Synopsys' New Enhanced Security Package for ARC HS Processors Protects Embedded Systems Against Evolving Threats

Enables Development of Isolated, Secure Environments for High-Performance Applications

MOUNTAIN VIEW, Calif., Feb. 27, 2019 /PRNewswire/ --

Highlights:

- New Enhanced Security Package option for ARC HS3x and HS4x processors enables development of secure environments in high-performance embedded applications
- Data integrity protection detects fault injection attacks to help prevent hackers from bypassing secure boot checks
- Multiple privilege levels and MPU-based access control isolates applications to reduce the SoC's vulnerability to attack
- Integrated watchdog timer detects and recovers system from failures that result from tampering

Synopsys, Inc. (Nasdaq: SNPS) today announced the new Enhanced Security Package for Synopsys DesignWare® ARC® HS Processors, enabling designers to develop isolated, secure environments that help protect embedded systems and software from evolving threats in high-end automotive, storage, and gateway applications. The Enhanced Security Package incorporates a range of features, including integrity protection, multiple privilege levels, and a watchdog timer that help protect system-on-chips (SoCs) against both logical and physical attacks, such as IP theft and remote attacks, without compromising performance. ARC HS Processors with the Enhanced Security Package enable SoC developers to create devices less susceptible to security threats while eliminating the increased area and power consumption that an additional security core and associated memories would impose.

Synopsys DesignWare ARC HS Processors are based on the scalable, 32-bit ARCv2 instruction set architecture (ISA) and are optimized for performance efficiency, making them ideally-suited for a wide range of high-end embedded applications. The Enhanced Security Package for ARC HS Processors offers integrity protection for registers and memory to detect fault injection attacks, which helps prevent the use of power or clock glitching to bypass secure boot checks or elevate the privilege level. Access control of hardware resources and the system bus is protected by the HS Processors' secure memory protection unit (MPU), helping to prevent an attacker from injecting executable code as data. The availability of multiple privilege levels enables software applications to be isolated, making them less vulnerable to attack. Hardware stack bounds checking and compiler-inserted canaries prevent stack overflows that can be exploited to achieve arbitrary code execution or privilege escalation. In addition, randomization of the base address for software prevents return-oriented programming (ROP) and jump-oriented programming (JOP) in larger systems running Linux.

"With the increasing amount of electronics in high-end applications like automotive safety systems, effective security measures are needed to limit external attacks," said John Koeter, vice president of marketing for IP at Synopsys. "By extending our portfolio of security solutions with Synopsys' new Enhanced Security Package for ARC HS Processors, we are enabling designers to implement the necessary functionality to safeguard their SoCs against malicious attacks while achieving the performance goals of their target application."

Availability and Resources

- The Enhanced Security Package option for ARC HS Processors is available now.

About DesignWare IP

Synopsys is a leading provider of high-quality, silicon-proven IP solutions for SoC designs. The broad DesignWare IP portfolio includes logic libraries, embedded memories, embedded test, analog IP, wired and wireless interface IP, security IP, embedded processors, and subsystems. To accelerate prototyping, software development and integration of IP into SoCs, Synopsys' IP Accelerated initiative offers IP prototyping kits, IP software development kits, and IP subsystems. Synopsys' extensive investment in IP quality, comprehensive technical support, and robust IP development methodology enables designers to reduce integration risk and accelerate time-to-market. For more information on DesignWare IP, visit https://www.synopsys.com/designware.

About Synopsys

Synopsys, Inc. (Nasdaq: SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. As the world's 15th largest software company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and is also growing its leadership in software security and quality solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest security and quality, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at www.synopsys.com.

Editorial Contact:
Norma Sengstock
Synopsys, Inc.
650-584-4084
norma@synopsys.com

SOURCE Synopsys, Inc.