Synopsys and Cypherbridge Accelerate TLS Record Processing for IoT Communication with Optimized Hardware/Software Security Solution

Combination of Cypherbridge uSSL SDK and DesignWare SSL/TLS/DTLS Security Protocol Accelerator Speeds Software Development

MOUNTAIN VIEW, Calif., Feb. 18, 2016 /PRNewswire/ --

Highlights:

- DesignWare SSL/TLS/DTLS Security Protocol Accelerator with the optimized Cypherbridge uSSL software development kit enables system architects to replace TLS record processing software implementations with more efficient hardware processing
- DesignWare SSL/TLS/DTLS Security Protocol Accelerator with built-in scatter/gather DMA capability offloads cryptographic functions from the CPU to speed record processing of the software transport layer security protocol stack
- Cypherbridge uSSL software development kit, an ANSI C thread-free library, requires minimal context switching for improved software performance
- Synopsys and Cypherbridge will demonstrate the hardware/software security solution at Embedded World 2016 in Nuremberg, Germany, February 23-25

Synopsys, Inc. (Nasdaq:SNPS) today announced a collaboration with Cypherbridge Systems to optimize Cypherbridge's uSSL™ software development kit (SDK) for the Synopsys DesignWare® SSL/TLS/DTLS Security Protocol Accelerator (SPAcc). The joint solution enables the offload of cryptographic functions to dedicated hardware, giving system architects the ability to reallocate the CPU to other functions or use a smaller CPU. The combined SDK and DesignWare SPAcc accelerate the development of device software drivers for the transport layer security (TLS) protocol, which is used as the encryption layer in web browser, Internet of Things (IoT), payment terminal and industrial control applications.

The DesignWare SPAcc speeds the record processing of commonly used security protocols including secure socket layer (SSL), TLS and datagram transport layer security (DTLS) via a highly configurable architecture that provides the exact functionality and performance level required for a specific application. The SPAcc can also accelerate lower-level cipher, hash/MAC and public key operations, as well as several high-level functions used during the handshake protocol performed by SSL, TLS, or DTLS protocols.

SDKs that rely on a system heap can result in memory fragmentation, negatively impacting system performance. The Cypherbridge uSSL SDK is an ANSI C thread-free library with an integrated memory manager for a zero-heap solution. It is available with out-of-the-box support for the most widely used embedded operating systems, TCP stacks and target development kits. The SDK and SPAcc solution offloads TLS record processing to the SPAcc for optimized performance and design efficiency, reducing CPU load and improving power balancing.

"Designers are finding that a significant percentage of their development time is spent optimizing their software stack for the SoC hardware," said Steve DeLaney, founder at Cypherbridge Systems. "By leveraging our uSSL SDK with Synopsys' DesignWare Security Protocol Accelerator, designers can accelerate their software development and ultimately get their products to market faster."

"Connected devices ranging from routers to baby monitors increasingly require stringent security technology to prevent malicious attacks and data breaches," said John Koeter, vice president of marketing for IP and prototyping at Synopsys. "Our collaboration with Cypherbridge helps designers, who may not have deep security protocol knowledge, to implement the TLS protocol quickly and efficiently."

View the Demo at Embedded World 2016,February 23-25

Visit Synopsys in the Cypherbridge Systems booth (4-449) at Embedded World 2016 in Nuremberg, Germany to see how Synopsys' DesignWare Security Protocol Accelerators, with the Cypherbridge uSSL SDK, can increase the performance of IoT applications.

Availability and Resources

The DesignWare SSL/TLS/DTLS SPAcc and Cypherbridge uSSL SDK are available now.

- Learn more about the DesignWare SSL/TLS/DTLS Security Protocol Accelerator
- Learn more about the Cypherbridge uSSL SDK

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 16th 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 quality and security solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest quality and security, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at www.synopsys.com.

Editorial Contacts:
Monica Marmie
Synopsys, Inc.
650-584-2890
monical@synopsys.com

SOURCE Synopsys, Inc.