NXP Secures the Edge with Two Industry-First Multi-Core Arm Cortex-M33 Solutions

October 10, 2018

News Highlights

- New platforms unify security subsystems and software ecosystem – features secure execution environment (SEE) to give developers access to unprecedented security capabilities
- LPC5500 single and dual-core 100MHz Arm Cortex®-M33 microcontrollers (MCUs) in 40nm flash technology for a broad range of industrial and IoT edge applications
- i.MX RT600 crossover processors with up to 300/600MHz Cortex-M33/Digital Signal Processor (DSP) cores in 28nm FD-SOI technology for high-performance voice and audio in ultra-low power edge processing applications

SAN JOSE, Calif., Oct. 10, 2018 (GLOBE NEWSWIRE) -- **(ARMTECHCON2018)** -- Delivering on the vision to secure IoT edge devices, and cloud to edge connections, NXP Semiconductors N.V. (NASDAQ:NXPI) combines hardened security subsystems and software into a secure execution environment (SEE) to raise the bar on trust, privacy, and confidentiality. The new security functionalities and capabilities are key highlights in its new Cortex-M33 based solutions, LPC5500 microcontrollers and i.MX RT600 crossover processors.

Multi-Layered Approach to Embedded Systems Security

Building on the company's security expertise, NXP brings multi-layered, hardware-enabled protection scheme that is unique in the industry today. Vital to physical and run-time protection, this layered security approach protects embedded systems with:

- Secure boot for hardware-based immutable root-of-trust
- Certificate-based secure debug authentication
- Encrypted on-chip firmware storage with real-time, latency-free decryption

These features in conjunction with Arm® Cortex-M33 enhancements of Arm TrustZone® technology for Armv8-M architecture and Memory Protection Unit (MPU), ensures physical and runtime protection with hardware-based, memory mapped isolation for privilege-based access to resources and data.

"The promise of the connected world through the Internet-of-Things is extraordinary," said Geoff Lees, senior vice president and general manager of microcontrollers at NXP. "Through NXP's in-depth security and processing expertise, software ecosystem and breadth of portfolio, we are uniquely positioned to bring innovative and accessible advancements in IoT security to all developers."

Unique Security Enhancements

A cornerstone to establishing device trustworthiness is NXP's ROM-based secure boot process that utilizes device-unique keys to create an immutable hardware 'root-of-trust'. The keys can now be locally generated on-demand by an SRAM-based Physically Unclonable Function (PUF) that uses natural variations intrinsic to the SRAM bitcells. This permits closed loop transactions between the end-user and the original equipment manufacturer (OEM), thus allowing the elimination of third-party key handling in potentially insecure environments. Optionally, keys can be injected through a traditional fuse-based methodology.

Furthermore, NXP's SEE improves the symmetric and asymmetric cryptography for edge-to-edge, and cloud-to-edge communication by generating device-unique secret keys through innovative usage of the SRAM PUF. The security for public key infrastructure (PKI) or asymmetric encryption is enhanced through the Device Identity Composition Engine (DICE) security standard as defined by the Trusted Computing Group (TCG). SRAM PUF ensures confidentiality of the Unique Device Secret (UDS) as required by DICE. The newly announced solutions support acceleration for asymmetric cryptography (RSA 1024 to 4096-bit lengths, ECC), plus up to 256-bit symmetric encryption and hashing (AES-256 and SHA2-256) with MbedTLS optimized library.

"Maintaining the explosive growth of connected devices requires increased user trust in those devices," said John Ronco, vice president and general manager, Embedded & Automotive Line of Business, Arm. "NXP's commitment to securing connected devices is evident in its new Cortex-M33 based products built on the proven secure foundation of TrustZone technology, while incorporating design principles from Arm's Platform Security Architecture (PSA) and pushing the boundaries of Cortex-M performance efficiency."

Accelerating Machine Learning and DSP Compute Performance

NXP strategically selected Cortex-M33 to leverage the first full-feature implementation of Armv8-M architecture to provide security platform benefits and substantial performance improvements compared to existing Cortex-M3/M0 MCUs (over 15 to 65 percent improvement, respectively). One of the

key features of the Cortex-M33 is the dedicated co-processor interface that extends the processing capability of the CPU by allowing efficient integration of tightly-coupled co-processors while maintaining full ecosystem and toolchain compatibility. NXP has utilized this capability to implement a co-processor for accelerating key ML and DSP functions, such as, convolution, correlation, matrix operations, transfer functions, and filtering; enhancing performance by as much as 10x compared to executing on Cortex-M33. The co-processor further leverages the popular CMSIS-DSP library calls (API) to simplify customer code portability.

LPC5500 Platform – Multi-core Cortex-M33 MCUs for Industrial & IoT Applications

Single- or Dual-core Cortex-M33 with integrated DC-DC delivers industry-leading performance at a fraction of power budget, of up to 90 CoreMarks™/mA. The high density of on-chip memory, up to 640KB flash and 320KBSRAM, enables efficient execution of complex edge applications. Further, NXP's autonomous, programmable logic unit for offloading and execution of user-defined tasks delivers enhanced real-time parallelism. For more information about the LPC5500 series, click here.

i.MX RT600 Crossover Platform – Power-Optimized Cortex-M33 / DSP MCUs for Real-Time Machine Learning (ML) / Artificial Intelligence (AI) Applications

Wide operating voltage and performance range, with up to 300MHz Cortex-M33, up to 600MHz Cadence® Tensilica® HiFi 4 DSP and shared on-chip SRAM of up to 4.5MB, enables efficient local audio pre-processing, immersive 3D audio playback and voice-enabled experience. The ML performance is further enhanced in the DSP with 4x 32-bit MACs, vector FPU, 256-bit wide access bus, and DSP extensions for special Activation Functions (e.g., Sigmoid transfer function). For more information about the i.MX RT600 series, click here.

Dover CoreGuard – Security with Hardware-Based Defense

NXP has partnered with Dover Microsystems to introduce Dover's CoreGuard™ technology in future platforms. CoreGuard is a hardware-based active defense security IP that instantly blocks instructions that violate pre-established security rules, enabling embedded processors to defend themselves against software vulnerabilities and network-based attacks. For more information, click here.

NXP at Upcoming Shows and Conferences

NXP plans to demonstrate its latest edge compute offerings at Arm TechCon this week in Booth #620. Also, NXP plans to demonstrate its industrial IoT solutions for ML at IoT World Barcelona this week in Booth #261 located in the Gran Via – Hall 2, Street B, Level 0.

About NXP Semiconductors

NXP Semiconductors N.V. (NASDAQ:NXPI) enables secure connections and infrastructure for a smarter world, advancing solutions that make lives easier, better and safer. As the world leader in secure connectivity solutions for embedded applications, NXP is driving innovation in the secure connected vehicle, end-to-end security & privacy and smart connected solutions markets. Built on more than 60 years of combined experience and expertise, the company has over 30,000 employees in more than 30 countries and posted revenue of $9.26 billion in 2017. Find out more at www.nxp.com.

For more information, please contact:

Americas
Tate Tran
Tel: +1 408-802-0602
Email:tate.tran@nxp.com

Europe
Martijn van der Linden
Tel: +31 6 10914896
Email: martijn.van.der.linden@nxp.com

Greater China / Asia
Esther Chang
Tel: +886 2 8170 9990
Email: esther.chang@nxp.com

NXP USA, Inc.