raelize

The Art of Fault Injection: Advanced Techniques & Attacks

Training Description

Type	Training Description
Classification	RESTRICTED
Date	November 22, 2023
Version	1.8
Reference	TAOFI-DESCRIPTION-V1.8
Contact	info@raelize.com

Document history

Version	Date
v1.8	December 14, 2023
v1.7	November 22, 2023
v1.6	October 17, 2023
v1.5	September 12, 2023
v1.4	September 6, 2023
v1.3	August 24, 2023
v1.2	August 16, 2023
v1.1	July 11, 2023
v1.0	July 6, 2023

Contents

1 Description

Fault Injection is often the weapon of choice for breaking into devices when exploitable software vulnerabilities are not known or absent. While *Fault Injection* attacks are nowadays common, typical concepts, methodologies, techniques, and attacks are often not sufficiently understood. While achieving success by simply glitching a target can yield results, it's important to note that this approach alone doesn't facilitate the creation of innovative attacks. In this training, students will experience and appreciate the *Art of Fault Injection (TAoFI)* to exploit the full potential of *Fault Injection* attacks.

This training assumes, though it is not strictly mandatory, that students possess prior experience with *Fault Injection* attacks, either obtained at work, at home, or at a previously attended training (e.g., from Colin, Joe, or Thomas). Students are encouraged to work together in teams of two, sharing their experiences, to tackle the challenges together more efficiently. Even though not recommended, students may work individually as well.

Students will be using advanced techniques to characterize the effects of voltage glitches on the Espressif ESP32 System-on-Chip (SoC). The faults resulting from these voltage glitches are carefully analyzed and described to build a thorough understanding of the target's susceptibility to voltage glitches. This enables the students to create powerful *Fault Injection* exploits. During this training, rather than focusing on a specific set of tools, the students will focus more on the concepts, methodologies, techniques, and attacks relevant to *Fault Injection* attacks.

Students will experience, with guidance from experts, performing real-world *Fault Injection* attacks, that were either disclosed by Raelize or other security researchers. Students will be using the NewAE ChipWhisperer-Husky, typical hardware lab tooling like an oscilloscope and a hardware debugger. Students are provided with a virtual machine (VM) with all the required tooling installed, as well as access to the required hardware.

Upon completing the training, students will be proficient in executing sophisticated *Fault Injection* attacks on real-world targets using commercially available tooling. The knowledge gained from understanding the underlying concepts, methodologies, techniques, and attacks, can be used by the students to perform novel *Fault Injection* attacks on other targets of interest.

2 Format

This training takes students on a multi-day journey during which they perform hands-on exercises (75%) and attend interesting lectures (25%). The students will share their past and current experiences to learn from each other (including the trainers).

Students will get access to a Virtual Machine (VM) that contains all the required software. Students will have access to all the required tooling throughout the training.

Students can continue with the exercises after the training has finished, if they possess the required tooling, which is commercially available from online retailers.

3 Level

The training level of this training is **Intermediate / Advanced**.

The fundamentals of *Fault Injection* are addressed systematically, but students are assumed to have some experience with *Fault Injection* attacks.

4 Agenda

The following list of topics are covered by practical exercises (75%) which are supported by (25%) presentations. Most of the exercises are performed on a custom development board based on the Espressif ESP32 System-on-Chip (SoC), on which **Raelize** performed multiple *Fault Injection* attacks.

This training starts by building up a solid understanding of the typical concepts and methodologies *Fault Injection*. Then, students dive straight into the advanced techniques and attacks, which are used to create powerful *Fault Injection* exploits. Throughout the training, there will be ample opportunity to discuss any relevant topic related to *Fault Injection* attacks and techniques.

Fundamentals

- Fundamentals of Fault Injection
- Building Fault Injection setups
- Raelize Fault Injection Reference Model (FIRM)
- Get familiar with the target (Espressif ESP32)
  - Creating a custom bootloader
  - Understanding its security features
- Get familiar with the tooling
  - NewAE ChipWhisperer-Husky
  - PicoScope 2000 Series Oscilloscope
  - Espressif ESP-Prog
  - Raspberry Pi Pico
  - Riden RK6006 Bench Power Supply

Advanced Techniques

- Target characterization; with and without custom code
- Analyzing faults to identify target behavior
- Plotting results to identify target behavior
- Modeling faults to build attack primitives
- Advanced trigger techniques for timing
- Vulnerability identification by reverse engineering
- Vulnerability verification with hardware debugger
- Effective glitch parameter selection strategies

Advanced Attacks

- Bypassing Secure Boot on ESP32 (CVE-2019-15894)
- Controlling the Program Counter on ESP32
- Glitching the OTP Transfer on ESP32 (CVE-2019-17391)
- Bypassing Encrypted Secure Boot on ESP32 (CVE-2020-13629)

Raelize used Riscure's *ElectroMagnetic Fault Injection (EMFI)* tooling to perform the research. The students will perform these attacks using the NewAE ChipWhipserer-Husky.

5 Key Learning Objectives

The key learning objectives of this training are:

- Understand *Fault Injection* techniques and attacks like an expert
- Identify non-trivial vulnerabilities using advanced *Fault Injection* techniques
- Create advanced *Fault Injection* exploits using commercially available tooling
- Reproduce top-notch security research originally performed by *Fault Injection* experts

6 Audience

This training is intended for:

- Security Analysts, Researchers & Enthusiasts
- Forensic Investigators
- Anyone else interested in advanced *Fault Injection* techniques and attacks

7 What students need to know

The students of this training are expected to:

- have experience performing basic *Fault Injection* attacks
- be familiar with communicating with embedded devices
- be familiar with typical hardware lab tooling
- be familiar with programming Python and C
- be familiar with reverse engineering software
- be familiar with common cryptography (RSA, AES, and SHA)

8 What students need to bring

The students of this training are expected to bring a modern x86-64 based laptop or workstation:

- where they are allowed to install software
- with sufficient memory (at least 8 GB)
- with at least four (4) available USB-A ports (i.e., use a USB hub)
  - **Raelize** will have extra USB hubs available during the training (USB-C / USB-A)
- installed with a modern browser (i.e., Google Chrome)
- installed with VMware Player/Workstation (or VirtualBox)

The *Fault Injection* tooling will be attached to the VM that **Raelize** provides. Please, make sure that forwarding different types of USB devices to the VM works as expected. In our experience, this works best using VMware products (e.g., VMware Workstation Player). Students with a Linux host may also decide to run the training environment without using a VM.

Important: the required tooling is only tested on x86-64-based systems. ARM-based systems (e.g., Apple M1, M2 or M3), or systems based on other architectures, are not supported