Freescale Semiconductor Backgrounder

The Security Objectives of PowerQUICC™ Secure Communications Processors

Prepared by Geoff Waters, Freescale Senior Applications Engineer, Security Technologies
Freescale Semiconductor, Inc.

April 2004

Launched by Motorola
freescale
semiconductor

Table of Contents

1. Secure Internet Traffic: A Market Imperative

The demand for secure networks is growing at a tremendous rate. While there is almost universal agreement among analysts and other pundits that 5–10 percent of all Internet traffic is encrypted today, there are divergent opinions about the future growth of encrypted traffic. Some industry observers seem to be overly exuberant in their predictions that all Internet traffic will be encrypted by 2005[1]. More realistic estimates range from 25–30 percent by 2004 to more than 75 percent by 2007. These estimates include all types of encrypted traffic, including secure sockets layer (SSL), transport layer security (TLS), Internet Protocol security (IPsec), secure Multiprotocol Label Switching (MPLS), Internet Small Computer System Interface (iSCSI) and other protocols.[2]

However, there does seem to be some bias toward the amount of SSL/TLS traffic increasing more rapidly than other traffic due to the expected increase in e-commerce traffic (online banking, inventory management and health care).[3]

To meet the challenge of ensuring secure networks, many classes of networking equipment—such as virtual private network (VPN) routers, regional routers, wireless access points, radio node controllers and network attached storage equipment—must support security protocols. While encryption can be handled in software, secure communications processors (communications processors containing integrated security engines) provide an optimal solution for acceptable system throughput when encryption is a frequent activity.

[1] http://online.securityfocus.com/news/197
[2] http://cert.uni-stuttgart.de/archive/isn/2001/04/msg00129.html
[3] www.vnunet.com/News/1120794 Asynchronous Transfer Mode (ATM) cell.

2. Overview of Network Security Technologies

In network communications, the term “security” generally refers to the three related techniques for ensuring the authenticity, integrity and confidentiality of data transmissions.

> Authentication/Non-Repudiation—Ensures that the origin of a message or electronic document is correctly identified, with assurance that the identity is not false. Given irrefutable knowledge that the parties at the other end of the communications link are who they claim to be, a wide variety of services are enabled, including network access control, electronic signatures with non-repudiation, and negotiation of session parameters and secret keys for virtual private network (VPN) tunnels. Authentication/Non-Repudiation relies on digital signatures, which are based on Public/Private Key encryption algorithms, such as RSA and elliptic curve cryptography, often in conjunction with secure hashing algorithms such as Secure Hash Algorithm (SHA-1).

> Integrity—Ensures that unauthorized modification of information can be detected. Modifying includes writing, changing, changing status, deleting, creating and delaying or replaying of transmitted messages. Accidental modification of data can be detected by Cyclic Redundancy Checks (CRCs) and Transmission Control Protocol/Internet Protocol (TCP/IP) checksums, which are also integrity checking mechanisms. However, it is trivial for an attacker to intentionally modify a packet and recalculate the non-cryptographic checksums. True integrity relies on cryptographic checksums, such as secure Hashed Message Authentication Codes (HMACs), using MD-5 or SHA-1.

> Confidentiality—Ensures that the information is only readable by authorized parties. Confidentiality is synonymous with encryption. Commonly used encryption algorithms include DES, 3DES, Advanced Encryption Standard (AES), ARC4 and Kasumi (f8).

3. Differences Between Encryption Algorithms and Security Protocols

An encryption algorithm, such as 3DES, is used to render data unreadable to anyone who does not have the key to decrypt the data. Algorithms are agnostic to the type of data being encrypted, other than some requirements that the data be evenly divisible by a specific block size, even if it requires padding the data. 3DES can be used to encrypt anything from the entire contents of a hard drive to an individual Asynchronous Transfer Mode (ATM) cell.

Algorithms are agnostic to the type of data, but some “tuning” of algorithm characteristics can make them more appropriate for use in the various security protocols. There is no single standards body responsible for testing algorithms. However, the National Institute of Standards and Technology (NIST) holds considerable influence through its evaluation of algorithms for use within the Federal Information Processing Standard (FIPS).

Security protocols combine one or more algorithms to protect a communications link. Security protocols are designed to protect specific types of data and/or specific types of communications links. A protocol defines the portions of the message that will be encrypted, as well as the acceptable options for encryption algorithms. The protocol will also define the portions of the message over which the integrity check will be calculated, and how. Higher-layer security protocols can also define the mechanism used to establish the keys used to encrypt/integrity-check the message.

A great deal more “tuning” goes into security protocol development. Protocols are developed to provide the necessary level of security with the lowest possible overhead and to minimize interference with nonsecure protocols. Standardization of protocols occurs primarily through the standards bodies associated with a specific type of communications system. The Internet Engineering Task Force (IETF) is responsible for IPsec and SSL/TLS (Layers 3–4), while the Institute of Electrical and Electronics Engineers, Inc. (IEEE) manages Layer 2 security protocols such as 802.11i. Authors of IETF and IEEE standards may specify algorithms that do not have the NIST seal of approval, but they do so at their peril.

Although they are built upon such algorithms as RSA, 3DES, AES and SHA-1, security protocols ultimately provide authenticity, integrity and confidentiality of data transmissions. There is a large and growing number of security protocols in use today. This backgrounder cannot attempt to address security protocols in their entirety. Instead, the purpose of this section is to describe several layers of network security and relate them to functions used in secure communications and networking equipment.

Frequently Used Security Acronyms

AES	Advanced Encryption Standard
CCM	Counter Mode with CBC MAC
CHAP	Challenge Handshake Authentication Protocol
CPU	Central Processing Unit
CRC	Cyclic Redundancy Checksum
DES	Data Encryption Standard
HMAC	Hashed Message Authentication Code
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	Internet Engineering Task Force
iSCSI	Internet Small Computer System Interface
MAC	Message Authentication Code
NIC	Network Interface Card
RADIUS	Remote Authentication Dial-In User Service
SHA-1	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMPLS	Secure Multiprotocol Label Switching
SNMP	Simple Network Management Protocol
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/Internet Protocol
WLAN	Wireless Local Area Networks

`

4. Integrated Security: Addressing the Need for Secure Communications

Freescale Semiconductor* has more than 30 years of experience in data and communications security. Traditionally, the company has applied its security expertise and technology to customer and market needs through its systems divisions, providing end-to-end, secure communications systems to some of the most sophisticated users of encryption technology—defense and national intelligence agencies. In addition to the full communications systems produced for governmental customers, Freescale has applied its expertise in security technology to wireless handsets, wireless infrastructure, wired Internet networks, smart cards and cable set-top boxes. In 2000, the company brought its security technology and expertise to the commercial networking market with the introduction of the S1 family of network security coprocessors.

Designed to work seamlessly with Freescale's industry-leading PowerQUICC™ integrated communications processors, Freescale network security coprocessors continue to offer system designers an easy way to enhance the encryption and authentication performance of networking equipment.

Answering the market need for secure networks in concert with higher on-chip integration and lower system-level cost, the next logical step was to integrate scalable security engines into PowerQUICC processors. This technology development was predicated on the belief that integrated security engines will become as essential to communications processor architectures as on-chip floating point units and vector processing engines have become for high-performance microprocessors.

Because Freescale's PowerQUICC processors are used in so many different applications, it was important to provide a wider breadth of security protocol support than what is typically seen in alternative communications processor products from other vendors. In Q3 and Q4 2003, the company announced the integration of security engines (see Figures 1 and 2) into new PowerQUICC I, PowerQUICC II™ and PowerQUICC™ III secure communications processors. The scalable integrated security engines used in these PowerQUICC devices offer competitive features and are designed to reduce system bill of material (BOM) cost when compared to two-chip security solutions.

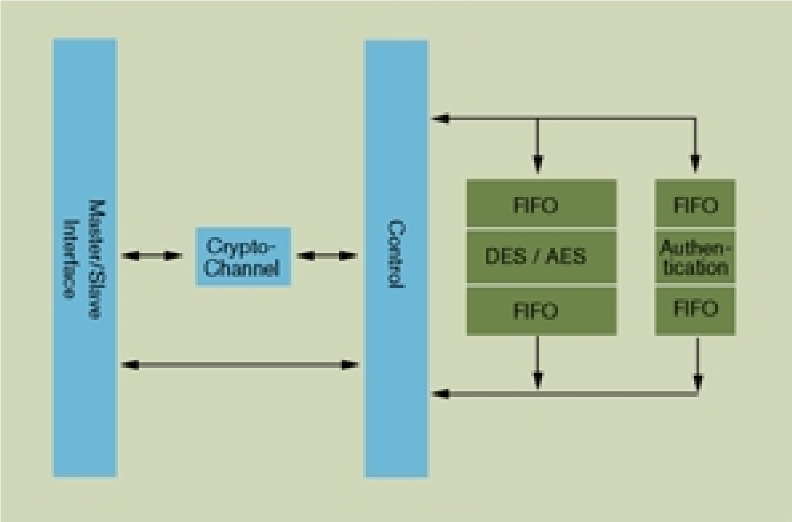

Figure 1: MPC885 PowerQUICC™ I Processor Integrated Security Engine

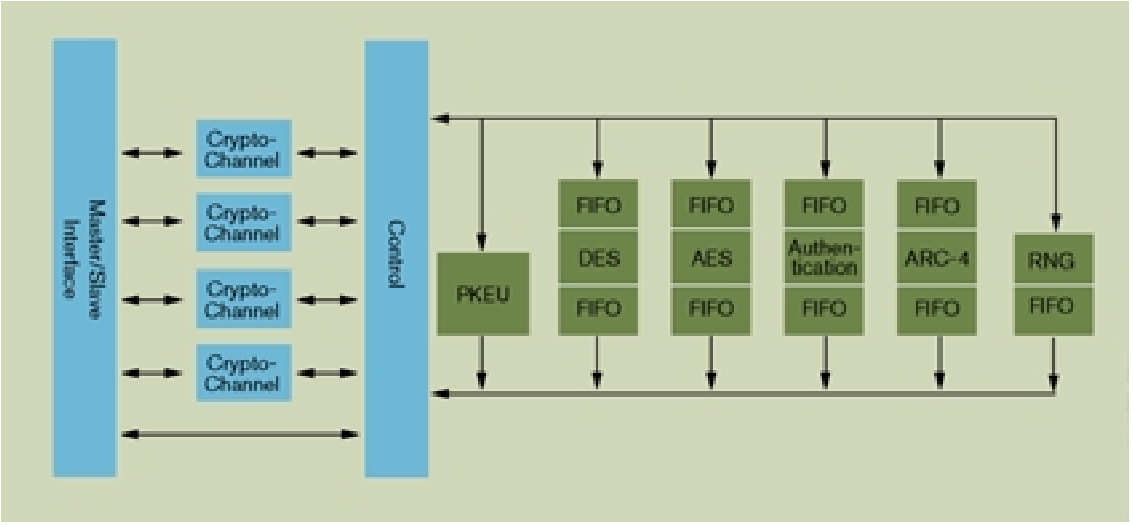

Figure 2: PowerQUICC II, PowerQUICC II Pro, PowerQUICC III Integrated Security Engine

5. Security Objective No. 1: Securing the Data Plane

The primary objective of PowerQUICC secure communications processors is to enable networking and communications equipment manufacturers and their customers to offer VPN services. Virtual private networks use IPsec to provide confidentiality and integrity for data as it travels across the public network—as if the two end-points (usually routers) were physically connected by a private point-to-point line. IPsec and other cryptographic security protocols are so effective that the greatest danger related to their use has been the reduction of throughput, which occurs in systems implementing encryption in software. If employees in a remote office formerly enjoyed T3 bandwidth of “clear” traffic, then see their bandwidth drop to 1–2 Mbps with IPsec enabled, there will be considerable pressure on the IT administrator to turn off IPsec. Systems built around PowerQUICC secure communications processors can expect to face less pressure to trade security for throughput.

While ensuring that the integrated security engine excelled at IPsec as commonly used today (3DES HMAC-SHA-1), Freescale has also looked into the future. The integrated security engine also supports AES, which is being incorporated into the IPsec standard, as well as the latest version of SSL/TLS. An emerging security protocol for voice and video, the Secure Realtime Transport Protocol, uses AES in Counter Mode, along with HMAC-SHA-1, which the integrated security engine supports. The wireless local area network (WLAN) security protocol, 802.11i, uses AES in Counter Mode with CBC MAC (CCM) mode to protect data between the wireless Network Interface Card (NIC) and the wireless access point.

While AES-CCM is implemented in some of the newer discrete IEEE® 802.11 MAC, the PowerPC® core’s ability to off-load the encryption functions to the integrated security engine is an attractive feature for PowerQUICC processor customers who prefer to run upper Message Authentication Code (MAC) functions in software, including Quality of Service (QoS) and security. Most versions of the integrated security engine are also capable of parallel security operations, meaning PowerQUICC II, PowerQUICC II Pro and PowerQUICC III devices can simultaneously process IEEE 802.11i traffic coming from a wireless interface while also processing IPsec traffic on a wired interface.

6. Security Objective No. 2: Securing the Control Plane

In addition to securing the data path, there is a growing requirement for control path security. Most network infrastructure uses the same physical connections for user data as control data. This means the control traffic is "in band," which has serious implications for security. Previously, control traffic was "out of band," meaning control information traveled on dedicated—and presumably secure—links. When out-of-band signaling exists, remote configuration of a router or server can only take place on that secure physical interface, and the other end of the link is known to be connected to an authorized administrator.

If separate physical links are impossible (satellites) or uneconomical (everything else), in-band control traffic must take on the characteristics of a physical link between the authorized administrator and the remote equipment. Strong encryption and authentication can satisfy this requirement. Control traffic can be tunneled through the data path via IPsec or SSL, and a control "port" in the remote equipment sees only the commands that pass through the secure tunnel termination point. Control traffic is not just between a network administrator and a control port of a router, though. Routers exchange significant volumes of routing table updates and other bindings; an attacker can also exploit this traffic if it is not at least authenticated. The addition of encryption to Simple Network Management Protocol (SNMP) (v3) and Session Initiation Protocol (SIP) is also a strong indication that the control plane will have a greater need for security acceleration in the future.

Failure to secure a control port with a secure link (physical or encrypted tunnel) undermines any security applied to the data path. Malicious outsiders, having failed in their attempts to read encrypted traffic, can attack the network infrastructure directly via an insecure control port and command the router to turn off encryption of user data.

Although control traffic is only a fraction of user data, the computational cycles taken away from the control plane of typical network infrastructure are sufficient to hurt overall system performance. Many of the same security features found in Freescale's integrated security engine are used in tunneling control traffic. Where differences between control path and data path security exist, Freescale has optimized the data path operations for maximum performance. However, the requisite set of functions has been included to provide a high degree of central processing unit (CPU) off-load in dealing with encrypted control traffic. In most versions of the integrated security core, control and data path security operations can be run in parallel.

7. Security Objective No. 3: Establishing Identity and Access Control

One of the first principles of security is to determine who can be trusted and what they can be trusted to do—and then ensure that is all they can do! Conducting background checks, setting up user accounts and providing physical access to the network are tasks best left to human operators since we are capable of synthesizing vast amounts of intangible clues into a feeling of suspicion or trust. Computers and networks do not comprehend "trust." They are programmed to process ones and zeros. In order for networks to block unauthorized users, access control software has been developed and deployed.

Access control software manages a database of user IDs and associated privileges linked to unique identifiers that each user must demonstrate possession of in order to be allowed network access. Unique identifiers may include:

> Passwords
> Smart cards and tokens
> Biometrics (fingerprint, voiceprint, retinal scan, etc.)
> Digital certificates (x509)

The majority of access control systems rely on password-oriented protocols, such as Challenge Handshake Authentication Protocol (CHAP), Terminal Access Controller Access Control System (TACACS) or Remote Authentication Dial-In User Service (RADIUS). When end-users attempt to gain access to the network, they supply their passwords to a PC-based access control client (i.e., RADIUS client), which hashes the password and transmits it to the RADIUS server. The RADIUS server (which may be a traditional server sitting behind other access devices or a server application running on a router) maintains a database of the hashed passwords and compares the received hash with the stored hash. If the hashes match, access is granted for the privileges associated with the user ID.

Most users can identify with the PC-based scenario described above. What is less apparent is the increasing number of access control operations occurring behind the scenes. Wireless NICs perform cryptographic authentication with wireless access points, while cell phones authenticate to the wireless network all the way through to the home agent. To meet service-level agreements for QoS, premium users must be identified to the network, and network nodes must communicate with each other to reserve the committed bandwidth. Unless premium services are made available for free, a great deal of accounting information will fly back and forth between the end user's system, a billing server and every node in between—all of it cryptographically secure—with a specific emphasis on non-repudiation. While most servers can manage a typical load of RADIUS authentications, the same number of digitally encrypted signatures will bring the system to its knees. For the nodes in between, CPU cycles spent encrypting and decrypting accounting and bandwidth reservation messages (or signing and verifying using Public/Private Key algorithms) will compete directly with traditional control functions.

Versions of Freescale's integrated security engines used in PowerQUICC II, PowerQUICC II Pro and PowerQUICC III secure communications processors offer Public Key acceleration and an on-chip random number generator primarily oriented toward secure session establishment via Internet Key Exchange (IKE). These same functions provide the basis for many access control protocols and for establishing trust between network nodes.

8. Conclusion

Encryption acceleration has gained mass commercial acceptance, fueled by the growth of the Internet and the need for secure transactions. As a market leader in hardware encryption and communications processing, Freescale is well-positioned to help drive network security through its existing families of security coprocessors and new PowerQUICC secure communications processors. After many years of working with industry leaders in embedded communications systems, Freescale understands the need for networking and communications equipment to have a long life in the field. The attention that Freescale has focused on the security requirements for data, control and AAA (authentication, access control and accounting) will make PowerQUICC processors an ideal choice for a wide range of communications systems, now and in the future.

*The Semiconductor Products Sector of Motorola, Inc. became Freescale Semiconductor, Inc. in 2004.