SIGPwny @ UIUC

University of Illinois Urbana-Champaign

Minh Duong, Jake Mayer, Nikhil Date, Krishnan Shankar, et al.
Advised by Prof. Kirill Levchenko

eCTF10
10 YEARS OF THE EMBEDDED CAPTURE THE FLAG

January 15 – April 25, 2025

Design Overview

Goal: Design a secure Satellite TV System!

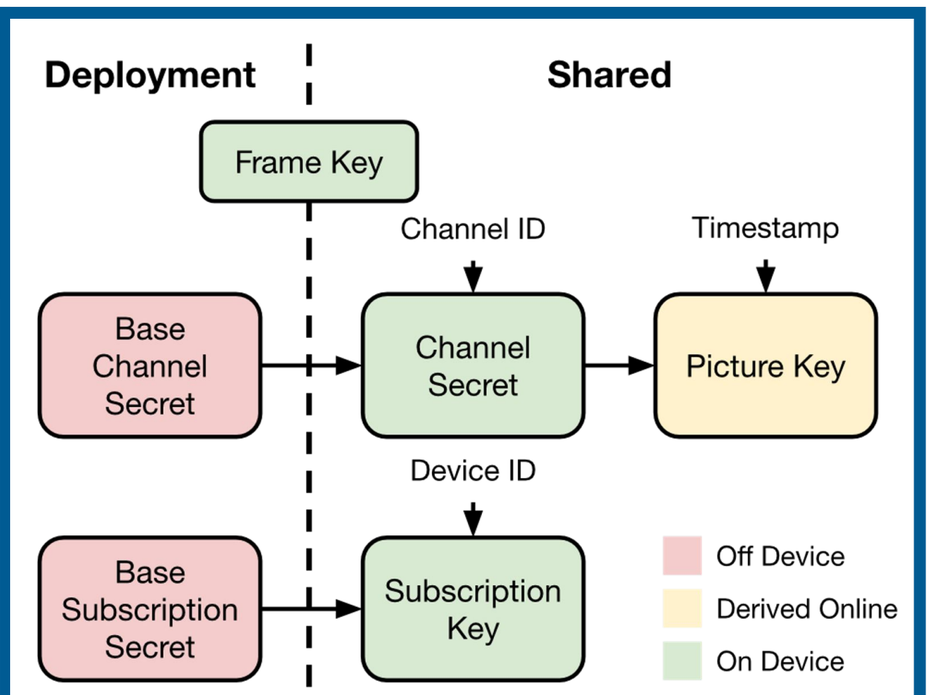
SR1: An attacker cannot decode TV frames without a Decoder that has a valid, active subscription.

SR2: Decoders should only decode valid TV frames generated by Satellites from the same deployment.

SR3: Decoders should only decode frames with strictly monotonically increasing timestamps.

- **Authenticated encryption** with Ascon-128 cipher protects confidentiality of frame
- Unique keys for every frame provide **defense-in-depth** against cryptographic leakage
- **Decoder-specific keys** prevent subscriptions from being loaded onto an unauthorized Decoder
- All secrets are derived **uniquely** per deployment

- **Global previous timestamp state** maintains in-order decoding of TV frames
- **Repeated checks** verify a timestamp matches the subscription range



Defensive Highlight

Mitigating Hardware Attacks

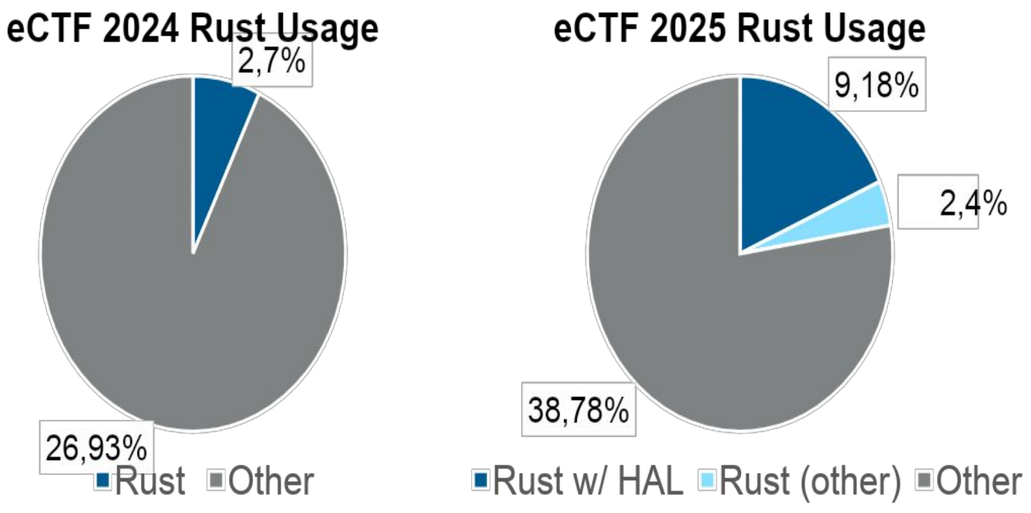
- Masked Ascon-128 implementation protects against power side-channel analysis
- Random delays on I/O bound operations make it difficult for attackers to find useful triggers for timing glitches
- Redundant checks for security-critical conditions
- Zeroize memory after sensitive secrets are no longer used
- Memory safe code with our Rust Hardware Abstraction Layer for the MAX78000 microcontroller

Future Improvements

- Use a GGM tree construction to restrict what timestamps can be decoded, even in complete Decoder compromise
- Digitally sign TV frames so that attackers cannot forge frames if Decoder secrets are leaked

Bringing Memory Safety to Everyone

We open-sourced our Rust HAL for the MAX78000 [1] at the start of eCTF 2025 to make it easier for teams to use Rust!

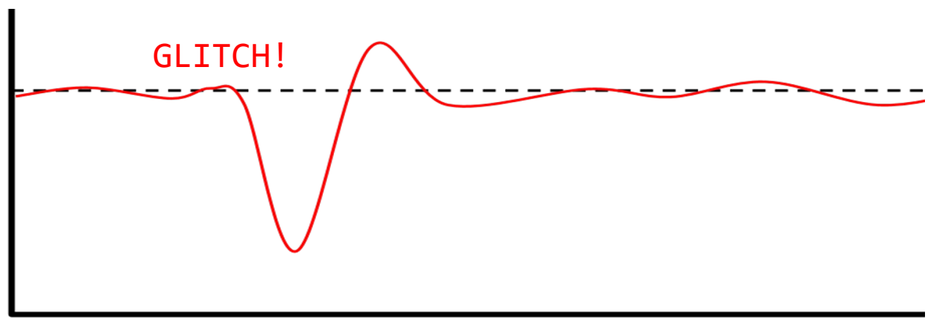


Offensive Highlight

Voltage Fault Injection w/ ChipWhisperer

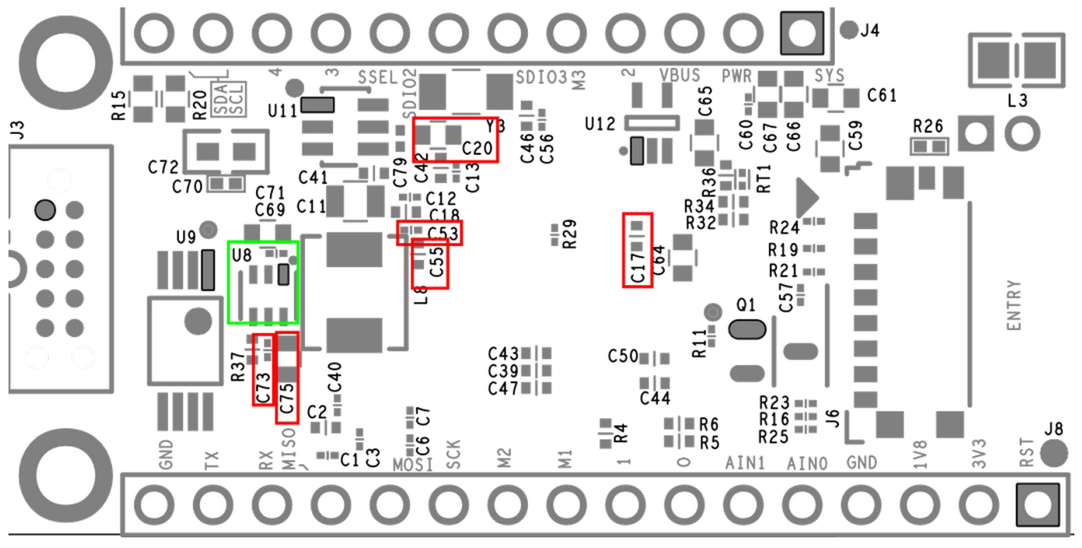
The ChipWhisperer is a fault injection platform that can induce "glitches" by precisely performing brief, controlled drops in the voltage powering the microcontroller core.

- Voltage faults can corrupt data values, modify branch behavior, or effectively bypass instructions.
- We use this behavior to skip security checks in teams' designs.



VCOREA voltage drops below nominal for a short period

- To increase the precision and effectiveness of glitches, most bypass capacitors on the VCOREA line are removed (marked red). Additionally, the buck converter may be removed (marked green) as MAX78000's internal regulator is sufficient for eCTF.



- Mitigations: Look at our defense highlight! Use random delays, redundant checks, and structure code to "fail closed."

References

1. https://github.com/sigpwny/max7800x-hal
2. https://github.com/sigpwny/2025-ectf-uiuc
3. Analog Devices MAX78000FTHR PCB