SiFive Secures RISC-V

By Bob Wheeler (November 11, 2019)

Security features are now table stakes for microcontrollers, but RISC-V has too few chips to play. At the recent Linley Fall Processor Conference, SiFive disclosed its secure-platform architecture, which includes hardware and software as well as provisioning services. The company announced specific features available now across its core line, and it disclosed a roadmap for additional capabilities, most of which it plans to release in 2020. The SiFive Shield umbrella brand encompasses hardware root of trust, cryptographic intellectual property (IP), and memory-protection features, as well as software drivers and secure-monitor code. Shield's baseline capabilities are similar to those of Arm's TrustZone, but SiFive is adding features and services unavailable from that competitor.

To build a root of trust for secure boot and debug, Shield offers unique-ID and key storage, a true-random-number generator (TRNG), key and certificate provisioning, secure-boot code, firmware-signing tools, and secure debug. Cryptographic (crypto) IP includes AES block ciphers, SHA-2 and SHA-3 hash algorithms, and RSA and elliptic-curve public-key algorithms; SiFive withheld performance specifications for these cores. The company plans to deliver open-source cryptographic libraries and drivers for FreeRTOS and Linux, supporting the S2N-TLS and OpenSSL stacks, respectively. It also plans to commission third-party evaluations of its crypto cores and formal verification of secure debug (JTAG), but it declined to provide a time line.

The other major Shield component is WorldGuard, which SiFive should roll out next year. Like Arm's TrustZone, WorldGuard creates a trusted execution environment by isolating resources. (Arm and SiFive call security domains "worlds.") It isolates caches, memories, DMA channels, and peripherals by domain using a world ID. In a typical multicore design, one CPU is trusted and all others are untrusted. The secure monitor runs on the trusted core and authorizes resource access for the untrusted cores. The shared level-two cache adds a world-ID tag to each entry, and a checker detects unauthorized accesses.

Single-core designs are more complex, as the secure monitor and untrusted applications share the same CPU and L1 cache. In this case, the monitor runs in RISC-V's machine (M) mode, whereas untrusted processes run in user (U) mode. In this process-driven approach, the monitor assigns a process ID to each untrusted domain, and it maintains a process-to-world translation table. Outside of the CPU, all other resources employ the translated world ID for access control. A new WorldGuard physical-memory-protection (WG-PMP) unit, which sits between the CPU core and memory controller, associates authorized IDs with memory regions. The DMA controller associates an ID with an individual channel.

When crossing a TileLink or Amba interface, WorldGuard passes the world ID in user-defined fields that are separate from the address, allowing bus agents to block illegal operations without regard to the target address. All agents must implement the world-ID field, but WorldGuard requires no changes to the TileLink or Amba bus. It enforces memory protection using fault detectors. The WG-PMP and L2 checker are new and generate faults on unauthorized accesses. The multidomain secure monitor handles fault-detector interrupts. In addition to WorldGuard, other 2020 roadmap items include DDR encryption/integrity, secure boot from eMMC, 25Gbps AES, and SiFive's key-provisioning service.

Because all tagging takes place outside the CPU core, WorldGuard works with both microcontroller and application CPUs, and the latter don't require MMU extensions. SiFive offers a wide range of 32- and 64-bit microcontroller cores, including the newest E7- and S7-series (see *MPR 11/12/18,* "SiFive Raises RISC-V Performance"). Its newest application CPU is the 64-bit superscalar U84 with out-of-order execution (see *MPR 10/28/19,* "SiFive U8 Takes RISC-V Out of Order").

Whereas SiFive is just getting started with Shield, Arm has built TrustZone IP, software, and certifications over the last 15 years (see *MPR 8/25/03,* "Arm Dons Armor"). Announced in 2015, TrustZone for Arm v8-M is the latest version available in Cortex-M cores (see *MPR 11/16/15,* "Arm Dons Thicker Armor"). The biggest difference between WorldGuard and TrustZone is the former's support for multiple untrusted domains. At the platform level, SiFive is promising features to match up with TrustZone, but Arm offers a more integrated solution (see *MPR 11/6/17,* "Arm Cooks Up Recipe for IoT Security").

Overall, Shield and WorldGuard plug a hole in SiFive's story, but it's unclear how much of the technology will proliferate through the RISC-V ecosystem. For now, the security roadmap keeps the company at the forefront for commercial applications of the open ISA. ♦