# Experiment 6
# Reverse Engineering Attack

We describe an experiment to understand reverse engineering attacks, which are used to understand a hardware IP and potentially clone it, leading to piracy or counterfeiting a product.

**Instructor**: Dr. Swarup Bhunia
**TAs**: Shuo Yang and Reiner Dizon

# Case Study

We describe an experiment to understand reverse engineering attacks, which are used to understand a hardware IP and potentially clone it, leading to piracy or counterfeiting a product.

Reverse engineering, also called back engineering, is the processes of extracting knowledge or design information from anything man-made and reproducing it or reproducing anything based on the extracted information. The process often involves disassembling something (a mechanical device, electronic component, computer program, or biological, chemical, or organic matter) and analyzing its components and workings in detail.

The reasons and goals for obtaining such information vary widely from every day or socially beneficial actions to criminal actions, depending upon the situation. Often no intellectual property rights are breached, such as when a person or business cannot recollect how something was done, or what something does, and needs to reverse engineer it to work it out for themselves. Reverse engineering is also beneficial in crime prevention, where suspected malware is reverse engineered to understand what it does, and how to detect and remove it, and to allow computers and devices to work together ("interoperate") and to allow saved files on obsolete systems to be used in newer systems. By contrast, reverse engineering can also be used to "crack" software and media to remove their copy protection, or to create a (possibly improved) copy or even a knockoff; this is usually the goal of a competitor.

Reverse engineering has its origins in the analysis of hardware for commercial or military advantage. However, the reverse engineering process in itself is not concerned with creating a copy or changing the artifact in some way; it is only an analysis in order to deduce design features from products with little or no additional knowledge about the procedures involved in their original production. In some cases, the goal of the reverse engineering process can simply be a re-documentation of legacy systems. Even when the product reverse engineered is that of a competitor, the goal may not be to copy them, but to perform competitor analysis. Reverse engineering may also be used to create interoperable products; despite some narrowly tailored US and EU legislation, the legality of using specific reverse engineering techniques for this purpose has been hotly contested in courts worldwide for more than two decades.

# Theory Background

Reverse engineering is the processes of extracting design information and reproducing it or reproducing anything based on the extracted information. The process often involves disassembling something (a mechanical device, electronic component, computer program, or biological, chemical, or organic matter) and analyzing its components and workings in detail.

One of the issues in digital content protection is known as the “Analog Hole”. Simply stated it means that if a person can view content then they can copy it. This is true in almost all aspects of life – from making mix tapes by recording radio stations to illegally copying a movie by pointing a camcorder at a television screen. Another important area of life that is subject to this hole is in Intellectual Property Protection. You can have all the IP Protection you want but if your adversary has physical access to the IP then you cannot guarantee that they will not be able to copy it.

Reverse engineering is an invasive and destructive form of analyzing a smart card. The attacker grinds away layer after layer of the smart card and takes pictures with an electron microscope. With this technique, it is possible to reveal the complete hardware and software part of the smart card. The major problem for the attacker is to bring everything into the right order to find out how everything works. The makers of the card try to hide keys and operations by mixing up memory positions, for example, bus scrambling. In some cases, it is even possible to attach a probe to measure voltages while the smart card is still operational. The makers of the card employ sensors to detect and prevent this attack. This attack is not very common because it requires a large investment in effort and special equipment that is generally only available to large chip manufacturers. Furthermore, the payoff from this attack is low since other security techniques are often employed such as shadow accounts.

# Experiment Set-up: Configuration

The instruments needed for this experiment are the HAHA Board.

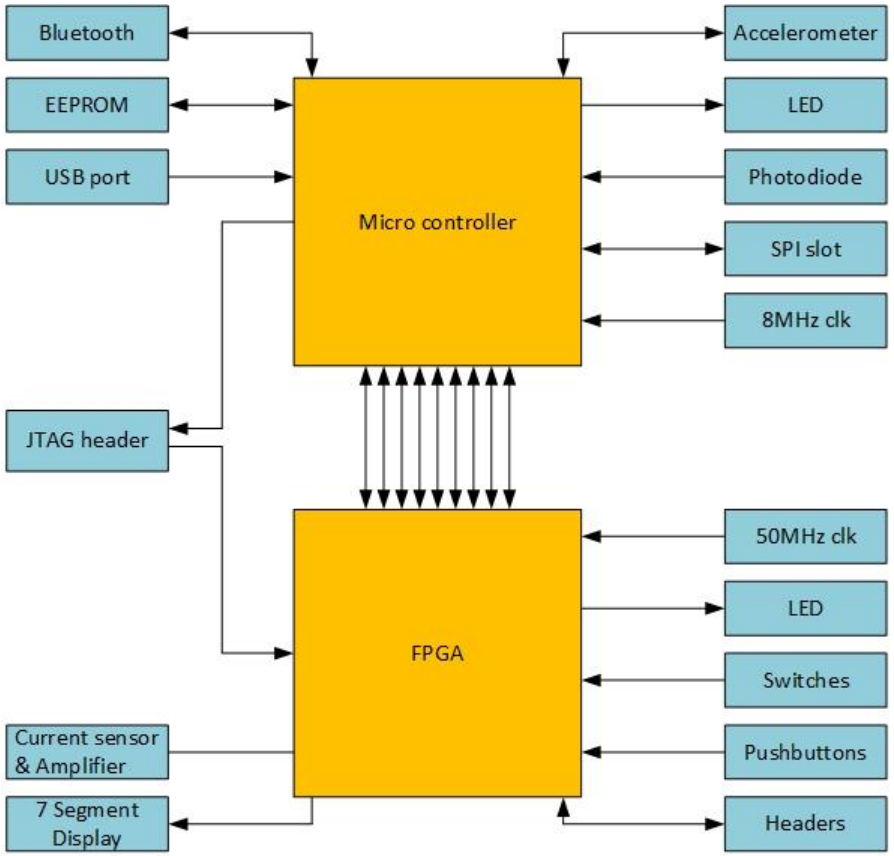


*Figure 1 Experiment set-up: HAHA Board block diagram.*

# Experiment Set-up: Instructions

In order to copy IP, one first needs to understand how it works. One way of doing this is to build up a schematic and a Bill of Materials. Most of this can be done by either visual inspection or by probing points on the board with a Digital Multi-Meter set to Continuity Mode. This will cause a loud beeping sound whenever the probes are making electrical contact together.

For a two-layer PCB (which the HAHA Board Demonstration is) this is typically all that is needed. One step that might be helpful is to look up datasheets for all known components to see how the component needs to be connected with the other components on the board.

Where are the known Power Pins?

Where are the known Ground Pins?

Are there any pins that only have one specific functionality?

Does the Integrated Circuit implement any known functionality (e.g., industry standards) that have to be attached a certain way? (Hint: Remember SPI?).

You will have one week to complete this experiment. Good Luck! This will take a fairly significant amount of effort. If you start the night before it's due, you will not have enough time to complete it.

# Measurement, Calculation, and Question

1) You are required to turn in a Bill of Materials (BOM). It should be structured as Table 1 (Of course the Bill of Materials your group will come up will be much longer). Please note that every element on the PCB will require a line-item in the BOM. Some components show up more than once, others will only show up once. Every component that you see should show up on the BOM. (Hint: Some components that look identical at first glance might be subtly different in some aspect, for example, the color of the component. Color can be important. Gold plating looks different than tin plating and is relevant to electronics.) Note: You will be expected to figure out the values of all components with the exception of the capacitors (and some resistors) on the PCB. There are different valued capacitors used. It is not important to figure out the values. (And is surprisingly difficult.) You do not need to include the values for any resistors, capacitors, or inductors in your Bill of Materials.

*Table 1 Bill of Material for HAHA Board*

| Reference | Manufacturer | Part No. | Description | Quantity |
|---|---|---|---|---|
| **U1** | Altera | 10M50SCE144C8G | 50K LE FPGA | 1 |
| **U2** | Atmel | ATmega16U4-au | 8-bit Micro controller | 1 |
| **D1, D2, D3, D4, D5, D6, D7, D8** | ? | ? | ? | 8 |
| **Y1** | ? | ? | ? | ? |
| **?** | ? | ? | ? | ? |

2) The second thing that you will need to turn in is as complete of a schematic as your group can generate BOTH as pictures/PDF and the schematic file from your CAD tools of choice. See Figure 2 for a partial example of a schematic that could be turned in (Your schematic must be drawn with a CAD program, such as [1-4]). The values for resistors, capacitors, or inductors are NOT needed for the schematic. Please separate out the different parts of the board as separate schematics rather than submitting one huge schematic of all components.

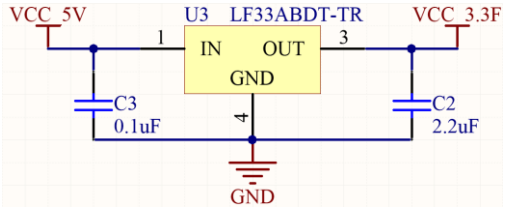


*Figure 2 A schematic example*

# Optional Follow-up

There is **NO** extra credit for this experiment. Physical Modification of the PCB is strictly prohibited! Any group found to have modified their PCB in any way will receive points taken off and possible failure of the course.

# ☞ Lab Report Guidelines

1. In your report, as required, there should be a whole list of all the parts included on the HAHA board. If you cannot find the part number from the mark of some components (e.g., an LED without marking), just leave it blank. However, give a description for any of them describing, for example, what's its function.
2. As required, give a schematic of the board. Do not try to include everything in just one page. You should separate the whole circuit into several sub-circuit so that all parts can be seen clearly. Do not mess up the connections. Draw the schematic with the help of a tool/software. Any circuit/PCB design tool can do the job. Please see references. We do NOT accept hand drawings of the schematics.
3. Answer these questions:
    a. Given the BoM and the schematic you created from just looking at the board, can you recreate this board?
    b. How would you go about recreating this board?
    c. What implications does the recreation of this board or other devices entail in the electronics supply chain?
    d. What else can an attacker do with this kind of information?
    e. How do you prevent an attacker from performing this visual inspection RE attack?
    f. Besides visual inspection, what are other RE attack techniques (not just on PCB), and why are they dangerous?
4. Video Demo is NOT required.

# References and Further Reading

[1] https://easyeda.com/

[2] https://www.kicad.org/download/

[3] https://www.autodesk.com/products/eagle/free-download

[4] https://www.altium.com/altium-trial-flow?light

You don’t need to take chips off the board to see the circuit underneath. Here is something that can help/mislead you. The pictures below are parts of some PCB designs. However, only several are known as parts from the HaHa board. Others are just some random circuits that are from some unknown designs. Please find the right pictures that can help your reverse engineering and ignore the others.