Building the 100% Encrypted Web

By Stephen Davis, P. Eng., Chief Architect, Chrysalis-ITS, Ottawa, Canada
iApplianceWeb
(09/26/02, 11:44:46 PM EDT)

Advances in silicon-based cryptographic and protocol accelerationtechnologies are allowing wire-rate Secure Sockets Layer (SSL) solutions to become a reality.

ASSPs (Application Specific Standard Products) are now available which support10,000 SSL session set-ups per second, utilizing an area of silicon of lessthan seven millimeters on a side. These products will off-load SSL processing,without imposing delays on other traffic in the same data path, requiring tight system integration and a detailed understanding of the SSL protocol.

But raw algorithmic performance without proper system design is wasted. Webswitches that currently provide 100,000 web (TCP/HTTP) transactions per second must be enabled to allow all of these connections to be encrypted with SSL, and web servers that currently slow to a crawl when SSL traffic is enabled must be accelerated back to pre-encryption speeds

Encryption performance can be addressed in two places: the web server and the web switch. Each platform presents different hurdles and thus different opportunities for introducing technological solutions.

SSL accelerated web servers are rapidly being replaced in high throughput sites with high-speed SSL accelerated web switches and unencrypted web servers. Chip level SSL acceleration solutions have evolved from single function, bulk encryption devices, suitable for simple web server acceleration, to integrated security protocol devices, suitable for high-speed web switch platforms. By making wire-rate SSL (Secure Socket Layer) possible, without affecting security or reliability, e-commerce sites will start to encrypt ALL web traffic.

Why Accelerate SSL?

Every time you connect to a web site from your computer you are using the Internet protocols TCP and IP to carry the commands and information typed into the browser across the Internet to the web server. When you enter a "secure" site, a new secure connection is established with the web server to allow information to be carried across the Internet, free from inquisitive eyes.

This secure connection use of SSL provides the security and data confidentiality lacking in standard Internet protocols. It is this additional protocol, SSL, which puts such an incredible load on the web server.
(The Basics of SSL)

Measurements performed on a Linux-based PIII-850 workstation, running Apache and OpenSSL show that performance will drop from over 2000 transactions a second for un-encrypted web pages to less than 200 when SSL is used. (These tests were run with 1K bytes pages, RSA key exchange mechanisms, RC4 encryption and MD5 authentication). The measurements were made on a web server that was not running CGI-scripts or database accesses. It is this performance degradation that must be eliminated to ensure that e-commerce vendors and other web site operators are free to provide secure access to any data on their site.

Analysis has shown that the raw processing requirements associated with 100,000 encrypted web transactions per second exceed 100,000 RSA-1024b operations per second and 10 Gigabits of hashing per second. These are two very different problems, with two very different solutions. The corresponding web pages and information transmissions associated with these ransactions could easily exceed 10 Gigabits per second, data that requires both encryption and hashing.

Hardware acceleration has long been identified as a mechanism for offloading the mathematically, and computationally intense cryptographic operations from the main CPU. It is possible to add additional processing capabilities to a web server to off-load the encryption and authentication operations, either on an add-in card on the system bus (typically PCI), or directly on to the motherboard.

Security Processors - A Little History

First generation cryptographic ICs have attempted to tackle the mathematically intense operations associated with the cryptographic algorithms used to secure SSL: RSA Private key decryptions, RC4 and 3DES for data encryption, and MD5 and SHA1 for hashing and authentication. Chips and boards were added to web servers and the web server CPU would make system calls to perform the various operations required by SSL.

The problem with these simple acceleration techniques is that the number of function calls, and thus the number of data transfers across the workstation bus, can become excessive. This offload can throw the optimized data flow of a workstation into disarray. In addition, these operations are typically non-blocking, introducing an added complexity into the optimized data flow of the SSL and TCP/IP stack. Recent attempts to combine encryption and authentication into a single hardware function call represent a move towards making the data transfers more efficient.

By forcing the CPU in the web server to move the data across the PCI bus to perform the cryptographic operations, the workload placed on the CPU is changed from mathematical operations to data moving operations. In some cases the acceleration provided by these first generation cryptographic

accelerators does not compensate for the extra overhead of the data transfer, actually slowing the web server down even further.

An alternative mechanism for providing increased performance in the web server is to install multiple non-accelerated web servers and load balancers to shift the traffic between these servers. Placing a web switch load balancer at the edge of the enterprise provides a virtual web server, at which, all web traffic can be directed.

This allows the web servers, which were previously able to provide 2000 transactions per second, to be ganged together in groups to provide many multiples of the reduced transaction rate (possibly as low as 200 transactions per second each), providing the ability to regain the previous performance levels of a single server. It is possible as well to make use of lower performance servers, each with SSL acceleration to provide the same level of web performance.

In order to properly load balance in front of the web server farm and to provide SSL session coherency it is necessary for the web switch to see un-encrypted traffic. This removes the need to have encryption in the web server and places the entire burden of the SSL encryption and decryption in the web switch. SSL traffic from the Internet is routed to the SSL Proxy by the web switch. The un-encrypted data stream is sent back to the web switch and is then load balanced and transmitted by the web switch to a specific web server.

Placed in front of a big enough server farm the requirements imposed on the web switch can easily exceed 100,000 new SSL Sessions each second, the capability to track 1,000,000 simultaneous SSL Sessions and data processing rates as high as 10 Gbits per second. This platform innovation is with driving force behind next generation SSL Acceleration ICs.

Security Processors - The Next Generation

In order to facilitate SSL cryptographic processing in high-speed web servers and SSL Proxy appliances, encryption ICs must become more intelligent and must take on a larger part of the SSL processing workload. ICs are separated at the high end of the performance scale into SSL Negotiation Processors (SNP, for the control path) and SSL Record Processors (SRP, for the data path).

The performance levels expected to be attained in the next two to three years are: 10K SSL Session Set ups per second (per IC); 10K RSA-1024bit Operations per second; ability to handle 512b, 1024b, 2048b, and 4096bit RSA, DSA and Diffie-Hellman operations; over 1Gbits per second of authentication (MD5/SHA1); support for over 1,000,000 Simultaneous SSL connections; over 2 Gbits per second of encrypted SSL Record Traffic; over 2 Gbits per second of RC4, 3DES or AES encryption; over 2 Gbits per second of MD5 and SHA1 authentication (including HMAC and SSL_MAC operations); and support for over 1,000,000 SSL Records per second.

In addition to performance, protocol support and function integration, security processing ICs will increasingly be distinguished based on cost, power and performance measurements such as transactions per second per dollar (TPS/$) and transaction per second per watt (TPS/watt).

These security processors (SP) must be tightly integrated into the optimized data flow of the web server, to ensure that the stated performance level can be attained. These SPs must also be tightly integrated with general purpose CPUs and network processors (NPU) to allow these systems to achieve the performance quoted above. Functions that will be implemented in the CPU and NPU devices will include: TCP Connection Negotiation; IP Packet Assembly; IP Packet Fragmentation; packet Classification (security protocol or not); and key Lookup (based on packet information).

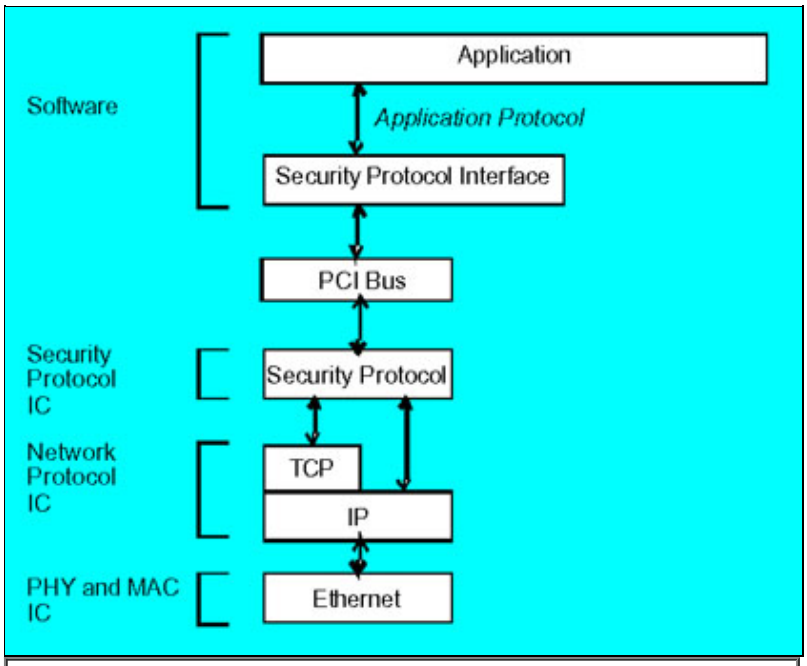

Figure 1: Moving SSL and TCP/IP to Hardware

Integrating SPs and associated CPUs along side network processing and routingICs, onto intelligent line cards, and other processing boards, turns security into a routing decision for the network processor.

Such next generation SSL Negotiation Processors (SNP) will provide all processing capability to negotiate an SSL Session (in association with a general purpose CPU), process the RSA Private Key operation required during the SSL Session set-up and provide the hashing capability to authenticate the packets as they are transmitted.

These chips will be separate from the record (data) processing capability and will likely act as a central resource in a system. Hence, there must be an optimized data path to get the SSL Records into the SRP and a separate control path to allow the distribution of keying information to the data path processors.

Depending on the speed of the interface to the web switch or server, the SNP can be co-located on a crypto-board with the SSL Record Processor (SRP) or placed in a central location in the system to act as a shared resource.

The SNP must be programmable to handle the various protocol versions and packet forwarding requirements. It should be able to act as a proxy, both in front of and beside a web switch, and as a simple cryptographic accelerator.

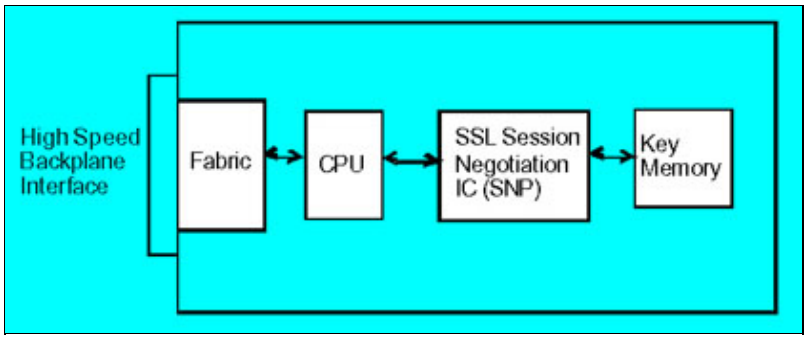

Figure 2: SSL Session Negotiation Board

The data path SSL Record Processor (or SRP) takes on an equally heavy workload,but a much different set of operations. Providing SSL Record encryption and decryption at speeds up to 10Gbits per second and supporting up to 1 million simultaneous SSL contexts requires tight integration with both the SNP and the data path components of the switch or server line cards.

On the line card the SSL Record processing IC will sit beside a network processor. The network processor will assume responsibility for packet classification and key lookups, before sending the packet into the SRP to have the SSL security layers added or removed.

To protect the keys forget software

Given dramatic technological advances being made in acceleration and packet processing architectures discussed above and allowing the concentration of more and more business-critical traffic onto single network nodes, key protection and integrity become an even more acute requirement. The use of hardware to protect critical keying data (especially a server's key used for SSL authentication) in any secure environment warrants mention.

The risk of storing keys in software and leaving them vulnerable to all kinds of attack should be understood by anyone considering setting up an e-commerce site, looking to increase performance of secured transactions, or rolling out a public key infrastructure. To truly bolster confidence in e-commerce, e-business and digital certificates, the underlying method in which digital keys are managed must include hardware protection.

Secure SSL processing boards can be architected, combining the technologies of SSL Negotiation ICs and SSL Record Processing ICs. Keying information is kept out of host systems and off the data path busses, increasing overall system security and preserving data integrity.

What Next?

As the technical hurdles presently preventing the use of 100% encryption are removed, what are e-commerce sites going to do once they can encrypt all their traffic? How will 100% encryption change the way the public interacts with the web?

Now that the technology innovations exist to make all this a reality, the e-commerce market can diversify the ways in which the web is presented, and deal with information in ways that have currently been unavailable.

For more information about the issues raised in this report, go to the iAppliance Web Views page and can call up the graphical Web map of the iApplianceWeb site and search for product information since the beginning of 2002.

For other technical articles, go to EETimes In Focus maps on the same Web page and browse or quickly search for all articles on a particular topic since the beginning of 1998.

These Web Maps can be browsed by date, by category, by title, or by keyword, with the results displayed *instantly either as a list of possible hits or with the specific Web page.*