UNLOCKING THE SECRETS WITHIN ROMs
// 3-Days Session //
- Training Program & Terms -

1. OBJECTIVES

The primary goal of our trainings is to provide security professionals and team leaders the skills, mindset and background information necessary to successfully perform the reverse engineering of Integrated Circuits (ICs), circumvent their hardware countermeasures and extract the data from them (Hardware and Firmware).

This intermediate training is focused on ROM memories as they often are the primary target of a security analysis at the transistor level. Rather than focusing on a particular device, the training has been designed so it can be used as a starting point to deal with any types of ROMs.

As ROM content is encoded physically, it is possible to take pictures of the bits and convert them to a proper binary. Of course, chip vendors are using different techniques such as data scrambling to make these optical dumps not practical.

This training aims at giving a complete understanding of how ROMs are constructed at the transistor level and will describe how analyzing the circuitry can be done to extract scrambling information necessary for the reconstruction of a proper binary.

Therefore, it starts with a theoretical sections where ROMs and their building blocs will be explained. This includes the different types of ROMs, the different types of bits encoding, the ROM circuitry (logic, row and column decoders).

With that knowledge in mind, the attendees will then be working on the hands-on section which will consist in the extraction of a ROM from pictures only. The attendees will have the opportunity to work from Scanning Electron Microscope pictures and to follow a step by step approach to extract a binary using python, Fiji (imageJ), photoshop and HDL (Hardware Description Language) tools.

At the end of the session, attendees will be familiar with ROM technologies and will be able to adapt the acquired knowledge to real life scenarios.

Without being fully exhaustive, the training has been built so the attendees discover how to:

- Identify ROMs on pictures of an Integrated Circuit
- Understand the building blocs of a ROM
- Identify the ROM type
- Extract a raw binary from pictures using simple scripts
- Reverse-engineer standard cells and semi-custom cells
- Reverse-engineer control logic, row and column decoders to find out about internal scrambling
- Convert the raw binary to binary candidates using most common scrambling schemes
- Get the binary of ROMs
- Strengthen ROM designs

2. COURSE DESCRIPTION

ROMs inside Integrated Circuits constitute an extremely interesting target as they can contain cryptographic material, boot sections, hidden booting modes such as programing and / or test modes, etc...

Knowing about the code contained in ROMs can be used for a wide variety of targets such as extracting Flash content from non-accessible boot modes or setting up non-, semi- and fully-invasive attacks for a deep security evaluation or extraction in clear of encrypted data.

These different tasks are interesting for people such as Law Enforcement Agencies for digital forensics, security evaluators, chip makers, integrators and hackers.

ROMs have their content physically encoded, meaning that the bits are actually visible. In such a context where a Scanning Electron Microscope can be used to image the content and the memory control circuitry, it is possible to extract at a rather low cost sensitive information.

This hands-on training is designed to give attendees a deep understanding of ROMs and how to dump them. It is based on a theoretical sections which describes the different circuits involved in reading from the memory. This knowledge base is then used on a practical case where pictures are analyzed to extract the content but also to reverse-engineer the control circuitry that can be used to scramble the data.

3. DETAILS

Texplained « Unlocking the Secrets Within ROMs » training is built to give a deep understanding of ROMs and how to dump them.

The different chapters are organized so as to let the attendees discover each new topic in a progressive manner that reflects the Reverse-Engineering specific mindset. This way, attendees will be able to derive their own workflows and methods while working on their own projects after the training session.

Finally, this training is also useful to discuss the current state of Integrated Circuits security and embedded counter-measures which can help chip designers improve their own security or help OEMs and integrators choosing the right device for their application.

A. Topics covered during the course

The theoretical introduction will deal with the following topics:

- Structure of a ROM
- Types of ROM
- Bit encoding
- Data scrambling
- Standard cell Reverse-Engineering
- Semi-custom cell Reverse-Engineering

The hands-on section will take this knowledge and expand it by exploring the following topics:

- Find a ROM on an Integrated Circuit picture
- Extract bits from Scanning Electron Microscope pictures using Fiji and python scripting
- Identify the type of ROM, its control circuit, row and column decoders
- Reverse-engineer the ROM logic
- Use reverse-engineering data from the ROM circuits to build a VHDL model of the complete memory and its content
- Write a VHDL testbench to simulate the ROM behavior
- Dump the ROM from the testbench
- Deal with scrambling

B. Who should attend

- Forensic investigators in law-enforcement agencies (LEAs)
- Government Services
- Pen Testers who want to assess the security of the embedded code, allowing for a complete hardware + Software evaluation
- Digital ICs designers & test engineers
- Engineers involved in securing hardware platforms against attacks
- Researchers willing to understand the nature of extraction methods based on IC RE
- Team leaders involved in IC security and exploration as well as device security
- Hardware hackers who want to become familiar with methods on ICs
- Parties involved in hardware reverse-engineering and Vulnerability analysis

C. Minimum software to install

The participants will be given slides that will cover the theoretical and hands-on sections. The hands-on section will be explained step by step with partial answers for attendees not familiar with the different used languages. Pictures will be provided as photoshop files.

In addition, to follow the training efficiently, the attendees are asked to come with a laptop with the following softwares installed:

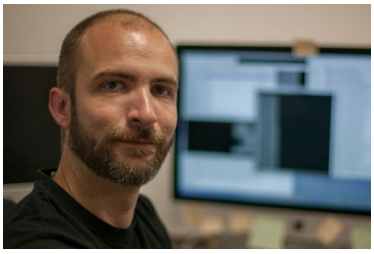
- Fiji or imageJ
- Python dev environment
- Photoshop (evaluation versions are ok)
- ModelSim

All of these tools can be downloaded as open-source tools or as demo / evaluation software.

D. Prerequisites

For this training, micro-electronics prior knowledge is not mandatory. The attendees should nevertheless be familiar with Python scripting and have some knowledge or understanding of HDL language. The training is designed in VHDL as it is closer to the actual design than verilog but people with verilog skills will have no difficulty to adapt to VHDL. To accommodate attendees with no prior experience with HDL (Hardware Description Language), the assignments are provided with scripts and files with blanks to fill.

3. TRAINER



Olivier THOMAS
Reverse Engineering Mentor

Oliver THOMAS studied Electrical Engineering (EE) and subsequently worked for a major semiconductor manufacturer designing analog circuits.

Then, Olivier began to work in the field of Integrated Circuit (IC) security as the head of one of the world's leading IC Analysis Labs.

The lab primarily focused on securing future generation devices as well as developing countermeasures for current generation devices to combat piracy and counterfeiting.

During this time Olivier helped develop many new and novel techniques for semi- and fully-invasive IC analysis.

He has an extensive background in all the Failure Analysis techniques and equipment necessary for accessing vulnerable logic on a target device. Combined with his experience as an IC design engineer, Olivier continues to develop techniques for automating the analysis process. These techniques are not only applicable to lower-complexity devices such as smartcards, which are the traditional targets for IC analysis, but they are applicable to modern semiconductor devices with millions of gates, such as modern System-on-Chips (SoCs). Olivier is the creator of ChipJuice, a software toolchain that efficiently operates the recovery of hardware designs, independently from their technology node, architecture or Standard Cell Library.

He is the founder and CTO at Texplained SARL.

4. INFORMATION & PRICE

- Duration of the training: 3 days
- Location: cf. quotation
- Language: English or French depending on the group speaking language
- Course material language: English
- Price: cf. quotation

Registration is considered complete when quotation has been signed and received by texplained and payment has been transferred, and before the closing date for registration which is indicated on Texplained website (www.texplained.com) and/or on the quotation.
The registration to one of our trainings constitutes acceptance of these conditions in full. Agreement shall be deemed upon written from. Verbal agreements cannot be taken into consideration or validated.

5. POSTPONEMENT - CANCELLATION OF THE TRAINING

Texplained reserves the right to postpone a session no later than 2 weeks before the starting date of the latter.

Cancellation of a session:
- Due to Texplained: Apart from a case of a training postponement, Texplained shall reimburse the sums already received
- Due to the attendee:
  - For an onsite training - at the customer's premises -: Any registration cancellation that has not reached Texplained in writing 1 month before the starting date of the session involves the payment of a compensation corresponding to 30% of the training cost (charge VAT at applicable rate).
  - For a training at Texplained premises: Any registration cancellation that has not reached Texplained in writing 2 weeks before the starting date of the session involves the payment of a compensation corresponding to 40% of the training cost (charge VAT at applicable rate).
  - For an online training: Any registration cancellation that has not reached Texplained in writing 2 weeks before the starting date of the session involves the payment of a compensation corresponding to 30% of the training cost (charge VAT at applicable rate).

One attendee can be replaced on the session he registered for by a person of the same company or organization, at any time and with no extra cost, provided that Texplained has been informed before the start of the training.

Due to the sanitary crisis, the locations and dates of the sessions may have to be modified.
The attendees will be informed in time of all rules to respect to ensure the security of our sessions, and of any change that may occur because of the pandemic.