Security Advisory

Title	Security Advisory Concerning Breaking the Hardware AES Core and Firmware Encryption of ESP32-ECO V3 Through Side Channel Attack
Issue date	2022/5/18
Advisory Number	AR2022-003
Serial Number	NA
Version	V1.0

Issue Summary

There are two hardware vulnerabilities of the ESP32-ECO V3 chip reported by security researchers at Ledger (Donjon).

The first vulnerability is about the hardware AES core, and second vulnerability is of the Flash Encryption feature of the ESP32-ECO V3 chip.

In the attack of the vulnerabilities, an attacker with physical access to the device is able to mount a Side Channel Attack (SCA), to obtain the encryption key from hardware AES core and the Flash Encryption key that resides in the eFuse of the chip.

For a successful SCA attack of the chip, an attacker needs to collect a several tens of thousands of power traces and apply an appropriate signal-to-noise ratio computation, to identify the temporal locality of the AES operations. They would then apply a CPA technique with Hamming Weight as the leakage model on the same locations to obtain the key used in the AES operation.

What is Side Channel Attack (SCA)?

An electronic device when functioning, may leak the information related to its internal operations. The information leak may exhibit in the form of variations in device power consumption or generated electromagnetic radiation.

When a device is processing some security sensitive data, e.g., a cryptographic key, this leaked information may be used to extract the key from the device, resulting in device security compromise. This is a non-invasive attack as it does not require to open the chip packaging, but it does require to open the device to tap the instantaneous power consumption traces. It is a real threat to the device, but it needs some skills from an attacker side to mount successful attack.

Some well-known SCA techniques are:

- ✓ Sequential Power Analysis (SPA)
- ✓ Differential Power Analysis (DPA)
- ✓ Correlation Power Analysis (CPA)

Impact Analysis

1) Hardware AES-256 Core Vulnerability

This attack compromises systems where the AES keys are long lived or permanently reside within the device.

In such use cases where AES keys are short lived, e.g., TLS session keys, this attack does not have any direct impact.

2) Hardware Flash Encryption Vulnerability

With flash encryption key extracted, an attacker may be able to extract confidential information from the device's encrypted flash.

Using some other exploit, an attacker would be able to replace the entire encrypted flash content with the content of their choice which are prepared out of band and take over the device.

However, if recommended practice is followed, and a unique flash encryption device key is provisioned in the eFuse then this attack would be device specific and scaling it to a class level attack would be cumbersome.

Mitigation

At present there is no hardware fix available for this issue. Future products will incorporate hardware countermeasures in the chip to address these issues.

Following are some recommendations to mitigate these issues.

- ### Software Countermeasures

It is possible to mask the actual AES operation on AES Core with dummy AES operations. This would make it difficult to identify the actual AES operation in the collected power traces. This countermeasure would however impact AES operation performance.

We will evaluate software countermeasures along with its performance impact and if it looks reasonable, we may integrate under additional project menuconfig option in future ESP-IDF release.

- ### Hardware Countermeasures

Protect the device from physical access by enclosing it with a tamper resistant mechanism which could not be broken without detection. Device should respond to tamper detection as per the predetermined action, e.g., reset the device, clear-out the secret information on the device.

- ### Design Countermeasures

Long lived encryption keys that are common between the devices or manufacturing batch should be avoided at all costs.

These attacks need significant effort, skill, expensive and sophisticated lab equipment to be carried out successfully on a device. If each device is provisioned with a unique secret tied to that specific device identity, then the attacker cannot scale it to an entire class of devices, making this attack less attractive.

Several Espressif products are available in System-in-Package (SiP) form-factor with flash pins terminated internally. These SiP (such as ESP32-PICO-V3) can protect against this type of attack better. This prevents usage of any external flash emulator or monitoring of flash pins as was used in the Flash Encryption related attack discussed in this advisory.

Other Espressif Products

SCA vulnerabilities reported in this advisory may be applicable for other Espressif SoC's including ESP32-S2, ESP32-C3 and ESP32-S3. We will incorporate hardware countermeasures in our future chips to address these vulnerabilities.

For hardware Flash encryption of ESP32-S2/ESP32-S3/ESP32-C3, the encryption algorithm has been upgraded to a more complex XTS-AES scheme; it increases the difficulty and cost of mounting an SCA, and hence, reduces security risks.

Credits

We would like to thank Karim M. Abdellatif, Olivier Hériveaux, and Adrian Thillard from Ledger, Donjon for reporting these vulnerabilities and assisting us with the disclosure.