ECE 446/579:04 Hardware and System Security (Spring 2023)

1. Basic Course Information

- Time: Thursdays 2-5 PM
- Location: SEC 208
- Instructor: Sheng Wei
  - sheng.wei@rutgers.edu
  - http://www.ece.rutgers.edu/~sw891

2. Course Description

- 3 Themes in Hardware & System Security
  - **Hardware for Security**: Advances in hardware security technologies that can provide fundamental support and enhancement for software and system security
  - **Security of Hardware**: Research efforts on hardware physical attacks and hardware security primitives
  - **System Security**: Attacks and defense techniques targeting computer system components
- No textbook is required. Recommended reading materials will be posted on Canvas under "Pages/Lecture Notes & Schedule".

3. Course Topics and Schedule

- Course Introduction (Week 1)
- Hardware for Security (Weeks 2-5)
  - Week 2: Physical Unclonable Functions (PUF)
  - Week 3: Trusted Platform Module (TPM)
  - Week 4: ARM TrustZone
  - Week 5: Intel SGX
- Security of Hardware (Weeks 6-8)
  - Week 6: Hardware Trojans
  - Week 7: Hardware Physical Attacks
  - Week 8: IC Piracy and Logic Locking
- System Security (Weeks 9-13)
  - Week 9: Memory Security
  - Week 10: Architecture Security
  - Week 11: Multimedia Security
  - Week 12: Machine Learning/AI System Security
- Project Presentation (Week 13)
- Review (Week 14)

4. Evaluation Criteria

- Homework Assignments (0%)
  - Homework will be posted on Canvas after each lecture; solutions will be posted the week after.
  - Homework will not be collected or graded but will be helpful for Quiz, Midterm & Final.
- Quizzes (10%)
  - 1 quiz per lecture (Lecture 3 through Lecture 12); 10 minutes each.
  - Open book & notes, no Internet; directly from homework.
- Midterm (20%) & Final (20%)
  - 1.5 hours each; open book & notes, no Internet; based on lecture slides/discussions and homework.
- Lab Projects (20%)
  - Hardware Security Lab (10%)
  - System Security Lab (10%)
- Research Project (30%)
  - Proposal (5%) + Presentation (15%) + Report (10%)
- Attendance
  - Required (Lecture 2 – Lecture 12); missing 3 lectures will reduce letter grade by 1 level.
- Bonus Points
  - Voluntary class presentations on specific topics (5%)
  - Active participation in class discussions (5%)
  - Completing optional exercises in lab projects (5%)
  - Research paper submissions based on course project (5%)