Enhanced Security Package Option for ARC HS Processor Family

Highlights

- Two privilege levels and MPU-based access control
- Data and instruction path integrity checking to prevent fault injection attacks
- Error detection codes on memories and key registers
- Stack bounds checking (hardware) and canaries (compiler)
- Address space layout randomization
- Firmware scrambling/encryption to counter ROP/JOP
- Integrated watchdog timer detects system failures that can result from tampering and enables countermeasures
- Secure debug capability

Target Applications

- Solid state drives
- Automotive systems
- Home automation
- Home networking
- Mobile

Enhanced Security Package for ARC HS Processors

The Enhanced Security Package option available for DesignWare® ARC® HS family processors enables designers to create a secure environment that protects their systems and software from evolving security threats such as IP theft and intentional remote attacks. The package includes the capability to protect critical processor registers like stack and instruction pointer registers as well as secure bus accesses and includes a memory protection unit (MPU) with up to 16 configurable memory regions to protect traditional instruction and data memory. Also included is data and instruction path integrity checks to prevent fault injection attacks, error detection codes (EDC) on memories and key registers, stack bounds checking and a watchdog timer. Designers can also add user-defined instructions and co-processors through the ARC Processor EXtension (APEX) technology for cryptographic or encryption purposes.

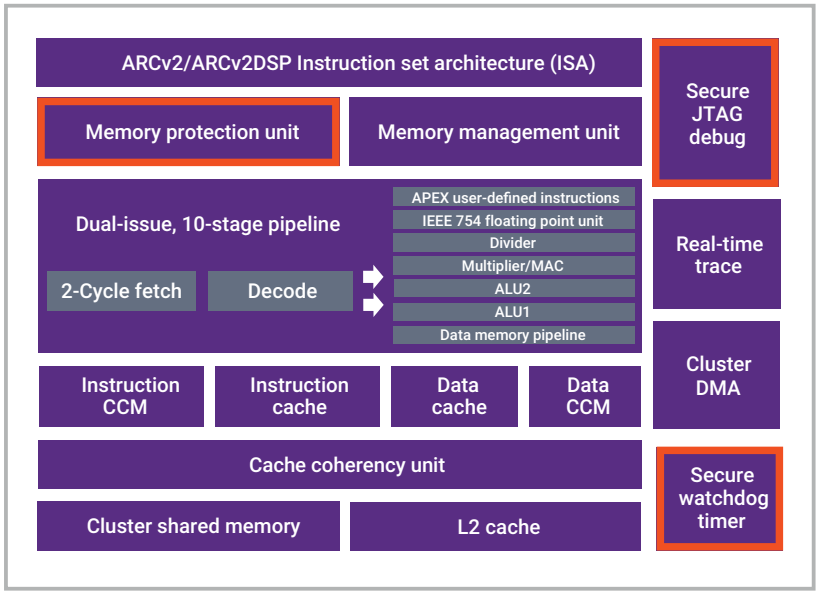

Figure 1: Enhanced Security Package Option on ARC HS Processor

Fault Injection Protection

The Enhanced Security Package option features EDC on memories and key registers. The EDC protection is available for the I-cache, D-cache, instruction close coupled memory (CCM) and the DCCM. The protected registers include the PC, the general-purpose registers, the AUX control/config registers, and the MPU/MMU control registers. The EDC detects single- and double-bit errors (SECDED), and many other cases using 6-bits of EDC for 32-bits of data using Hamming-4 coding. The EDC protects against the injection of a fault by glitching the power or clock. Injected faults often cause the processor to hang but can also cause bit errors in a register or memory. A carefully timed attack can cause glitching to bypass checks for secure boot, elevate the privilege level or enable attacks on cryptograph circuits.

Software Attack Protection

Hackers can exploit buffer and stack overflows to achieve arbitraray code execution or privilege escalation. To prevent this the Enhanced Security Package option includes countermeasures to protect the stack and address space. These countermeasures include hardware stack boundary checking, compiler generated canaries, 'no-execute' protection for the stack and other data, and address space layout randomization to protect against return-oriented programming (ROP) and jump-oriented programming (JOP).

The hardware stack boundary check is coarse-grained protection that looks at accesses to the allocated block of memory so that they cannot go beyond the allocated space. Compiler-generated canaries are inserted by the compiler and consist of values that are placed on the stack between buffer and control data to monitor overflows. If the buffer overflows it is likely that the first data corrupted will be the canary, which is a know value, so easy to identify and deal with.

No-execute protection available in the Enhanced Security Package for the stack and other data marks regions in memory as non-executable using the MPU or MMU, so that an attempt to execute code in these regions will cause an exception.

Address space layout randomization (ASLR) is available and is used to counter ROP and JOP attacks. This capability is typically used on larger systems and guards against attacks by randomizing where the system executables are place in the memory. Hackers can often be successful if they know of or can guess the positions of functions in memory. ASLR prevents this by putting functions in unpredictable locations. If a hacker trys to exploit an incorrect address location, the application will crash stopping the attack.

Watchdog Timer Protection

The watchdog timer is used to bring the processor back to a known state in when a hacking attempt or some other event causes the CPU to hang. The watdog timer output is brought out at the top level of the processor and can be used to reset the processor or for other functionality if desired. After the watchdog timer signal is asserted it remains active until the processor is reset.

ARC Processor EXtension (APEX) Interface

The HS processors are designed to be extendable with the addition of custom instructions. Proprietary functions implemented using APEX extensions are much harder to hack, making your code and the processor more secure. These instruction extensions may include more processor and auxiliary registers, new instructions, and additional condition code tests. Custom instructions can be implemented in Verilog or systemC and enable designers to efficiently add their proprietary hardware to the processor to further increase security or to add an almost unlimited range of functionality including encryption or cryptographic capabilities to the processor. The HS processors support 64-bit APEX instructions.

Complete Suite of Development Tools

To facilitate rapid development, the processors are supported by a complete suite of development tools. This includes the MetaWare Development Toolkit that generates performance optimized code, which takes advantage of the high-performance HS pipeline delivering highly efficient code for embedded applications. The tools also include the ARC xCAM and nSIM simulators and the ARChitect configuration tool.

Documentation

The following documentation is available for the DesignWare ARC HS processors:

- ARCv2 Programmers Reference
- ARC HS Series Databook
- ARC HS APEX Databook
- ARC HS4x Series Databook

Testing, Compliance and Quality

Verification of the DesignWare ARC processors follows a bottom-up verification methodology from block level through system level. Each functional block within the product follows a functional, coverage-driven test plan.

The plan includes testing for ARCv2 ISA compliance as well as state- and control- specific coverage points that have been exercised using constrained pseudo-random environments and a random instruction sequence generator.

About MIPS:

MIPS by GlobalFoundries delivers software to silicon with RISC-V for building physical AI platforms. MIPS delivers software-hardware co-design, optimized AI, and custom ASSP design and manufacturing. Together with ARC, MIPS delivers the open, standards-based processor IP portfolio for embedded applications. Physical AI is built on MIPS.

For more information, visit **www.mips.com/arc.**