LTE radio transport security

Vulnerabilities, threats and controls
Table of Contents

1. Objective of this paper ................................................................. 3

2. Introduction .................................................................................. 3
  2.1 LTE security compared to GSM and UMTS ................................................. 4

3. Risks in an unprotected radio transport network ....................... 5
  3.1 Backhaul connectivity vulnerabilities ....................................................... 6
  3.2 Backhaul connectivity threats ................................................................. 7
  3.3 X2 interface vulnerabilities ................................................................. 9
  3.4 X2 interface threats ............................................................................. 10
  3.5 S1-U interface vulnerabilities .............................................................. 10
  3.6 S1-U interface threats .......................................................................... 11
  3.7 S1-MME interface vulnerabilities ....................................................... 13
  3.8 S1-MME interface threats .................................................................... 14

4. Unprotected LTE radio transport risk assessment .................. 17
  4.1 Risk matrix ......................................................................................... 17
  4.2 Risk ratings ......................................................................................... 17

5. Mitigating controls specified by 3GPP ..................................... 18
  5.1 Nokia and Check Point Carrier Security Solution .............................. 18
  5.2 Case study: Large European mobile operator .................................... 22

6. Conclusion ..................................................................................... 24
1. Objective of this paper

This white paper aims to provide mobile network engineers and information security teams with technical insights on the vulnerabilities inherent in an unsecured radio access network.

The paper presents an overview of the risks that operators should consider when assessing the security requirements of their radio access networks. The vulnerabilities described can pose a serious security risk to the operator and its subscribers and also have the potential to cause large scale degradation of network performance. The threats exist regardless of whether or not the operator owns the backhaul network infrastructure, however, the severity of the risk certainly increases if shared backhaul or microwave links are used.

2. Introduction

The introduction of IP into radio transport and mobile backhaul networks has led to an architecture that is inherently open. Unless this is addressed, an operator’s core network is vulnerable to different kinds of threats. These threats include risks of eavesdropping and unauthorized access to operator systems and even denial of service attacks that can bring down the whole network. A malicious intruder may gain access to the core or Radio Access Network (RAN) from an Ethernet port at an eNodeB (eNB) site, for example. This could be achieved quite easily, as not all RAN equipment is installed in physically secure locations.

The use of secure IP protocols such as IPSec and TLS is vital to ensure the confidentiality and integrity of the network traffic (payload and control data), as well as the availability of the mobile service. Authentication and authorization of genuine networks nodes is required to ensure this confidentiality and integrity. Furthermore, brand, regulatory compliance and other policies require tighter security when IP is used and the number of known vulnerabilities increases.

Unlike the legacy 3G Iub interface between the base station and Radio Network Controller (RNC) (with classical ATM or E1 lines), the LTE S1 interface between the eNB and the Evolved Packet Core (EPC) is not encrypted and is based on IP/Ethernet protocols. This means that even though the air interface between mobile and base station is encrypted, the interface between base station and core is not. In LTE EUTRAN architecture, there is no platform, such as the 3G RNC, that defines the border between RAN and core.
The act of adding encryption is complicated and can take time, delaying the deployment of the network and, ultimately, an operator’s ability to launch a service. In addition, unless implemented well, it can lead to significant increases in OPEX. To achieve unambiguous authentication in a highly secure and automated way, we propose a combination of Public Certificates and encryption keys as the best solution.

The business benefits provided by the Nokia Radio Access Security Solution include:

- Fully 3GPP compliant, fully automated solution.
- Solution designed specifically for mobile operators, ensuring performance and interworking with RAN and core network elements.
- Full support of automated base station enrollment, allowing 25 percent faster roll out and 25 percent cost savings compared to manual commissioning.
- Solution is fully resilient, achieving Telco grade 99.999 percent availability, with additional geographical redundancy to ensure service continuity.

2.1 LTE security compared to GSM and UMTS

Due to changes introduced in the LTE Evolved Packet System (EPS) architecture, there are significant differences in the threats to an LTE network when compared to previous generations of mobile networks. The main differences are:

1) The All-IP Network means that all Network Elements (NEs) now have IP addresses and are vulnerable to common cyber security attacks.

2) The physical boundaries have moved: where previously Radio Network Controllers would have been in highly secured locations, in the EPS their main functionality has been moved to the base station, which typically has lower physical security.

3) The ciphering that was previously in place in 2G/3G to protect user and control plane traffic over the backhaul network is no longer in place with LTE and traffic is sent completely in clear text.
Figure 1 shows the air interface encryption extending across the backhaul network to the RNC in a UMTS network and LTE architecture, where encryption terminates at the eNB and S1 traffic is sent across the backhaul network in clear text.

### 3. Risks in an unprotected radio transport network

Because the native backhaul security controls in previous network generations are no longer in use, new threats have to be evaluated when designing and implementing an LTE network. The first is the interception of subscriber data from any point along the backhaul network. The second is the interception of signaling messages, which also has the same exposures. The third is the exposure of the EPC to attacks originating from southbound interfaces.

The following section provides detailed descriptions of individual risks associated with unprotected LTE backhaul networks. These are categorized into four areas of risk, backhaul connectivity, the X2 interface, the S1-U interface and the S1-MME interface.
3.1 Backhaul connectivity vulnerabilities

The move to a flat architecture with end-to-end IP connectivity means that there is now a threat to the EPC if security is not implemented on the backhaul network. This threat is more severe than that associated with IP-enabled base stations in GSM and UMTS (in the case of Packet Abis and lub over IP), because backhaul ciphering is not natively implemented in LTE and the eNB connects directly to the EPC. This risk exists regardless of the ownership of the backhaul network infrastructure, as there is always the possibility that the physical security of an eNB site can be compromised, especially given that there are typically thousands of sites in the field that are often unmanned. Each of those sites now contains a direct entry point into the operator’s core network.

There are two main backhaul connectivity vulnerabilities in an unsecured LTE backhaul network that expose the EPC to attack:

- Weak authentication of network elements
- Inadequate trust zone segregation

3.1.1 Weak authentication of network elements

Without a deployed 3GPP-compliant LTE security solution, there is no authentication of hosts making IP connections to the core network. This means that anyone with physical or logical access to eNBs and/or the transport network elements can potentially launch an attack on core NEs such as the MME and S-GW. Access to the backhaul network also does not necessarily require circumvention of physical controls, as many operators use microwave backhaul, which can be intercepted from any point with line of sight to the transmitting points. The increasing maturity of software defined radio and the low cost of interception hardware - below $500 in
some cases - has made the interception of microwave links a very simple task and therefore a very realistic threat.

The risk associated with a breach of physical security controls is significantly increased when operators introduce small cells to the network. Home eNBs and outdoor base stations are typically easy to gain access to, becoming simple entry points into the network.

3.1.2 Inadequate trust zone segregation

The physical network boundaries in an LTE network have moved because RNC functions are now performed by the eNB. Physical security is now the only real measure preventing access to critical functions such as signaling, which were previously housed in high security buildings in the case of the RNC. This means that the radio backhaul environment now has a completely different threat profile and the trust zones have changed radically. Previously, the backhaul network could be considered a relatively trusted area of the network due to the ciphering that was in place, however it should now be considered less trustworthy than the packet core.

As a result, the backhaul network should be segregated from the EPC with network and application layer control over S1 communications to provide protection for core NEs. This segregation is part of the 3GPP NDS/IP technical specifications - if it is not implemented as part of the network design, then the EPC can be exposed to attack.

3.2 Backhaul connectivity threats

There are a number of ways that vulnerabilities in an unprotected backhaul network can be exploited. A compromised backhaul network link, either via a physical or radio security breach, would expose the EPC to attack. A physical security breach could take place through an eNB cabinet break-in, a contractor accidentally leaving a shelter door unlocked or simply via access to a cable from an outdoor base station. An example of a radio security breach is the use of a transceiver with line of sight access to a microwave backhaul link from an attacker’s vehicle.

All of these breaches can occur regardless of the operator’s ownership of the backhaul infrastructure. However, if the infrastructure is not owned by the operator (e.g. in the case of leased lines or shared backhaul) then these compromises could also take place via logical and physical access to nodes on the transport network that are outside the operator’s security control.
3.2.1 Network reconnaissance

The first activity an attacker would typically perform once access to the backhaul network has been obtained would be network reconnaissance to identify high value targets.

The All-IP network architecture means that an attacker would be able to use freely available network scanning tools to perform this (e.g. NMAP). There would be no need to assign an IP address to the attacker’s system, as the attacker could use the source IP address assigned to an eNB that they identified from captured traffic and then simply monitor the network for the responses. This would not be detectable in a typical unsecured LTE network, as the replies from scanned hosts would be discarded by the spoofed eNB. Using this method, an attacker would build up a picture of the topology of an operator’s network.

Once this reconnaissance step has been completed, the next phase for the attacker would typically be to attempt to compromise the NEs that have been identified. The information that has been gathered on those hosts would be used as part of that step.

3.2.2 S-GW denial of service

An example of a denial of service attack that can be performed against an S-GW is a GTP (GPRS Tunneling Protocol) flood over the S1-U interface. An attacker with sufficient processing resources can send a large number of malformed GTP messages to the S-GW, for example packets containing invalid TEIDs (Tunnel Endpoint Identifier), forcing the S-GW to perform separate lookups for each one. An attack such as this could cause high CPU use on the S-GW and prevent the handling of legitimate EPS bearer traffic.

The effect of a successful DoS attack on one or more S-GWs would be significant, especially if Voice over LTE (VoLTE) is used. All subscribers could lose data connectivity as well as Mobile Terminated (MT) and Mobile Originated (MO) call access if Circuit Switched Fall Back is not used. In the best case scenario, service quality and network performance would be affected.

3.2.3 MME denial of service

SCTP (Stream Control Transmission Protocol) is relatively resilient to DoS attacks when compared to TCP and UDP, however, the fact that peers are not authenticated in the LTE implementation means that messages can be spoofed to cause issues at higher layers. One example of this would be to spoof the NAS (non-access stratum) messages encapsulated by SCTP. There are known vulnerabilities in MME software implementations that can cause an MME to crash if the S1AP message content is malformed.
Also, the MME forwards User Equipment (UE) attach requests to the HSS prior to any authentication being performed. This means that malformed S1AP messages can also be targeted at the HSS stack.

A successful DoS attack on one or more MMEs would have a major effect on the network, as all cell sites served by those NEs would effectively be taken off air until the incident has been resolved. A successful DoS attack on the HSS via the MME would result in attach requests failing and subscribers being unable to receive service.

3.3 X2 interface vulnerabilities

The X2 interface provides connectivity between neighboring eNBs for handover operations initiated when a UE moves to a cell served by another eNB. All eNBs require IP connectivity to their neighbors in order to allow inter-eNB handover over X2. This exposes base stations to attack from other points on the network, which is often a large routing domain allowing IP connectivity from hundreds of other physical sites.

Similar to the backhaul connectivity risks, there are two main X2 interface vulnerabilities in an unsecured LTE backhaul network:

- Weak authentication of neighboring eNBs
- Inadequate trust zone segregation.

3.3.1 Weak authentication of neighboring eNBs

X2 connections between neighboring eNBs are unauthenticated. This means that a compromised eNB or any other host on the backhaul network is potentially able to launch an attack on other eNBs. This can expose the network stacks on eNBs to common Internet attack techniques used to obtain unauthorized system access and affect service availability.

3.3.2 Inadequate trust zone segregation

The only preventative control in place to protect eNBs from network attack is the physical security layer. A breach of physical security at a single eNB site would expose all neighboring eNBs and potentially others depending on the routing segregation implemented. Given that each eNB is typically located in a different physical location, this means that each site should be treated as a separate trust zone with network and application layer control over X2 communications to limit exposure to this threat.
3.4 X2 interface threats

3.4.1 eNB denial of service

If a physical site is compromised, an attacker could use that access to launch a DoS attack on all neighboring eNBs. Besides a bandwidth saturation attack, one example of a more sophisticated attack would be the transmission of a large number of maliciously crafted handover requests to a target eNB in order to trigger a CPU utilization overload.

3.4.2 Signaling storms

A compromised eNB site can also be used to cause a signaling storm on neighboring eNB air interfaces. Using a man-in-the-middle attack, it is possible to inject malicious SCTP messages containing paging messages for Globally Unique Temporary IDs (GUTI) that have been extracted from captured S1AP streams. This would not only potentially congest paging channels but would also result in a large number of reply messages to associated MMEs.

3.5 S1-U interface vulnerabilities

The S1-U interface handles the carriage of subscriber data, including VoLTE calls. The protocol used to encapsulate this user data is the GPRS Tunneling Protocol, which contains very limited security features.

There are three main S1-U interface vulnerabilities in an unsecured LTE backhaul network that allow for the interception of subscriber data:

- No native user plane encryption
- Weak integrity protection in GTP
- No authentication in GTP

3.5.1 No native user plane encryption

All GTP traffic sent over the S1-U interface is unencrypted unless IPSec is used, as opposed to the packet switched user plane in GSM and UMTS, which is natively ciphered. This means that all user data is sent without any form of confidentiality protection unless the subscribers themselves use network or application layer encryption. This vulnerability is particularly serious for VoLTE where voice calls can easily be intercepted, recorded and replayed unless a protocol such as Secure Real-time Transport Protocol (SRTP) is enforced by the IMS.
3.5.2 Weak integrity protection in GTP

The only integrity protection control implemented in GTP-U v1 (the version used in S1-U) is the optional sequential numbering of packets. GTP uses User Datagram Protocol as the underlying transport layer protocol which, unlike Transmission Control Protocol (TCP), does not perform any sequencing checks. This means that unless GTP sequencing is enabled, there is effectively no integrity protection. Even when sequence numbers are used in GTP packets, this control can be bypassed fairly easily.

3.5.3 No authentication in GTP

The main authentication mechanism in GTP-U v1 is the TEID. The main purpose of this 32-bit value is to identify individual S1 bearers within a tunnel established between the eNB and the SGW, rather than provide any form of strong authentication. This value can be easily spoofed and therefore subscribers can be impersonated by injecting traffic with a valid TEID. The TEID value itself is not protected, so this means that anyone with access to the S1-U traffic can view the TEIDs in use and use them to inject traffic into existing data sessions as part of an overbilling attack.

3.6 S1-U interface threats

3.6.1 VoLTE eavesdropping

It is possible to capture and replay voice calls if encryption is not implemented on either the LTE backhaul network or within the software on the UE and the IMS. This is because GTP does not protect the confidentiality of the data that it encapsulates, in this case the Realtime Transport Protocol (RTP) payload, which is the two-way subscriber voice transmission.

Once physical or radio link access is obtained, eavesdropping on subscriber calls can be carried out very easily using freely available packet capturing software such as Wireshark. The screenshot below is from the Wireshark Voice over IP player. It shows the decoding of a voice conversation directly from an S1-U interface packet capture.
3.6.2 Account hijacking

A common assumption made when assessing the requirement for LTE radio transport security is that all confidential data transmitted by subscribers will be protected at the application layer. For example, online banking data is typically encrypted using Transport Layer Security (TLS). However, there are still systems in use that do not protect potentially sensitive communications, one example being POP3. Although some providers use TLS to protect POP3, there are still many implementations without it.

What this means is that subscriber emails can be intercepted if IPSec is not in place to protect backhaul communications. This can be used as part of a targeted attack to, for example, hijack a cloud service account. In an account hijacking scenario, an attacker with access to a compromised backhaul link could request a password reset on behalf of a subscriber and intercept the subsequent email to take over that subscriber’s account.

3.6.3 Man-in-the-middle attack

Even if TLS is used to protect subscriber data, this is not a panacea for data confidentiality. TLS implementations typically depend on the end user to verify the authenticity of certificates that cannot be automatically verified using a Public Key Infrastructure (PKI) chain of trust. This means that an attacker with access to a backhaul link can proxy the TLS connection via their own system with an invalid certificate that the user will be prompted to verify. In many cases, the security
warning presented to the end user will be ignored, allowing the attacker to decrypt all confidential communications, including online banking logins and transactional information. In the worst case scenario, the attacker could inject their own packets into a packet stream and carry out fraudulent transactions.

### 3.6.4 Overbilling attack

The fact that there is no authentication and integrity checking implemented in GTPv1 means that LTE subscribers are vulnerable to overbilling attacks from an attacker able to access a backhaul link. Packets crafted with a valid TEID can be sent to impersonate legitimate user plane data across existing EPS bearers, thereby causing subscribers to be billed for data usage that they did not initiate.

### 3.7 S1-MME interface vulnerabilities

The S1-MME interface handles signaling between the eNB and the MME for functions such as UE attaches and paging. The protocol used to encapsulate this control data is the Stream Control Transmission Protocol. The signaling messages themselves are constructed in conformance with the S1 Application Protocol (S1AP).

There are two main S1-MME interface vulnerabilities in an unsecured LTE backhaul network that allow the interception of signaling messages:

- Limited control plane encryption
- No authentication in SCTP

#### 3.7.1 Limited control plane encryption

The only messaging within S1-MME that is natively encrypted is a subsection of the LTE non-access stratum (NAS) messages. However, this is optional and does not protect the entire sequence of NAS messages, leaving confidential data such as IMSI numbers unprotected even if it is enabled. All other signaling messages are sent in clear text, with S1AP dissectors freely available on the Internet to extract the content of those messages.

Data that is exposed in clear text includes IMSI numbers, APNs and the IP addresses of critical NEs, including the MME, S-GW and DNS servers. The IP address allocated to the UE is also exposed.

The interception of this data can be conducted completely passively, meaning that it would be almost impossible for the operator to detect that such an interception was being conducted.
3.7.2 No authentication in SCTP

The S1-MME implementation of the SCTP provides no form of chunk authentication. This means that the MME allows SCTP associations from any host on the network.

3.8 S1-MME interface threats

3.8.1 IMSI catching

The IMSI is used to uniquely identify subscribers on a mobile network. It can be used to identify and track subscribers and as such is considered confidential. The protection of IMSIs is catered for in the 3GPP LTE specifications to the extent that it is replaced by a temporary value, the Globally Unique Temporary ID (GUTI), once the UE has completed the attach procedure.

However, the ciphering of NAS messages (if NAS security is enabled on the network) does not protect the IMSI, as this is always sent in clear text. This means that an attacker with access to an unsecured backhaul link will be able to track subscribers.

The following screenshot shows an NAS attach message dissected by Wireshark. The cleartext IMSI is highlighted in blue:
3.8.2 Network enumeration

Besides the IMSI, other data can be extracted from unprotected S1AP messages to assist an attacker with enumerating the network as part of their network reconnaissance activity. An example of information that would be useful for an attacker is shown in the Wireshark screenshot of an S1AP InitialContextSetup procedure. The highlighted fields in this screenshot show the IP addresses of the MME, eNB and S-GW. The GTP TEID is also shown, which would be useful for hijacking sessions.

Figure 5 - Network Enumeration via S1AP
If the NAS is not ciphered, the S1AP message will also reveal the APN and the assigned UE and DNS server addresses as shown in the screenshot below.

Figure 6 - Network enumeration via un-ciphered NAS
4. Unprotected LTE radio transport risk assessment

4.1 Risk matrix

The following risk matrix is used to rate each of the risks discussed in this paper. The ratings themselves are indicative only and are intended to provide guidance to operators based on their risk appetite and corporate governance controls.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Catastrophic</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>2. Major</td>
<td>Yellow</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>3. Moderate</td>
<td>Yellow</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>4. Minor</td>
<td>Yellow</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>5. Insignificant</td>
<td>Yellow</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
</tbody>
</table>

Figure 7 - Risk matrix

4.2 Risk ratings

This section provides an indicative rating of each risk described in this paper, based on the above matrix and a typical operator environment.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network reconnaissance</td>
<td>3</td>
<td>5</td>
<td>Low</td>
</tr>
<tr>
<td>S-GW denial of service</td>
<td>3</td>
<td>2</td>
<td>Medium</td>
</tr>
<tr>
<td>MME denial of service</td>
<td>3</td>
<td>1</td>
<td>High</td>
</tr>
<tr>
<td>eNB denial of service</td>
<td>2</td>
<td>3</td>
<td>Medium</td>
</tr>
<tr>
<td>Signalling storms</td>
<td>2</td>
<td>3</td>
<td>Medium</td>
</tr>
<tr>
<td>VoLTE eavesdropping</td>
<td>3</td>
<td>2</td>
<td>Medium</td>
</tr>
<tr>
<td>Account hijacking</td>
<td>2</td>
<td>3</td>
<td>Medium</td>
</tr>
<tr>
<td>Man in the middle attack</td>
<td>2</td>
<td>3</td>
<td>Medium</td>
</tr>
<tr>
<td>Overbilling attack</td>
<td>2</td>
<td>3</td>
<td>Medium</td>
</tr>
<tr>
<td>IMSI catching</td>
<td>3</td>
<td>3</td>
<td>Medium</td>
</tr>
<tr>
<td>Network enumeration</td>
<td>3</td>
<td>5</td>
<td>Low</td>
</tr>
</tbody>
</table>

Figure 8 - Risk ratings
5. Mitigating controls specified by 3GPP

5.1 Nokia and Check Point Carrier Security Solution

**Check Point 61000 Carrier and 21000 Carrier**

The Check Point Carrier-Grade 61000 and 21000 platforms provide the industry’s most powerful Telco security solution, offering the utmost performance and capacity to protect the continuous growth of 3G and 4G LTE network infrastructures. These unique platforms enable operators to use a unified platform to secure all interfaces including Radio Access, Internet and Roaming. These scalable platforms come with advanced inspection and security for LTE protocols to protect against sophisticated attacks such as Spoofing, DDoS, Signaling Storm, Over-billing attacks and Malware.

Check Point carrier platforms comply with 3GPP specifications. They allow operators to: connect thousands of 4G LTE eNBs to the EPC network securely; use IPSec to authorize radio stations’ connectivity and to encrypt user data traffic; easily provision the IPSec connectivity when adding more radio stations; ensure service availability with backend services using Dead-Pear-Detection and fully redundant hardware platform; support ESP and IKEv2 to deliver data traffic confidentiality and integrity with AES, SHA-1 or TripleDES encryption algorithms. It also protects against eavesdropping and data tampering on the control plane and user traffic.

The Check Point Carrier Security platforms can also inspect and secure 3G and 4G IP protocols including GTP, SCTP and Diameter. They allow mobile operators to connect the packet core securely to untrusted interfaces such as the roaming partners or the radio network. Operators can define advanced Diameter and GTP protocols policies to protect subscribers’ data in MME and HSS.

**Nokia Carrier Security Solution**

In a nutshell, Nokia security recommends the encryption of all traffic planes (U, C and M planes) from the base station to the core network. To achieve this, a SEG (Security Gateway) is placed in front of the core network to act as a gate keeper, allowing only authenticated and authorized traffic into the core network, as shown in figure 5:
The main motivation for encrypting all traffic planes is not to cipher the traffic, but moreover, to protect the core network by literally hiding it behind the SEG. This way, only traffic that is authenticated and authorized by the SEG is allowed to reach the core networks. From the transport network perspective, the entire core network is not visible (no IP routing). Only traffic inside the VPN tunnel is forwarded to the core network - for this traffic, the transport network is fully transparent.

In IP networks, ensuring authentication and authorization means using IPSec (Internet Protocol Security). This protocol encrypts all communications, helping mitigate eavesdropping and traffic manipulation.

IPSec has been used in IP networks since the mid-1990s. It is also well known to mobile operators through interconnection of data center sites or infrastructure. The new challenge in the proposed solution is in the number of connections from one side and the traffic throughput that must be managed on the other side. Simultaneously, service availability must be ensured at all times.

These challenges have been addressed by Nokia security R&D over the past years in close cooperation with our partners.

One of these challenges is managing thousands of IPSec connections with the SEGs. Nokia has relied on the 3GPP (TS 33.310) mandating the use of digital certificates to manage the connection of base stations to the SEGs. As seen in figure 6, Nokia has worked with one of its partners to develop a PKI solution, also known as a Certificate Authority or CA solution. This fulfills both the 3GPP standards and the full automation required in a mobile operator environment.
5.1.1 3GPP compliance


The 3GPP spec TS 33.401 has, since Release 8, mandated confidentiality and integrity protection on the backhaul link user plane between the eNB and Serving GW (not Packet GW, which is further into the core), cf. clause 12: “In order to protect the S1 and X2 user plane as required by clause 5.3.4, it is required to implement IPSec ESP according to RFC 4303 [7] as profiled by TS 33.210 [5], with confidentiality, integrity and replay protection.”

In regards to the solution described in this document, we refer to the following 3GPP documents and sections that underline how the described solution directly improves network quality as defined by 3GPP:

- 3GPP TS 33.401 (Security Architecture), chapter 5.3.2:

  “Security associations are required between the EPS core and the eNB and between adjacent eNBs, connected via X2. These security association establishments shall be mutually authenticated and used for communication between the entities.”

Here, 3GPP directly defines that compliance with its security architecture cannot be achieved, for example by planting a firewall in front of the EPC perimeter. Much more, it is stated later in the document that all eNB connections are full IPSec connections.
• 3GPP TS 33.821 (Rationale of Security Decisions in RAN), chapter 5.2 & 5.3

A wide variety of threats arising from unsecured S1 connections is described directly in chapters 5.2 and 5.3 of this rationale, and indirectly with other threats mentioned in the same document. The described solution mitigates those threats directly and therefore needs to be considered along any LTE solution or transport network modernization that is supposed to be SAE capable.

5.1.2 Solution benefits

Encrypting all communication between base stations and core network and only allowing traffic to reach the core network after being authenticated and authorized ensures that all security challenges are addressed and mitigated as follows:

Authentication

A first step to securing the EPC and the eNBs is to identify the entities that allow connections to the EPC/eNB. Security is achieved using PKI.

The solution includes:

1. A Certificate Authority that issues, deletes and revokes certificates for the eNBs and the SEG.
2. Protocols (IKEv1/v2 IPSec Key Exchange) that use the certificates to create mutual authentication between eNBs and SEG.
3. A revocation mechanism (CRL Certificate revocation list) to distribute certificates that are no longer trusted.

Both SEG and eNBs should include the three elements above.

Communication confidentiality and integrity protection

After SEG and eNBs authenticate each other, both entities can generate encryption and authentication keys for the traffic that flows between the eNBs and the SEG. Both the SEG and the eNB accept only trusted IPSec traffic, which means untrusted traffic is blocked, ensuring the integrity and confidentiality of the communication.

Usually, the X2 traffic that flows between eNBs passes through the SEG, which acts as a hub. This removes the overhead configuring IPSec tunnel between each and every eNB, mitigating the security risks from a full mesh interconnected radio access network over which a mobile operator has no or only limited control.
Access control/Stateful inspection

On top of the IKE/IPSec capabilities, the SEG can offer additional security layers.

The first layer is an access control and SCTP/GTP stateful inspection engine to validate that the traffic arriving inside the IPSec tunnel is legitimate. The second layer is a monitoring layer that alerts when traffic deviates from normal flow. The third layer is DOS protection and rate limits that limit the amount of signaling and data that can arrive from a compromised eNBs into the EPC.

All of the above functionality adds security to the LTE protocol, but also introduces additional points of failure.

Redundancy

When implementing the security architecture, it is important to add layers of redundancy, to mitigate these potential points of failure. The key components for a robust architecture are:

1. Ability to establish thousands of IPSec tunnels in a short time (seconds). The SEG should be able to negotiate thousands of IKEs per second.
2. Detection mechanism in case the tunnel is dead. This is done by supporting a DPD (dead per detection) mechanism.
3. Redundancy of IKE/IPSec keys inside a single SEG (in the case of chassis based solutions).
4. Clustering solution between two SEGs on the same physical site, including full redundancy of IKE/IPSec keys between the cluster members.
5. Geo-Cluster solution. Ability to set SEG/clusters at two different geographical locations.

5.2 Case study: Large European mobile operator

A large European mobile operator chose Nokia and Check Point to protect its 4G LTE network from unauthorized access, manipulation and other threats. Further benefits from the solution include authentication of network elements and lower costs due to the automatic rollout and lifecycle management of base station certificates. The implementation is based on the architecture elements described above, consisting of IKE/IPSec with DPD between the eNBs and the SEG.

All traffic and all the encryption keys are synced across the Check Point 61000 Security Gateway clusters. The 61000 carrier chassis acts as a single security gateway, aggregating encrypted traffic from thousands of eNBs. The solution allows the operator to scale up performance by adding more Gateway Module hardware blades to secure more traffic from more eNBs.
The operator uses Geo-clustering between different data centers, with sites located hundreds of kilometers from each other. Figure 7 shows the geo-redundant architecture at a high level.

*Figure 11 - Geo-redundant SEG deployment*
6. Conclusion

The LTE S1 and X2 interfaces used for the transport of both user- and control data from the base station to the packet core and between base stations expose the mobile infrastructure to a wide range of attacks.

However, the risks of these attacks can be mitigated using a 3GPP-compliant security architecture. Furthermore, with the correct approach to solution selection and deployment, it is possible to avoid unnecessary complexity in the network, in turn avoiding the introduction of additional points of failure. This gives operators an LTE transport security solution that is simple, redundant and easy to scale.
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP</td>
<td>The 3rd Generation Partnership Project</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>APN</td>
<td>Access Point Name</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial-of-Service</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial-of-Service</td>
</tr>
<tr>
<td>DPD</td>
<td>Dead Per Detection</td>
</tr>
<tr>
<td>eNB</td>
<td>eNodeB</td>
</tr>
<tr>
<td>EPC</td>
<td>Evolved Packet Core</td>
</tr>
<tr>
<td>EPS</td>
<td>Evolved Packet System</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>EUTRAN</td>
<td>Evolved Universal Terrestrial Radio Access Network</td>
</tr>
<tr>
<td>GGSN</td>
<td>Gateway GPRS Support Node</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>GTP</td>
<td>GPRS Tunneling Protocol</td>
</tr>
<tr>
<td>GUTI</td>
<td>Globally Unique Temporary ID</td>
</tr>
<tr>
<td>GW</td>
<td>Gateway</td>
</tr>
<tr>
<td>HSS</td>
<td>Home Subscriber Server</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identity</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution</td>
</tr>
<tr>
<td>MME</td>
<td>Mobility Management Entity</td>
</tr>
<tr>
<td>MO</td>
<td>Mobile Originated</td>
</tr>
<tr>
<td>MT</td>
<td>Mobile Terminated</td>
</tr>
<tr>
<td>NAS</td>
<td>Non-Access Stratum</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>NDS</td>
<td>Network Domain Security</td>
</tr>
<tr>
<td>NE</td>
<td>Network Element</td>
</tr>
<tr>
<td>POP3</td>
<td>Post Office Protocol, version 3</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>RAN</td>
<td>Radio Access Network</td>
</tr>
<tr>
<td>RNC</td>
<td>Radio Network Controller</td>
</tr>
<tr>
<td>RTP</td>
<td>Realtime Transport Protocol</td>
</tr>
<tr>
<td>S1 AP</td>
<td>S1 Application protocol</td>
</tr>
<tr>
<td>S-GW</td>
<td>Serving Gateway</td>
</tr>
<tr>
<td>SAE-GW</td>
<td>System Architecture Evolution Gateway</td>
</tr>
<tr>
<td>SEG</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>SCTP</td>
<td>Stream Control Transmission Protocol</td>
</tr>
<tr>
<td>SEG</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>SHA-1</td>
<td>Secure Hash Algorithm version 1</td>
</tr>
<tr>
<td>SRTP</td>
<td>Secure Real-time Transport Protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TEID</td>
<td>Tunnel Endpoint Identifier</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TripleDES</td>
<td>Triple Data Encryption Algorithm</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UE</td>
<td>User Equipment</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications Service</td>
</tr>
<tr>
<td>VoLTE</td>
<td>Voice over LTE</td>
</tr>
</tbody>
</table>
Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

Nokia
Nokia Solutions and Networks Oy
P.O. Box 1
FI-02022
Finland

Visiting address:
Karaportti 3,
ESPOO,
Finland
Switchboard +358 71 400 4000

Product code C401-011931-WP-201510-1-EN

© Nokia Solutions and Networks 2015