White Paper

The Security Vulnerabilities of LTE: Risks for Operators

A *Heavy Reading* Executive Overview

Prepared by

Patrick Donegan
Senior Analyst, *Heavy Reading*
www.heavyreading.com

on behalf of

www.juniper.net

September 2013

Executive Summary

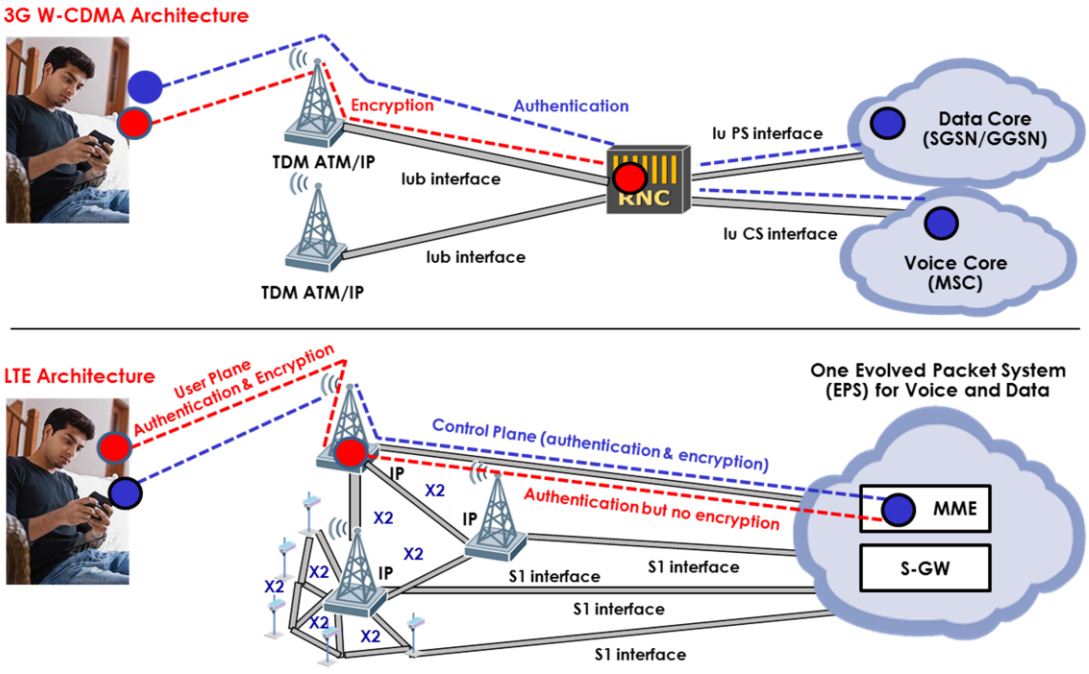
LTE brings powerful new cost-saving and revenue-generating features for operators, as well as work and life enhancing capabilities to end users. But there is a significant new security vulnerability in the LTE network that never existed with 3G: Whereas 3G traffic is encrypted at the end-user device and terminated deep in the network, LTE's encryption terminates at the base station or eNode B.

The 3GPP-prescribed fix for this – the use of IPsec from the eNode B back into the network – has not been deployed in many of the early LTE launches, but is starting to be introduced now, especially in Europe. Driven by the recognition that allowing clear text to transit freely across the network will expose subscribers to theft of private information or network outages by hackers, *Heavy Reading* is forecasting increased adoption of IPsec with LTE so that a majority of LTE cell sites will support the standard by the end of 2017. The rest of this white paper explains why.

Security Exposures in the LTE Network

Mobile operators have become so used to world-class network security being baked in to their network infrastructure that many executives in these companies tend to just assume it is there. When they initially rolled out 3G, for example, there was one single, seamless instance of 3GPP encryption all the way from the handset to the base station and on, deep in the network, to the RNC. Moreover, the E1 or DS1 pipes between the base station and the RNC were based on TDM, a highly-robust, highly-secure telecom grade networking technology.

Figure 1: Encryption in 3G & LTE Networks



Source: Heavy Reading

The introduction of mobile data capabilities in the network, beginning with GPRS and CDMA 2000, drove operators to do a little more of their own thinking where network security is concerned. With the GGSN exposing the network and subscribers to the wilds of the external Internet via the Gi interface, mobile operators began having to design, procure and deploy firewall and intrusion protection capabilities to block malicious traffic. When GPRS roaming was launched, operators had to give similar consideration to monitoring and securing the Gp interface that supports billing of data roaming services between operators.

The balance between the kind of security that is already baked in and the kind that must be layered into the network by the operator shifts still further toward the do-it-yourself model with LTE. As shown in **Figure 1** (above), the 3G model of a single, seamless instance of encryption is transformed in LTE by the elimination of the dedicated RNC node and distribution of its radio resource management functions out to the eNode B and Evolved Packet Core (EPC), respectively. In the LTE network, encryption terminates at the eNode B with the result that the traffic that emerges from eNode B is clear text.

In cases where the operator considers the intermediary transport network between them to be "untrusted," 3GPP prescribes using IPsec encryption on the S1 and X2 interfaces between the eNode B and the EPC. This paper examines take-up of IPsec by LTE operators worldwide up until now, considers the driving forces behind those that have deployed it and those that haven't, and shares *Heavy Reading*'s expected adoption rate over the next five years.

Adoption of LTE Security Measures

In the three years since the first commercial launches, each operator that launched LTE has had to decide whether or not to invest in securing the S1 and X2 interfaces across what can still be thought of as the backhaul domain of the LTE network.

The diversity of conclusions that different operators have reached is striking. Japan's NTT Docomo launched with IPsec, but it was the exception rather than rule in that first wave of launches. None of the major U.S. carriers have leveraged IPsec up until now; nor have operators in South Korea. In Europe, however, an increasing number of operators are using IPsec. For example:

- **Deutsche Telekom** operates a policy that any of its affiliates that it controls should deploy IPsec at all of their LTE sites.
- **Orange** operates a similar policy, although one with greater flexibility that allows for local market circumstances.
- Reflecting the positions of its parent companies, **Everything Everywhere's** LTE sites all have IPsec in service.
- **Telecom Italia** is also using IPsec.

While Europe is becoming the global driver for IPsec adoption, many new LTE networks over the last 12 months still continue to be launched without it. As shown in **Figure 2** (below), this trend of greater, but still patchy, adoption has been captured quite closely by *Heavy Reading* surveys of mobile operators. In two surveys on mobile backhaul and mobile network security (in December 2010 and September 2012, respectively), we asked different samples of qualified respondents in mobile operators worldwide the exact same question about the need for IPsec in LTE: *"For the first three years following the launch of LTE, to what extent do you expect that IPsec will be needed between the LTE cell site and the LTE core?"*

Figure 2: Mobile Operator Outlook on Requirement for IPsec Between LTE Cell Site & LTE Core

	DECEMBER 2010 (N=92)	SEPTEMBER 2012 (N=69)
All cell sites will need IPsec implemented	20%	32%
At least half of all cell sites will need IPsec implemented	13%	13%
A subset of cell sites will need IPsec implemented	19%	23%
IPsec will probably not be needed in the backhaul	17%	4%
IPsec will definitely not be needed in the backhaul	1%	3%
It's still unclear at this stage	29%	14%
Don't know	Option not offered	10%

Source: Heavy Reading

As of September 2012, only a third of mobile operator respondents worldwide were convinced of the case for routinely securing all the operator's LTE cell sites with IPsec. But what's also interesting is the trend compared with the responses to the same question 21 months earlier. The trend is in favor of adoption – albeit the acceleration is modest and coming from a low starting point. Notably, 32 percent expected to secure all LTE sites in September 2012, compared with just 20 percent in December 2010. Only 7 percent in the 2012 survey believed that IPsec will not be needed at all, compared with 18 percent a year and a half earlier.

What's Driving Some Operators to Adopt?

So what is driving operators to invest in IPsec as they roll out LTE? From their perspective it ought to be clear enough – literally. If there is clear text coming out of the LTE eNode B, there is a substantial security exposure that requires closing off right there for the following reasons:

An attacker that is able to intervene in the network at the cell site or at any other point on the S1or X2 interface and gain access to the clear text stream can potentially gain access to the network. From here they can potentially trigger an outage or obtain access to the private voice and data transmissions of the operator's customers. And while there aren't many voice calls going over the LTE network yet, VoLTE is sure to change that.

It's not just that traffic is unencrypted across the backhaul in LTE, whereas it is encrypted in 3G; the distributed architecture of the LTE network means the number of network elements that can potentially be impacted by an attacker is substantially larger than in 3G. In 3G the RNC node serves as a form of security buffer between the core network and the access network, whereas in LTE gaining access to the S1 interface exposes the attacker directly to the core because there is no RNC. The so-called S1-Flex feature has already been implemented by several LTE operators, allowing different subscribers attached to any one eNode B to be connected to a diversity of EPC elements to enhance load balancing. And each eNode B can be associated with as many as 32 X2 interfaces to other eNode Bs.

Small cells continue to throw up a moving target of new security challenges that even the world's leading operators are only just managing to stay ahead of. For example, Verizon Wireless has publicly admitted that in March 2013 it had to apply a security fix to its "Network Extender" private femtocell product line. The flaw had rendered these products vulnerable to exposing customer phone and data communications to hackers. *Heavy Reading* expects 700,000 3GPP public access small cells requiring new backhaul to be in live service worldwide by the end of 2017, with the overwhelming majority using LTE. Small cells are inherently more vulnerable than macro cells, which tend to have layers of physical security that are either practically unfeasible or cost-prohibitive for small cells. But small cells in the public access domain represent an even greater security risk than in the private femto domain, because they are liable to have communication paths to many more neighboring cells and are much more vulnerable to physical tampering.

Some Early Adopters Have Concluded the Risks Need Mitigating

The operators previously listed as having implemented IPsec with their LTE networks have concluded that the risk is too high to allow clear text running across their backhaul network. To varying degrees, they have done so for three main reasons:

The foregoing of current revenue that arises during an outage (when subscribers can't access service) and immediately following when operators have to resort to crediting customers with free services that they might otherwise have been able to charge for by way of compensation for the outage.

The reputational damage that arises from leakage of personal information and network outages, which can manifest itself in increased subscriber churn rates, immediately following such incidents.

The undermining of long-term revenue opportunities from new business models. In May 2012, for example, Randall Stephenson, chairman, CEO and president of AT&T, told an audience at The Milken Institute that "the long pole in the tent" when it comes to capturing new revenue opportunities in areas such as mCommerce and mHealth, "is going to be getting the ecosystem to be robust in protecting data and making sure you control who sees the data, how it's shared and how it's transmitted. Until you get it right, there is going to be inherent apprehension and concern by all of us about this."

What's Driving Others to Stay Exposed?

Heavy Reading has undertaken a lot of research into LTE security during which operators have shared their reasons for hesitating to deploy IPsec. These reasons are highlighted below, along with the potential flaws in these arguments.

In many developing markets, information privacy is not a significant issue at the consumer level. This is because much of the population in developing markets doesn't actually have any personal information in any format, let alone a digital format. Large parts of the population in such countries don't even have formal street addresses, much less bank accounts or credit cards. So for these operators – particularly those focused on the "value" end of the consumer market – IPsec is inevitably a low priority when they roll out LTE.

Some operators believe that there are easier, more effective, lower cost ways for an attacker to trigger an outage or expose private information than intervening on the S1 – for example by more common attack vectors like a DDoS attack from the

Internet or via smartphone malware. That may be true in some cases today but that doesn't mean the risk can be ignored just because there are few known precedents for an attack on the S1 or X2. It shouldn't detract from the fact that without IPsec traffic coming out of the eNode B is in clear text. A complacent view on this also neglects the fact that attackers are driven by volume. So as the volume of LTE subscribers increases, so does the size of the attacker's opportunity for disruption or financial gain. This argument also under-estimates how quickly attackers learn and apply new techniques.

Some operators have a tendency to segment their traffic into that which requires high security and that which doesn't. They argue that applications that require high security can be encrypted at the application layer and that there is no point encrypting huge volumes of subscriber's Facebook updates and YouTube viewings. This argument is appealing at a superficial level. However, the obvious flaw in it is that the email, text and other messaging applications of these subscribers are typically not going to be encrypted at the application layer and so will be exposed without IPsec encryption in the network.

Many operators do understand the risk but believe that the cost of implementing IPsec is too high relative to the amount of risk entailed. It's certainly true that operators have limited security budgets and that each security business case must be evaluated in terms of the scale of the risk and the investment needed to mitigate it. However, one cost component of the IPsec deployment model that is sometimes misunderstood is that initial LTE deployments typically consist of a single IPsec tunnel being instantiated at the eNode B, and then kept in service permanently. This a far lower-cost approach than the model that has characterized many enterprise-based deployments of IPsec – huge volumes of tunnels being dynamically set up and torn down again – which can indeed be opex-intensive.

Some operators believe they can wait for a network-wide upgrade to IPv6 so as to leverage IPsec once it is natively embedded in the v6 standard. They are holding out for this model as an alternative to deploying IPsec today on top of their IPv4 infrastructure according to what they view as a sub-optimal overlay security architecture. This, however, relies on a multi-vendor implementation so the risk is that the time required for all the operator's vendors to support all the relevant IPv6 security features will leave an extended period of time during which S1 and X2 traffic will continue to remain exposed.

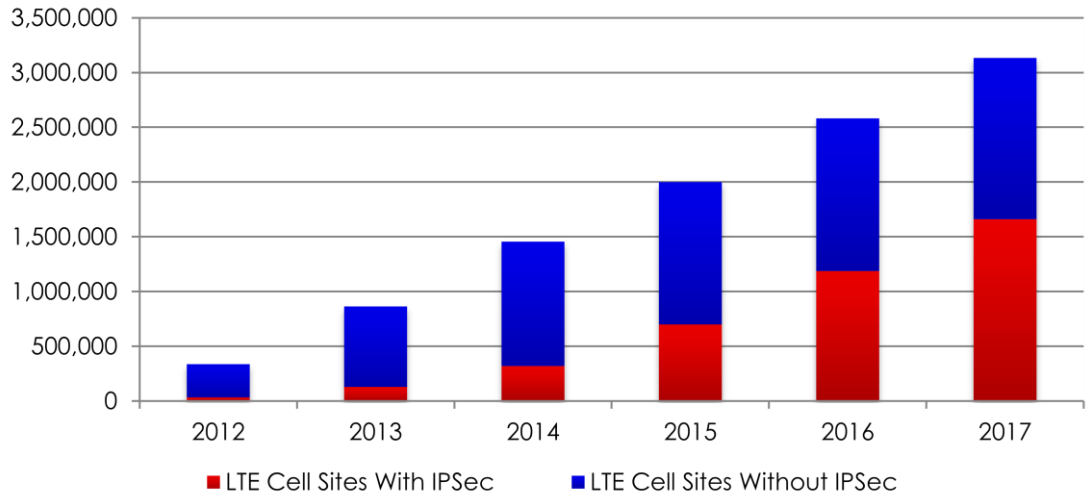
Some operators fear that encrypting traffic between the LTE RAN and the core will jeopardize the operator's end-to-end latency target, typically 20-30 milliseconds. Again this is a wholly legitimate consideration, but with the right network engineering rules in place, leading operators have already proved that in partnership with vendors IPsec can be supported in a manner consistent with LTE's latency targets. And while some operators have investigated using alternative encapsulation and encryption techniques on the S1, IPsec is still the only standard that is formally 3GPP approved for S1 and X2 security.

As they roll out LTE, some operators have in mind securing only their public access small cells and those sites where they leverage leased backhaul that they deem to be "untrusted." In this model, the operator believes that it need not extend the same security to those among its macro-cells where it has built out the backhaul itself and are therefore "trusted." For some operators this may appear as an optimal compromise between costs and security, but it still leaves many of its sites exposed. It also creates two parallel security environments, which can be challenging from an operational perspective, in that it requires different skillsets and operational procedures depending on the specific cell site.

The Outlook for IPsec Adoption

Figure 3 shows *Heavy Reading*'s forecast for the adoption of IPsec with LTE over the next four years. As shown in red, we expect the proportion of the world's LTE cell sites that support IPsec will grow from 15 percent at the end of 2013 to 35 percent at the end of 2015 and 53 percent by the end of 2017.

Figure 3: Forecast for IPsec Adoption in LTE Backhaul



Source: Heavy Reading's Ethernet Backhaul Tracker, June 2013

We expect growth will be driven by several factors, including: the ongoing migration of hacker time and attention from the wireline to the mobile networking environment; competitive pressures arising from one operator in a market deploying IPsec, driving competitors to respond; the probability of threat incidents arising from operators failing to deploy IPsec and becoming publicized; and the growing recognition that lack of bulletproof or near-bulletproof security will be a show-stopper when operators look to drive the next generation of revenue opportunities with major vertical industry partners, such as health insurance providers.

We assume that there will still be a sizeable number of LTE operators that are still allowing clear text to transit across their backhaul networks four years from now. But we also expect that a financial analysis of LTE operators four years hence will show a pretty close correlation between support for end-to-end network security and superior financial performance.

Background to This Paper

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. More information can be found at www.juniper.net/us/en/dm/mobile-lte.