ACELab®

Mobile Devices with a Dedicated Cryptographic Processor

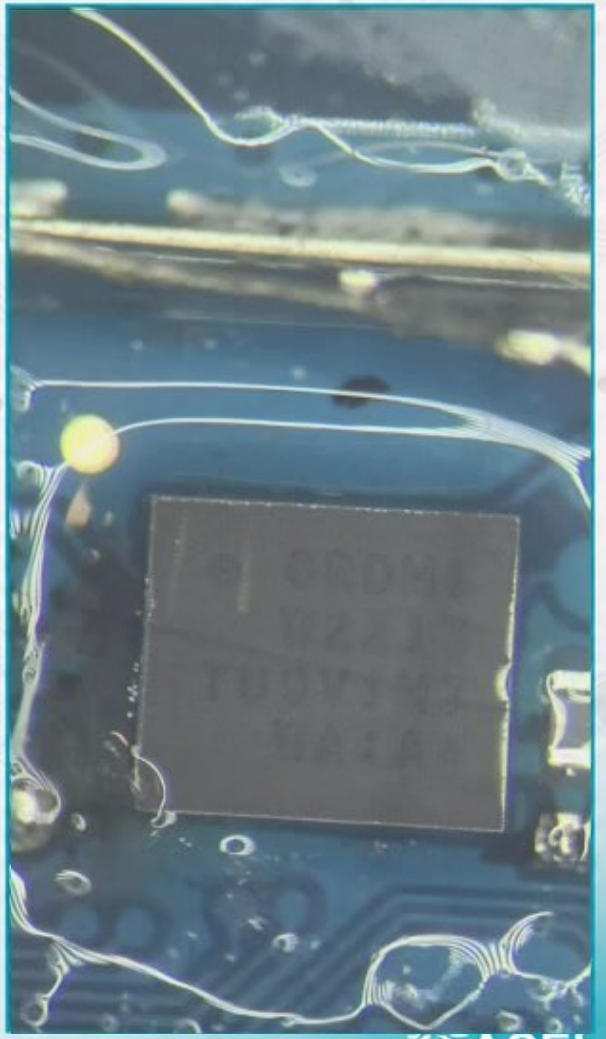
2026

Introduction

We examine two platforms where CryptoMCU is a separate chip that communicates with the main CPU over an external bus.

- **MTK and Unisoc** — We will look at Samsung implementations for these devices
- **Kirin / Exynos** — An even more complex challenge

> **Goal: understand when password processing can be moved off the phone, and when CryptoMCU makes this fundamentally impossible.**



Devices and Interfaces

Samsung Galaxy TAB A8 SM-X205

CPU
Unisoc Tiger T618

CryptoMCU
S3FV9RRYDW-UK3A

Interface: SPI

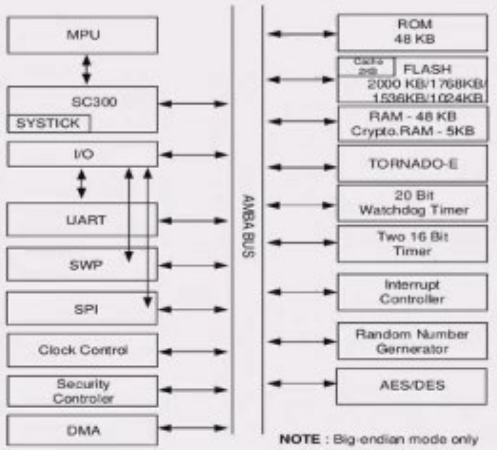
Samsung Galaxy A06 SM-A065

CPU
MTK Helio G85

CryptoMCU
S3K250AFDY-MF35

Interface: I²C

S3FV9RRYDW-UK3A (S3FV9RR)

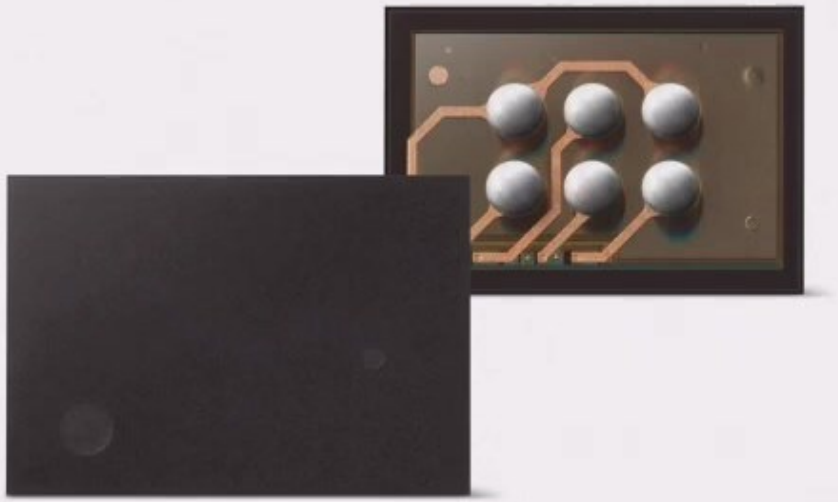


S3FV9RR eSE

S3FV9RR Public Specifications

Category	eSE
Applications	Mobile, Lifestyle
Core	SC300 · 70 MHz
Flash / RAM	2000 KB / 53K
Crypto	DES · 3DES · AES · RSA · ECC · Tornado-E
Interfaces	SPI slave · SWP · GPIO

S3K250AFDY-MF35 (S3K250AF)



Samsung Secure Element S3K250AF

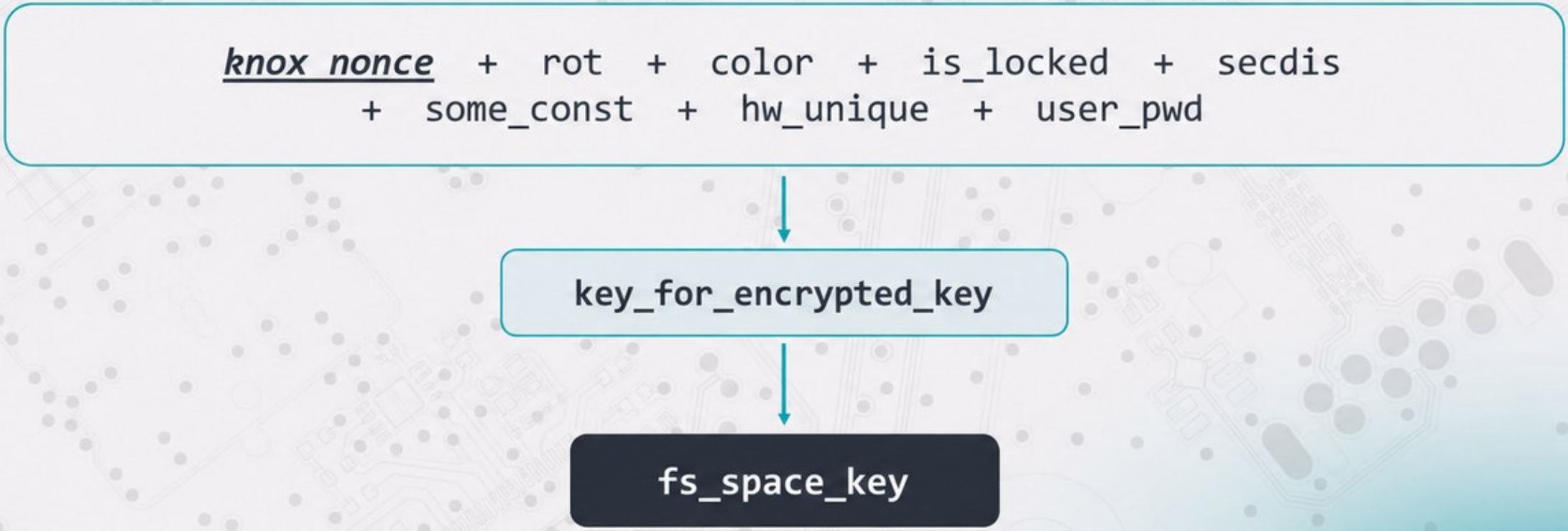
S3K250AF Public Specifications

Type	Secure IC
Applications	Mobile, Lifestyle
Core	SC000
Memory	Flash 252K · ROM 17K · RAM 11K
Crypto	DES · 3DES · AES · RSA · ECC · TORNADO-T
Interfaces	**ISO 7816 · I²C**

ACELab® 2026

Galaxy TAB A8: Key Derivation

A blob (knox_nonce) must be obtained from CryptoMCU. Once it is available, password verification can be moved off the device.



Galaxy TAB A8: Accessing CryptoMCU



SPI-monitoring does not reveal knox_nonce: the challenge and encrypted exchange prevent it.

Why Passive SPI Monitoring Is Not Enough

Even a physical connection to the bus does not provide knox_nonce.



You must participate in the transaction as a legitimate party, or control it through the device CPU, rather than merely observe it.

Obtaining knox_nonce: Passive Approaches

1. Monitor SPI

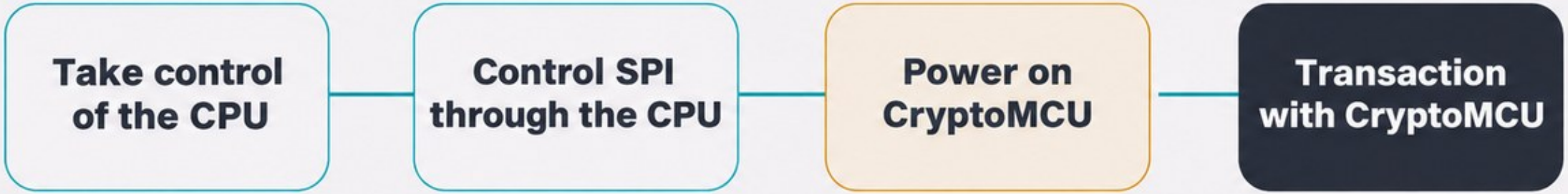
Not feasible: the challenge and encrypted exchange prevent extraction of a usable knox_nonce from passive traffic.

2. Obtain the Challenge Key

Removing and reading the chip looks more promising, but the key is bound to the CPU.

Conclusion: move from observation to control of the device CPU.

Obtaining knox_nonce: The Active Approach



Key difficulty: CryptoMCU is powered only during transactions, through a separate protection system.

Feasible, but complex

TAB A8: Interim Conclusion

High Complexity

The challenge, secure channel, CPU-bound key and CryptoMCU power control create a hardware barrier.

Off-Device Processing Is Possible

Once knox_nonce is obtained, user_pwd is used in an algorithm that can run outside the phone.

Despite the complexity, this design allows user password brute-forcing to be moved off the device.

Moving to Galaxy A6 / SM-A065



Key point: Weaver moves control of user authentication into CryptoMCU.

Why Success Is Not Guaranteed

If Only a Secret Blob Is Needed

Obtain the blob
+
Verify user_pwd off-device

TAB A8 Logic

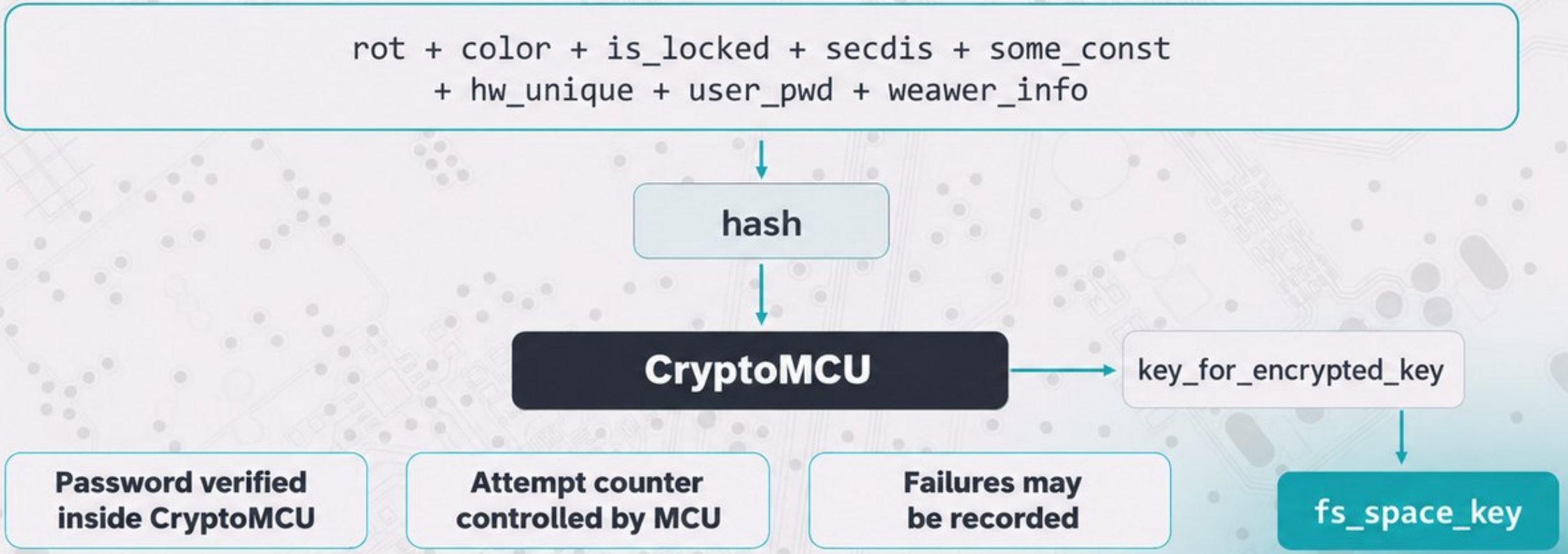
If Verification Is Inside CryptoMCU

user_pwd is verified through CryptoMCU

Weaver Logic

Weaver Changes the Security Model

CryptoMCU participates in verification and controls attempts.



What Weaver Changes

1
Authentication Control in CryptoMCU

Verifying user_pwd is not simply an algorithm that can run indefinitely outside the device.

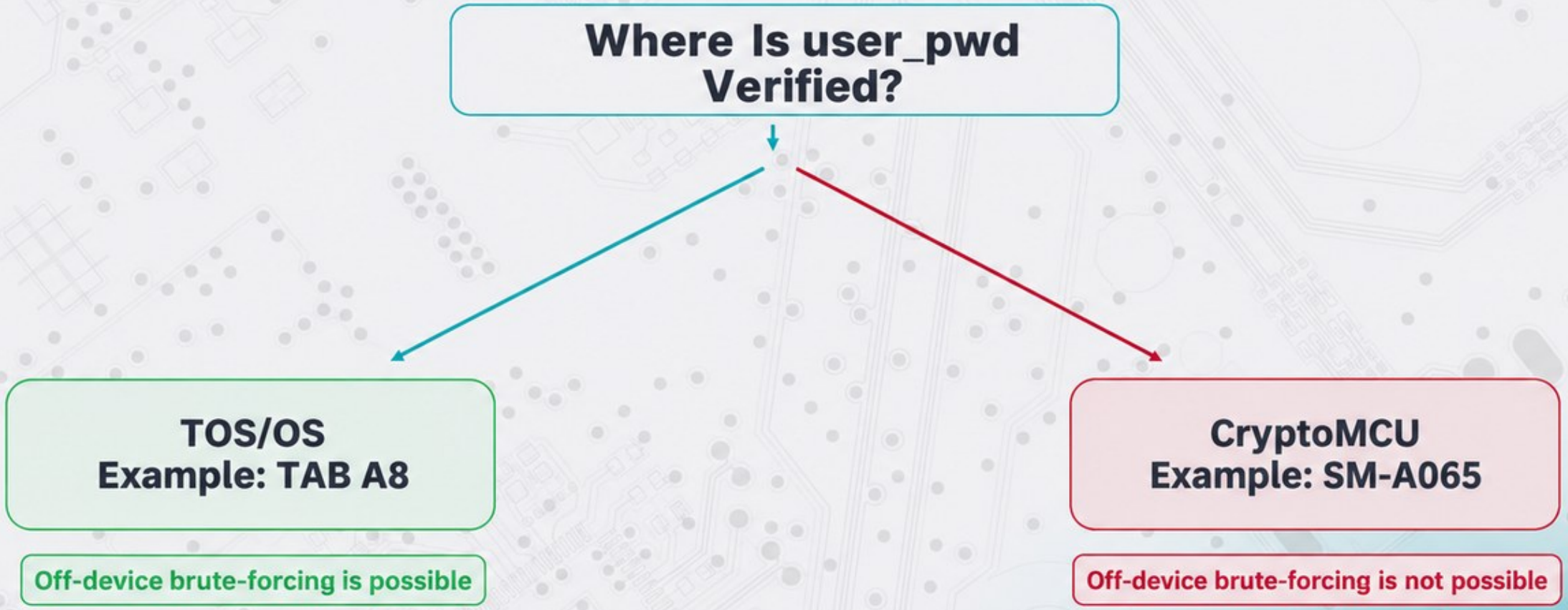
2
Attempt Counter

CryptoMCU can limit the number of attempts and thereby affect the brute-force rate.

3
Failure Tracking

Failed attempts may be recorded inside the device, and the device may stop responding.

When Off-Device Brute-Forcing Is Possible



Thank You
for Your Attention!

ACELab®
2026