0x5 HEX–Five Security

RA Ecosystem Partner Solution

MultiZone® Security

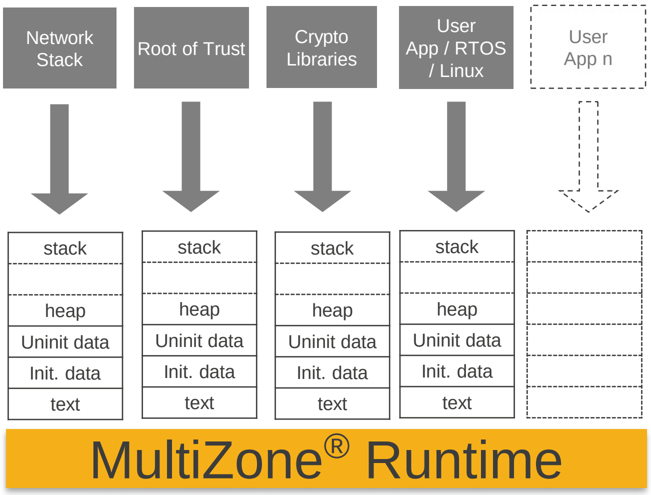
Solution Summary

MultiZone® Security provides hardware-enforced, software-defined separation of multiple trusted execution environments. It is a complete RA Ready solution that shields critical functionality from non-verified third-party components, and protects the entire platform from remote attacks.

Features/Benefits

- Integrated with FSP (Flexible Software Package) on the RA6M3
- Safe and quick way to add security through isolation - Trusted execution environment
- Easy retrofit of existing hardware and software - No redesign
- Multiple equally secure isolated domains (zones) – RAM, ROM, I/O, Irq handlers
- Hardware-enforced - Software-defined, Policy-driven RWX
- Extremely lightweight: Codebase ~ 2KB – Formally verifiable

Block Diagram



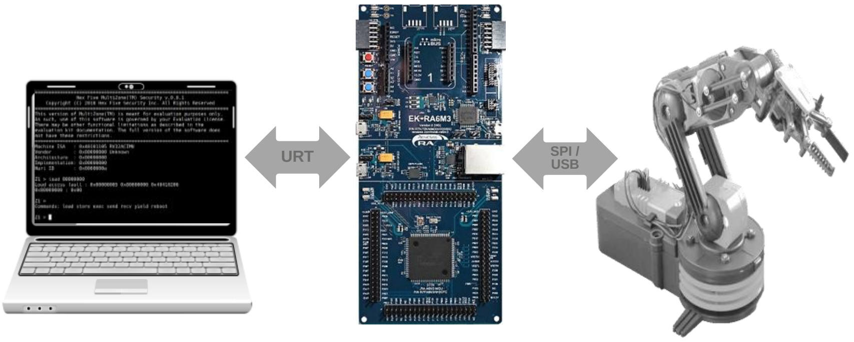
Hardware-Grade Security

Rapid Development

Easy Integration

Target Applications

- IoT
- Healthcare
- Meter
- Industrial
- Connectivity
- Building Automation

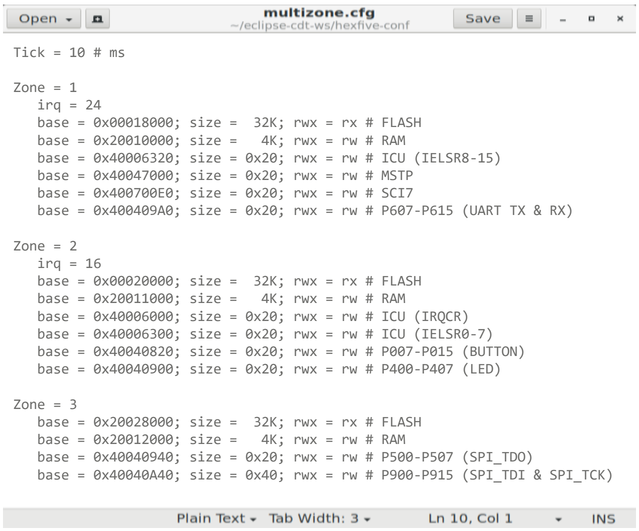


Multiple Domain Demo on EK-RA6M3

***MultiZone** is a registered trademark of Hex Five Security, Inc. - Patent pending US 16450826, PCT US1938774* 2020.03

0x5 HEX–Five Security

How it works



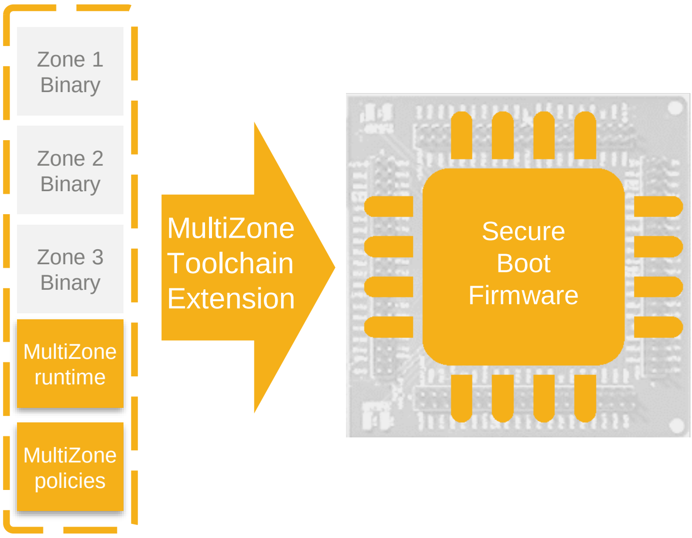
```
Tick = 10 # ms

Zone = 1
   irq = 24
   base = 0x00018000; size =  32K; rwx = rx # FLASH
   base = 0x20010000; size =   4K; rwx = rw # RAM
   base = 0x40006320; size = 0x20; rwx = rw # ICU (IELSR8-15)
   base = 0x40047000; size = 0x20; rwx = rw # MSTP
   base = 0x400700E0; size = 0x20; rwx = rw # SCI7
   base = 0x400409A0; size = 0x20; rwx = rw # P607-P615 (UART TX & RX)

Zone = 2
   irq = 16
   base = 0x00020000; size =  32K; rwx = rx # FLASH
   base = 0x20011000; size =   4K; rwx = rw # RAM
   base = 0x40006000; size = 0x20; rwx = rw # ICU (IRQCR)
   base = 0x40006300; size = 0x20; rwx = rw # ICU (IELSR0-7)
   base = 0x40040820; size = 0x20; rwx = rw # P007-P015 (BUTTON)
   base = 0x40040900; size = 0x20; rwx = rw # P400-P407 (LED)

Zone = 3
   base = 0x20028000; size =  32K; rwx = rx # FLASH
   base = 0x20012000; size =   4K; rwx = rw # RAM
   base = 0x40040940; size = 0x20; rwx = rw # P500-P507 (SPI_TDO)
   base = 0x40040A40; size = 0x40; rwx = rw # P900-P915 (SPI_TDI & SPI_TCK)
```

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



1. Compile, debug, and link each zone into separate binary files
2. Define hardware separation policies into a plain text configuration file
3. Run the toolchain extension to produce the signed boot firmware

Technical Specs

- Up to 8 separated Trusted Execution Environments (zones) – hardware-enforced, software-defined
- Up to 16 memory-mapped resources per zone – i.e. flash, ram, rom, i/o, uart, gpio, timers, etc
- Preemptive scheduler for safety-critical applications: cooperative, round robin, configurable tick
- Secure inter-zone communications based on messages – no shared memory, no buffers, no stack, etc.
- Built-in trap & emulation for all privileged instructions – i.e. SVC, MRS, MSR, CPS, WFE, WFI
- Full support for secure user-mode interrupt handlers mapped to zones – up to 128 interrupt sources
- Full support for Wait For Interrupt and CPU suspend mode for low power applications
- Formally verifiable runtime ~2KB, 100% written in assembly, zero 3rd party dependencies
- C library wrapper for protected mode execution – optional for high speed / low-latency
- Hardware requirements: Arm Cortex-M0+/M3/M4/M7 processor w/ Memory Protection Unit
- System requirements: 4KB for program, 2KB for data – CPU overhead < 0.01%
- Development environment: any versions of Linux, Windows, Mac running Java 1.8 or greater
- GNU-based Open source SDK freely available at https://github.com/hex-five/multizone-sdk-arm

MultiZone is a registered trademark of Hex Five Security, Inc. - Patent pending US 16450826, PCT US1938774

Scan me