INFONETICS RESEARCH

INFONETICS RESEARCH WHITE PAPER

Security at the Speed of VoLTE

Infonetics Research White Paper
Written by Principal Analyst Stéphane Téral

February 2014

Contents

“The security gateway provides both high security and QoS control to the LTE network.”

Executive Summary

2013 ended with more than 6.5 billion mobile subscribers worldwide, of which 175 million are LTE subscribers and 8 million VoLTE subscribers, most of them (90%) in South Korea. This faster than anticipated migration to LTE opens the door to malicious (e.g., hacking) and non-malicious threats (e.g., signaling traffic storms). Good old PLMNs (public land mobile networks) are super secure because they have their own backhaul physical infrastructure with dedicated leased lines (T1s in the US, E1s in Europe; the majority of E1s in Europe were and still are on microwave), making the overall network extremely difficult to hack. Three fundamental factors are making LTE networks more vulnerable than old PLMNs:

- The flat IP architecture that directly links the cell site to the packet core
- The addition of small cells that further increases the number of potential access points
- The rising popularity of network sharing between several mobile operators

Consequently, security must be a foundational element of LTE network deployments. Although IPsec encryption was defined as the key mechanism by the 3GPP and the NGMN Alliance, its optional implementation has resulted in sporadic deployments with less than 20% of mobile operators worldwide having it in their LTE network. The main caveats are the use of private backhaul considered “trusted” by the operator, an increased computational impact on eNodeBs, and a bigger overhead at Layer 1 transmission, which translate into additional costs. Though US and South Korean operators have been slow to embrace IPsec, European and Latin American mobile operators have made it a mandatory component of their LTE rollouts.

As IPsec adoption for transporting LTE flows continues to grow significantly, the need for a security gateway, which has been considered optional by many operators, increases. As defined by 3GPP/S1 interface, its fundamental function is to perform authentication and encryption/decryption for the IPsec tunnel, and handle IKEv2 authentication to secure the delivery of voice and data services. Given the pace of LTE adoption worldwide, the security gateway needs to be highly scalable to manage hundreds of thousands of concurrent IPsec tunnels.

And finally, the security gateway needs to be tactically deployed to do more than perform IPsec encryption and decryption. By placing it at the RAN-EPC edge, it needs to efficiently process small VoLTE packets—64 bytes—in networks that are generally optimized based on the median packet size of 512 bytes or IMIX distribution, and manage potential data-, application- or VoLTE-induced signaling storms. As a result, the security gateway provides both high security and QoS control to the LTE network. Traditional approaches such as firewalls aren’t the same as security gateways unless they meet a stringent set of criteria that meet the scalability, low latency, and security requirements of an exponentially growing data and voice network, a far different scenario from enterprise.

“An S1-focused security gateway can not only perform IPsec encryption and decryption, but can also process small VoLTE packets and protect the EPC from overwhelming signaling traffic.”

Introduction

More than two decades of history in the mobile industry teach us that good old PLMNs (public land mobile networks) have been resilient and highly secured, based on the single fact that a major event has never occurred. All PLMN outages thus far have directly resulted from equipment failures and software bugs; none of them was linked to a malicious attack.

As the world moves to LTE at a faster than anticipated pace, malicious and non-malicious threats are rising, because the flat IP, simplified LTE network architecture provides a new range of hacking opportunities and exposes the EPC (evolved packet core) to an onslaught of signaling traffic that used to be captured at the 3G RNC (radio network controller). In addition, voice services now starting to migrate to LTE (VoLTE) are characterized by very small packets for which current mobile networks are not fully optimized, and are also generating their share of signaling traffic.

The good news is that there is a 3GPP remedy: IPsec and the security gateway, optional for “trusted” networks and left to mobile operators’ own consideration. And the bad news: given the assumed additional cost and complexity associated with IPsec implementation along with an LTE network rollout, IPsec is far from being mainstream. The situation is rapidly changing: more and more mobile operators make IPsec a mandatory component of their LTE rollout, creating the need for the security gateway.

In this paper, we discuss the broader role the security gateway can play in LTE networks as LTE subscribers ramp up by the millions every quarter and VoLTE services start to emerge. By revisiting recent work released by the 3GPP and the NGMN Alliance, we argue that an S1-focused security gateway can not only perform IPsec encryption and decryption, its basic function, but can also process small VoLTE packets and protect the EPC from overwhelming signaling traffic. Put another way, the security gateway provides better VoLTE QoS control and protection of the EPC.

The Need for Securing LTE Networks Has Never Been Greater

So far so good, more than 6.5 billion people have been enjoying mobile communications services without experiencing a major hacker-induced mobile network outage. The major reason is those traditional 2G and 3G radio networks had their own backhaul physical infrastructure with dedicated leased lines (T1s in the US, E1s in Europe, mostly on microwave links), making the overall network extremely difficult to hack. But spying events do happen: the NSA is suspected of listening to the German Chancellor’s cell phone, and has been collecting data on nearly every US phone!

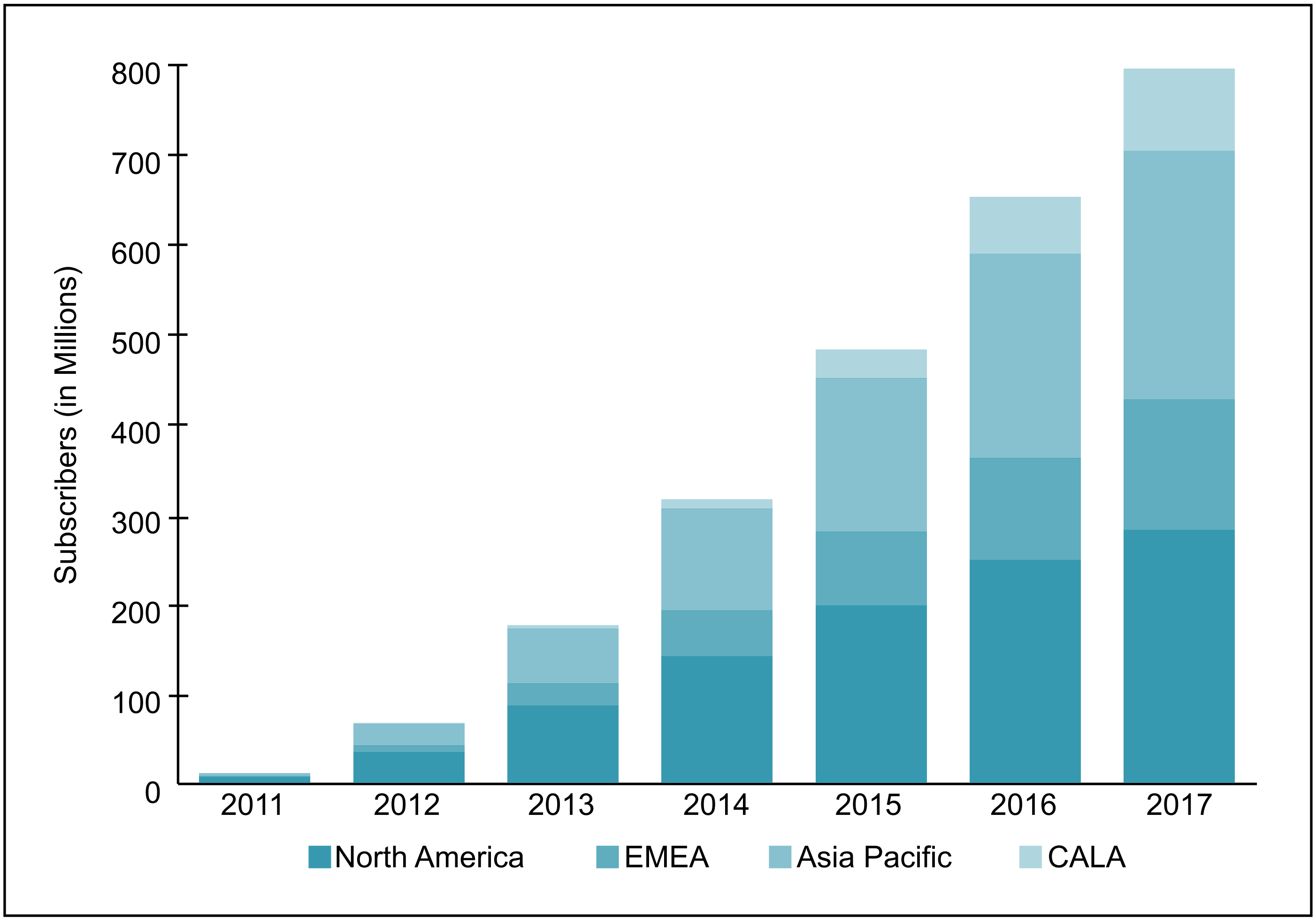
All substantial reported mobile network outages were essentially caused by glitches in core networks (e.g., O2’s and Orange’s HLRs in 2012), and bugs in NodeB software (e.g., Telecom New Zealand in 2012) rather than hackers. Nonetheless, another substantial looming non malicious threat is coming from unexpected traffic surges generated by a large variety of events such as sports (e.g., FIFA World Cup, Super Bowl, Wimbledon tennis finals. . .), politics (e.g., presidential elections), and natural disasters (e.g., the Icelandic volcano eruption). As more and more mobile subscribers flock to shiny LTE networks, all of this is going to get worse!

The world is moving to LTE at a fast and unstoppable pace

The ongoing migration to LTE is happening at a faster pace than what history taught us. Typically it takes 10 years to achieve full migration from one generation (2G) to the next (3G). For example, Japan was the first nation to launch commercial 3G W-CDMA in 2001 and had no 2G left in 2011. Looking at the LTE ramp up, it's very likely that by 2016, most Japanese subscribers will be on LTE. Taking this new pattern into account, Infonetics Research forecast 755 million LTE subscribers by 2017 from 175 million in 2013. With more and more subscribers flocking LTE networks, voice services will inevitably move to LTE, with 2014 as the VoLTE ramp-up year.

Infonetics Research predicts total global wireless subscribers will reach 7.4 billion by 2017, and LTE subscribers will account for just 10% of total mobile subscribers worldwide at that time. The subscriber forecast is directly derived from service providers' LTE plans. As a result, early adopters in North America—such as Verizon Wireless with 42.7 million subscribers in the fourth quarter of 2013, up from 21.7 million in the same period a year ago—drive the forecast and will likely continue to maintain a significant share throughout given current uptake. Then, a strong ramp-up is expected from 2014 throughout 2017, dominated by Asia Pacific, mainly fueled by China.

Exhibit 1: Worldwide LTE Subscriptions



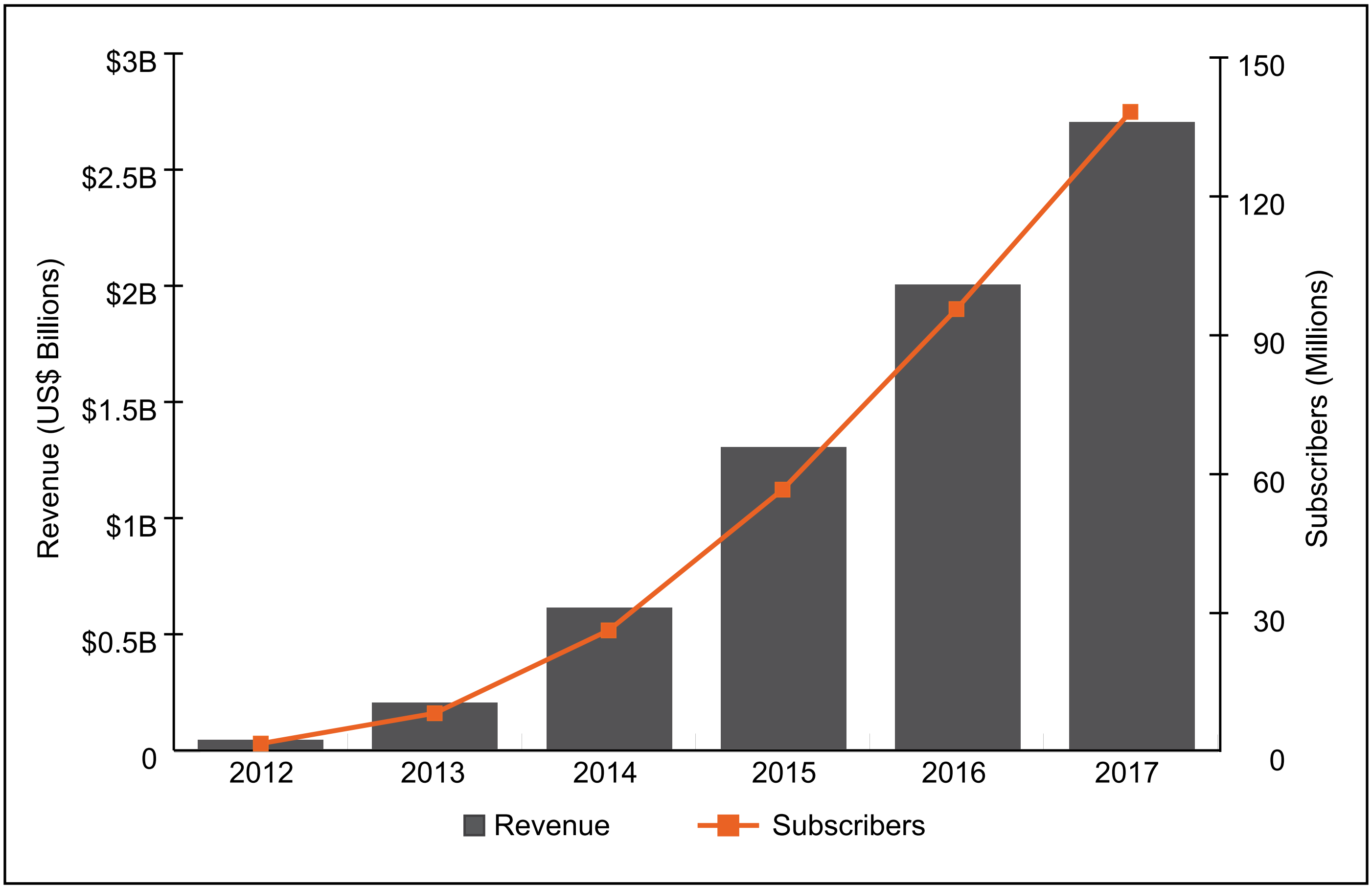
Source: Infonetics Research, *2G, 3G, 4G Mobile Infrastructure and Subscribers Market Size, Share and Forecasts*, December 2013

And voice, still half of total mobile service revenue, is inevitably moving to LTE as well

Despite the onslaught of videos and apps crowding LTE networks, voice is not going away. But moving TDM mobile voice, a cash cow business that is still paying the bills and is delivered over one of the most cost-efficient telecom infrastructures, to a brand-new LTE infrastructure is a risky and complicated task. In the 12/12/13 2nd edition of Infonetics Research's *2G, 3G, 4G Mobile Services and Subscribers: Voice, SMS/MMS, and Broadband* biannual market size and forecasts report, total worldwide voice revenue, a $450-billion yearly business, would stay above 50% of total mobile services through 2016, and may decline in 2017. Mobile operators are looking to VoLTE as a profitable service differentiator and revenue stream but at the same time face challenges—the biggest one being the migration of the lucrative $500-billion per year traditional mobile voice business—in combining the unique requirements of VoLTE with protecting the network. Everyone agrees that a VoLTE service needs to have at least the same performance and quality as current circuit-switched voice services.

By 2017, worldwide VoLTE subscribers are expected to top 138 million from 8 million in 2013, a 17X increase, and service revenue is expected to reach $2.7B, with a significant chunk, $1.6B, coming from Asia Pacific due to large subscriber numbers as developed economies wake up, despite lower ARPU than in North America. In fact, SK telecom, which was the first to launch commercial VoLTE in June 2012, reported that blended LTE ARPU increased from $35.81 in 1Q12 to $42.84 in 1Q13. What we don't know yet is the VoLTE impact.

Exhibit 2: Worldwide VoLTE Market Opportunity



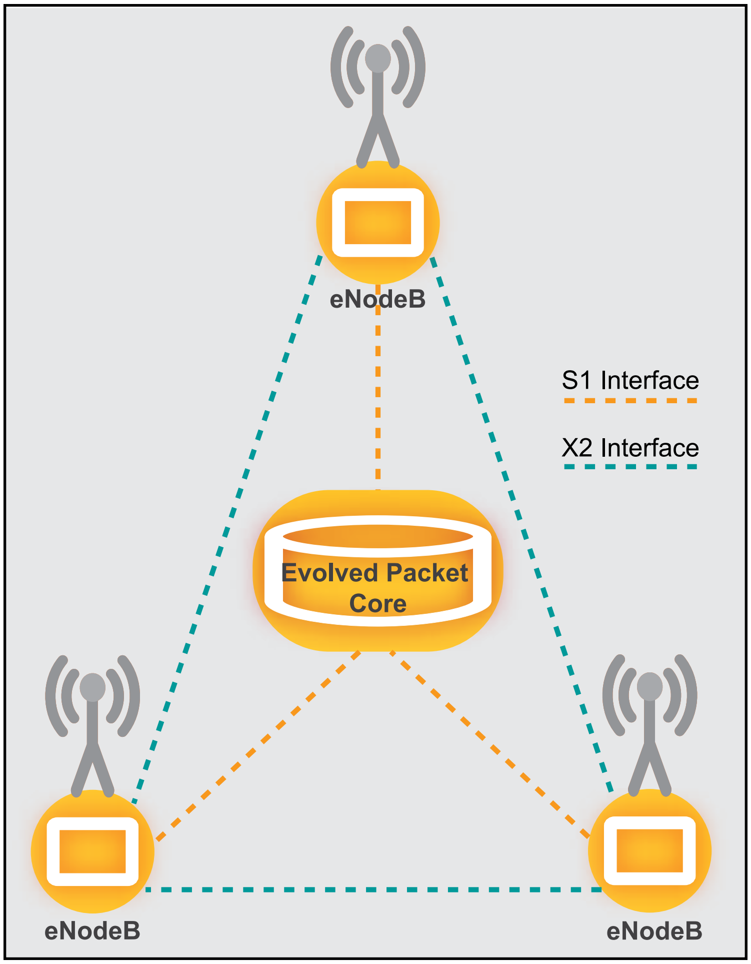
Source: Infonetics Research, *Mobile VoIP and Subscribers Worldwide and Regional Market Size and Forecasts*, June 2013

This Developing LTE World Provides Hackers with a New Eldorado!

Nowadays, there is not a single day without a major cyber-attack that breaks down the website of a major corporation, non-profit organization, or government agency. Hacking, which has so far stayed confined to wireline networks, is no longer a hobby but rather a growing big business. With the migration of hundreds of millions of mobile subscriptions to LTE over the next two decades, more and more people are using their mobile devices to go online for apps, videos, mobile banking, and accessing social networks and sensitive information. As a result, there is no question that the LTE network hacking opportunity will be substantial; the LTE architecture pushes more mobility function out to the cell sites, enabling hackers to disrupt subscribers and penetrate new data applications. Three fundamental factors are making LTE networks more vulnerable:

1. The flat LTE topology provides a direct route from eNodeBs (eNBs)—cell sites—to the serving gateway (SGW) in the evolved packet core (EPC), opening the door for denial of service (DoS) attacks and interception of user communications; in other words, there is no centralized intelligent controller, formally BSC and RNC, and the eNodeBs are interconnected via the X2 interface, and connected to the EPC through the S1 interface
2. The addition of small cells or "mini eNodeBs" in the form of microcells, picocells, femtocells, and metrocells. as well as remote radio heads to boost existing capacity will further increase the challenge of physically protecting the resulting heterogeneous network against criminal activity
3. The rising popularity of network sharing that allows several mobile operators to use the same cell site to save cost

Exhibit 3: LTE Network Architecture



Source: 3GPP

> *"The number of large attacks increased massively in 2013: up more than eight times the number in 2012."*

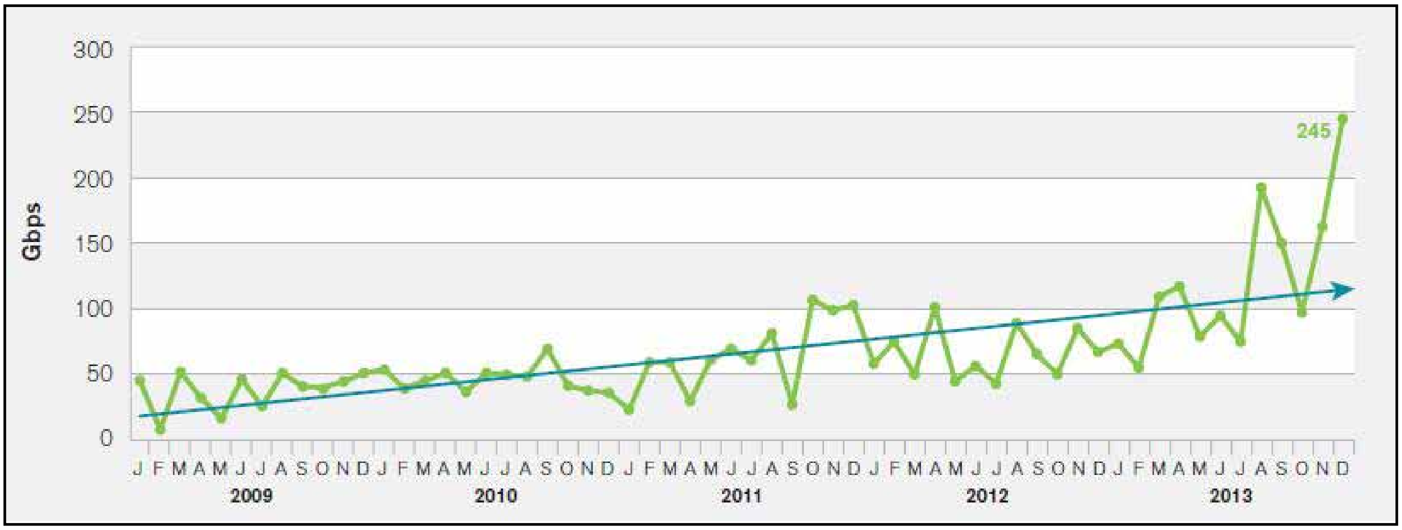
Meanwhile, potential threats to mobile networks are real and fully documented

There are many standards and documents that describe the attacks and risks in telecommunications networks. As a reference, the security framework defined by the ITU-T X.800/X.805 recommendations shows a threats model summed up as follows:

- Destruction of information or network resources (e.g., Denial of Service)
- Unauthorized tampering of an asset
- Theft, removal or loss of information and resources
- Eavesdropping or unauthorized access to an asset
- Network breakdown or outage

Arbor Networks' *Worldwide Infrastructure Security Report Volume IX* (3Q2013) indicates that accidental or deliberate denial of service (DDoS) attacks against customers still remain the most commonly experienced security threat. There is no end in sight; even worse, the size of the attacks is swelling. Exhibit 4 shows data collected by the Arbor ATLAS system that gathers statistics from 290+ Peakflow SP customers around the world. These statistics include anonymized details of the DDoS attacks monitored by Arbor Networks survey participants. The largest verified, monitored attack in 2013 was 245Gbps, versus 100Gbps in 2013. The number of large attacks monitored by ATLAS (defined as being over 20Gbps) increased massively in 2013—up more than eight times the number in 2012.

Exhibit 4: Monthly ATLAS Peak Monitored Attack Sizes



Source: Arbor Networks, Inc.

Consequently, Security Must Be a Foundational Element of LTE Deployments

No matter how extensive the network, today no operator owns the entire end-to-end communications chain. And as in the IP world no one can be trusted, the all-IP flat architecture of LTE networks requires new types of protection because some 2G and 3G functions that initially were performed in the controller—BSC and RNC, respectively—have moved to the eNodeB. The backhaul needs to be all IP as well, which raises another issue: shared transport network infrastructure for the potential coexistence of fixed and mobile services on the same packet network. And finally, the presence of the X2 interface that supports direct handover among the vicinity eNodeBs, involves stronger security requirements on the nodes.

IPsec encryption is the key mechanism. . .

Security issues in LTE networks have already been addressed by both the 3GPP and the NGMN, which made recommendations that are left to mobile operators themselves to adopt or not. Three hierarchical scenarios are proposed, starting from an unprotected trusted network, meaning in total absence of IPsec and just leveraging existing mechanisms available in packet core networks. The second scenario uses IPsec for protecting the LTE control traffic (S1-C, X2-C), often considered as the most sensible for the service continuity. And in the third scenario, full IPsec protection is proposed for both control and user traffic.

. . . but full IPsec introduces new considerations

The main advantage of full IPsec protection is clearly the protection offered to all of the traffic with no distinction but the main caveat is the potential for increased computational impact on eNB and a bigger overhead at L1 transmission and perceived operational complexity. As a result, mobile operators have been reluctant to implement IPsec, especially if they consider their networks and backhaul "trusted."

It's interesting that US and South Korean service providers, early LTE adopters together accounting for more than 50% of worldwide LTE subscribers, have been slow to embrace the need for IPsec, whereas their European counterparts—led by Deutsche Telekom—are adopting IPsec at a fast pace. It's only in 2013 that Europe's Big 5 (Deutsche Telekom, Orange, Telefónica, Telecom Italia, and Vodafone) started significant LTE deployments, almost four years after Japan, South Korea, and the US, but they made IPsec a chief requirement, despite the additional cost.

Conversely, time-to-market was so important in the US and South Korea that mobile operators preferred to tackle the issue later. There was also a common belief that the networks were sufficiently closed to be adequately secured, but the requirement for various alternative backhaul strategies (e.g., the use of small cells, wireless hand off, and roaming services) effectively introduced a number of entry points for potential threats. Infonetics Research's *Carrier WiFi Equipment* market share, size, and forecast report (November 15, 2013) indicates that $8.5 billion is to be spent on carrier WiFi equipment over the next 5 years, and operators are looking to consumer femtocells to increase ARPU via new apps and services. Meanwhile, Japan's NTT DOCOMO saw the issue differently and was successful in deploying IPsec and achieving time-to-market at the same time.

Now IPsec is gaining momentum, setting the stage for security gateway implementations

With more than 260 commercial LTE networks up and running across the globe, more and more mobile operators are implementing IPsec. However, Infonetics Research's quarterly LTE deployment tracker, a part of the *2G, 3G, 4G Mobile Infrastructure and Subscribers* report, indicates only 20% of mobile operators worldwide had deployed IPsec in their LTE network by the end of 2013.

As IPsec adoption for transporting LTE flows continues to grow significantly, the need for a security gateway, which has been considered optional by many operators, increases. As defined by 3GPP/S1 interface, its fundamental function is to perform authentication and encryption/decryption for the IPsec tunnel, and handle IKEv2 authentication to secure the delivery of voice and data services. Given the pace of LTE adoption worldwide, the security gateway needs to be highly scalable to manage hundreds of thousands of concurrent IPsec tunnels.

In the meantime, the very few mobile operators that deployed a security gateway in the first place while constructing their LTE networks are clearly seeing the benefits of high security, particularly in non- controlled backhaul environments, and expect better QoS control when launching VoLTE.

Security Gateways Also Provide High VoLTE Network Performance and QoS Control

Jitter-free and latency-free traffic are the chief stringent VoLTE requirements that can be met by prioritizing and optimizing voice traffic, a function that can be offered by a robust security gateway. The mobile Internet is a very unique world: it is set it apart from typical enterprise network traffic by the required exponential level of scalability and traffic volume processing, the ability to adapt to signaling issues, chatty apps, and network outages creating thousands of reconnection attempts and other events.

In addition to performing IPsec, a security gateway can also manage IP sessions and do IP charging functions and policy enforcement although these are not primary functions; some of these functions may have already been implemented in the core networks—the IMS core for instance. And of course introducing a security gateway in an LTE network should not degrade network performances, starting with latency that is the most important requirement for real-time traffic such as voice.

In its February 2012 *Security in LTE Backhauling* paper, the NGMN Alliance made the case for security gateway implementations beyond the simple need for securing the transport of LTE flows and listed the effects of the security gateway, which are directly linked to its position in the network, given the overall network topology, and required scalability, and performance.

Focusing on the S1 interface provides the highest benefits

The extreme and unlikely option would consist in placing the security gateway close to the eNodeB and focusing on the X2 interface, which in turn would lead to a vast array of security gateways, a costly and ineffective proposition. The opposite option places the security gateway just in front of the EPC, directly connected either to the MME or the S/P-GW, or in an intermediate aggregation center, depending on the operator network topology. In this case, one redundant security gateway can support hundreds of thousands of eNodeBs or HeNodeBs, significantly reducing the equipment needed. That way, the security gateway protects and manages efficiently the S1 wide open area that opens the door to the most sensitive part of the network; specifically, it can process small VoLTE packets, and manage potential signaling storms.

As an illustration of the potential signaling damage an S1-focused security gateway can shield, research from the UK's University of Surrey provides a baseline for calculating MME/SGW/PGW signaling load increase: a macrocell with radius of 1km and 64 users. As the cell size decreases the number of achievable handovers, the signaling load due to mobility events increases significantly. For instance, 10 times more signaling load to the MME/SGW/PGW when cell radius reduces to 100m.

An S1-focused security gateway can process tiny VoLTE packets

As long as the security gateway delivers line rate performance that sustains throughput levels at core network aggregation points regardless of packet size, it will treat a VoLTE packet the same way as any other packets. In RFC 2544, IETF recommends that seven standard frame sizes (e.g., 64, 128, 256, 512, 1024, 1280 and 1518 byte) be tested multiple times, for a specified length of time. This is because all these frame sizes are used in the network and so the results for each must be known. However, most networks are optimized based on the median packet size of 512 bytes and are not ready to meet the performance requirements for VoLTE, because voice packets are less than 100 bytes. For example, the Adaptive Multirate Wideband (AMR-WB) voice codec has a low transmission rate of 23.85Kbps and a packet size of 64 bytes.

And manage signaling storms

As the security gateway sits in front of the packet core, it can filter and manage the signaling traffic it reaches the core—the MME and the HLR/HSS—and causes a major outage. Early LTE adopters such as SK telecom, KT and Verizon Wireless have made no secrets of the tremendous amount of signaling traffic that hit their core networks. In 3G, this traffic stormed the RNC, which eventually collapsed as seen in the AT&T network back in 2007 after the introduction of the iPhone.

Over-the-top applications are very well known for their overwhelming signaling effects on mobile networks that are triggered by the simple need to maintain active sessions, even more so for VoIP services. VoLTE services require additional signaling for setting up a dedicated GBR (guaranteed bit rate) bearer to fulfill the QoS requirement. Although the resulting signaling traffic is expected to have minimal impact on core networks when compared to the existing OTT signaling tsunami, the impact is not yet known because of the low starting subscriber numbers; it could be significant due to the events IMS-based VoLTE architecture generates.

Bottom Line

Back in the 3G days, mostly around 2007, discussions about the role of a security gateway in the packet core network led to many debates and various schools of thoughts that basically left it stuck on the vendor's shelf.

Today, the situation is dramatically different: the rapid migration to LTE is making the IP flat architecture look like an appealing hacking platform and exposes the EPC to a never seen onslaught of signaling traffic that used to be caught by the RNC. Consequently, the need for a security gateway that can effectively manage hundreds of thousands of concurrent IPsec tunnels, process tiny VoLTE packets, and filter signaling traffic—all without negatively affecting the overall performances of the network—has never been greater.

White Paper Author

Stéphane Téral
Principal Analyst, Mobile Infrastructure and Carrier Economics
Infonetics Research
stephane@infonetics.com
+1 408.583.3371

Commissioned by Stoke to educate the industry about security gateways, this paper was written autonomously by analyst Stéphane Téral based on Infonetics' independent mobile and security research.

About Infonetics Research

Infonetics Research is an international market research and consulting analyst firm serving the communications industry since 1990. A leader in defining and tracking emerging and established technologies in all world regions, Infonetics helps clients plan, strategize, and compete more effectively.

Report Reprints and Custom Research

To learn about distributing excerpts from Infonetics reports or to learn about custom research opportunities, please contact:

North America (West), Asia Pacific
Larry Howard, Vice President, larry@infonetics.com, +1 408.583.3335

North America (East, Midwest, Texas), Latin America
Scott Coyne, Senior Account Director, scott@infonetics.com, +1 408.583.3395

Europe, Middle East, Africa, India, Singapore
George Stojsavljevic, Senior Account Director, george@infonetics.com, +44 755.488.1623

Japan, South Korea, China, Taiwan
http://www.infonetics.com/contact.asp

695 TECHNOLOGY PARKWAY SUITE 200 CAMPBELL, CALIFORNIA 95008 TEL 408.583.0011 FAX 408.583.0031 www.infonetics.com
SILICON VALLEY – BOSTON METRO – LONDON – AMSTERDAM – SHANGHAI – TOKYO

INFONETICS RESEARCH