Code Review Report

Secure Authentication Module
Experimental Leakage Analysis (Training Exercise)

Project Name:	IRIS
System Type:	Field-Deployed Secure Access Terminal
Testing Platform:	ChipWhisperer-Nano
Assessment Period:	November–December 2025
Version:	1.0

Systems Security Group
Lead Engineer: [REDACTED]

December 2025

Contents

1 System Context

Project IRIS is a field-deployed secure access terminal intended to protect time-sensitive payloads stored in publicly accessible locations. Authorized users authenticate using a fixed-length access code entered through a keypad interface.

The terminal is designed to tolerate temporary physical access by untrusted parties without immediately exposing stored authentication credentials.

1.1 Design Constraints

- Public physical accessibility
- Short interaction time during authentication
- Fixed-length credential input (20 bytes)

2 Threat Model

The assumed adversary has temporary physical access to the terminal and basic electronic measurement capabilities. The following classes of attacks are considered in scope:

- Timing analysis of authentication behavior
- Correlation Power Analysis (CPA)

Invasive physical attacks and full device decapsulation are considered out of scope.

3 Authentication Logic Overview

The authentication routine compares a 20-byte user-supplied input against a stored reference value held in non-volatile memory.

3.1 Verification Structure

- All 20 byte positions are processed unconditionally
- No early exit behavior on mismatch
- A single aggregate mismatch variable is updated using bitwise logic
- The final access decision is evaluated only after full traversal

This structure ensures that instruction flow and execution length remain independent of where incorrect bytes occur in the input.

4 Constant-Time Behavior

Because the comparison loop does not branch on secret-dependent values and always executes the same number of iterations, the routine exhibits constant-time behavior with respect to credential correctness.

As a result, timing-based extraction of credential position, prefix length, or partial correctness is not feasible under standard measurement conditions.

5 Testing Infrastructure

5.1 Hardware

All measurements were collected using:

- ChipWhisperer-Nano capture platform
- STM32F030 target microcontroller
- On-board current shunt for power observation

5.2 Firmware Build Procedure

The firmware was compiled using the standard ChipWhisperer-Nano build environment with **cryptographic acceleration explicitly disabled**.

The build followed the conventional **CWNANO** workflow using the GNU toolchain and standard runtime libraries keeping the **optimization at level one**. This compilation procedure was used explicitly to ensure direct compatibility with ChipWhisperer-Nano capture and triggering infrastructure while still reflecting realistic embedded build practices.

6 Trace Acquisition Methodology

6.1 Input Pattern Selection

Test inputs were constructed using repeated single-byte values across all 20 positions (e.g., `0x0D` repeated 20 times, `0x4B` repeated 20 times).

This pattern-based approach was selected as a standard testing procedure to confirm the absence of early breakout on the wrong input byte and to ensure the constant time nature of the code.

6.2 Capture Parameters

- Total traces captured: 100
- Samples per trace: 700
- Trigger source: GPIO synchronized to authentication routine entry
- Input coverage: Uniform sampling across a common ASCII-range subset

7 Attack Models Evaluated

The following side-channel attack classes were evaluated:

- Timing analysis
- Correlation Power Analysis (CPA)

No higher-order statistical models or multi-channel acquisition techniques were applied.

8 Results

8.1 Timing Behavior

Response latency remained stable across all tested inputs. No timing skew correlated with partial or full credential correctness.

This is consistent with the constant-time structure of the verification loop.

8.2 Correlation Power Analysis (CPA)

CPA was evaluated for all 256 byte hypotheses using standard correlation techniques and the repeated-input trace set.

Result: No statistically significant correlation peaks were observed. Under the tested conditions, first-order CPA does not recover credential material.

9 Trace Count Rationale

The dataset was limited to 100 traces because the device enforces a lockout after 150 measurement attempts, which constrained how many acquisitions could be collected in a single session. With only this window available, any strong first-order implementation leakage would typically still reveal itself as visible structure under CPA. Nothing of that sort appeared.

This does not rule out higher-order leakage; however, under the enforced lockout constraint and in the absence of any first-order correlation, practical exploitation within the available trace budget is unlikely.

10 Scope Limitations

This evaluation is limited to:

- First-order correlation power analysis
- Single-channel power measurements

Electromagnetic analysis, multi-channel correlation, and advanced statistical models were not evaluated as part of this exercise.

11 Conclusion

The Project IRIS authentication routine demonstrates constant-time execution behavior and no observable first-order power leakage under CPA using ChipWhisperer-Nano in the described configuration.

Within the scope of this evaluation:

- Timing analysis does not reveal credential structure
- First-order CPA does not recover credential information

This document serves as the technical narrative frame for a controlled training challenge and represents an intentionally scoped experimental assessment rather than a formal certification result.

Appendix: Technical Artifacts

- Power trace dataset archived in NumPy format
- Compiled firmware binaries retained for reproducibility