Chrysalis-ITS launches security chip using five RISC cores

Loring Wirbel

4/25/2000 1:06 PM EDT

KANATA, Ontario (ChipWire) -- Chrysalis-ITS Inc. here today debuted a single-chip security processor for handling encryption and virtual private network (VPN) management. The Luna 340 utilizes five i
Chrysalis-ITS launches security chip using five RISC cores
KANATA, Ontario (ChipWire) -- Chrysalis-ITS Inc. here today debuted a single-chip security processor for handling encryption and virtual private network (VPN) management. The Luna 340 utilizes five independent RISC cores from ARC Cores, four dedicated to symmetric security processing and the fifth used for asymmetric and control functions.

The Luna 340 began life as a VPN accelerator card, but morphed into a project to add programmed support for higher-level protocols in a single processor, said Neil MacAskill, director of IC operations Chrysalis-ITS. The security chip market currently is segmented into processor and card-level developers working primarily in file encryption, and programmable solutions handling a mix of encryption, firewall and VPN duties.

MacAskill said that the company's optimization of multiple RISC cores on a single chip came about through its work with Checkpoint Software Inc. and Nokia Inc., and that Chrysalis-ITS worked with Mosaid Inc. and ARC Cores in optimizing the implementation in a standard CMOS device.

"When we looked at the software from a cryptographic point of view, customers wanted us to support emerging protocols directly on the chip from a library point of view, things like Secure Sockets Layer and IPsec Internet Protocol Secure," said Stephen Davis, security IC software manager at Chrysalis-ITS.

A network security processor operates on IP headers, just like a general-purpose packet-parsing network processor. But it is optimized for the tasks of encrypting the payloads of each data packet and of creating secure-transaction capabilities for individual IP "flows." As such, a security processor often is used in conjunction with a network processor.

Ironically, Chrysalis-ITS' first two partners in this arena are Vitesse Semiconductor Inc. and Sitera Inc., which have just announced plans to merge (see April 20 story).

Intel Corp. also is a minority investor in Chrysalis-ITS, but Davis emphasized that his company works on application programming interfaces independently from Intel. Chrysalis-ITS will take a close look at the APIs Intel is developing based on its acquisition of NetBoost Inc., but won't necessarily follow Intel API programming models, he said.

The Luna processor handles all proposed algorithms for the new Advanced Encryption Standard, which is slated to replace the Data Encryption Standard, including Blowfish, Twofish and Elliptic-Curve Cryptosystem. The 340 is designed to handle packets at OC-3 (155-Mbit/sec.) speeds in full-duplex fashion. It includes hardwired "zero-izing" circuitry, as well as a random-number generator.

The four symmetric RISC processors can be used for such duties as bulk encryption and hashing, while the

fifth can be a manager for Public Key Infrastructure (PKI) functions such as certificate authority. Chrysalis-ITS has partnered with RSA Security Inc. for a broader range of PKI library tools.

To provide the broadest flexibility for working with network coprocessors and host processors, Chrysalis-ITS elected to embed two complete Peripheral Component Interconnect bus interfaces on-chip. Because the 340 must make calls to both the system host and the network processor, a single PCI interface could have created bottlenecks, designers decided. The processor also includes a real-time clock and support for a battery-backed nonvolatile RAM.

The early applications for the 340 are obvious ones: routers and remote-access servers that implement VPNs, and dedicated PKI add-in hardware products. But MacAskill said the secondary markets are intriguing and may emerge fairly quickly, as secure financial transactions become important. These include applications such as Web switches, Wireless Application Protocol (WAP) servers and voice-over-IP gateways. Because the 340 can handle 1,000 SSL sessions simultaneously, for example, it could become standard for Web switches and server-farm switches handling secure transactions for retail or wholesale Web sites.

WAP servers may represent an important arena for Chrysalis-ITS, particularly since the formation of a security alliance three weeks ago by Motorola, Nokia and LM Ericsson to drive new SSL translation methods for secure transactions in cellular phones and PDAs. At last fall's NetWorld+Interop show, Chrysalis-ITS created a Network Security Processor Alliance.The 340 is packaged in a thermally enhanced 304-pin ball grid array. It is available in prototype for developers, along with a development platform offering software utilities and a series of APIs.

Volume pricing will be announced as Luna 340 moves into production later this year.