RISC-V Security

Arm® TrustZone® Technology vs RISC-V MultiZone™ Security

Mar, 2019
Did you feel the Earth Shake in Feb?

9.8

CVE-2019-8912 Detail

Current Description
In the Linux kernel through 4.20.10, af_alg_release() in crypto/af_alg.c neglects to set a NULL value for a certain structure member, which leads to a use-after-free in sockssetattr.

Source: MITRE
Description Last Modified: 02/18/2019

Impact
CVSS v3.0 Severity and Metrics:
Base Score: 9.8 CRITICAL

CVSS v2.0 Severity and Metrics:
Base Score: 7.5 HIGH

Exploitability Metrics
- Attack Vector (AV)*
- Attack Complexity (AC)*
- Privileges Required (PR)*
- User Interaction (UI)*

Low (AC:L) High (AC:H)
None (PR:N) Low (PR:L) High (PR:H)
None (UI:N) Required (UI:R)

Scope (S)*
- Unchanged (S:U) Changed (S:C)

Impact Metrics
- Confidentiality Impact (C)*
- Integrity Impact (I)*
- Availability Impact (A)*

None (C:N) Low (C:L) High (C:H)
None (I:N) Low (I:L) High (I:H)
None (A:N) Low (A:L) High (A:H)
Security Through Separation

Systems are composed of a stack of 100s of libraries.
Security Through Separation

Arm® TrustZone® Technology

Non-Secure RichOS

Trusted OS and Apps

Arm® TrustZone® Trusted Firmware

RISC-V MultiZone™ Security

Root of Trust

Network Stack

Crypto Libraries

OTA Update

Rich OS

Linux / RTOS

Each Zone Compiled and Linked Separately

Stack

Heap

Uninitialized data (bss)

Initialized data

Text

Secure InterZone™ Communications – no shared memory

Secure MultiZone™ nanoKernel – boot room

Arm and TrustZone are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.
Key Components of SoC Platform Security

- **Trusted Execution Environment**
  - Hardware enforced separation between code, data and memory mapped resources

- **Root of Trust**
  - Tamper-proof storage for unique ids and certificates
  - Tamper-proof storage for secrets (priv keys)

- **Secure Boot**
  - Prevent boot of unauthenticated code

- **Tools**
  - Transparent, intuitive and integrated with tools and processes the designer is already familiar with
Hardware Comparison
Arm® TrustZone® Technology vs. RISC-V Privileged Architecture
Hardware Security

Arm® TrustZone® for Armv8-A
Linux/Android Systems

Arm® Cortex®-A

AXI Bus
NS Bit

User
Supervisor
Hypervisor
Secure Monitor

IRQ
FIQ

TZASC
TZMA

Memory
Peripheral

Two Domains Hardcoded in Hardware

Arm® TrustZone® for Armv8-M
RTOS or Bare Metal Systems

Arm® Cortex®-M

AHB Bus

Non-Secure State
Priv. Non-Secure State
Secure State
Priv. Secure State

SAU/IDAU

Optional Memory Protection Controller
Optional Peripheral Protection Controller

Memory
Peripheral

Two Domains Hardcoded in Hardware

RISC-V Privileged Architecture v1.1

RISC-V

AHB Bus

User
Supervisor
Machine

PMP/PMA

IOPMP

Memory
Peripheral

Hardware Enforced Software Defined Domains

Arm and TrustZone are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.
Software Comparison
OP-TEE and PSA vs. MultiZone™ Security

Arm and TrustZone are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.
Armv8-A / OP-TEE Software Model

Two worlds – Mobile Phone / Gateway

- Code Size: 244kB\(^1\); RAM Requirements: 32MB\(^2\)
- Configuration and tools are outsourced from multiple Arm Ecosystem partners

“...the design complexity associated with correctly implementing [security] technologies like memory protection units (MPUs) often results in them not being used at all.

Brandon Lewis, Editor-in-Chief, Embedded Computing Design

Source: https://www.linaro.org/blog/op-tee-open-source-security-mass-market/
Armv8-M PSA Software Model

IoT Endpoint / RTOS – Smart Watch / Sensor

- Boot Loader: 3,366 lines / 38kB\(^1\)
- Kernel Size: 6,596 lines / 75kB?\(^2\)
- Solution ships with TCP/IP stack
- HW is just rolling out, L1 of PSA software is available higher levels pending
- Unified Development / Debug requires 3\(^{rd}\) party tools such as Kiel MDK or IAR EWARM

Source: https://developer.arm.com/products/architecture/security-architectures/platform-security-architecture

---

2. trustedfirmware.org repo
RISC-V MultiZone™ Security Software Model

Zero Trust Model for Unlimited # of Equally Secure Worlds

- **Tiny**: 0 stage Boot Loader: 600B, nanoKernel Size: 1.6kB
  - Designed for Formal Verification
- **Simple**: existing open source tools – gcc / gdb and Eclipse IDE
  - All security settings in a single flat file
- **Fast**: Context Switch ~100 instructions, <0.01% of core cycles
- **Universal**: Works on standard RISC-V Cores;
  - runs your existing code
- **Open Source** – available on github.com/hex-five
MultiZone™ Security Policy Configurator

# Copyright(C) 2018 Hex Five Security, Inc. - All Rights Reserved

Tick = 10 # ms

Zone 1

    base = 0x20410000; size = 64K; rwx = rx # FLASH
    base = 0x80001000; size = 16K; rwx = rw # RAM
    base = 0x10002500; size = 0x100; rwx = rw # PlM
    base = 0x8C000000; size = 0x400000; rwx = rw # PLC

Zone 2

    base = 0x20420000; size = 64K; rwx = rx # FLASH
    base = 0x80005000; size = 16K; rwx = rw # RAM
    base = 0x60000000; size = 8K; rwx = rw # XEMACLITE

Zone 3

    base = 0x20430000; size = 64K; rwx = rx # FLASH
    base = 0x80000000; size = 4K; rwx = rw # RAM
    base = 0x820000FF; size = 0x8; rwx = r # RTC
    base = 0x10012000; size = 0x100; rwx = rw # GPIO

Zone 4

    base = 0x20440000; size = 64K; rwx = rx # FLASH
    base = 0x8000A000; size = 4K; rwx = rw # RAM
    base = 0x10013000; size = 0x100; rwx = rw # UART
    base = 0x10012000; size = 0x100; rwx = rw # GPIO
MultiZone™ Security Live Demo

Zone #1
- RTOS [FreeRTOS]
- GPIO / IRQs

Zone #2
- TCP/IP Stack [picoTCP]
- ETHERNET

Zone #3
- Key Management [wolfSSL]
- OTP

Zone #4
- TEE CONSOLE [MultiZone]
- USB / UART

InterZone™ Secure Communications
Hex Five MultiZone™ nanoKernel
X300 Bitstream (RV32ACIMU + Ethernet)
Hex Five MultiZone™ Security

Hex Five Security, Inc. is the creator of MultiZone™ Security, the first trusted execution environment for RISC-V. Hex Five patent pending technology provides policy-based hardware-enforced separation for an unlimited number of security domains, with full control over data, code and peripherals. Contrary to traditional solutions, Hex Five MultiZone™ Security requires no additional cores, specialized hardware or changes to existing software. Open source libraries, third party binaries and legacy code can be configured in minutes to achieve unprecedented levels of safety and security.