IC REVERSE ENGINEERING & CODE DUMP

https://hardwear.io/germany-2021/training/ic-reverse-engineering-code-dump.php

COURSE DESCRIPTION:

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.

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

Details:

Texplained IC Reverse-Engineering & Code Dump training is 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 & Code Dump training is also useful to discuss the current state of Integrated Circuits and embedded countermeasures security which can help chip designers improve their own

security or help OEMs and integrators choosing the right device for their application.

Topics covered during the course:

- **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 Dump**
- **Linear Code Extraction Based Methods**
- **Automating the Entire Process**
- **How to use the RE and code extraction results**

KEY LEARNING OBJECTIVES:

When it comes to encrypted devices, one may want to gather embedded evidence 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 provide Digital Forensics & Security Professionals as well as Government Services the skills, mindset and background information necessary to successfully:

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

The Students will be shown how such information 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.**

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.**

PREREQUISITES:

The training is derived from Texplained « IC RE & Attacks 101 » which means that there are overall no 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.

Attendees should be familiar with python scripting. If that is not the case, they will still be able to attend and work on the algorithmic parts while the instructor will help on the « language part.

Minimum software to install:

Students will be provided assignments on paper as well as the training material as a .pdf file. For working on the examples and handling the image processing steps, Fiji (ImageJ) and Photoshop will be needed. Executables for Windows and Macs will be given if not already installed on their laptop.

ABOUT THE TRAINER:

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.