ELEC 7970 – HARDWARE SECURITY II
Spring Semester, 2018, TUESDAY-THURSDAY, 11AM, BROUN 113

Catalog Data: ELEC 7970/7976. Special Topics in Electrical Engineering Link Icon (Credit To Be Arranged, 1 to 5). Pr., departmental approval.

References Books*:* 1. *Understanding Cryptography: A Textbook for Students and Practitioners*, C. Paar, and Jan Pelz, Springer-Verlag Berlin Heidelberg, 2010, ISBN 978-3-642-04100-6
2. *Counterfeit Integrated Circuits: Detection and Avoidance*, M. M. Tehranipoor, U. Guin, and D. Forte, Springer International Publishing, 2015, ISBN: 978-3-319-11823-9
3. *Introduction to Hardware Security and Trust*, M. Tehranipoor, C. Wang, Springer-Verlag New York, 2012, ISBN 978-1-4419-8079-3

Coordinator: Ujjwal Guin, Assistant Professor of Electrical & Computer Engineering

Goals: Secure electronics has been playing an important role in safeguarding our society and day-to-day lives. Many different electronic devices that are connected to the Internet and have exhibited an increasing level of heterogeneity in recent years. Maintaining security over all these different devices becomes extremely challenging as they are being designed and manufactured in an environment with limited trust and visibility. Various new attacks are emerging to circumvent existing security measures. To enable secure and trust-worthy operation, it is absolutely necessary to understand various attacks and incorporate appropriate security measures. This course is intended for the graduate and undergraduate students who are interested in designing secure systems. This course provides an in-depth analysis of various topics, which includes cryptography, hardware Trojans, RFID, Internet of Things, JTAG, security primitives and side-channel attacks.

Prerequisites by topic: ELEC 5970/ELEC 6970 INTRODUCTION TO HARDWARE SECURITY

Topics (with approximate distribution of lectures):

1. Introduction (1 class)
2. Block Ciphers: Modes of Operation (2 classes)
3. Elliptic Curve Cryptosystems (4 classes)
4. Hash function: SHA-3 (1 class)
5. Key Establishment (2 classes)
6. Side-Channel Analysis (4 classes)
7. Hardware Trojans (4 classes)
8. Detection and Avoidance of Counterfeit Integrated Circuits (2 classes)
9. Physically Unclonable Functions (PUFs) (4 classes)
10. JTAG Security (2 Classes)
11. RFID Security (2 Classes)
12. Internet of Things (IoT) (4 Classes)

Methods for evaluating student performance:

Homework	15%
Design Project	30%
Research paper presentation and report	30%
Final Examination	25%
TOTAL	**100%**

Homework: Problems will be assigned throughout the semester to reinforce the class material.

Research Presentation and Report: Two research papers will be assigned to each student for evaluating the effectiveness of the solution(s) presented. The presentation should contain a clear problem statement, existing research in that domain, the solution(s) presented in the paper, and the simulation results. It is also required to comment on the shortcomings of the solution. The presentation should contain 10 slides. Each student need to submit a 4 to 6-page report on their selected topics. The report must follow IEEE guidelines (https://www.ieee.org/conferences_events/conferences/publishing/templates.html).

Justification for Graduate Credit in ELEC 7970: Graduate students are challenged with a current security problem and are also expected to research and report their ideas to solve it.

Academic Honesty Policy: All portions of the Auburn University student academic honesty code (Title XII) found online at http://www.auburn.edu/academic/provost/academicHonesty.html apply to this class. Every student is expected to do his/her own homework and research. Discussion of various aspects with fellow students is acceptable, provided that they are not similar. Copying of another student's solution will be considered a violation of the academic honesty code by both students.

Class attendance: Class attendance is highly encouraged but will not be accounted for in the course grade.

Policy on unannounced quizzes: There will be no unannounced quizzes.

Accommodations: Any student requiring special accommodations should come by my office within the first two days of class, bringing your letter from the Office of Students with Disabilities, 1244 Haley Center, 844-2096 (V/TT).

Prepared by: Ujjwal Guin Date: 01/09/2018