

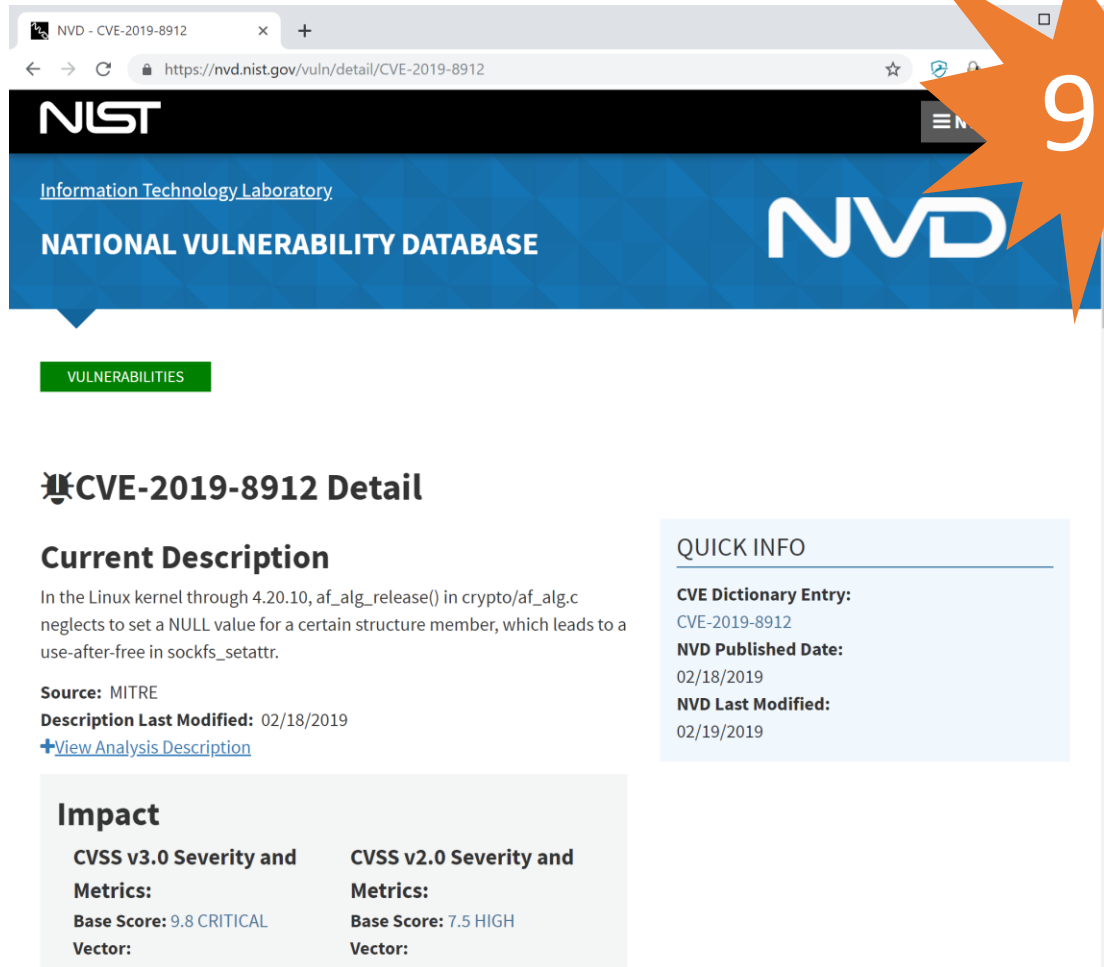


# RISC-V Security

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

Mar, 2019

# Did you feel the Earth Shake in Feb?



The screenshot shows the NIST National Vulnerability Database (NVD) entry for CVE-2019-8912. A large orange starburst with the number '9.8' is overlaid on the page. The page header includes the NIST logo and 'NATIONAL VULNERABILITY DATABASE'. The main content area is titled 'CVE-2019-8912 Detail' and includes a 'Current Description' section. A 'QUICK INFO' sidebar on the right lists the CVE Dictionary Entry, NVD Published Date (02/18/2019), and NVD Last Modified (02/19/2019). At the bottom, an 'Impact' section compares CVSS v3.0 and v2.0 severity metrics.

**NIST**  
Information Technology Laboratory  
**NATIONAL VULNERABILITY DATABASE**

**VULNERABILITIES**

## 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 sockfs\_setattr.

**Source:** MITRE  
**Description Last Modified:** 02/18/2019  
[View Analysis Description](#)

### Impact

CVSS v3.0 Severity and Metrics:	CVSS v2.0 Severity and Metrics:
<b>Base Score:</b> 9.8 CRITICAL	<b>Base Score:</b> 7.5 HIGH
<b>Vector:</b>	<b>Vector:</b>

### QUICK INFO

**CVE Dictionary Entry:**  
CVE-2019-8912  
**NVD Published Date:**  
02/18/2019  
**NVD Last Modified:**  
02/19/2019

## Base Score Metrics

### Exploitability Metrics

#### Attack Vector (AV)\*

**Network (AV:N)** Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

#### Attack Complexity (AC)\*

**Low (AC:L)** High (AC:H)

#### Privileges Required (PR)\*

**None (PR:N)** Low (PR:L) High (PR:H)

#### User Interaction (UI)\*

**None (UI:N)** Required (UI:R)

#### Scope (S)\*

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

### Impact Metrics

#### Confidentiality Impact (C)\*

None (C:N) Low (C:L) **High (C:H)**

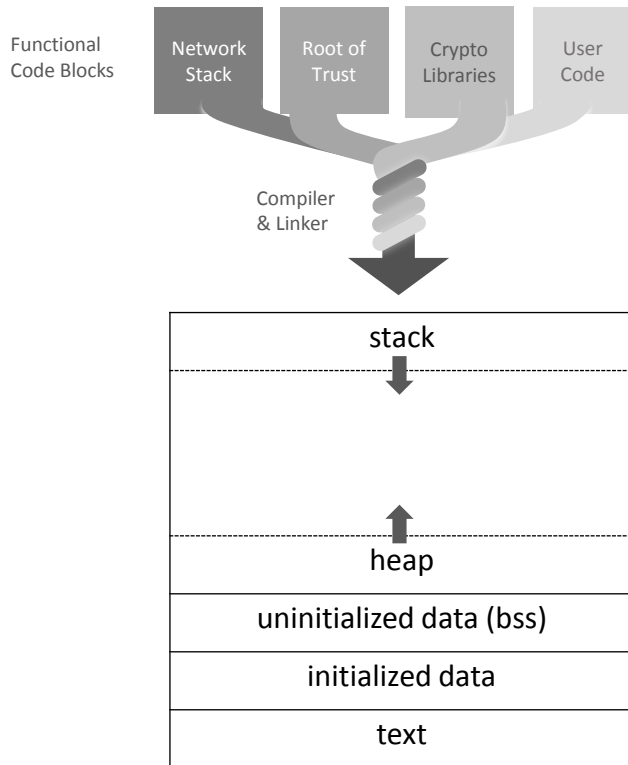
#### Integrity Impact (I)\*

None (I:N) Low (I:L) **High (I:H)**

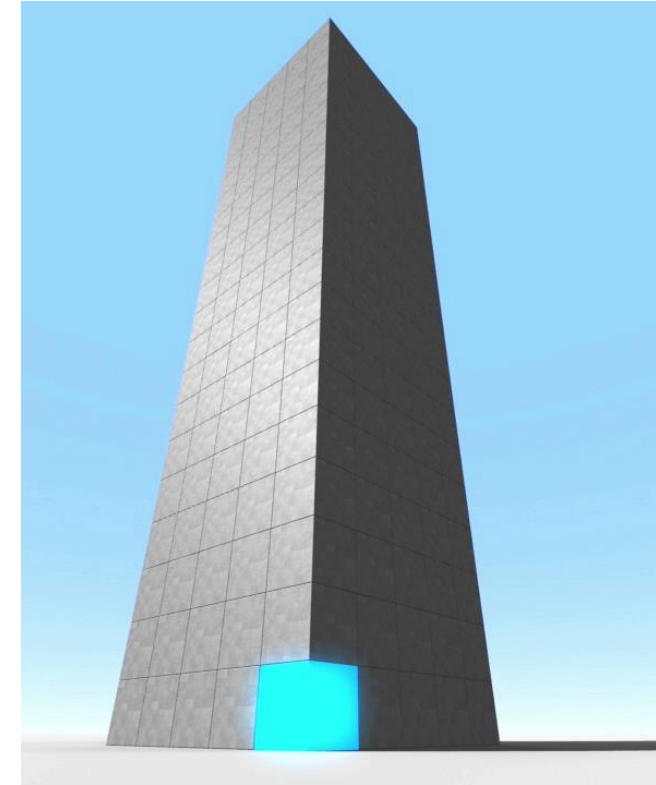
#### Availability Impact (A)\*

None (A:N) Low (A:L) **High (A:H)**

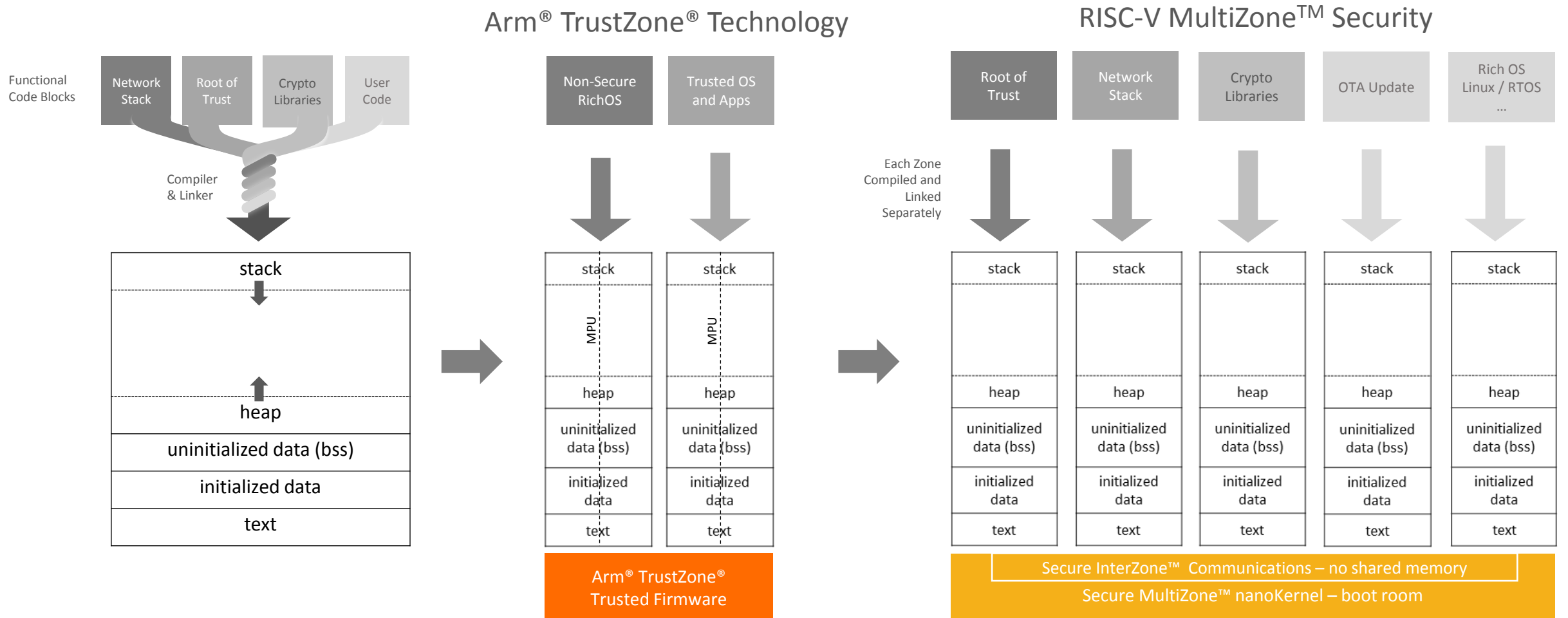
# Security Through Separation



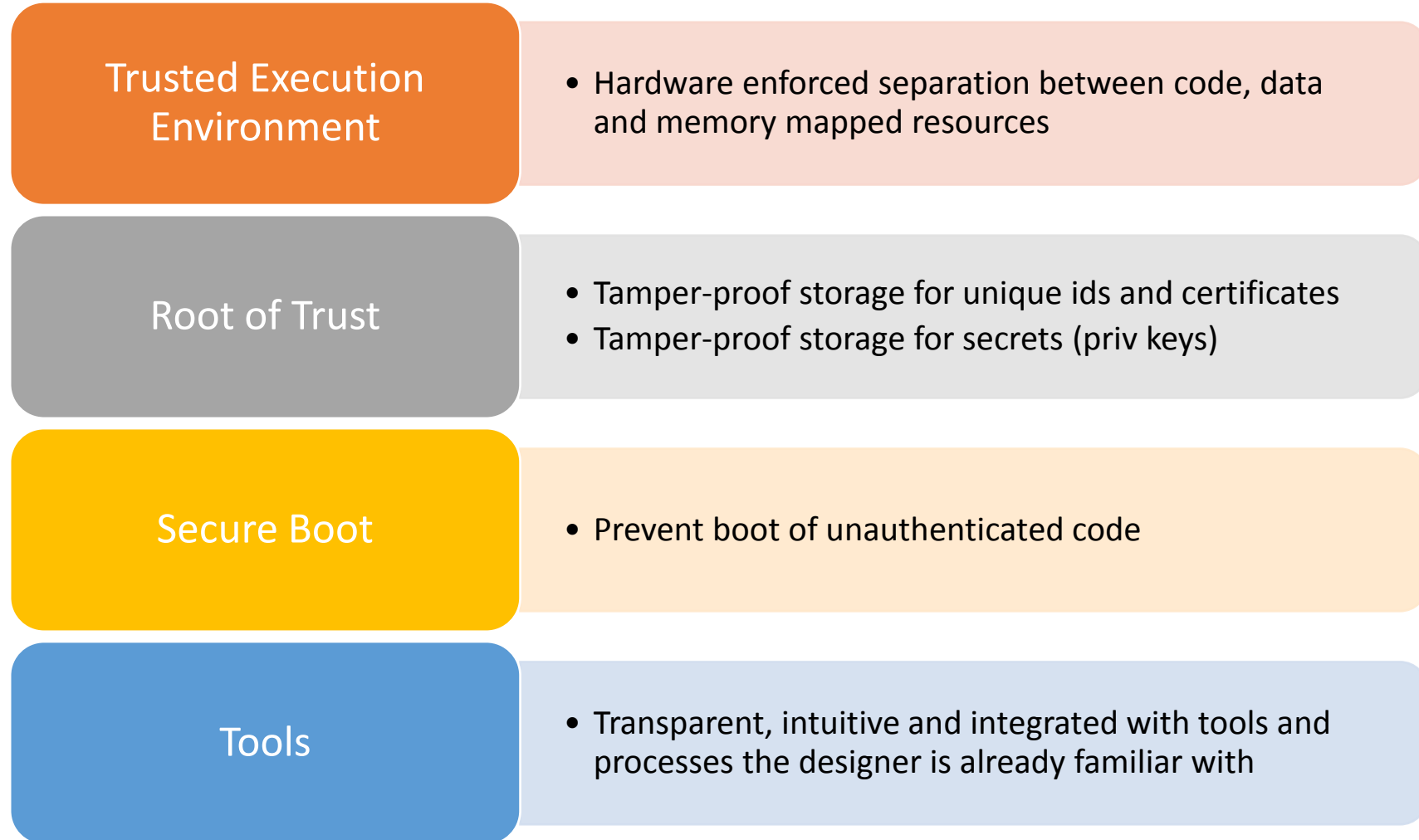
Systems are composed of a stack of 100s of libraries



# Security Through Separation



# Key Components of SoC Platform Security

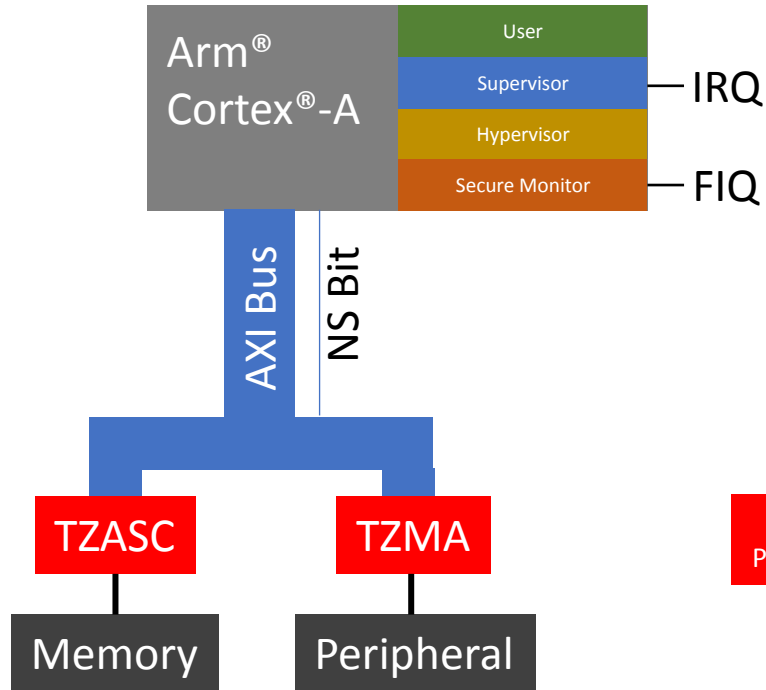


# Hardware Comparison

Arm<sup>®</sup> TrustZone<sup>®</sup> Technology vs. RISC-V Privileged Architecture

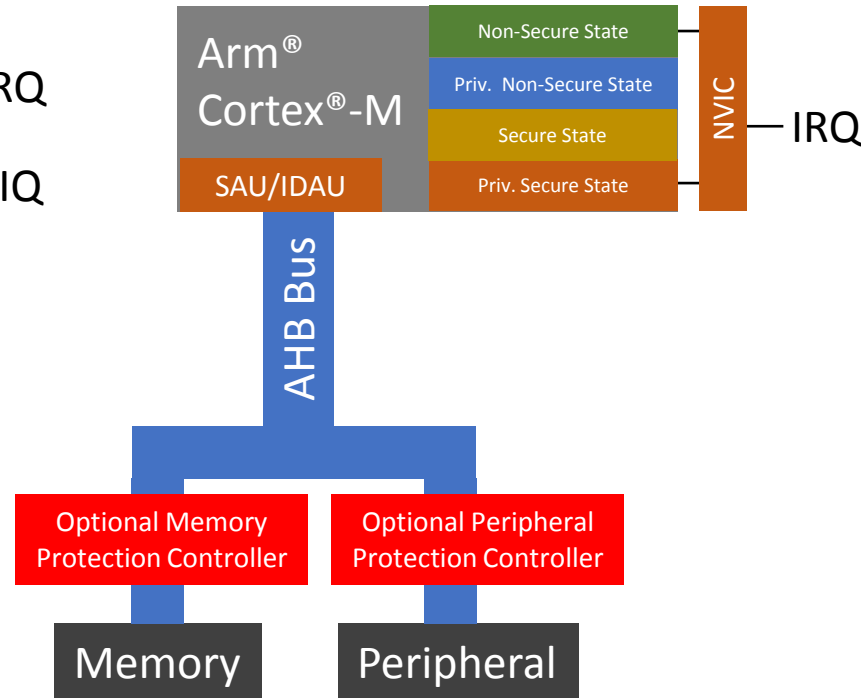
# Hardware Security

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



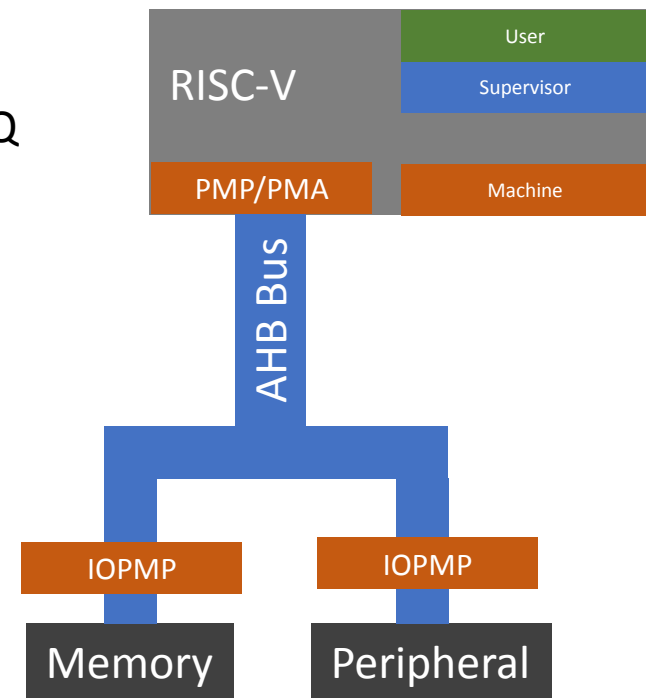
Two Domains Hardcoded  
in Hardware

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



Two Domains Hardcoded  
in Hardware

RISC-V Privileged  
Architecture v1.1



Hardware Enforced  
Software Defined Domains

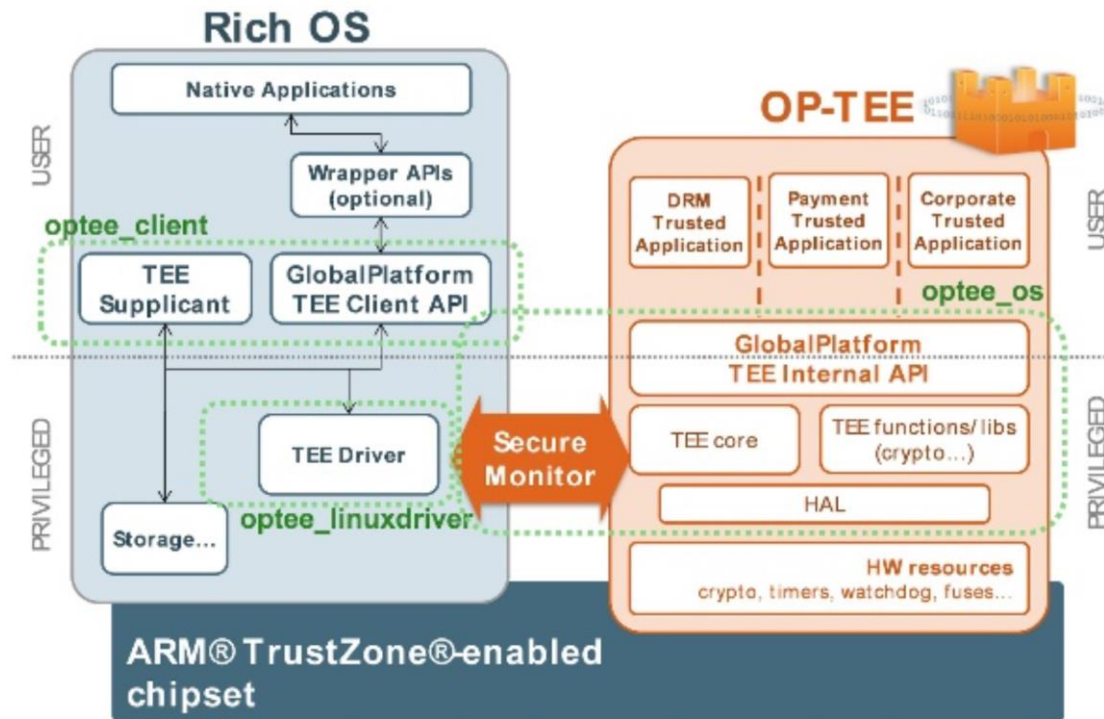


# Software Comparison

## OP-TEE and PSA vs. MultiZone™ Security



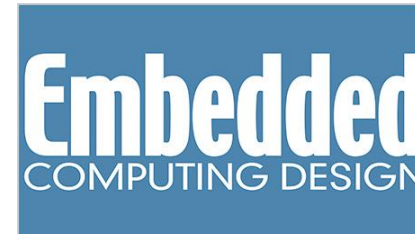
# Armv8-A / OP-TEE Software Model



Source: <https://www.linaro.org/blog/op-tee-open-source-security-mass-market/>

## Two worlds – Mobile Phone / Gateway

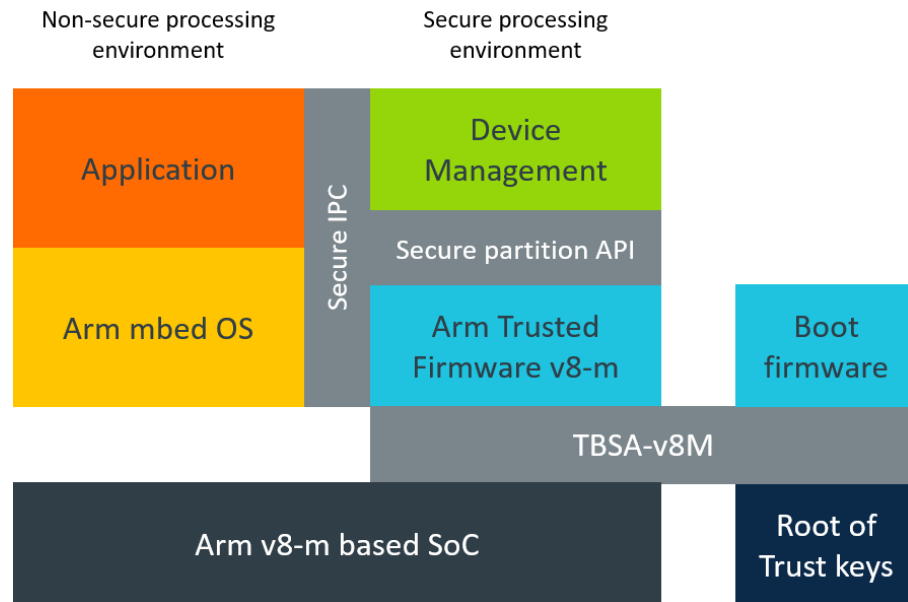
- Code Size: 244kB<sup>1</sup>; RAM Requirements: 32MB<sup>2</sup>
- Configuration and tools are outsourced from multiple Arm Ecosystem partners



*“...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

# Armv8-M PSA Software Model



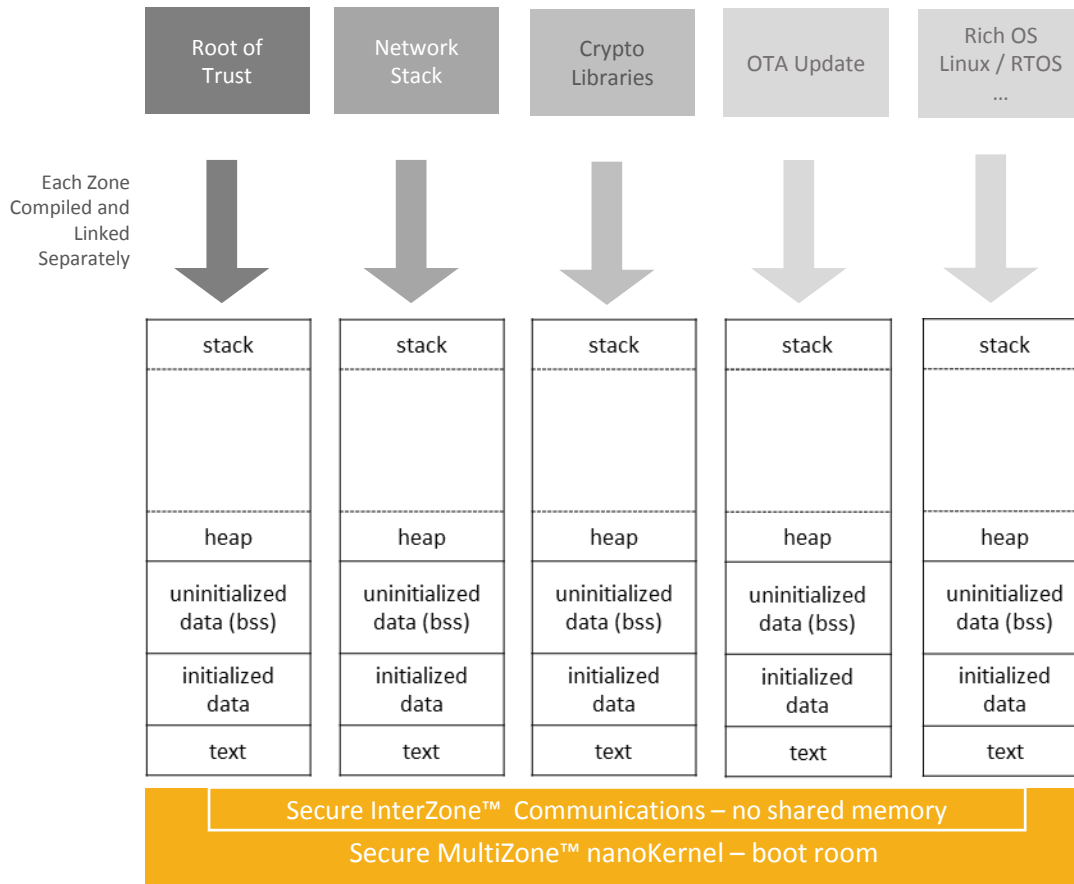
Source: <https://developer.arm.com/products/architecture/security-architectures/platform-security-architecture>

## IoT Endpoint / RTOS – Smart Watch / Sensor

- Boot Loader: 3,366 lines / 38kB<sup>1</sup>
- Kernel Size: 6,596 lines / 75kB<sup>2</sup>
- 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<sup>rd</sup> party tools such as Kiel MDK or IAR EWARM

# RISC-V MultiZone™ Security Software Model

## RISC-V MultiZone™ Security



## 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](https://github.com/hex-five)

# MultiZone™ Security Policy Configurator

```
multizone.cfg
~/eclipse-cdt-ws/hexfive-conf

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

Tick = 10 # ms

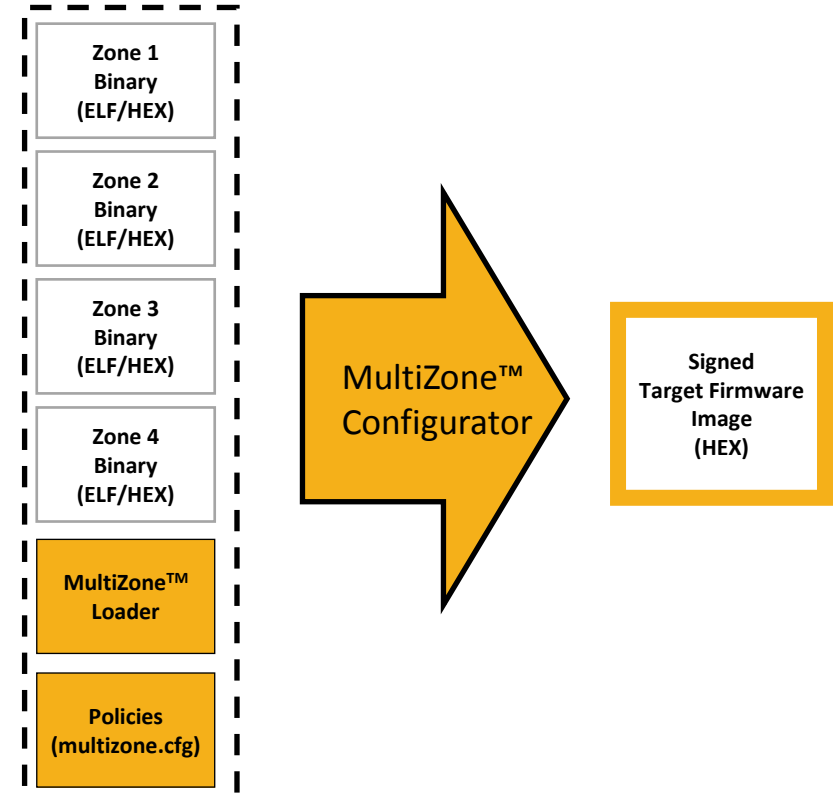
Zone = 1 #
    irq = 16, 17, 18 # BTN0 BTN1 BTN2
    base = 0x20410000; size = 64K; rwx = rx # FLASH
    base = 0x80001000; size = 16K; rwx = rw # RAM
    base = 0x10025000; size = 0x100; rwx = rw # PWM
    base = 0x10012000; size = 0x100; rwx = rw # GPIO
    base = 0x0C000000; size = 0x400000; rwx = rw # PLIC

Zone = 2 #
    base = 0x20420000; size = 64K; rwx = rx # FLASH
    base = 0x80005000; size = 16K; rwx = rw # RAM
    base = 0x60000000; size = 8K; rwx = rw # XEMACLITE

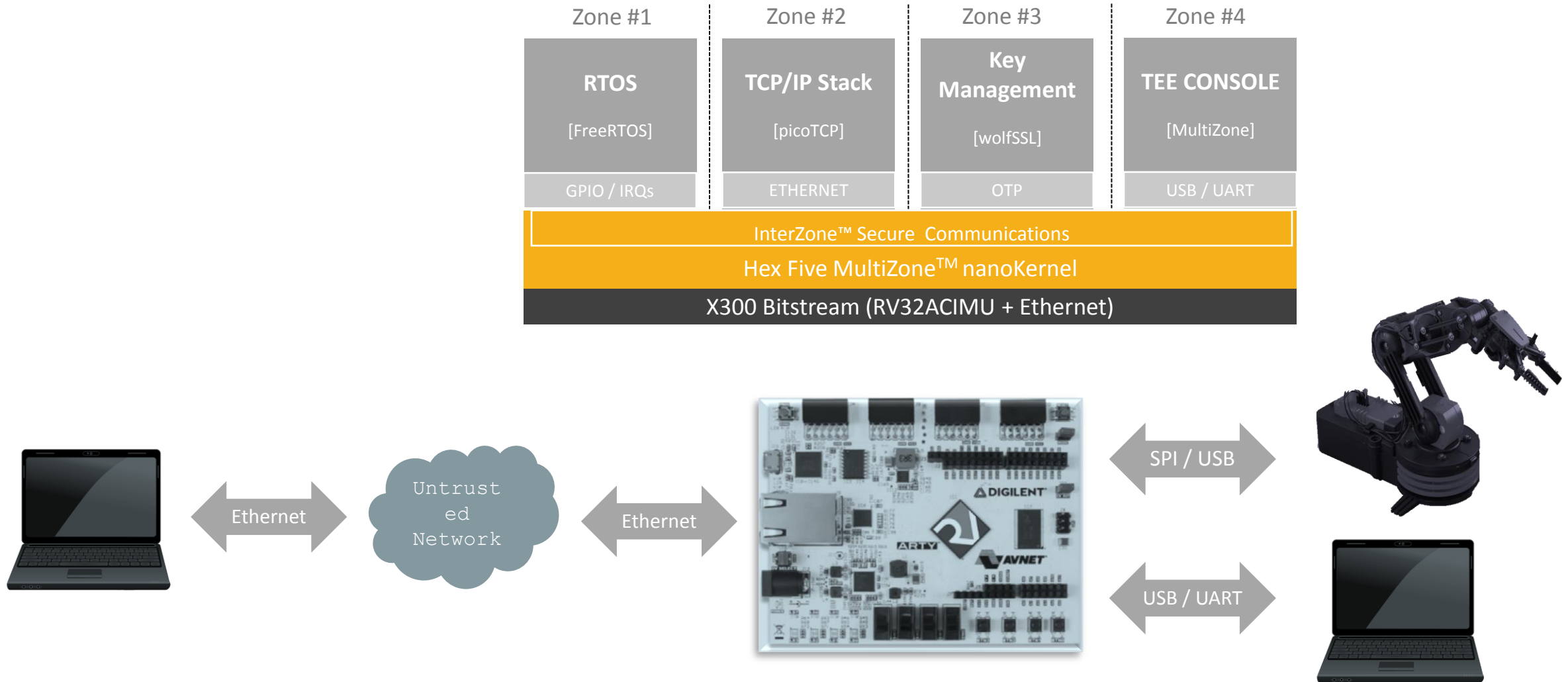
Zone = 3 #
    base = 0x20430000; size = 64K; rwx = rx # FLASH
    base = 0x80009000; size = 4K; rwx = rw # RAM
    base = 0x0200BFF8; size = 0x8; rwx = r # RTC
    base = 0x10012000; size = 0x100; rwx = rw # GPIO

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
```

Plain Text ▾ Tab Width: 3 ▾ Ln 10, Col 1 ▾ INS



# MultiZone™ Security Live Demo







HEX-Five™

# 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.