USENIX WOOT'25 Artifact Appendix: Security through Transparency: Tales from the RP2350 Hacking Challenge

Marius Muench
University of Birmingham

Aedan Cullen
(Independent)

Kévin Courdesses
(Independent)

Thomas 'stacksmashing' Roth
Hextree

Andrew Zonenberg
(IOActive)

A Artifact Appendix

A.1 Abstract

This artifact contains five proof-of-concept attacks against the secure bootloader of an RP2350 MCU. The attacks aim to read-out a secret stored in the one-time programmable (OTP) memory of the RP2350, after the chip has been locked down following the instructions provided with the RP2350 Hacking Challenge [1].

A.2 Description & Requirements

The paper describes five attacks in Section 4, which are all implemented independently of each other:

- **(A-1)** Attack on the OTP power-on state machine.
- **(A-2)** Forced Vector Boot.
- **(A-3)** Signature Check Bypass fia Laser Fault Injection.
- **(A-4)** OTP read command double-instruction fault.
- **(A-5)** FIB/PVC based antifuse data extraction.

A.2.1 Security, privacy, and ethical concerns

This artifact does not pose any security, privacy, or ethical concerns. All attacks were disclosed to the affected vendor and publicized before submission of this artifact and the corresponding paper [2].

A.2.2 How to access

The artifact is publicly available at: https://github.com/bhamsec/woot25-rp2350-challenge, and the artifact evaluation was carried out on v1.0[1].

Each individual attack is linked as a git submodule. To fetch all attacks at once, execute:

```
git clone --recursive \
https://github.com/bhamsec/woot25-rp2350-challenge
```

A.2.3 Hardware dependencies

Each attack requires a different hardware setup as listed below. Furthermore, (A-1) and (A-3) require additional physical modifications to the RP2350 MCU.

- **(A-1)** Custom prepared RP2350 chip and voltage fault injection setup.
- **(A-2)** RP2350 chip and voltage fault injection setup. Additional, for glitch simulation, a debugging probe.
- **(A-3)** Custom prepared RP2350 chip and laser fault injection setup.
- **(A-4)** RP2350 chip and electromagnetic fault injection setup.
- **(A-5)** RP2350 chip and focused ion beam / passive voltage contrast imaging setup.

Please note that the required modifications to the RP2350 are irreversible and, potentially, destructive.

A.2.4 Software dependencies

Please refer to the specific submodules in the artifact repository for their respective instructions.

A.2.5 Benchmarks

None.

A.3 Set-up

A.3.1 Installation & Basic Test

Please refer to the specific submodules in the artifact repository for their respective dependencies, where applicable.

[1] https://github.com/bhamsec/woot25-rp2350-challenge/tree/v1.0

A.4 Version

Based on the LaTeX template for Artifact Evaluation V20231005. Submission, reviewing and badging methodology followed for the evaluation of this artifact can be found at https://secartifacts.github.io/usenixsec2025/.

References

[1] Raspberry Pi. RP2350 Hacking Challenge. github.com, 2024.

[2] Upton, Eben. Security through transparency: RP2350 Hacking Challenge results are in. Raspberry Pi Blog, 2025.