implement a design of their choice. As part of the learning experience, students will discuss ideas, devise a plan, and divide up the work in small teams. Toward the end of class, project presentations will be delivered by each team. It is recommended that students begin forming teams and considering project topics as soon as possible.

Disability Statement
Any student requiring an accomodation based on the impact of a disability should contact the Office of Disability Services at 865-974-6087 to coordinate reasonable accomodations for documented disabilities.

Prerequisites
ECE 351 or instructor permission

Topics Covered
- Introduction to Hardware Security and Trust
- Introduction to Cryptography
- Design of Hardware Encryption/Decryption Engines
- Side-Channel Analysis (SCA) Attacks
- Hardware-based Random Number Generators
- FPGA Security Considerations
- Overview of the Semiconductor Supply Chain – Identification of Potential Threats
- Integrated Circuit Counterfeiting and Piracy
- Physical Unclonable Functions (PUFs)
- Watermarking of Intellectual Property (IP) Blocks
- Passive and Active Metering
- Hardware Trojans – Insertion, Detection and Isolation
- Logic Obfuscation Techniques