CSCI 4974/6974 Hardware Reverse Engineering
Course Syllabus

Professor: Bülent Yener; TA: Andrew D. Zonenberg
Department of Computer Science
Rensselaer Polytechnic Institute

1 Course Information

1.1 Description

Reverse engineering techniques for semiconductor devices and their applications to competitive analysis, IP litigation, security testing, supply chain verification, and failure analysis. IC packaging technologies and sample preparation techniques for die recovery and live analysis. Deprocessing and staining methods for revealing features below top passivation. Memory technologies and appropriate extraction techniques for each. Study of contemporary anti-tamper/anti-RE methods and their effectiveness at protecting designs from attackers. Programmable logic microarchitecture and the issues involved with reverse engineering programmable logic. Real-world case studies built around off-the-shelf commercial ICs ranging from above the $1\mu m$ node down to $45nm$ and below. PCB RE techniques including methods for extracting netlists, identifying components, and dumping firmware.

1.2 Prerequisites

The course is largely self-contained and will introduce the necessary chemistry, physics, and layout technologies required for a qualitative (rather than quantitative) understanding of the functioning of semiconductor devices. Either ECSE 2610, MATH 2800+CSCI 2500, or equivalent understanding of gate-level Boolean logic is required.

We are trying to keep the class accessible to Computer Science, Computer Engineering, and Electrical Engineering students and will be reviewing basic material as necessary.

1.3 Textbook

There is no textbook. We will discuss material in class and often refer students to papers or web resources relevant to the material at hand. All are either freely

available to the public or may be accessed through RPI's journal subscriptions at no cost to the student.

1.4 Website

The course website is http://security.cs.rpi.edu/courses/hwre-spring2014/. Announcements, past lecture notes, etc will be posted here.

1.5 Office hours

Professor: TBA

TA: AE 119 immediately after class until 6 PM.

1.6 Learning Outcomes

Upon successful completion of this course, students will:

- Demonstrate a qualitative understanding of CMOS logic and be able to translate a logical function between Boolean algebra, gate-level schematics, transistor-level schematics, and silicon layout. *The focus here is on understanding the functionality of existing devices. We do not cover layout in sufficient depth to actually design semiconductor devices, although this course's material may prove helpful to students who plan to study VLSI.*
- Understand the fundamentals of semiconductor device packaging and recommend sample preparation techniques based on visual inspection of a packaged device and the analysis to be performed.
- Understand basic procedures for printed circuit board reverse engineering including methods for extracting firmware images. *This course is not a software RE class and does not cover techniques for analysis of extracted firmware.*

1.7 Attendance and Classroom Policies

Attendance of lectures is not strictly required, however valuable material may be discussed in class which goes beyond the posted notes. Students are responsible for learning all material discussed in class regardless of whether it is covered by the posted notes or not.

Attendance of quizzes *is* required and no makeups will be allowed unless scheduled in advance or a formal emergency excuse from the Dean of Students is provided. Students must bring their laptop to quizzes.

1.8 Students with Special Needs

Federal law requires all colleges and universities to provide specified types of assistance to students with disabilities. If you have such special assistance, please

obtain an authorizing memo from Disability Services for Students by contacting Mark Smith, Dean of Students, in the Dean of Students Office (x6266). Information about a student's special needs will be treated as confidential.

Please submit a copy of your authorizing memo to the instructor well in advance of any affected exam or assignment. Failure to do so may result in a lack of special accommodations.

Note that this course focuses heavily on visual analysis of imagery including optical and electron micrographs. Students with visual impairment are strongly advised to discuss the specifics of their condition with the instructor prior to signing up for the class.

1.9 Software

Students are expected to have access to, and be familiar with the use of, image editing software such as GIMP or Adobe Photoshop. Exposure to image stitching and registration tools such as Hugin is helpful but not required.

We will be using KiCAD in this class for drawing circuit schematics. No prior CAD/EDA experience is required, we will cover the fundamentals of using it in class.

Basic familiarity with image processing libraries for C/C++, Matlab, or another general purpose programming language may be helpful if you choose to automate analysis. We will keep all datasets for the class small enough that they can feasibly be traced out by hand, so programming experience is by no means required.

We may recommend additional specialized analysis tools during the course of the semester.

2 Grading

Your grade will be based on four components, weighted equally. There is no final exam.

The grading is intended to measure how well you would be able to perform the work taught by the course in industry, not how well you can fill in bubbles on a piece of paper. Assignments will be very "applied" and "hands-on" in nature.

2.1 Submissions

To ensure timely grading, all assignment submissions should be provided as unformatted text or a typed (not scanned) PDF, unless otherwise stated. If you submit any other format, including hard copy, scanned handwriting, or proprietary word-processing software, your grade may be delayed as we attempt to find a way to view the files or decipher your chicken scratch :)

When submitting image files, use PNG (recommended) or JPEG unless otherwise stated. Do not submit XCF, PSD, or any other "native" file format which

is only readable by one editing software.

2.2 Quizzes

About once a week, at the start of a lecture, there will be a short (15 minute) in-class quiz covering the most recently used material. The primary emphasis of the quizzes will be demonstrating your ability to apply knowledge, not memorize facts. For example, you may be given a photo of a simple standard logic cell and asked to produce a transistor-level schematic and describe the logical function it implements.

Quizzes are to be taken individually. You will be permitted to use your laptops for typing up solutions or marking up provided images however you must not use them to collaborate or access online resources.

Rationale: The quizzes cover basic domain knowledge that an analyst should be able to perform at a glance.

2.3 Labs

About once a month, there will be a laboratory demonstration showing off sample preparation, invasive attacks, data capture, etc. Depending on enrollment and available resources, there may or may not be a hands-on component to some or all of the labs. You will be expected to write a short (1-2 page max) report after each lab session describing the procedures performed and the results obtained.

You may discuss labs freely with other students but must write up reports individually.

Rationale: After performing an experiment, it is necessary to explain to the customer what was done and what data was obtained.

2.4 Homework

There will be several homework assignments over the course of the semester. These will be similar in nature to the quizzes but involve larger-scale problems. For example, instead of simply creating a schematic from a single gate, you may be given photos of a larger part of a device and expected to produce a gate-level schematic.

You may work in groups on the homework but must write up solutions individually. You may not receive direct help from any person who is not a student of the class (forums, IRC, etc) without the permission of the instructor, however you may consult any outside websites/textbooks/papers or freely available software that you wish. You must cite your sources/tools appropriately.

Rationale: During a real-world analysis project, confidentiality requirements typically prevent release of any data related to the customer's sample to anyone outside the company. Given this restriction, you are expected to deliver results; the customer doesn't care if you had to read a paper on a new technique or not. We are testing your analytical and research skills, not your memory.

2.5 Project

The final project will run in parallel with the second half of the course. A (simple) commercially available IC will be photographed at each layer and each team will be assigned a portion of the device to reverse engineer. Your goal is to generate a gate-level schematic of the circuit as well as a report describing any challenges you faced, the techniques you used, and a high-level description of what role your module plays in the functioning of the chip as a whole. Depending on enrollment, we may reverse the entire device or only a portion of it.

The policy on use of outside resources is the same as for homework.

2.6 Academic Integrity

From The Rensselaer Handbook of Student Rights and Responsibilities: Intellectual integrity and credibility are the foundation of all academic work. Academic dishonesty is, by definition, considered a flagrant offense to the educational process. It is taken seriously by students, faculty, and Rensselaer and will be addressed in an effective manner.

If found in violation of academic dishonesty policy, students may be subject to two types of penalties: (1) the instructor administers an academic (grade) penalty; and/or (2) the student may be subject to the procedures and penalties of the student judicial system outlined in the handbook.

For details on what collaboration or resources are permissible on specific assignments, please see the relevant subsections above.

3 Draft Schedule

Week	Date	Subject
1	1/21/2014	**Lecture 1:** Motivation, course overview, legal/ethical issues. Review of CMOS logic (schematic level) only. Use of KiCAD EESchema.
1	1/24/2014	**Lecture 2:** Package construction and wire bonding.
2	1/28/2014	**Quiz 1:** Describe the logic function corresponding to each of several transistor-level gates in a schematic. **Lecture 3:** Depackaging techniques, bond removal, live analysis considerations.
2	1/31/2014	**Lab 1:** (MRC EM lab) Group A only: Demo of several types of decap (die recovery, nitric dropper, etc)
3	2/4/2014	**Lab 1:** (MRC EM lab) Group B only: Demo of several types of decap (die recovery, nitric dropper, etc)

3	2/7/2014	**Quiz 2:** Given photos of packaged devices and the analysis requested, describe how to decap them **Lecture 4:** Intro to CMOS layout, Mead-Conway layout notation, standard cells **Homework 1 out:** Given photos of portions of a device (1um 2-metal, use SecurID SID600 and ST 24C02), extract a schematic
4	2/11/2014	**Quiz 3:** Given SEM/optical micrographs or schematic layout of cells, describe what they do **Lecture 5:** Fabrication processes, determining technology level
4	2/14/2014	**Lecture 6:** Delayering and staining techniques. CMP, HF wet etching, Dash etch.
5	2/18/2014	**NO CLASS:** Follow Monday schedule.
5	2/21/2014	**Quiz 4:** Given top-metal photos, estimate the process node and describe how to deprocess to reveal a specific feature (poly, implants, metal 3, etc) **Lecture 7:** Microscopy, image capture, stitching, registration. Use of Hugin.
6	2/25/2014	**Lab 2:** (MRC EM lab) Group A only: Demo of SEM imaging of a couple of samples at varying stages of deprocessing.
6	2/28/2014	**Lab 2:** (MRC EM lab) Group B only: Demo of SEM imaging of a couple of samples at varying stages of deprocessing.
7	3/4/2014	**Homework 1 due** **Lecture 8:** Mask ROM layout
7	3/7/2014	**Lecture 9:** PROM/EPROM/EEPROM/efuse/Flash layout
8	3/11/2014	**NO CLASS:** Spring break
8	3/14/2014	**NO CLASS:** Spring break. Happy Pi Day!
9	3/18/2014	**Lecture 10:** SRAM layout
9	3/21/2014	**Quiz 5:** Given photos of various memory arrays, determine what you're looking at **Lecture 11:** Non-invasive attacks on logic (glitching, DPA, JTAG, UV, firmware dumping, etc)
10	3/25/2014	**Lecture 12:** Non-invasive attacks on crypto
10	3/28/2014	**Lecture 13:** Microprobing, semi-invasive attacks, backside analysis **Lab 3:** (in class during lecture, both groups) Demo of UV light attack on previously decapped PIC12F683
11	4/1/2014	**Lab 4:** (Cleanroom test area) Group A only: Demo of microprobing internal flipflop state on an XC2C32A. May also include rebonding a decapped die.
11	4/4/2014	**Lab 4:** (Cleanroom test area) Group B only: Demo of microprobing internal flipflop state on an XC2C32A. May also include rebonding a decapped die.

12	4/8/2014	**Quiz 6:** Given top-metal photos of various devices, recommend the best way to extract contents of a given memory array **Lecture 14:** Anti-tamper / anti-analysis techniques
12	4/11/2014	**Lecture 15:** PCB RE: Component identification and block-diagram extraction
13	4/15/2014	**Lecture 16:** PCB RE: Netlist extraction
13	4/18/2014	**Quiz 7:** Draw quick block diagram for a provided PCB photo/photo set **Homework 2 out:** Find an off-the-shelf PCB in tech dumps etc. Write a 3-page report describing what you think it does, where the major functional blocks are, etc. **Lecture 17:** I/O pads, buffers, tri-states, ESD protection.
14	4/22/2014	**Guest lecture:** Christopher Tarnovsky, IOActive (date may change)
14	4/25/2014	**Lecture 18:** Programmable logic: product term CPLDs (including XC2C32A bitstream analysis)
15	4/29/2014	**Lecture 19:** Programmable logic: FPGAs
15	5/2/2014	**Lecture 20:** Machine vision, automated RE tools (Degate, ROM dumping, etc) **Homework 2 due**
16	5/6/2014	Final project presentations. No final exam.