Joe Grand's Cryptocurrency Wallet Exploitation Training Course Agenda

Last updated: September 10, 2026

This two-day course focuses on advanced hardware hacking tools and techniques used to exploit common cryptocurrency hardware wallets and their associated STM32-based microcontrollers. It is a hands-on environment where students will learn how to recover the PIN and seed phrase/wallet backup from Trezor One, Trezor Model T, and KeepKey devices using electromagnetic (EMFI) and voltage (VFI) fault injection. Students will be able to apply the same or similar approach to future targets outside of the classroom.

Prerequisites: Joe Grand's Hardware Hacking Basics, Firmware Extraction and Manipulation, and Defeating Microcontroller Code Protection or with prior approval from instructor

A. Introduction

- Trezor and KeepKey cryptocurrency hardware wallets
- Fault injection and side channel analysis (SCA)
- Attack hardware and required features

B. STM32 Exploration

- STM32 security model and attack history
- Hands-on exercise: Read/write Flash memory of STMicroelectronics development tool
- Hands-on exercise: EMFI attack against development tool to cause intentional corruption
- Hands-on exercise: STM32 bootloader extraction and analysis

C. Trezor One (STM32F205)

- Attack Process (EMFI)
  - Device characterization and fault injection parameters
  - Demonstration of Trezor One memory extraction attack using EMFI

- Attack Process (VFI)
  - STM32 Flash Patch and Breakpoint Unit (FPB)
  - Device characterization and fault injection parameters
  - Hands-on exercise: Trezor One memory extraction attack using VFI

D. Trezor Model T (STM32F427)

- Attack Process (VFI)
  - Additional security features of the STM32F4 series
  - Device characterization and fault injection parameters
  - Hands-on exercise: Trezor Model T memory extraction attack using VFI

E. PIN Cracking

- Trezor and KeepKey data encryption schemes, firmware version differences
- Hands-on exercise: PIN cracking and seed phrase decryption using data retrieved from Trezor(s)

F. Open Lab

- Reinforce attacks by repetition
- Experiment with other Trezor devices or STM32F2/F4 microcontrollers
- Apply attack process to any personal/case-specific targets