

EMBEDDED HACKING

Reverse Engineering the Raspberry Pi Pico 2

Operation Iron Net: Classified Intelligence Briefing

ARM Cortex-M33 • GDB • Ghidra

October 11, 2026

For educational and defensive security research only

```

+-----+
|                TOP SECRET // NOFORN                |
+-----+
| OPERATION IRON NET                                   |
| CLASSIFIED BRIEFING: LIVE CHALLENGE 0x03            |
| NATIONAL SECURITY AGENCY / GMU RHET                 |
+-----+

```

1. The Advice

INT. NSA EXPLOITATION CELL. 04:10.

A grey field junction box sits on the bench, its lid peeled back. Inside, secured in potting compound, is a covert environmental sensor node recovered from a contested waterway.

On the top of the enclosure, a status diode glows a steady red. Beside it, a REYAX RYLR998 LoRa transceiver is wired to `UART1` on `GP8` and `GP9`. A three-wire ribbon terminates in a DHT11 temperature and humidity canister. A thin jumper loops from `GP15` up to the `3V3` rail.

The Director sets down a field report and looks at the red diode.

DIRECTOR: What is it?

ANALYST: A remote environmental trigger. The adversary seeds these along a river corridor. The DHT11 samples the air. When the conditions hit a preset window, the node arms a payload channel and broadcasts a strike authorization over LoRa.

DIRECTOR: Is it live?

ANALYST: Armed and listening. The payload relay on `GP18` is wired. One authenticated strike frame and the cell downstream fires.

DIRECTOR: Run it through Buddy.

ANALYST: Already did. Four minutes with the stripped flash image.

She turns her monitor toward him.

```

+-----+
| BUDDY // CLASSIFIED EXPLOITATION ASSIST // CONF: 0.98 |
+-----+
| ACTION      : Replay the environmental checksum window. |
| MECHANISM   : DHT11 humidity byte XOR 0xAF, masked by 0x3C. |
| PREDICTION  : Force (humidity ^ 0xAF) & 0x3C == 0x18, node arm. |
| CONFIDENCE  : 0.98 |
+-----+

```

DIRECTOR: 0.98. Forge the reading, arm the node, learn its payload.

ANALYST: Buddy found the bitwise window. Buddy did not find the door behind it. There is an authorization token, and there is a trap.

DIRECTOR: Buddy says 0.98.

ANALYST: Buddy disassembled `evaluate_environment`. Buddy never followed the SRAM the state machine lives in. Buddy never read the fault counter.

2. What Buddy Is

Buddy is not a person. It is a model. It has parsed more disassembled machine code than any engineer on earth, and it speaks with total, unhesitating certainty.

That certainty is lethal when the target is a live payload channel.

Buddy scanned the flash image and found a tidy bitwise test. It concluded that satisfying the arithmetic is the whole game. It published the mask and the window and declared the node owned.

What Buddy failed to model is that adversary tripwires are engineered for exactly this attack. A real node does not trade a payload on a single sensor byte. It runs a state machine, validates an encrypted token carried over the air, and counts its own faults so that a spoofer who fumbles the protocol three times burns the node instead of arming it.

There is also a physical seal. Cut the sense loop and the node latches shut. The correct env window is necessary. It is nowhere near sufficient.

Buddy saw the bitwise test. Buddy did not verify the ground truth.

3. The Operation

At 01:55, a Riverine Technical Intelligence team recovered an intact node before adversary recovery could zeroize it. The enclosure is a single-board design built around a bare-metal RP2350 (ARM Cortex-M33).

There are no debug symbols. There is no operating system. There is no SVD file to label the registers. All you have is `0x001aa_cb.bin` mapped into Flash at `0x10000000`, and the physical breadboard hardware in front of you.

- **Pin 11 (GP8):** LoRa UART1 TX (to RYLR998 RXD).
- **Pin 12 (GP9):** LoRa UART1 RX (from RYLR998 TXD).
- **Pin 19 (GP14):** DHT11 single-wire data line.
- **Pin 20 (GP15):** Anti-tamper sense loop (jumpered to 3V3).
- **Pin 21 (GP16):** Red LED (`NODE ARMED // LISTENING`).
- **Pin 22 (GP17):** Green LED (`STRIKE AUTHORIZED`).
- **Pin 24 (GP18):** Payload trigger relay.
- **Pin 36 (3V3):** RYLR998 VDD rail and GP15 pull-up source.
- **Pin 38 (GND):** Ground reference.

Inside this image there is an environment gate, an over-the-air authorization token, a fault counter, and a tamper latch. Whatever mechanism actually authorizes a strike is buried in the stripped ARM Thumb-2 machine code.

4. The Mandate

The Director crosses his arms.

DIRECTOR: Prove Buddy right, or prove it wrong.

ANALYST: I need thirty minutes with GDB and Ghidra.

DIRECTOR: You have twenty. Trace the environment routine. Map the state machine. Do not forge a reading over LoRa until you know with certainty what that firmware will do with the next frame, and what it will do to you if the frame is wrong.

The orders are clear:

1. **Recover the Environment Gate:** Locate the bitwise validation routine and work out which DHT11 humidity value satisfies it.
2. **Recover the Authorization Token:** Find the custom cipher that is applied at boot and decrypt the plaintext strike token it protects.
3. **Respect the Traps:** Determine what the node does after repeated faults, and what happens if the GP15 sense loop is broken.
4. **Neutralize the Node:** Execute a verified exploit, either by recovering the token and satisfying the gate, by mutating the state machine in SRAM with GDB, or by patching the binary in Flash.
5. **Verify the Hardware:** Transition the live breadboard from the Red LED on GP16 to the solid Green LED on GP17 on physical silicon.

A machine's 0.98 guess does not authorize a strike.

5. The Challenge

You have the image. You have the board. You have the tools and the time Buddy did not need.

Buddy has given you its answer, and it is confident.

Is it that simple?

Go find out.