Embedded Processor Offers Advanced Security Features

Targeting the growing network transport, enterprise and consumer markets, the APM86791 PacketPro Gen2 embedded processor from Applied Micro Circuits is designed to deliver the industry's most advanced but cost effective network security measures for enhanced protection against intrusion threats, system hacking and theft of system-level intellectual property. The APM86791 leverages AppliedMicro's SLIMpro Trusted Management Module (TMM) to offer multi-layered encryption and authentication capabilities that manufacturers and network administrators need to make systems impervious to the most sophisticated attacks on security keys, proprietary software code and hardware.

The Trusted Management Module resides in a secure on-chip cryptographic boundary region designed to replace multi-chip solutions which are vulnerable to attack. The TMM makes keys, passwords and digital certifications invisible to hackers and supports the industry's highest level of SoC integrity and privacy.

The TMM also enables:
• Secure Boot to decrypt and authenticate software during reboot
• Secure Communication to enable connectivity with a remote host using secure communications
• Secure Software Updates to decrypt and authenticate new software images
• Secure Software Checks to detect violations and breaches with periodic exams.

The SLIMpro TMM is part of AppliedMicro's PacketPro Gen 2 family designed to provide a tamper-proof hardware platform for secure network communications to enable system administrators to prevent unauthorized activity typically used to attack a variety of systems ranging from residential gateways to enterprise backhauls. "Keelback" APM86791 utilizes dedicated secure boot ROM, EFUSE array, encryption engine, RTC, Public Key Accelerator and True Random Number Generator (TRNG) to enable the TMM features. These featured drivers are necessary to support the growing premium placed on digital rights management through storage security and virtual private network (VPN) applications as networks converge and data traffic becomes more pervasive in the cloud.

"With network connectivity becoming even more pervasive, mainstream, embedded systems are faced with security threats ranging from intellectual property theft and network intrusions to system hacking," said Majid Bemanian, senior director of marketing for AppliedMicro. "AppliedMicro offers a customizable approach with its Trusted Management Module as a tamper-proof hardware platform that is impervious to software and hardware attacks, providing developers with the most advanced security for embedded systems."

The TMM enables enhanced security features through inline Internet Protocol Security (IPSec) for protecting network traffic between hosts, lookaside security for line rate performance at minimal CPU and system overhead utilization, an on-chip protected cryptographic boundary for private/public storage and authentication handshaking, and a crypto engine for quality of service and protected data integrity. The inline IPSec supports Advanced Encryption Standards (AES) AES-GCM and AES-GMAC along with Encapsulating Security Payload (ESP) encryption and authentication at wirespeed performance. Lookaside security includes an integrated DMA engine as well as a true random number generator and a Public Key Accelerator.

“Over the last decade, system security has risen to the top of the list of features that many embedded developers require,” said Joseph Byrne, Senior Analyst at the Linley Group. “AppliedMicro’s TMM has encryption and authentication features baked in to the silicon that are designed to harden embedded systems from the types of attacks that are common today. The on-chip secure zone provided by AppliedMicro’s Trusted Management Module should be appealing to many developers who place the highest priority on system integrity and protection of intellectual property.”

The "Keelback" APM86791 features a single-core, 1.0-GHz PowerPC® 465 processor with floating point unit, 32KB L1 I-cache, 32KB D-cache and 256 KB L2 cache with hardware I/O coherency and DDR3 memory controller with optional ECC. The Trusted Management Module is part of a set of advanced features enabled by SLIMpro in AppliedMicro's PacketPro Gen 2 family. Other features available through SLIMpro include intelligent power management, asymmetric multiprocessing, queue and traffic management, and offload acceleration features. The APM86791 has four 10/100/1000 Ethernet ports (RGMII & SGMII), two PCI-Express® Gen1/2 ports, two USB 2.0 hosts with integrated PHY/Serdes and one SATA 2.0 port.

Samples of AppliedMicro APM86791 are expected in the third quarter. For more information about PacketPro and other AppliedMicro processing products, visit: http://www.apm.com/products/process.html [1]

Source URL (retrieved on *05/25/2013 - 4:30pm*):
http://www.ecnmag.com/product-releases/2011/07/embedded-processor-offers-advanced-security-features

Links:
[1] http://www.apm.com/products/process.html