Cyonix
Bühlstr. 1
73432 Aalen
info@cyonix.io

Projektangebot: STM32F2 FPGA-timed Voltage-Glitch Flash Dumper

Gesucht wird ein Elektroingenieur (m/w/d) mit guten Programmierkenntnissen (C, HDL) und ausreichend Know-How, um folgendes Projekt umzusetzen:

Ziel ist es, ein Hardware-Setup[1] aufzubauen, um zeitkritische Voltage-Glitches bei einem STM32F205-Chip auszuführen. Der erste Voltage-Glitch muss beim Bootprozess nach exakt 170µs ausgelöst werden, um das Read Protection Option Byte zu glitchen. Wenn die Pins *Boot0* auf high/1 und *Boot1* auf low/0 gesetzt sind und das RDP Byte nicht Level 2 beträgt, wird das Serial Command Interface vom BootROM Bootloader freigegeben. Nun können Read Memory Commands[2] gesendet werden, gefolgt von einem Voltage-Glitch, um erneut den RDP Level Check vom Command Handler zu umgehen. Bei einem Fehlschlag muss das System neu gebootet werden bis der ganze Speicher ausgelesen ist.

Nach erfolgreichem Proof of Concept Versuchsaufbau kann überlegt werden, für ein darauf aufbauendes Projekt eine preisgünstige All-in-One Platine zu entwickeln.

Angebote mit folgenden Informationen bitte an info@cyonix.io

- Erfahrungsprojekte in diesem Bereich

- Preisvorstellung zzgl. Hardwarekosten, falls Equipment nicht vorhanden

- Geplante Projektdauer bis zum Proof of Concept

- Instant-Messenger Kontakt Ihrer Wahl zur Terminplanung für ein Erstgespräch

[1] https://blog.kraken.com/post/3662/kraken-identifies-critical-flaw-in-trezor-hardware-wallets/

[2] https://www.st.com/resource/en/application_note/cd00264342-usart-protocol-used-in-the-stm32-bootloader-stmicroelectronics.pdf