Integrated Circuit Reverse-Engineering & Data Extraction with Lab Hands-On Session
// 4-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) and their code extraction but also to evaluate the efficiency of the existing counter-measures and understand how to design the most efficient ones.

This training is designed to give to Integrated Circuit professionals a deep understanding of the complete Reverse-Engineering and Attack chain to help them better understand the hardware and the way it is protected, but also to discover how to exploit the intrinsic weaknesses in order to recover fundamental data like Netlists and NVMs' binaries in clear.

In addition, a two-day lab session will be performed. The attendees will then get even more familiar with the sample preparation techniques, the imagery tools and the more invasive aspects of data extraction through demos of Focused Ion Beam (FIB) edits and micro-probing.

Students who complete this course will extend their knowledge of all important classes of low-level hardware attacks (shield and hardware counter-measures bypass – ROM and Flash/EEPROM dump – circuit imagery and modification - bus passive and active probing – ...) through real world examples covering the entire analysis workflow from the lab to the data analysis.

The training will be presented through theoretical and on-paper assignments chapters for two days followed by another two days in our lab.

2. COURSE DESCRIPTION

When it comes to encrypted devices, one may want to gather embedded evidences while another would like to be able to check if a hardware backdoor is present or if the component and / or its embedded firmware (boot ROM / user code) contain intrinsic breaches, that could be exploited by a pirate.

The primary goal of this training is to provideDigital Forensics & other Security Professionals as well as Government Services the skills, mindset and background information necessary to successfully:

- Recover ICs internal architectures
- Extract NVMs contents (ROM & Flash), in order to analyze and evaluate the security of the embedded firmware, and extract secret informations
- Evaluate the efficiency of existing countermeasures

The Students will be shown how such informations can be used to define easier methods to find / exploit firmware + hardware weaknesses for vulnerability analysis as well as for embedded evidence extraction purposes.

Concretely, Students who complete this course will:

- Find out how to perform low-level hardware reverse engineering
- Develop analysis strategies for the target devices and apply these strategies to recover their embedded data
- Get to know the laboratory techniques used for netlist reconstruction and data extraction from secure ICs

3. DETAILS

Physical tampering techniques are composed of three main families from non-invasive (clock and VCC glitches, side channel analysis, etc) and semi-invasive (laser fault injection, photo-emission, etc) to fully-invasive methods requiring the use of equipments such as deprocessing tools, Scanning Electron Microscope, Focused Ion Beam, etc.

The latter class is known to be the most potent. On top of that, it also often brings sufficient knowledge about the target for the creation of easier-to-perform methods (non- and semi-invasive) to exploit weaknesses found in the embedded firmware and the hardware itself.

This training is designed to give to Integrated Circuit professionals as well as newcomers a deep understanding of the complete Reverse-Engineering and Exploitation chain for various purposes such as building more secure designs, choosing the right device for a given application, improving the security risk assessment by taking the embedded firmware into consideration but also to find vulnerabilities in « Secure Elements » so as to conduct forensics analysis.

An introduction to non- and semi-invasive attacks will be given so as to be able to exploit the results of the IC RE and Data Extraction results.

This training will be a mixture of theoretical lectures and practical assignments which will give the attendees all the key knowledge to perform such complete hardware + software analysis to reach their specific needs from in depth security evaluation to forensics data extraction. Two entire days will be spend in Texplained's laboratory to further describe the RE and data extraction process.

Texplained Hands-on sessions are also built to give a complete understanding of Integrated Circuits while analyzing the different means of extracting embedded firmware and data from Secure Devices. 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.

This proposed learning curve aims at letting the attendees complete the training by strategizing low level physical methods involving Reverse Engineering, circuit modification and micro-probing. Explanations regarding other types (non- and semi-invasive) of hardware methods will be given as they are often used in conjunction with the invasive results to derive exploitation methods that do not require the entire set of equipments used to perform the initial process.

Finally, the IC RE & Data Extraction Hands-on training is also useful to discuss the current state of Integrated Circuits and embedded counter-measures security which can help chip designers improving their own security or help OEMs and integrators choosing the right device for their application.

A. Topics covered during the course

- Theoretical and Assignments:
  - Integrated Circuits Structure
  - Transistors, CMOS logic and associated weaknesses
  - Digital logic and Memories
  - Failure Analysis and Reverse-Engineering Methods
  - Embedded Firmware and Secret Data Dump: ROM & Flash Dump
  - Analytical and Invasive ROM Dumps
  - Linear Code Extraction Based Methods
  - Automating the Entire Process
  - How to use the RE and code extraction results
  - Choosing the right types of attacks for a given study
  - Non-, semi- and fully invasive attacks with a focus on the latter
  - RE based attacks

- Lab:
  - Depackaging
  - Top metal and substrate sample preparation
  - SEM imagery
  - X-section and Shallow Angle Polish
  - Deprocessing
  - Wire bonding
  - FIB edits
  - Micro-probing

B. Who should attend

- Digital police investigators
- Forensic investigators in law-enforcement agencies
- 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 who want to understand the nature of many hardware investigation methods
- 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

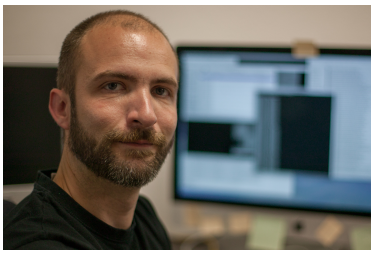
- Students will be provided assignments on paper as well as the training material as a .pdf file.
- No specific softwares are needed for the session

D. Prerequisites

The training does not requires specific prerequisites. The instructor's goal is to convert attendees to operational Integrated Circuit Reverse-Engineers no matter their original skills and expertise.

No particular electronic knowledge is mandatory as the training will start with digital electronic basics. Basic understanding of micro-controllers architecture and assembly language is a plus but will also be covered in the initial theoretical sections.

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: 4 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 or PO received and payment has been operated, 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.