1. **Course Number and Course Title:**

   COE 694-05 – Hardware Security and Trust

2. **Credit Hours:**

   3 – 0 – 3

3. **Prerequisites and/or Co-Requisites:**

   Prerequisite: Approval of the CSE Head of Department
   Co-requisites: None
   Competencies: Undergraduate-level knowledge of computer architecture and hardware

4. **Name and Contact Information of Instructor:**

   Name: TBD
   Email: TBD
   Office: TBD
   Phone: TBD
   Office Hours: Posted on office door and iLearn; also by appointment

5. **Course Description (Catalog Description):**

   Presents attacks and countermeasures associated with the design, manufacturing, and deployment of hardware. Covers key topics including reverse engineering, side channel attacks, fault injection attacks, hardware trojans, IP piracy, and microarchitectural attacks. Examines hardware security primitives, security-by-design, hardware support for system security, and the use of emerging technologies such as AI and Blockchain in securing hardware.

6. **Textbook and other Supplemental Material:**

   Textbook:

   - S. Bhunia and M. Tehranipoor, *Hardware Security: A Hand-on Training Approach,* Morgan Kauffman, 2018.

   Other supplemental material:

   - M. Tehranipoor, K. Z. Azar, N. Asadizanjani, F. Rahman, H. M. Kamali, and F. Farahmandi, *Hardware Security: A Look into the Future*. Springer, 2024.
   - C.H. Chang and Y. Cao, Eds., *Frontiers in Hardware Security and Trust: Theory, Design and Practice*. The Institution of Engineering and Technology, 2020.
   - W. Hu, C. H. Chang, A. Sengupta, S. Bhunia, R. Kastner and H. Li, "An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 6, pp. 1010-1038, June 2021.
   - S. Akter, K. Khalil and M. Bayoumi, "A Survey on Hardware Security: Current Trends and Challenges," in *IEEE Access*, vol. 11, pp. 77543-77565, 2023.
   - H. Sayadi *et al*., "Towards AI-Enabled Hardware Security: Challenges and Opportunities," *2022 IEEE 28th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, Torino, Italy, 2022, pp. 1-10.

7. **Course Learning Outcomes:**

   Upon completion of the course, students will be able to:

   1. Analyze the security and trust vulnerabilities and challenges arising from the design practices and supply chain of hardware.
   2. Compare hardware design choices and trade-offs and their security implications.
   3. Evaluate the efficacy of countermeasures to hardware attacks.
   4. Appraise the role of hardware security for overall system security.

5. Analyze the use of emerging technologies such as Artificial Intelligence and Blockchain in securing electronics and computer hardware.
6. Critically review current research work in hardware security and trust.
7. Conduct independent research in the field of hardware security and trust.

**8. Teaching and Learning Methodologies:**

Methods include lectures, problem and project-based learning methods (assignments, exams, literature review, academic paper review, research project, presentation), and class discussions. Students learning is assessed via homework assignments, paper reviews, team research project, and exams.

**9. Course Topics and Schedule:**

| Topic/Activity | Weeks |
|---|---|
| Introduction: hardware security and trust | Week #1 |
| Principles: hardware design and supply chain | Week #2 |
| Attacks and countermeasures: Physical and invasive | Week #3 |
| Attacks and countermeasures: Non-invasive and side-channel | Week #4 |
| Attacks and countermeasures: Semi-invasive and fault injection | Week #5 |
| Attacks and countermeasures: supply chain vulnerabilities and hardware trojans | Week #6 |
| Attacks and countermeasures: Hardware trojans | Week #7 |
| Attacks and countermeasures: IP/IC piracy and counterfeiting + Midterm exam | Week #8 |
| Attacks and countermeasures: Microarchitectural | Week #9 |
| Paper review presentations | Week #10 |
| Security-by-design: Principles and approach | Week #11 |
| Security-by-design: Hardware security primitives | Week #12 |
| Security-by-design: Hardware support for system security | Week #13 |
| Emerging topics: Use of AI in hardware security | Week #14 |
| Emerging topics: Use of blockchain and digital twins in hardware security | Week #15 |
| Final Exam | Week #16 |

**10. Schedule of Laboratory and other Non-Lecture Sessions:**

The paper review is done individually and is due in Week #10. Students must conduct a review on a research paper that they choose from an assigned pool, analyze it critically, and write a short paper to summarize their analysis and findings, presenting the same to the class.

The research project is conducted by teams of 2-3 students and is due at the end of the semester. Student teams are required to research potential innovative uses of emerging technology in securing sector-specific hardware. Students are assigned different sectors and asked to choose at least two types of associated hardware, analyze relevant vulnerabilities and potential attacks, and propose mitigations utilizing emerging technologies. They need to submit a comprehensive report justifying their choice of hardware and explaining the vulnerabilities and the proposed mitigations.

**11. Out-of-Class Assignments with Due Dates:**

| Assignment | Due Date (tentative) |
|---|---|
| Homework 1: Fundamentals of hardware and system security | Week #3 |
| Homework 2: Side-channel attack methods | Week #6 |
| Research project proposal | Week #7 |

| | |
|---|---|
| Homework 3: IP/IC piracy and counterfeiting | Week #9 |
| Paper review | Week #10 |
| Homework 4: Security by design | Week #13 |
| Research project | Week #15 |

**12. Student Evaluation:**

| Assessment | Weight | Due Date (tentative) |
|---|---|---|
| Homework | 15% | cf. Section 11 |
| Paper Review | 15% | cf. Section 11 |
| Paper Presentation | 5% | Week 10 |
| Research Project | 20% | cf. Section 11 |
| Midterm Exam | 20% | Week 8 |
| Final Exam | 25% | Week 16 |

**13. Assessment Instruments:**

| Assessment | Course Learning Outcomes |
|---|---|
| Homework | O1, O2, O4 |
| Paper Review | O2, O3, O6 |
| Paper Presentation | O2, O3, O6 |
| Research Project | O2 – O5, O7 |
| Midterm Exam | O1-O3 |
| Final Exam | O1 – O5 |

**14. Contribution of Course to Program Outcomes:**

| MSCoE Program Outcomes | Emphasis in this course | Course Learning Outcomes |
|---|---|---|
| 1. Perform research emphasizing creativity, independent learning and scientific methods in a chosen area of computer engineering. | ● | O1-O7 |
| 2. Apply advanced mathematics and engineering knowledge in identifying, formulating and solving engineering problems. | ◑ | O1-O7 |
| 3. Select and use techniques, skills and modern tools necessary for research or professional practice. | ◑ | O6-O7 |
| 4. Communicate effectively. | | |
| 5. Recognize the need for, and engage in, lifelong learning. | | |
| 6. Attend to professional and ethical responsibilities. | | |

Emphasis: ● High; ◑ Medium; ○ Low; Blank – Nothing Specific Expected

**15. Letter Grade Policy:**

| Total (T) | Letter Grade |
|---|---|
| $90 \leq T$ | A |
| $85 \leq T < 90$ | A- |
| $80 \leq T < 85$ | B+ |
| $75 \leq T < 80$ | B |
| $70 \leq T < 75$ | B- |
| $65 \leq T < 70$ | C+ |
| $60 \leq T < 65$ | C |
| $T < 60$ | F |