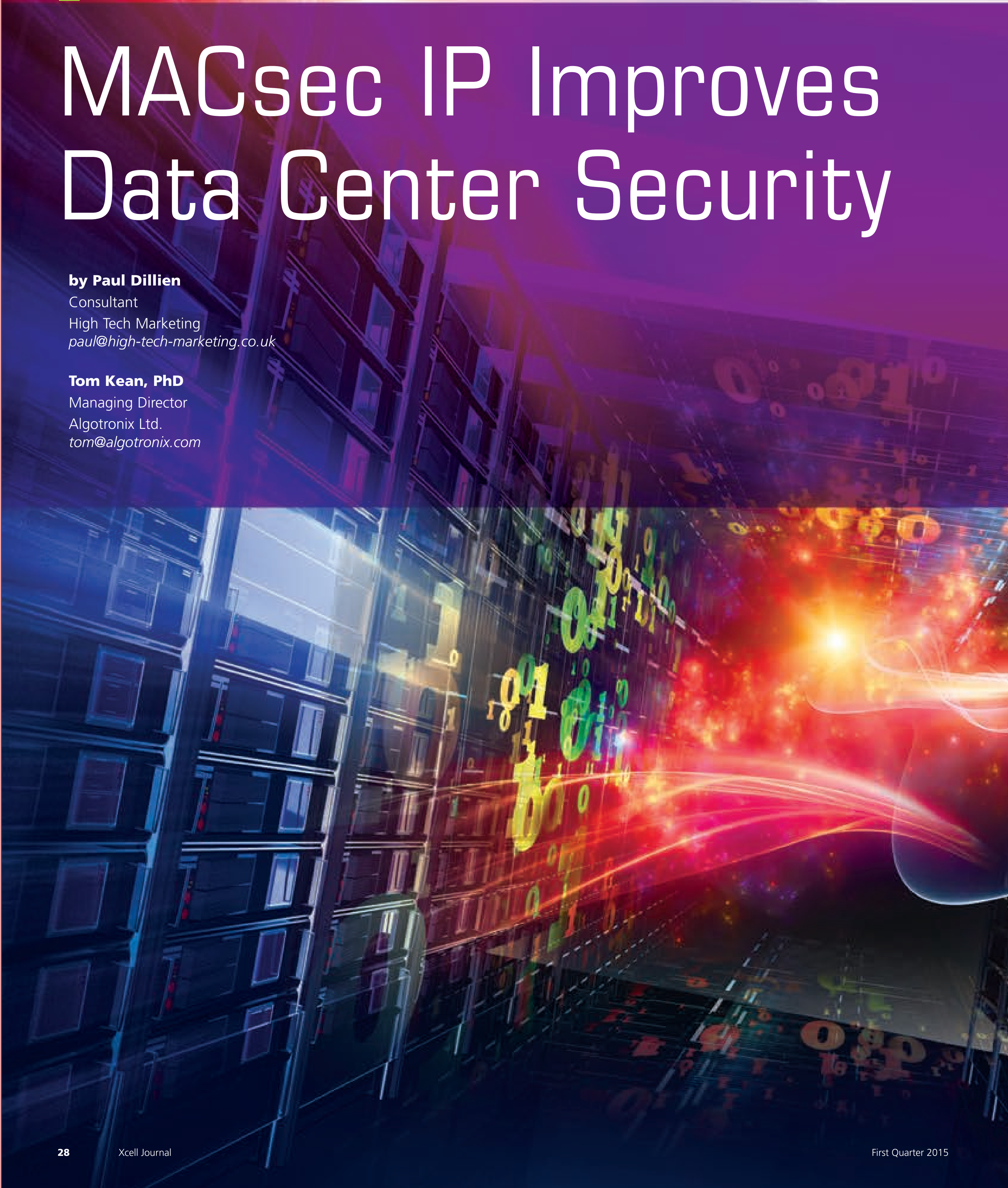
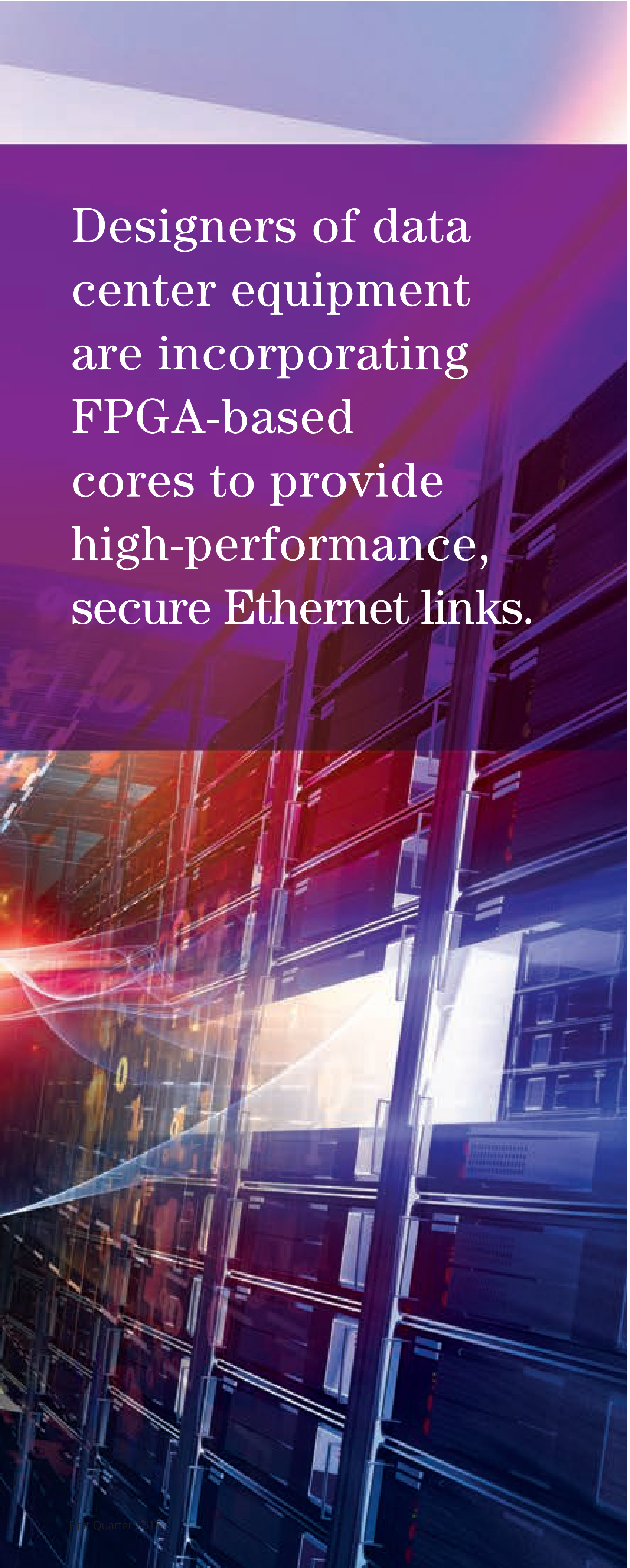


MACsec IP Improves Data Center Security

by Paul Dillien
Consultant
High Tech Marketing
paul@high-tech-marketing.co.uk

Tom Kean, PhD
Managing Director
Algotronix Ltd.
tom@algotronix.com



Designers of data center equipment are incorporating FPGA-based cores to provide high-performance, secure Ethernet links.

Cloud storage and the outsourcing of IT services hold a number of attractions for IT managers, because these options can save costs and reduce the support burden. But one big disincentive about allowing sensitive data outside a company's firewall is the concern about security. The hesitation is understandable, as information is one of the most valuable assets for many companies, whether it is accountancy, customer or manufacturing-related data.

But now equipment manufacturers can add performance and raise the bar on security with a Xilinx® FPGA-based solution. A comprehensive security subsystem from Algotronix, which meets the new Ethernet standard known as MACsec, uses a high-performance, low-latency and power-efficient intellectual-property (IP) core inside a Xilinx FPGA.

An FPGA-based solution is much faster than one based in software. In addition, the dedicated hardware offloads the system processor and frees it for other tasks, such as deep packet inspection. Alternatively, the designer could use a lower-cost processor.

ENCRYPTION AND AUTHENTICATION

An obvious tactic for protecting information is to encrypt data as it transits the network and moves around the data center. Encryption ensures that, should the data be intercepted by an unauthorized party sniffing the link, it cannot be read. Ideally, too, the data should be authenticated to ensure its integrity. Message authentication is designed to detect where the original encrypted data has been altered, either by means of a transmission error or from being maliciously tampered with by an attacker seeking to gain an advantage.

Ethernet transmission has grown to dominate communications because it is both efficient and extendable to high-speed transmissions. The popularity of the Ethernet standard has driven down costs, making it even more attractive, and this virtuous circle ensures the continuance of Ethernet as the Layer 2 technology of choice. However, up until a few years ago, the specification did not include any encryption, leaving the job to technologies such as IPsec that operate in the upper layers of the communications protocol stack.

Now, a new extension to Ethernet adds a raft of security measures, under the specification IEEE 802.1AE. Specified a few years ago, this technology features an integrated security system that encrypts and authenticates messages while also detecting and defeating a range of attacks on the network. The specification is known as the Media Access Control Security standard, or more commonly as MACsec, and Algotronix set out several years ago to produce

IP cores that provide hardware-accelerated encryption over a range of data rates. (Algotronix also supplies an intellectual-property core for IPsec that has a very similar interface to the MACsec product and would be a good choice in systems that need to support both standards.)

A brief overview of the MACsec system will serve to illustrate the comprehensiveness of the specification, as well as give an insight into the complexity of implementing it.

TRUSTED ENTITIES

The concept of MACsec is that nodes on a network form a set of trusted entities. Each node can receive both encrypted and plaintext messages, and the system policy can dictate how each is handled. The core includes a bypass option for plaintext messages, which are not authenticated or verified. Unlike protocols such as IPsec, which operates at Layer 3/4 and is an end-to-end technology, MACsec decrypts and verifies each packet whenever a packet enters or leaves an Ethernet LAN. MACsec is suitable for Ethernet topologies such as star-connected or bus-based LANs, as well as point-to-point systems.

The MACsec specification uses what are called Security Entities (SecY), an approach in which each node or entity has a unique key linked with its Ethernet source address. We designed the 1G variant of the core to support multiple virtual SecYs. As a result, a single Ethernet MAC can have multiple MACsec SecYs associated with it for applications like multiple-access LANs. MACsec typically works in conjunction with IEEE 802.1X-2010 or the Internet Key Exchange (IKE), which provides the secure key distribution around the network.

The reason that data centers might choose to use Layer 2 connectivity for moving packets inside the center is to achieve high speed with a minimum of latency and overhead data in the packet. By contrast, in communications using secure Layer 3 technologies such as IPsec, the message has to be passed up the stack for processing, with added latency.

A Layer 2 solution also eliminates the complexities of creating Layer 3 security policies. Data centers can adopt MACsec to provide protection behind the firewall or use it on direct links between data centers. The system administrator can authorize equipment to communicate in a secure fashion. The equipment can detect errors or misuse, such as attempted denial of service (DOS).

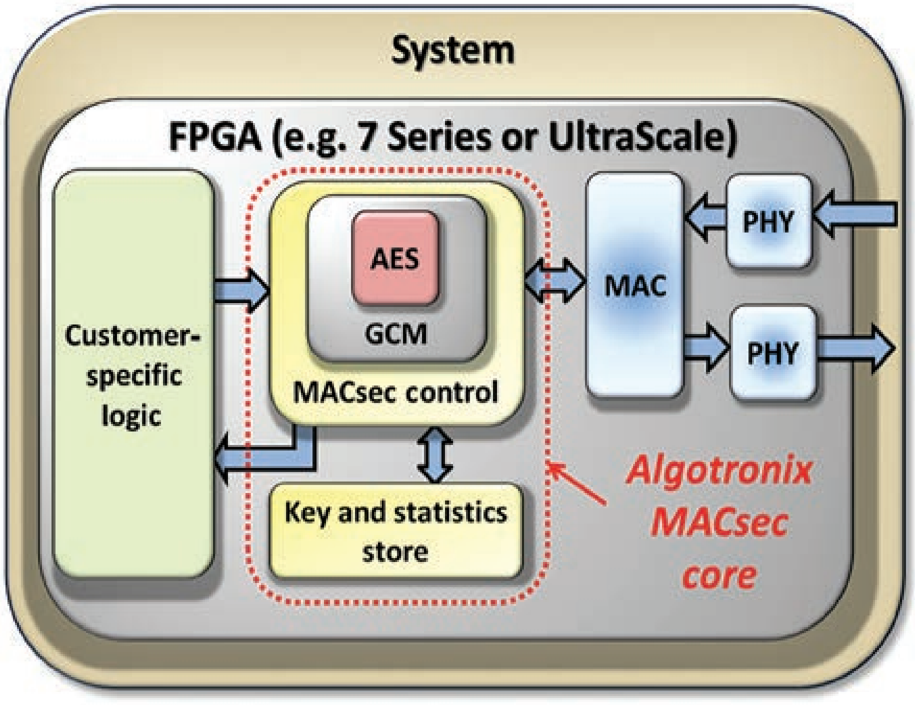


Figure 1 – The MACsec IP core sits entirely within the FPGA for maximum security.

PRIME FOR PROGRAMMABILITY

A customizable FPGA solution is ideal for MACsec, as the market is fragmented by differing requirements. Originally, MACsec was conceived as a technology to be applied to metropolitan-area networks, but it is now also finding use in data centers, which increases the overall demand for an FPGA-based solution.

It was a natural evolution for Algotronix to develop a MACsec core, because we had already created a range of crypto engines called AES-GCM. These cores operate at 1G, 10G and 40G. We achieved that speed by pipelining, increasing the clock speed and moving progressively from, say, Xilinx Artix® to Kintex® devices and then on to Virtex® FPGAs. We are adopting these techniques to push the throughput to 100G on Virtex UltraScale™ devices.

The performance we can achieve using an IP core in an FPGA is selectable to support anywhere from Gigabit Ethernet to 10 GbE (that is, the actual throughput through the core under worst-case conditions), with 40G and 100G versions planned. This is much faster than a software-based system could achieve. The cores are normally connected directly to the hardware MAC, as shown in Figure 1, because software on the embedded processor on the FPGA chip can struggle to transfer data fast enough to handle their throughput. If the security functions are implemented in hardware and additionally, unencrypted keys are never available to software, then the system is less vulnerable to common software-based attacks such as Trojan horses and viruses. This makes it easier to analyze for vulnerabilities than in a case where IT professionals must consider the entire software side of the system.

Another important consideration is the dramatic power saving in systems where FPGAs accelerate algorithms such as cryptographic functions that would otherwise be implemented in software. FPGAs are dramatically more power efficient than a software solution.

One useful attribute built into all Algotronix encryption cores is the ability to implement crucial blocks, called S-Boxes, in either Block RAM or in the lookup tables (LUTs) of the FPGA fabric. This option allows customers to squeeze the design into the available resources by trading off the two resource types, for example using Block RAM to implement the S-Boxes if the design outside of the MACsec core did not use BRAM heavily or LUTs if it did.

INS AND OUTS OF MACSEC

The MACsec system features the concept of each source of data using different encryption keys. When a message is received, the receiver looks it up in a list held in on-chip CAMs to determine the correct key to use to decrypt the packet. Each packet is also numbered to ensure that repeated or replayed packets can be detected and rejected, a technique that defends against “man-in-the-middle” attacks.

MACsec also collects statistics about the number of packets that are rejected and the reasons for rejection. Providing statistics to support detection of attacks is a further layer of security beyond the basic cryptographic privacy, authentication and replay prevention, allowing a system manager to proactively respond to an attack in progress.

We took the approach of “wrapping” the MACsec logic around the proven AES-GCM core. That said, designing an efficient and fast encryption core is only part of the design challenge. The MACsec specification is extensive and includes many variables. For example, the standard originally specified only 128-bit encryption keys. With 128-bit keys, the data undergoes 10 transformations (known as rounds) to complete the encryption process within the core. The standard was later revised to include an option for 256-bit keys, which have 14 rounds of processing through the encryption. This is achieved by adding pipeline stages and increasing the width of the memory used for storing the keys.

MACsec is agnostic as to the Ethernet traffic type, and it is transparent to higher-layer protocols. With the introduction of these cores, it’s easy to add MACsec to systems to provide an additional layer of protection in a network. Sites equipped with MACsec can still communicate with other sites, but without the extra security of MACsec.

Ethernet packets are fed to the MACsec core from the media-access controller (MAC). You can build a compact and efficient solution using, say, the 1G MACsec core in conjunction with on-chip transceivers and a trimode Ethernet MAC (TEMAC). Each of the packets contains the destination and address of the source that initiated its transmission. This standard is retained in a MACsec system, but an important aspect is that in a multihop transmission, the “source” will be the address of the last equipment to forward the packet. So, unlike IPsec—which can be considered an end-to-end scheme—MACsec works on a hop-by-hop basis. For each hop, MACsec requires that all encrypted data on the ingress is decrypted and then re-encrypted with the unique key assigned to that equipment for forward transmission. The decrypted plaintext allows the option for packet inspection at each stage, as illustrated in Figure 2, and can be used by traffic managers to regulate the flow of data.

In the MACsec standard, the header shown in Figure 3 includes an additional field known as the MAC Security TAG (SecTAG), which defines the EtherType and flags whether the packet is encrypted or not. Authentication is achieved by appending data to the end of the message in a field called ICV. The ICV works with the encryption key to authenticate the frame, including the header and MACsec tag, to ensure that not even the source or destination address of the frame could be manipulated. We implemented this logic in the FPGA fabric to ensure that it would have fast and predictable timing to minimize any latency.

The MACsec core includes a lookup table that is linked to each source address. The table includes the key that needs to be used to successfully decrypt the message, and we designed this feature to be implemented efficiently in the LUTs and Block RAM on the devices. We exploited the flexibility of the FPGA solution by designing the core with implementation options such as a choice between 128- and 256-bit keys and the ability to vary the number of virtual SecYs that the core supports.

Another useful feature of the new standard is the collation of statistics by MACsec at the packet level. The system administrator can, for example, see how many packets were rejected because they were delayed, failed integrity checks due to an invalid decryption key or used the wrong key, and compare those statistics with the number of correct packets transmitted.

The MACsec standard has a simplified option for point-to-point applications. This eliminates the need for a CAM to determine the key from an explicit Secure Channel Identifier in the packet and an option for point-to-multipoint operation. Our core also supports multiple virtual SecYs associated with a single Ethernet so that different keys can be used to encrypt data transmitted from that MAC to different destinations. The MACsec standard defines this kind of configuration as a multi-access local-area network, since it is as if the destinations were on different Ethernet LANs. This feature allows the system to partition the receiving equipment by encrypting the output with different keys.

A data center might use multiple SecYs to create a virtual division so that data from Customer A is partitioned

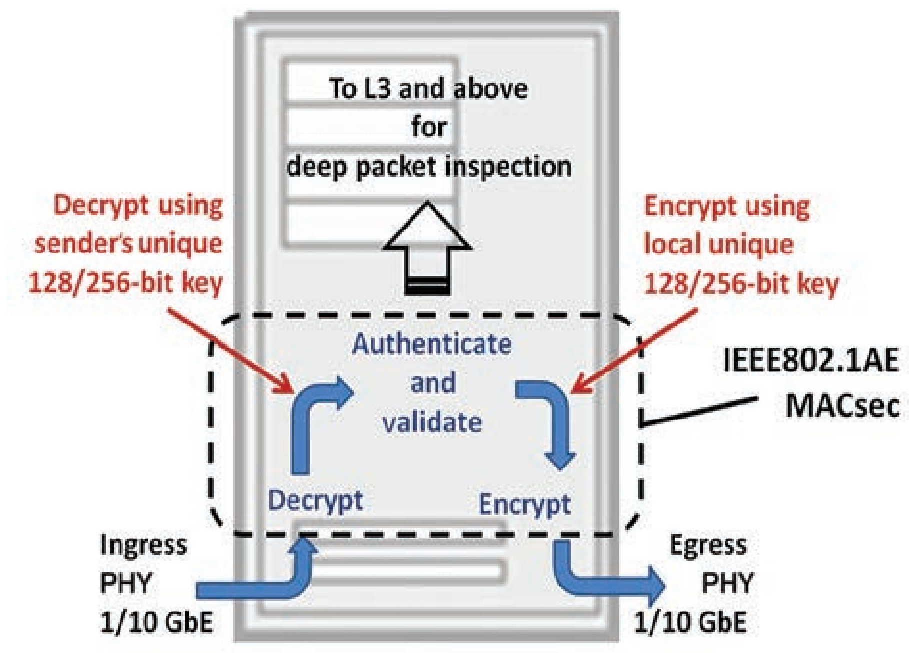


Figure 2 – The message is decrypted on the ingress port and encrypted on the egress port.

from that of Customer B by virtue of a unique encryption key. Communications internally in a data center could, if required, be organized to segregate selected racks to provide virtual isolation areas. This capability can address data integrity and separation concerns in data center and cloud applications. Whether from an accidental wrong connection or a malicious act (see Figure 4), the MACsec system will detect packets that are unauthenticated and the system administrator can set the policy to quarantine or delete them.

All data encryption and decryption are performed at the port level. Apart from the additional MACsec header and small added latency, there is no overhead or performance impact when turning on port-level encryption.

Equipment vendors can use these cores today to differentiate their systems by incorporating an encrypted Ethernet Level 2 scheme compliant with IEEE 802.1AE. Cloud-based users, who may be mutually suspicious of other customers, can benefit from the confidentiality and data source authentication MACsec offers for added reassurance that their data is protected. Equipment manufacturers have a choice of IP cores that are available to cover the needs of 1- and 10-Gbit Ethernet throughputs. The architectural design makes it easy to achieve 10 Gbps in Kintex or Virtex FPGA devices. The design supports both jumbo frames and minimum-size packets with a key change on every packet. This scenario represents the worst-case situation for the system. The cores comply with the full specification, and each MACsec core can support a range of popular FPGA families.

COMES WITH SOURCE CODE

Algotronix takes the unusual step of supplying the HDL source code for every core licensed. The main motivation is to allow customer inspection so as to prove that the code has no virus or Trojan code incorporated, and that it cannot be forced into unauthorized states or operations. Having the source code therefore reduces the cost and complexity of a security audit for customers. In addition, the source code speeds up the design process, because engineers can easily experiment with configuration variables such as encrypt, decrypt or encrypt/decrypt and with key length, and can see the state of signals within the

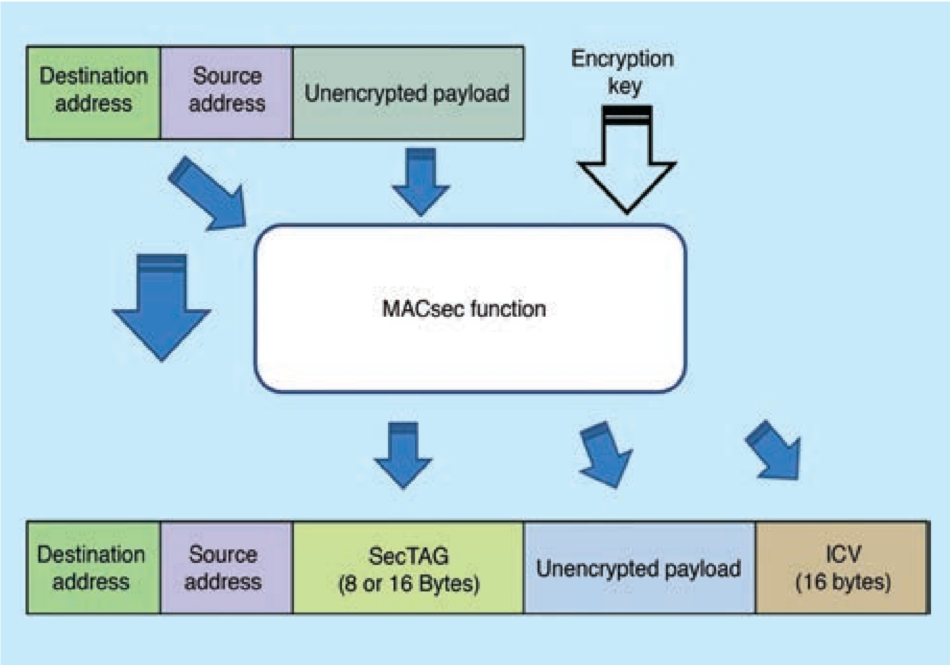


Figure 3 – The MACsec frame structure includes a field known as the MAC Security TAG (SecTAG), which defines the EtherType and flags whether the packet is encrypted.

core in their own simulations. You can configure the cores for high throughput by implementing a wide data path or for minimum FPGA footprint by selecting a narrow data width. Further benefits of having source code are that it is easier to understand the operation of the core; that makes documenting and archiving easier and quicker.

An extensive verification testbench is also included, allowing customers to confirm the correct operation in tools such as ModelSim. The testbench includes a behavioral model of MACsec and a self-checking version of the MACsec IP core where the outputs of the synthesizable hardware are checked against the behavioral model. This self-checking design can be instantiated in user simulations, making it easy to test the core in the context of the actual user design and providing useful diagnostic messages if it is driven incorrectly.

As there are so many options available in the core, the precise resource count will depend on your choice of parameters such as data rate, key length and number of SecYs selected, among others. However, the 10G MACsec core listed on [the Intellectual Property section of the Xilinx website]() uses 6,638 slices, 20,916 LUTs and 53 BRAM blocks. Contact Algotronix for licensing options.

The combination of low-power Xilinx FPGAs and the Algotronix MACsec core offers a high-performance and low-latency solution for equipment manufacturers to differentiate their products. The security features allow data centers to assure their customers of confidentiality, while also enabling security administrators the ability to detect and defeat malicious acts.

Figure 4 – MACsec will reject packets that arrive via wrong connections, either accidentally or maliciously.