Andes ASICs bypass TCP layer to secure transactions

Loring Wirbel

2/12/2001 11:01 AM EST

A startup called Andes Networks Inc. has devised a way to dramatically accelerate Secure Socket Layer transactions by bypassing the Layer 4 Transmission Control Protocol (TCP) session. The company is aiming for nothing less than a radical revision of **Andes ASICs bypass TCP layer to secure transactions** A startup called Andes Networks Inc. has devised a way to dramatically accelerate Secure Socket Layer transactions by bypassing the Layer 4 Transmission Control Protocol (TCP) session. The company is aiming for nothing less than a radical revision of how secure HTTP transactions are conducted.

Andes, whose designers have roots at Sun Microsystems Inc., Synopsys Inc. and RSA Data Security Inc., lays claim to a security solution for Web transactions that uses ASICs to packetize SSL. Andes' Zoo ASICs will be at the heart of a scalable, rack-mounted system that will sit at the front end of the Web switches and specialized caching systems used in corporate Web server farms, managed-service provider Web server sites and Internet service provider points of presence.

Andes' proxyless technology and the imminent arrival of proxy-based single-chip accelerators from such vendors as Chrysalis-ITS suggest that security hardware may be able to blow past the Internet Protocol Secure (IPsec) layer and support the application layer directly.

The Internet Engineering Task Force (IETF) two years ago completed IPsec, a robust Open Systems Interconnect protocol Layer 3 standard that allowed the creation of secure virtual private network tunnels and the encryption of packet traffic within them. But IPsec has been slow to be adopted because of compatibility questions.

"Compatibility is often hard to show between equipment from different vendors when you're at Layer 3," said Mark Taber, vice president of marketing and sales at security-processor specialist Chrysalis-ITS.

That was the impetus for higher-layer solutions, particularly SSL, which can demonstrate interoperability at the end application. SSL authenticates traffic bidirectionally between the Web browser and server. It is invoked from the application layer and creates a secure session tunnel for HTTP traffic and other traffic types. Secure Web sites usually use some form of SSL for monetary transactions. But because SSL acceleration in hardware requires the storage of TCP session states and the use of complex TCP proxies, SSL's usage has not reached its promised potential.

Dedicated accelerators

Indeed, SSL requires so much dedicated processing power that such companies as RSA and Rainbow Technologies Inc. have developed dedicated SSL hardware accelerators as adjuncts to routers and Web switches.

But the NonStop SSL architecture proposed by Andes could speed SSL by 100 to 1,000 times over the acceleration enabled by Rainbow, SonicWall and Intel Corp.'s IPivot product group, claimed Tony Bailey, a director of market analysis firm Enterprise Management Associates Inc. (Denver).

"It's easy to be skeptical about numerical claims like that," Bailey said. "But the more I took a look at the architecture, the more I was convinced that the level of expertise in this company in 64-bit processor design and overall architectural and application engineering could allow them to really pull this off. SSL processing puts enormous burdens on both compute power and memory, and their method of algorithmic processing could take off some of that pressure."

Paul Gordon of RSA recently joined Andes, formerly called BeeLine Networks, as president and chief executive officer after examining the ASIC solutions being developed by company founders Glen Anderson, co-architect of Sun's UltraSparc, and Guillermo Maturana, former chief scientist of Synopsys and founder of Radiant Systems Inc. Gordon helped bring in venture capital from Vantage Point Venture Partners, PacRim Venture Partners and Infinity Capital LLC.

Bill Miller, a former General DataComm and Fujitsu executive who recently joined Andes as vice president of marketing and business development, said he was attracted to the company when he realized that the SSL speedup could justify SSL's use in more than 90 percent of transactions through Web browsers. That prediction eclipses even the aggressive Forrester Research projection that SSL traffic will account for one-third of all Internet traffic by 2004. Andes claims that its systems will be able to process 2,500 to 5,000 SSL client sessions per second and pass through packet traffic at up to 1 Gbit/second.

Special sauce

Andes has seven separate patents issued or pending for its architecture. Most surround the hardware process for packetizing SSL operations. "Our special sauce is in the exception handling for TCP," Gordon said. "We can operate on each packet with virtually no TCP overhead."

Steve Davis, semiconductor architect at security-processor specialist Chrysalis-ITS Inc. (Ottawa), countered that many IPsec and bulk-encryption companies, including Chrysalis-ITS, are successfully using traditional TCP proxy methods to accelerate SSL to levels of several thousand sessions per second. Chrysalis-ITS will be able to meet or exceed Andes' claims within a matter of months using single-chip SSL accelerators, Davis predicted.

But the bigger concern with any method that bypasses a TCP proxy, he said, is that "as soon as you take something away from TCP, you remove the ability to do the packet reordering and other functions that TCP was meant to provide."

In addition, said Chrysalis vice president of marketing and sales Mark Taber, the method seems to imply a "morphing" of SSL, which may require changes to end-user client software.

Miller said the concept for the SSL hardware came largely from founder John Wawrzynek, a Berkeley electronics engineering professor famous for his work in reconfigurable-array processors and analog VLSI for auditory processing. Anderson and Maturana helped Wawrzynek refine his ideas for practical implementation.

"While we're not offering the chips outside the systems, we think this will obsolete security approaches from people like Broadcom's BlueSteel team," Miller said.

Gordon said that there may be cases where Andes collaborates with a Web switch vendor but that the company won't follow the lead of some IPsec vendors in making its intellectual property more embeddable or even turning to chip sales. "We have no intention of churning out intellectual property blocks for licensing," he said.

Analyst Bailey said the onus is on Andes to convince OEMs, service providers and enterprise customers

that they need one more piece of equipment in their racks. It might be wise for Andes to begin with the financial services industry, where secure Web transaction needs are greatest, he said. But in any event, Andes will have to come to a skeptical market with plenty of case studies to back up its claims.

Service providers and enterprise managers alike often have a tough time grasping the ways that hardware security acceleration can aid their networks, because some solutions dwell almost exclusively on one layer of the Open Systems Interconnect protocol stack, while others entail multiple layers, from the physical layer to end-user application.