Application Using TrustRAM and TrustZone on SAML11

This application demonstrates the enhancing security features on the SAML11 microcontrollers for security, which are Trusted RAM and TrustZone.

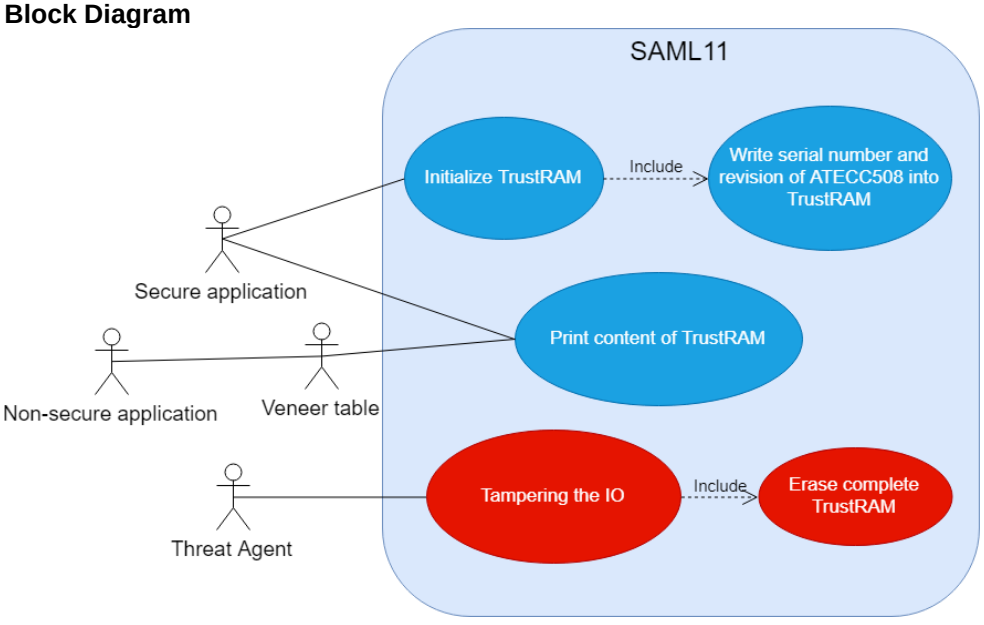
For more information please visit:
GitHub

Or contact
jpiwek@arroweurope.com

TrustZone
TrustZone provides the flexibility for hardware isolation of memories and peripherals, therefore reinforcing the ability of Intellectual Properties (IP) and Data protection. SAML11 provides up to six regions for the Flash, up to two regions for Data Flash, up to two regions for SRAM and the ability to assign peripherals, I/O pins, interrupts to secure or non-secure application.

TrustRAM
Trusted RAM implements 256 bytes of secure memory with address and data scrambling by user-defined key. Trusted RAM is also equipped with chip-level tamper detection and rapid tamper erase to resist micro-probing attacks.

Block Diagram



TrustRAM use case

Description

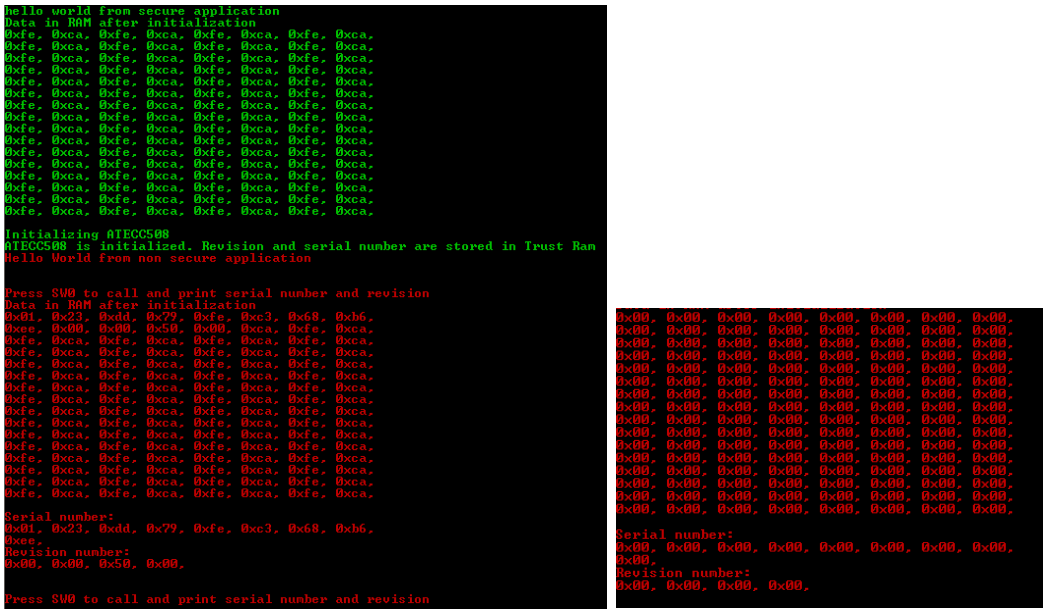
Inside SAML11, there are two applications running which are the secure and non-secure application. The secure application initializes the TrustRAM and prints the content of it on the console terminal. Then the secure application writes the serial number and revision of the onboard ATECC508, which are, in this case, considered as sensitive data into the TrustRAM.

Features/Benefits

> IP protection
> Software isolation
> Secure storage
> Tamper detection

Key Components

> SAML11
> Arm TrustZone
> TrustRAM



Content inside TrustRAM before and after being tampered

The non-secure application is initialized by the secure application. Non-secure application is not allowed to call any functions directly from the secure application but through a veneer table. In this case, it is the function to print the content of the TrustRAM.

When a tamper attempt is detected, the content in the TrustRAM will be automatically erased so the sensitive data is not exposed.

Possible Application

> Session keys storage
> Sensitive data storage