Hardware Security and Trust: CMPE 297

Course Outline

Just as software can have exploitable flaws and vulnerabilities, hardware carries similar risks, but with one major setback: "patching" hardware vulnerabilities requires manual labor and much more time than software, which can be patched for millions of users with a click of a button. With billions of devices being created and released each year, researchers are developing advanced methods of improving and testing hardware security, making sure hardware is secure from the beginning.

In this course, we first understand the main idea of security and trust from the hardware perspective. Upon completing the course, students will understand the vulnerabilities in current digital system design flow and the physical attacks to these systems. They will learn that security starts from hardware design and be familiar with the tools and skills to build secure and trusted hardware.

Instructor: **Nima Karimian** (email: nimakarimian@sjsu.edu).

Classes: Monday for 2:45 minutes (details: http://nimakarimian.com /teaching).

Grading: Mid-term exam, Final exam, Quiz, Class Participation, 65%, Group Project – 35%.

Frequently Asked Questions

Q) I do not have theoretical computer hardware background; can I take this course?

A) Yes. The topics covered in this course assume that you have basic understanding of digital design. No additional expertise of theoretical computer hardware is required. Further, as hardware security involves interdisciplinary effort, students from other disciplines are encouraged to take this course.

Q) I do not have cryptography algorithm background; can I take this course?

A) Yes. The course will explain the basics of cryptography algorithm required to build, understand, and analyze hardware security system. No prior background in control theory is required.

Q) Are similar course offered in other universities?

A) Yes. Similar courses are offered at MIT, UF, UConn, UCSD, UMD college park

Q) What will I learn from this course?

A) This course will look at interesting techniques to tackle hardware security problem such as Counterfeiting, hardware Trojan, design intellectual property against piracy and tampering. These techniques can be applied to other disciplines to explore interesting research directions. If you are interested in one of the applications (such as AI, IoT, Power Grid systems), you can do a course project in which you can apply hardware security metrics in your own research.

Some Projects in Similar Courses

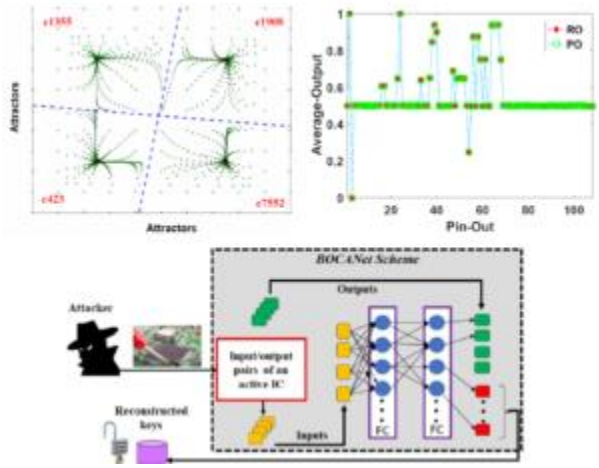

Figure 1 Broken Obfuscation Technique using Deep learning

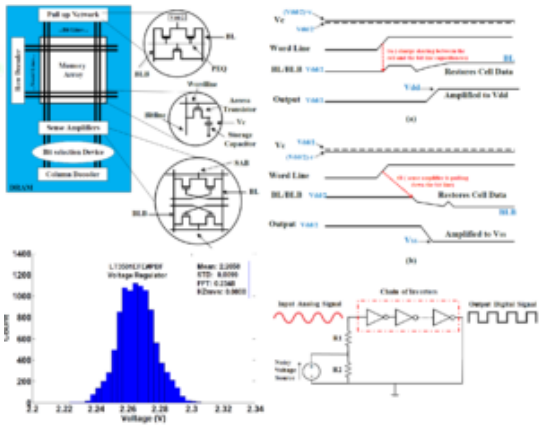

Figure 2 Fingerprint ICs and attacks on Memory

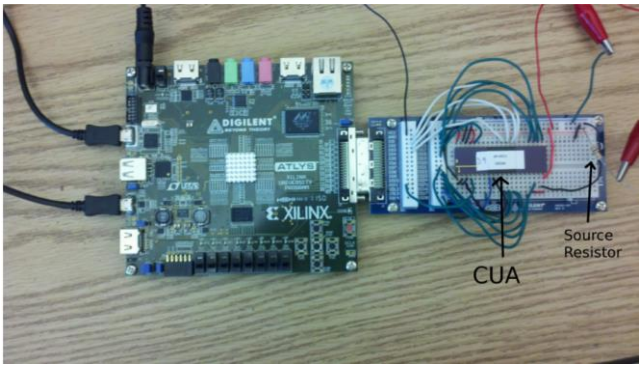

Figure 3 Hardware Trojan Detection using ML

Register for the course to participate in such exciting projects!