12 March

Feature

Building Next-Generation Network Security Processors

By Stephen Davis and Mel Roberts

As business-critical virtual private networks (VPNs) flourish, security considerations are compounded. A solution encompassing software programmability and scaleable hardware is an important step toward designing and implementing tomorrow's secure networks.

The demand for security processing capability in common communication products such as edge access equipment, routers, and cable head-end gear has forced communication systems designers to become network security specialists. As the installed base of business-critical virtual private networks (VPNs) surges, so too does the importance of a scaleable, flexible security processing solution.

The rush for faster security processing in coprocessors has forced IC designers to hardwire cryptographic algorithms and introduce devices with limited flexibility as well as performance. These hardwired devices, however, are unable to respond to changes in security technologies. In fact, systems based on hardwired cryptographic coprocessors are quickly made obsolete if customers must adopt new security protocols such as the advanced encryption standard (AES).

Therefore, a new approach to security processing is required. Under this new approach, hardwired technologies are combined with software programmable components to speed up existing processors and provide the flexibility to grow as technologies change.

This article details the key security specifications that network security processing solutions must support. Additionally, the article highlights the key security requirements that designers should look for in security processing solutions. Let's start with an overview of some key security standards.

IPSec

As Internet security became a problem, the Internet Engineering Task Force (IETF) approved different security protocols to make Internet communications safer. The Internet protocol security (IPSec) standard is one of the most interesting protocols accepted by the IETF. In fact, this protocol has been designed into a number of browsers, Web servers, firewalls, and routers.

IPSec is receiving growing acceptance in North America as a method for implementing VPNs. IPSec is a suite of standards for performing encryption, authentication, and secure tunnel setup. IPSec ensures confidentiality, integrity, and authenticity of data.

The IPSec standard suite essentially creates private end-to-end tunnels out of the public bandwidth available on the Inter-net and is a flexible solution for deploying network-wide security policy. The value of IPSec is that it runs at the IP Network Layer (layer 3) and allows scaleable end-to-end tunneling (see Figure 1 and Figure 2).

IPSec makes use of Diffie Hellman (D-H) key exchange for deriving keys and public cryptography for signing D-H exchanges to guarantee identity. Bulk encryption algorithms such as the digital encryption standard (DES) and triple DES (3DES) are used to encrypt the data, with hashing algorithms such as MD-5 or SHA-1 handling the packet authentication. Internet Key Exchange (IKE) is the protocol used to create and tear down security associations.

Although discreet encryption solutions exist today, these solutions are typically hardwired to perform specific algorithms, the most common being 3DES, DES, SHA-1, and MD-5. Performance in terms of the rate at which data can be processed starts at T1 and T3 line rates. In most cases, half-duplex SONET OC-3 (155-Mbps) rates are the highest being offered. As VPNs become widely accepted, higher data rates will be required to deal with high-speed links such as those offered at full-duplex SONET OC-3 and OC-12. To add to the security-processing burden, IKE algorithms must be performed for every secure tunnel that is created.

The need for multiple-chip solutions to perform IPSec encryption and authentication is a potential problem when security issues are considered. Acceleration of public-key operations using asymmetric algorithms such as Rivest, Shamir, Adleman (RSA), digital signature algorithm (DSA), or Elliptic

algorithms such as Rivest, Shamir, Adleman (RSA), digital signature algorithm (DSA), or Elliptic Curve can require a separate device. Separate devices may compromise the overall solution by adding complexity to the physical security of the system.

Scaleability and adaptability of solutions that provide secure tunnels are also a key concern when working with IPSec specification. As IPSec evolves, new algorithms may be introduced or improved. The security processing solution must adapt without forklifting out the underlying architecture and software, as system requirements change. These concerns have created an opportunity for a new generation of programmable, scaleable security processors that perform public-key authentication and high-speed encryption.

SSL

An increasingly popular alternative to IPSec is the secure sockets layers (SSL) standard. This standard e-Commerce security protocol is evolving from a client-server model to a server-to-server implementation. SSL differs from IPSec in that it also places an extreme burden on the host CPU, but this burden consists almost exclusively of asymmetric operations. Where the design of IPSec-based VPN equipment is concerned with total throughput in terms of Mbps, the design of SSL-based security products is concerned with session setups per second.

Web content providers, e-Commerce Web fronts, and service providers need to deliver instantaneous bandwidth and high-availability services to maintain customer satisfaction. Infrastructures ideally should be nonblocking and wire speed to eliminate choke points. Web servers that can establish thousands of sessions per second, unencrypted, will see their performance drop to 20 sessions per second when running SSL. A security processor that is able to offload the session setup and asymmetric operation is required. In addition, the security processor should be scaleable to allow the server to address higher performance as the server's capability increases.

Hardwired cryptographic accelerators are able to offload the underlying mathematical operations required to implement RSA and DSA, which are the basis for SSL. Next-generation programmable security processors will implement the entire SSL negotiation protocol and will be flexible enough to address the inevitable changes within it. These security processors should also be able to address implementation differences that occur when SSL is implemented in a server, Web switch, or other load-sharing device.

WAP

The advent of Wireless Application Protocol (WAP)-enabled phones with microbrowsers (such as the Nokia 7110) on a wide scale has resulted in predictions of massive growth in mobile commerce (mCommerce) through most major industry sectors. WAP includes a specification that implements options for authentication and encryption, both optimized for the limited-bandwidth mobile

environment. It provides end-to-end security for messages ensuring that information travels securely to the end user. The importance of a flexible security solution is clearly desirable and allows manufacturers of WAP gateways and WAP servers to differentiate their product offerings and provide solutions in lockstep with WAP specification changes (see Figure 3).

WAP provides an open universal standard for bringing Internet content and enables trusted end- to-end mobile e-business transactions. The growth of WAP-enabled phones and wireless PDA appliances will spawn a similar demand for WAP gateways and servers. The WAP forum (www.wapforum.com) has recommended wireless transport layer security (WTLS) and is based on SSL. WTLS is optimized for use over narrowband channels and provides data integrity, privacy, authentication, as well as denial of service (DOS) protection. Evolving specifications and security technology demand that the solution be flexible to deal with evolving standards.

Today, WAP server certificates can be purchased from a variety of companies. As the number of certificates issued rapidly increases, servers and gateways will increasingly require high-performance network security processors to offload the cryptographic processing function.

Processor evolution

As the Internet becomes the backbone for business-to-business and business-to-partner communications (extranet), the provision of effective security for sensitive systems, networks, applications, and data is critical. In the case of VPNs implemented over extranet environments, the need for efficient and flexible authentication solutions will escalate.

A new generation of converged firewalls/routers from companies such as Nokia and Lucent are set to displace traditional firewalls. In addition, new equipment rollouts are offering network-policy processing functionality that lets service providers define security, quality of service (QoS), class of service (CoS), class-based queuing (CBQ), network address translation (NAT), and packet-filtering options. The key function, one that has the most impact on CPU loading, is security processing.

In today's VPN-enabled router, an engineer will typically find first-generation network security processors that resemble early math coprocessors. These devices are successful in that network equipment vendors have been able to introduce products into the high-growth VPN arena. However

equipment vendors have been able to introduce products into the high-growth VPN arena. However, these vendors have discovered that the current network processor solution is not scaleable, does not offer high performance, and is certainly not programmable. Also, as packet processing and security processing become more tightly coupled, the need for a "flow through" topology must also be supported.

Security processing is essential to VPNs. However, the math-intensive computations have the most dramatic impact on CPU loading relative to other types of network processing. Packet routing, filtering, and proxy management consume far fewer cycles or CPU time compared with intensive 3DES operations. This additional processing can impose unanticipated bandwidth requirements. Both of these issues must be addressed in the next-generation network security processor (as shown in Figure 4).

Connecting to evolve

Security-enabled network equipment will continue to evolve as network security processing technology evolves. Three anticipated developments are hardware-enhanced firewalls, security-enabled edge equipment, and integrated security processing.

Firewalls and authentication systems are traditionally installed at the choke point in the network. When security is implemented, there is a reduction in traffic throughput.

Enhancing the security process is the key to maximum efficiency and throughput. Today, 50% of the firewalls installed in front of servers are software based. As VPNs cross the threshold from "nice to have" to "mission critical," software-based security will be unacceptable. Software-based security

chokes the server, causing severe delays. Integrating a hardware accelerator into the firewall can substantially reduce the delays.

For maximum efficiency, the firewall and router will become more closely coupled and will be designed as an integrated system. PCI-based modules and other boards employing early encryption as well as compression devices are used in first-generation integrated routers/firewalls. However, major concerns will arise:

- Is the system scaleable to provide security processing bidirectionally over OC-3 and above network interfaces?
- Is the security solution programmable to allow for complete flexibility as new standards are introduced and differentiating features are added?
- Can the system adapt to various network architectures such as "flow through" or "coprocessor" models?

Intregrated security processing

A high-performance network-security processing IC will provide the necessary form factor and cost to be integrated into enterprise communication equipment and access equipment. Although the number of simultaneous tunnels and maximum throughput for each tunnel is an important factor, the time to create and tear down tunnels will become a major issue as the number of tunnels for branch-to-branch and remote access increases. The integration of symmetric data encryption and asymmetric tunnel-negotiation algorithms on a single device provides a flexible solution.

New devices with built-in flexible processing for asymmetric algorithms used in authentication, combined with key management software, will enable thousands of tunnels to be set up and torn down on the fly. As the number of transactions and issuance of digital certificates increases, an increasingly higher-performance integrated solution is required (see Figure 5.)

A new class of network security processor optimized for the needs at the edge of the network provides the mandatory performance and combines a highly programmable and flexible architecture. Converged edge equipment that is now being designed demands a security processing solution that is programmable, scaleable, and high performance.

A highly programmable architecture enables the same device to be used across a range of platforms where the requirements can vary widely. This may be an important factor for customers who want to maintain a common security solution and minimize the impact of adding new algorithms or adopting new protocols.

Maximizing performance

Extensible RISC processors and multipath data architectures will be the keys to maximizing performance and throughput of security protocols. A RISC processor with enhanced instructions can perform complex cryptographic operations using one clock cycle. Conversely, although programmable DSPs are capable of running communication algorithms such as voice compression in real time, cryptographic algorithms cannot be run with the same efficiency using programmable DSPs.

When a public-key processor, a control CPU, and several optimized RISC devices are combined, symmetric and asymmetric algorithms can be executed simultaneously at very high speed. A device

symmetric and asymmetric algorithms can be executed simultaneously at very high speed. A device with these attributes will be able to perform bulk encryption (such as 3DES), hashing algorithms (such as MD-5), and public-key authentication at the same time. Add on-chip global memory, direct memory access (DMA), and two PCI buses to this mix, and the resulting system-on-a-chip (SOC) solution will be ideal for flow-through designs where network processors play a key role. Clearly, there are some obvious advantages to this converged functionality. However, what may not be obvious is that this same flexibility will also make the overall solution more physically secure, enabling system designers to easily meet Federal Information Processing Standard (FIPS) requirements.

Ideal product features

Architecturally, the following format is desirable for next-generation network security processors:

- Secret and public encryption processing on the same chip for converged security processing.
- Parallel processors using multiple embedded RISC cores with optimized cryptographic instructions providing maximum flexibility and performance.
- On-chip control CPU to minimize external component count and cost.
- Dual PCI 2.2-compliant 32-bit, 66-MHz PCI buses for flow-through implementation.
- PCI host and bus-mastering functionality to leverage the full potential of the security processor.
- On-chip global memory.
- On-chip PLL.
- Expansion port for external memory and storage of security associations.

To properly support the next generation of communication systems where flexibility and performance are required, the network security processor must be capable of the following:

- Supporting IPSec (3DES-MD5) or ATM encryption (3DES-CBC or 3DES counter mode) at full-duplex OC-3 rates (300 Mbps).
- Supporting bulk DES encryption up to Gigabit Ethernet rates.
- Supporting 80,000 security associations.
- Supporting public-key unit capable of up to 300 IKE SA setups/sec.
- Supporting multiple encryption algorithms, such as DES, 3DES, RC2, RC4, RC5, Diffie-Hellman, ECDSA (over GF(p) and GF(2^n)), ECC (over GF(p) and GF(2^n)), Esign, ElGamal, GSM A3, A5, and A8.
- Supporting multiple protocols such as IPSec (AH and ESP), IKE, MPPE, L2TP, SSL v2 and v3, TLS, SKIP, SMIME, SET, PPP DES, and 3DES.
- Conforming to AES requirements.

The next-generation network processor must also support a host of security features. These include random-number generation, battery-backed nonvolatile RAM (NVRAM) for optional secure boot, and FIPS 140-1 Level 3 security validation.

New approaches needed

New requirements are constantly challenging system architects to increase performance and reduce cost. As security features become increasingly important to customers, a flexible, high-performance network security processor must be designed in at an early stage in system development. Doing so will ensure that mission-critical equipment including routers, multiservice access switches, and Web switches will readily adapt to new protocols such as AES, ATM encryption, and evolving WAP standards. After all, e-commerce is more than networks. It encompasses end-to-end delivery of services over a dynamically changing network infrastructure where security processing is playing a growing role in the successful delivery of applications.

Illustrations

Figure 1
Figure 2
Figure 3
Figure 4
Figure 5

Stephen Davis is a system architect for Chrysalis-ITS in Ottawa, Ontario. Davis received his Bachelor's Degree in computer engineering from Carleton University in Ottawa. He can be reached at sdavis@chrysalis-its.com.

Mel Roberts is the director of IC business development at Chrysalis-ITS in Ottawa, Ontario. Prior to joining Chrysalis-ITS, Roberts was with Tundra Semiconductor for 2 years and Mitel Semiconductor for 16 years. He can be reached at mailto:mroberts@chrysalis-its.com.

Return to the Table of Contents