Securing LTE Backhaul with IPsec

Introduction

The mobile network has grown and changed radically from its origins in the early 1980s as an infrastructure designed to deliver commercially available, portable telephony service. Evolving rapidly over the past three decades from first- to fourth-generation technology and from voice-only to multimedia and Internet access services, the mobile network had, by December 2011, achieved a global penetration rate of 87 percent. According to the International Telecommunications Union (ITU), the worldwide mobile network now supports about 6 billion mobile-cellular subscriptions, and its 1.2 billion mobile-broadband subscriptions around the world outnumber fixed-broadband subscriptions by two to one. Furthermore, according to mobithinking.com, a compendium of mobile statistics and research, mobile devices within the next five years will overtake the personal computer as the most popular way to get on the Web.

Despite the rapid growth in the mobile network in general and the mobile Internet in particular, one characteristic remained constant, at least until the mid-1990s: there was no standard, widely-deployed method for securing mobile Internet-based communications against attacks by hackers and other unauthorized users. As more and more individuals, enterprises and governments began to rely on mobile-broadband services, providing secure communications over the IP-based network became an increasingly complex challenge.

Over the last few years, the industry has produced several mechanisms to tackle the mobile network’s security problems, but most of these, such as the Secure File Transfer Protocol (SFTP) and Transport Layer Security (TLS), are application-specific. And, because they operate at the higher layers of the Open Systems Interconnection (OSI) protocol stack, they cannot protect all Internet-based communications.

To provide end-to-end security that operates at the packet-processing layer to protect the network and higher-layer applications, the Internet Engineering Task Force (IETF) has defined a suite of security protocols, collectively known as Internet Protocol Security or “IPsec.” Capable of securing communications on a host-to-host, network-to-network and network-to-host basis, IPsec basically authenticates and encrypts each IP packet within a communications session.

Since the emergence of the first version of the IPsec standard in 1995, its use has been optional for IPv4-based traffic. Citing the complexity and cost of IPsec configurations, many operators have chosen to implement proprietary VPN solutions instead.

However, two developments now underscore the need for widespread IPsec implementation: the roll-out of IPv6 standard, which mandates the use of IPsec, and the roll-out of LTE networks, which present numerous security concerns.

As mobile operators around the world deploy LTE technology to provide higher data-throughput rates and reduce costs, they recognize that its IP foundation and its architecture, compared with that of 3G networks, make the backhaul network and mobile core more vulnerable to attack. Consequently, a backhaul solution with IPsec is a critical component of their network-evolution strategies. In addition, operators especially need an IPsec-capable solution that is cost-effective to implement and easy to configure and use.

Overview of IPsec and Its Capabilities

As part of its efforts to develop IPv6, the IETF defined the IPsec protocol suite to defend against security threats. Such threats include data theft and corruption; network-based attacks; theft of user credentials; and unauthorized administrative control of the network and network servers.

Using the flexibility built into the IPsec standards, two or more IPsec-capable network elements can establish a secure link between/among themselves. This is done by determining the specific security protocols they will use to communicate and the specific algorithm they will use to encrypt the data. Based on these choices, they exchange the “key” necessary to decode the data, and then transmit/receive the information.

The IPsec protocol suite comprises two core mechanisms, which are headers inserted into the IP datagram to encode information, and three support components, which enable the core mechanisms to function properly.

The core IPsec protocols required to provide traffic security are:

The Encapsulating Security Payload (ESP), a vital component of LTE backhaul operations, encrypts the IP datagram’s payload to protect the privacy of that information; IPsec-compliant equipment must support ESP. For cases in which operators use ESP without encryption to provide authentication service only, the Authentication Header (see below) is redundant.

The Authentication Header (AH), which is not required in LTE backhaul operations, verifies the origin of an IP datagram, as well as its integrity to ensure that no devices between originator and recipient have altered that datagram. The AH also protects against “replay” attacks, in which an attacker fraudulently captures and repeats or delays a valid data transmission.
The three primary IPsec support mechanisms are:

1. **Encryption/Hashing Algorithms** - used by the AH and the ESP to specify the encryption mechanism.

2. **Security Association (SA)** - a connection that provides security services to the traffic riding on it. The standard defines two types of SAs: tunnel mode and transport mode. Operators typically use a transport mode SA between a pair of hosts to provide end-to-end security. But, if either end of an SA is a security gateway, the IPsec standard mandates use of the tunnel mode SA. This applies in LTE where the IPsec gateway is an intermediate device, thereby requiring a tunnel to route traffic to the gateway first. The IPsec tunnel's IP header uses the IP address of the IPsec gateway as the destination address.

Operators also must determine whether both user traffic and control traffic require IPsec protection. Because the IPsec tunnel “sees” the S1 control stack as similar to the S1 user stack, an edge switch operating as the IPsec gateway can use its virtual routing and forwarding (VRF) function, along with the transport layer IP address, to route the control traffic to the Mobile Management Entity (MME). Consequently, IPsec, by simply using a single security association, can protect both user and control traffic.

3. **Key Exchange Framework** - IPsec uses cryptographic keys, along with mechanisms for putting these keys in place. Although leading IPsec-compliant solutions support both manual and automated distribution of keys, many LTE operators prefer the latter because there may be hundreds of eNodeBs for each gateway. IPsec-compliant solutions support the Internet Key Exchange v2 (IKEv2) protocol for automated management of public keys.

**History and Development Status of IPsec Standard**

As part of its development work on IPv6, the IETF in 1995 published the first set of IPsec protocols, in RFC 1825 and RFC 1829, and followed up three years later with newer versions, RFC 2401 and RFC 2412. The IETF then published in late 2005 its third version of IPsec standards, RFC 4301 and RFC 4309, along with the second version of the IKE standard. IPsec maintenance and extension efforts are the responsibility of an IETF working group which was established in 2008.

As noted earlier, the IETF, when developing IPv6, mandated that all standardized implementations of IPv6 include IPsec support. Because the industry only now is beginning to deploy IPv6, operators and their vendors have been using IPsec over the last few years to ensure the security of IPv4 traffic, for which IPsec support is optional.

**IPsec Addresses Security Issues within LTE**

Backhaul security requirements in the LTE network differ from those in 2G and 3G networks. For one thing, LTE’s basic goals – high data-throughput rates, improved spectrum efficiency, reduced latency, improved coverage and packet-based support for multiple radio access technologies – are driving the evolution of the mobile network to a more efficient, all-IP infrastructure; that includes the backhaul transport. IP-based transport is more open and therefore more vulnerable than 3G transport.

Next, operators usually implement security in their 3G networks by encrypting traffic that flows between the subscriber equipment and the radio network controller (RNC) – which is installed in a so-called “trusted” environment, such as a secure building.

By contrast, in LTE air interface security (encryption) measures are terminated at the base stations, or eNodeBs, to protect traffic between the subscriber device and these network elements. However, they often deploy eNodeBs in publicly-accessible locations and, in an effort to increase network capacity, deploy femto cells in equally accessible areas, such as airports and shopping centers, where it is nearly impossible to protect the active electronics. The result is that traffic between the eNodeBs and the core is not protected, a situation made worse by the fact that LTE’s “flat” architecture eliminates the RNC, leaving the cell-site path to the core wide open and eNodeB-to-core traffic even more vulnerable to attack.

Finally, 3G’s architecture typically links each node with a single RNC. However, LTE’s architecture, according to the Next Generation Mobile Networks (NGMN) Alliance, potentially enables each eNodeB to support up to 32 X2 interfaces (meshed with other eNodeBs) and up to 16 S1 interfaces to the core network. As a result, many more elements in an LTE network are vulnerable to attack than in a 3G network.

Clearly, operators must implement IPsec in their LTE networks if they expect to provide secure connections that protect the mobile core, neighboring eNodeBs and the radio access network (RAN) transport.

Although IPsec is a proven technology, operators and their vendors thus far have been reluctant to implement it on a widespread basis because of the cost and complexity of IPsec-compliant equipment, as noted earlier, and the resulting increase in operational costs.

Further, IPsec creates additional delay and overhead. If all the traffic is encrypted, the IPsec tunnel header overhead is estimated to be about 15 percent of the total overhead. These factors underscore operators’ need for a solution that not only ensures secure connections but also is cost-effective and easy to deploy and manage.
Different Backhaul Topologies, Different Security Requirements

Operators implement their backhaul networks in various ways, depending on their choice of physical infrastructure. Fiber connections and microwave links are the most typical physical layers, with IP/MPLS technology deployed on top of the physical infrastructure. Compared with pure IP, MPLS provides better traffic management and isolation.

Because the S1 interface is based on IP, it is vulnerable to attack, so operators need a solution that can secure the S1-U (eNodeB to core gateway) and S1-C (eNodeB to MME) interfaces. With eNodeBs implementing IPsec functionality, IPsec tunnels from those S1 interfaces can terminate at a compliant edge-switch solution deployed at the former RNC location.

It is important to note that in their initial deployments of IPsec, operators are likely to put security gateways at centralized locations within the mobile network, where they would function as standalone devices providing dedicated security functionality via connection to transport devices. Eventually, however, the growing need for a more distributed architecture will prompt operators to deploy IPsec in a more distributed fashion as well, that is, as a functionality integrated with the transport devices. Because of the greater number of locations requiring IPsec and the resulting management effort required, distributing IPsec functionality will make more sense from both an economic and operational perspective.

LTE’s X2 interface between eNodeBs can be either clear text or protected by IPsec. When choosing to protect X2 traffic, leading operators prefer not to create SAs between eNodeBs but instead route that traffic through an advanced platform’s gateway. This simplifies IPsec usage and requires only one pair of SAs from each eNodeB. If X2 is clear traffic, it does not need to go through a gateway.

The following illustrates backhaul connectivity implemented with full-mesh IP VPN.
The IP VPN model also enhances the security of the backhaul infrastructure itself because the interfaces to the IP VPN have IP connectivity only to the security gateway. The IP VPN routing inherently blocks access to IP addresses associated with infrastructure outside the IP VPN.

Creating a separate routing domain for backhaul, VRFs route IPsec tunnels at the untrusted part of the backhaul. A default routing table also can route the IPsec tunnels, which is a simpler but less isolated solution, as shown in the following illustration. In this approach, the IPsec tunnels are used as attachment-circuits to VRF at the IPsec gateway.

To reduce the number of required processing resources, operators may choose to implement only authentication, leaving traffic encryption to the users. If concerned about security, users may handle encryption tasks themselves.

Further, operators may implement IPsec to protect only the most untrusted cell sites and rely on physical protection mechanisms for the other cell sites. In addition, they may need to establish IPsec SAs according to QoS class; different traffic classes typically experience different delays, which can lead to packet discarding by the IPsec anti-replay mechanism. Operators must take this into account when defining their IPsec scalability requirements.

Advanced Solutions Evolving to Support IPsec

Advanced backhaul solutions already feature a broad set of IP/MPLS, multiservice and Ethernet capabilities. Operators can expect to see new versions of these edge and access platforms that provide the IPsec capabilities, such as mandatory support for ESP, which secure LTE backhaul requires. With protection of the S1 interface as its primary purpose, a new platform version clearly must be interoperable with eNodeB.

This platform version integrates IPsec gateway functionality with the existing router/switch and thus supports the tunnel-mode SA, as mandated by the IPsec standard for security gateways. Further, because the existing router/switch is expected to be typically deployed at the site of the former RNC, its integrated IPsec gateway functionality is ideally located for IPsec termination in a distributed architecture.

This integration-and-deployment strategy reduces operational complexity and equipment cost and, by combining the enhanced platform with the appropriate network management system, operators can provision and monitor IPsec functionality in their LTE networks quickly, easily and cost-effectively.

The enhanced platform implements IPsec by means of a high-capacity line card which operators insert into the line-card slot in the router chassis. Featuring a high-performance processor for IPsec processing, the line card supports directly high speed Ethernet interfaces.

With the edge switch deployed at the location of the former RNC, the new line card can deliver the required scalability. If, on the other hand, operators have deployed the edge switch higher in the network, where greater scalability is required, they can install a second pair of line cards in the system chassis.

See tellabs.com for more information about Tellabs Solutions
Operators deploying this enhanced platform can build in equipment redundancy by creating a link-aggregation group across two of these line cards. Other load-balancing mechanisms can be used as well. The load-balancing algorithm that is used must ensure that all the packets in one IPsec tunnel are routed to the same line card. If a card or interface fails, all the IPsec tunnels are switched to one line card.

Acknowledging that IPsec functionality causes additional delay, leading vendors are designing their enhanced platforms in ways that guarantee their IPsec implementations will not break operators’ delay budgets for various applications. Equally important, these vendors are ensuring their platforms will scale quickly and cost-effectively, enabling operators to break open even critical bottlenecks such as the number of IKE exchanges per second.

Conclusion

Enterprises, government agencies and individuals around the world today rely on the mobile Internet to carry their business and personal communications. Indeed, the mobile Internet has become a vital component of the world’s infrastructure and, like all other forms of infrastructure, it and the information that rides on it, must be protected from attack. Nowhere is this more critical than in the backhaul segment, with its open Ethernet and IP interfaces and protocols.

Fortunately, end-to-end protection is available in the IETF IPsec standard and, as required by the latest version of the Internet Protocol, vendors must implement IPsec capability in their platforms to comply with IPv6 requirements.

Equally important, more and more mobile operators around the world are evolving their infrastructures, including their backhaul networks, to IP-based technology and launching LTE services. The architecture of LTE, combined with the open nature of IP, make LTE networks far more vulnerable to attack than their TDM-based predecessors. The security challenges presented by LTE are prompting operators to seek advanced backhaul platforms that provide IPsec protection.

Such platforms must be cost-effective, both in terms of capital expenditures and operating expenditures, and they must be easy to configure and use.

For operators that already have deployed an advanced backhaul solution, implementing IPsec functionality only requires a new line card or intelligent software for the edge switch or access switch. Operators that are still evaluating a backhaul solution now have the option of investing in a cost-effective platform that protects LTE backhaul traffic and simultaneously supports 2G and 3G operations.

In both cases, this type of backhaul solution, enhanced with IPsec capabilities, enables operators to secure not only their networks and the traffic riding on them but also their own long-term success in the competitive marketplace.