MWR InfoSecurity

LTE Security Testing

Black Hat Edition

6th November 2012

Contents

1. Introduction

It is an exciting time in the world of telecommunications and mobile working. We have seen the unprecedented proliferation of mobile devices including smartphones and tablets coupled with the increasing accessibility of 4G network services. The result is a highly versatile and mobile workforce that wants to consume new technology faster than ever and wants to innovate their working practices and methods. So at the point where the adoption of 4G technology by business and consumers alike is set to rise massively it is important we have considered security and that it isn't used to slow the adoption process.

First let's be clear about the definition of 4G, we are talking about the 3GPP Long Term Evolution (LTE) Advanced standards, and not any of the other competing technologies such as WiMAX. The LTE standard is primarily about improving the user experience for mobile communication; however, also includes added benefits for the operators.

In simple terms the LTE standard aims to support the delivery of network services that:

- Are extremely fast offering high bandwidth
- Have lower levels of latency
- Facilitate user equipment moving at high speeds
- Use a simplified and scalable back-end architecture

The number of components, interfaces and protocols that existed in older methods of mobile data delivery has historically created a barrier during deployment. The lack of geographic scalability has resulted in less than optimal population coverage from network providers. The LTE specification aims to enable the delivery of improved mobile services and to reduce the complexity and cost of deploying mobile data networks.

In LTE, this has partly been achieved by consolidation of components that are used in legacy infrastructures to produce a flatter network topology. Radio layer components have been redesigned for faster deployment with a modular design that allows for the effective handover of user sessions from one geographic node to another and aspects of the non-radio layer more closely resemble traditional IP networks. These result in improvements to the service delivered to customers, additionally lower deployment and maintenance costs for the network provider should act as an incentive to increase coverage.

So why might someone play the security card with LTE? After all, the standards address some of the concerns raised by previous incarnations of mobile technology, so surely it must be more secure than 3G, as well as everything that came before it. I can already hear you saying "No", it uses IP for all back-end communications so it must be easier to attack and therefore must be more insecure. After all, the older technology used weird and wonderful protocols and you couldn't easily plug your laptop into the base station and start attacking the back-end network with common tools.

When you look at LTE you will clearly see that it uses IP networks throughout and you can now use the tools you know and love against the back-end components. This includes the Base Station equivalent, known as the evolved NodeB (eNodeB), therefore making it much easier to attack. This is where we begin to run into some of the problems we typically encounter when looking at the security of telecoms environments, namely acronyms and strange sounding protocols.

When looking at a 4G network for the first time these may seem a little daunting, from the aforementioned eNodeB to the systems within the Evolved Packet Core (EPC). Additionally, components like the MME, HSS, PCRF, SGw and PGw may be new to you, particularly if you haven't also looked at a 3G network. Secondly, there are some protocols that you might not be that familiar with, for example, have you ever looked at SCTP? Do you know what S1AP is? What about GTP and all its different flavours? Putting the protocols and the components together, what are the most profitable attacks, what can you try and spoof? Where would you most like to be able to route packets to? Which protocols should we be tuning our fuzzers to?

When it comes to preparing for testing in an LTE environment there are probably a whole range of questions that you would like to be able to answer. Additionally, when you do find bugs lurking within the environment, what is a sensible way of addressing them?

In this white paper we will provide you with a starting point on the subject of LTE so you can have confidence in the testing you do. It will outline the important components in an LTE environment, scenarios for security testing that should be considered and some key security controls you should be implementing to protect the network.

2. The Components

The objective of this white paper isn't to provide you with a full description of all the systems and protocols that comprise an LTE network. However, it provides an insight into the roles of key attributes of the system so that you can clearly understand what is important when you come to test its security. Let's start with some of the main components as illustrated in Figure 1, and followed by more detailed descriptions of the key components.

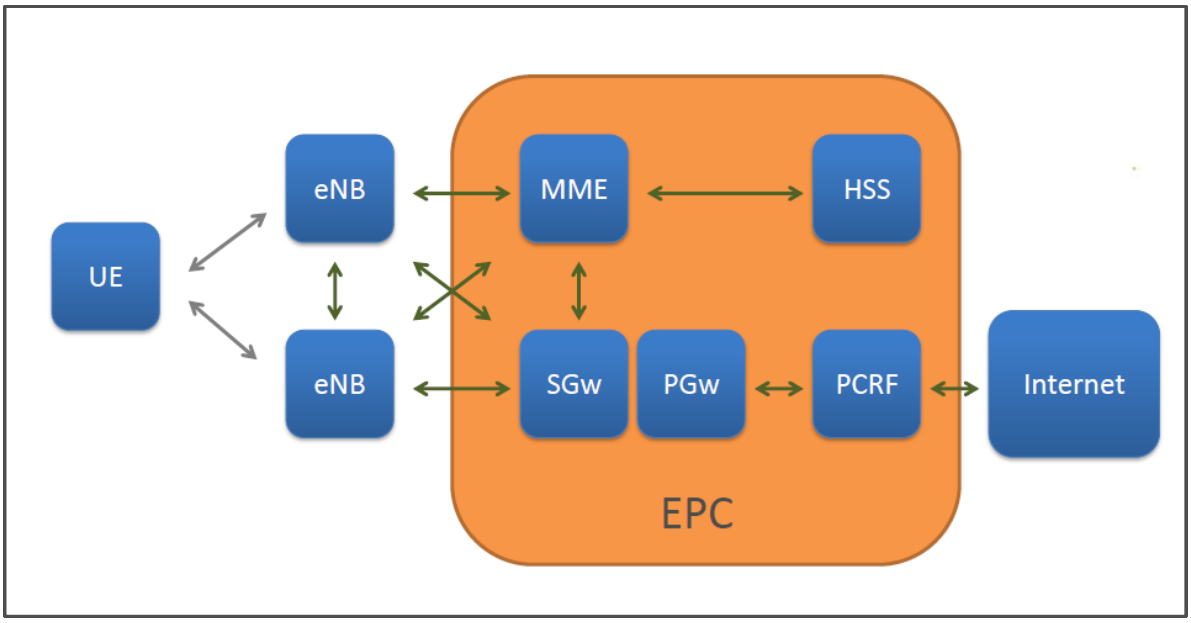

Figure 1 – A conceptual view of an LTE environment

User Equipment

UE is a generic term that refers to any device or system that consumes IP services in the environment. At present UE is primarily composed of USB dongles and LTE network hubs, but there are now increasing numbers of smartphones and tablets that are 4G enabled. UE should only be capable of consuming services on the Internet or those specifically facilitated by the network operator; they should never to able to participate in direct IP communication within the environment.

Evolved NodeB

An eNodeB comprises an evolution of the Base Transceiver Station (BTS) as present in previous GSM implementations and acts as the bridge between wireless and wired networks. An eNodeB will typically have three LTE specific interfaces, one wireless or air interface (known as Uu), one for inter-eNodeB communication (known as X2) and one for communication with the MME and Serving Gateway (known as S1). These devices may also contain other interfaces, such as those used for management, that use IP or Universal Serial Bus (USB) communication although these are not specified by the LTE standard. The eNodeB will typically be attached to an external aerial via the Uu interface.

Evolved Packet Core

The EPC is the collective term for the back-end infrastructure that the eNodeBs communicate with and through which user traffic passes. The EPC contains a number of discrete components that play different roles. The primary change in an environment from that which exists in previous technologies is the use of the Internet Protocol (IP) in all wired communication.

Home Subscriber Service

The Home Subscriber Service (HSS) is a central store of all user related subscription data. These profiles identify the level of access that user equipment will have on the network and the services and data bearers that are mandated by these profiles. The HSS participates in the management of UE across cells, call establishment support, user authentication and authorisation. UE is authenticated to the network using data that is derived from keys that are stored within a Universal Subscriber Identity Module (USIM) and within the HSS.

Mobility Management Entity

The MME is the control node for the LTE network. It is responsible for the tracking and management of UE that is in idle mode. The MME is involved in the brokering of data bearers and the assignment of a Serving Gateway (SGW) to UE during the registration process. By interacting with the HSS, the MME handles authentication of UE in the registration phase.

Serving Gateway

The Serving Gateway (SGW) is primarily responsible for the management of UE state information and the routing of user data packets. Additionally, the SGW is used as an anchor point for UE crossing from one eNodeB’s coverage area to another.

Packet Data Network (PDN) Gateway

The Packet Data Network Gateway (PGW) provides an entry and exit point for UE that is accessing external packet data networks. The PGW implements deep packet inspection for the profiling of data channels and the provisioning of suitable data bearers.

Unified/Consolidated Gateway

A unified or consolidated gateway combines the functionality of both the SGW and PGW into a single component with internal communication between the two.

3. The Protocols

One of the major changes between LTE and previous technologies is the use of the Internet Protocol (IP) for communications between components in the environment. This use of IP provides greater scope for an attacker to abuse the features of the IP protocol, specifically because the network design is more likely to share components between user and control planes. More interestingly a number of additional protocols use IP for their transport and require specific knowledge and understanding. The following protocols used within the wired network are critical to the security of an LTE environment and testing activities should include analysis of them and the manner in which they interact with individual components:

Session Control Transport Protocol
Alongside both TCP and UDP, SCTP is used for a number of communication streams within the back-end network. The primary use of SCTP is for the handling of critical communications between eNodeBs and the MME where robust communication is critical to the successful operation of the environment.

S1 Application Protocol
S1AP supports the transfer of data between eNodeBs and the MME. This protocol is used to transfer signalling information between the UE and the MME and to manage session state between eNodeBs and the MME. The protocol uses the SCTP for underlying session management and guaranteed delivery. Within S1AP, a pair of IDs are used to track the identity of an individual UE in the data that is communicated. Generation of one of these IDs is the responsibility of the eNodeB and the other is that of the MME.

X2 Application Protocol
X2AP provides the communication of data between individual eNodeB components and is similar to S1AP in its structure. This is used to transfer information about UE when performing a mobile handover. The protocol uses the Session Control Transport Protocol (SCTP) for underlying session management and guaranteed delivery.

GPRS Tunnelling Protocol User
GTP-U is used for the transfer of user data between the eNodeB and the Serving Gateway as well as between eNodeBs during X2 handover. The protocol is used to encapsulate a user's IP Traffic so that it can be transported into the EPC where it is subsequently unencapsulated and routed onwards to its destination. As a GTP packet can be encapsulated inside another, it is possible to construct an IP packet with multiple layers of GTP data. If not correctly handled by the equipment this might allow an attacker to use Encapsulation to bypass security controls. The eNodeB will always add one layer of IP data to the packet sent by the UE when encapsulating the data therefore an attacker does not have full control over its construction.

GPRS Tunnelling Protocol Control
GTP-C can be used for communication between back-end components within the EPC although it is not a principle part of the standard. The protocol is also used by legacy 3G components although transport over IP is a requirement in LTE.

4. Testing Approach

When performing testing within an LTE environment, a number of attack scenarios should be considered based on viable threat scenarios that will exist in any implementation. Attacks that are conducted across the air interface of the environment are assessed to be of greatest concern and therefore a large amount of testing should be conducted from this perspective. However, it is important that a threat modelling based approach is used to identify where the critical controls are within any given deployment and that an appropriate level of testing is used to provide assurances about them.

There are four primary testing locations that should be considered when planning a security testing engagement within an LTE environment. These are illustrated in Figure 2.

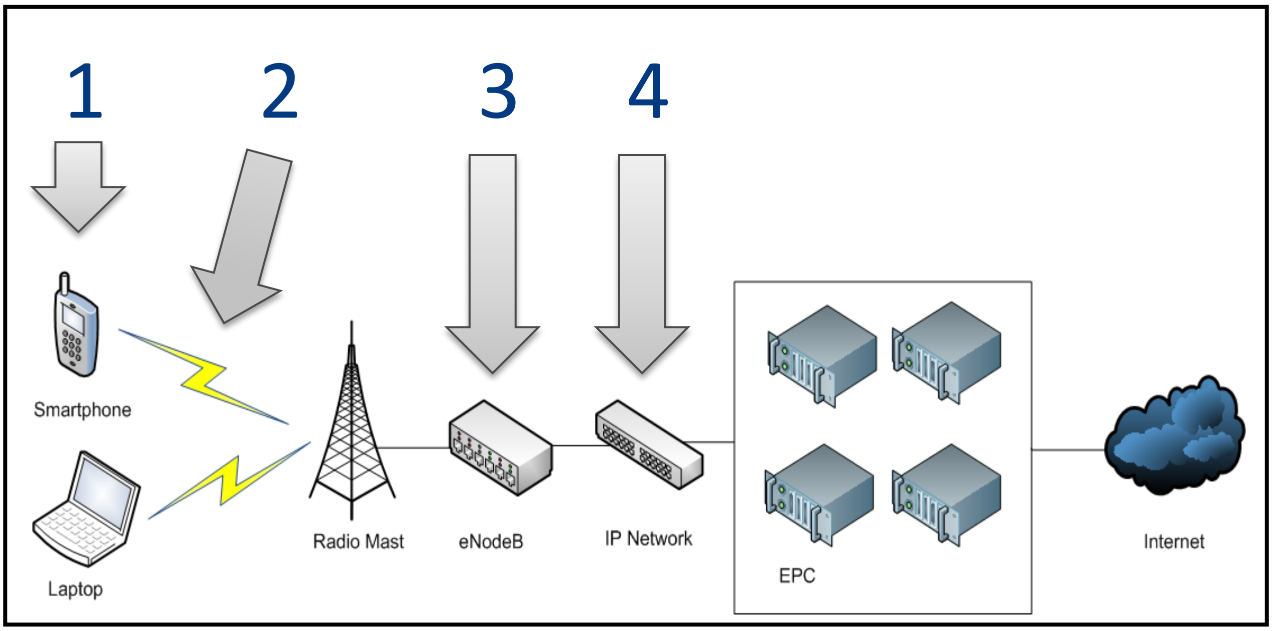

Figure 2 – Proposed security testing locations within an LTE environment

Location 1

Tests conducted from this location emulate an attacker with wireless access to an LTE environment through an operator-provided dongle, home router or smartphone. The attacker could potentially attack the environment through routing and spoofing attacks, primarily using IP Traffic sent from a laptop or other connected system.

The following types of testing activities are recommended at this location:

- Extent of UE access to the EPC
- Accessibility of other UE
- IP spoofing attacks
- Use of special IP addresses (eg 0.0.0.0 and 127.0.0.1)
- SCTP enumeration and endpoint discovery
- GTP-C analysis and probing
- GTP-U spoofing and tunnel ID guessing
- Multiple encapsulation attacks

Location 2

Tests conducted from this location emulate an attacker with the ability to monitor and intercept wireless communications passing between a user and an operator's radio mast. Without access to vendor equipment, it will be very difficult to perform practical attacks at this location given the sophistication of the wireless technology that is used; however, as has been illustrated recently it is possible to build LTE stacks that could be used to test this interface although this is non-trivial to do.

The following types of testing activities are recommended at this location if appropriate tools can be built:

- Baseband fuzzing
- Wireless protocol manipulation
- Traffic sniffing
- Fake base station deployment

There are controls built into the standard to provide protection against some of these techniques; however, implementation quality is still a big factor in these being effective in practice.

Location 3

This emulates an attacker with physical access to an eNodeB and any associated cabling or network equipment. The attacker could attempt to compromise the eNodeB physically and connect to unused ports or tamper with the network cables that are attached.

The following types of testing activities are recommended at this location:

- Testing of management interfaces
- Traffic sniffing on wired interfaces
- Probing exposed USB ports
- Assessment of physical security controls

Location 4

This emulates an attacker with IP access to the network between the eNodeB and EPC and is assumed possible at any location between them. Conducting testing from this location emulates an attacker who has identified a mechanism for sending and receiving traffic at this location. This could be through unauthorised physical access or through a logical attack from the air interface. At this location, the testing should include analysis of both the control plane (used for signalling) and the user plane (used for transferring a user's data).

The following types of testing activities are recommended at this location:

- SCTP fuzzing
- SCTP session parameter analysis
- S1AP logic and protocol attacks
- S1AP eNodeB spoofing
- X2AP logic and protocol attacks
- GTP spoofing and tunnel ID analysis
- Routing and VLAN hopping attacks
- IPSec configuration assessment

5. Conclusions

There are number of recommendations that are assessed as being critical with respect to the implementation of security controls within an LTE environment. The most important of these controls are the use of IPSec between eNodeBs and the EPC and secure design and configuration of IP routing. Each of these key controls should be covered by the testing approach outlined previously and more detail about each of the key controls is described here.

5.1. Design and Configuration of IP Routing

Ensuring that UE cannot access any services within the EPC is a fundamental requirement of the security model. The design of the architecture in the core is therefore important to being able to achieve this in an effective manner.

Preventing the routing of traffic from UE into the inner part of the EPC should be achieved by a combination of secure design and effective routing configuration. One of the primary considerations is how traffic on the Internet facing side of the PDN Gateway is routed and this should ideally avoid any switches or network equipment that has a route into the core of the EPC.

The design of IP routing in the environment is complex and will typically require the use of different types of network device will utilise multiple VLANs and use multiple IP address ranges. If both IPv4 and IPv6 support is required for both users and within core this can also increase complexity. Ensuring a robust architecture is designed is one of the most fundamental steps that is required in securing the environment. This should be validated with security testing as described previously.

5.2. IPSec

In a default configuration, there is no method of providing authentication, confidentiality or integrity protection for any communication that occurs between eNodeB and the EPC. As eNodeBs will be placed in locations that may have poor physical security controls, these communications need to be secured using other means.

IPSec is accepted as being the recommended method of securing communication on the S1, X2 and user plane connections within an LTE environment. However, there are several challenges to implementing it in a secure manner.

It is recommended that any IPSec connections to the eNodeB are terminated in the host as the ability to control network level access into the EPC is vitally important. This can be achieved by terminating IPSec either at a gateway or within the individual EPC components.

When configuring systems in the EPC and eNodeB to use IPSec for secure communication, it is recommended that services and interfaces are not accessible without using IPSec. This is of particular concern when physical access can be gained to exposed interfaces on an eNodeB. IPSec also needs to be enforced on all interfaces that are enabled but not used. The quality of the IPSec implementation is another key area for security testing as described previously.

IPSec was not part of the LTE standard; however, it is required to secure the network when an eNodeB is located at an insecure location. In particular, it should be noted that the authentication that can be provided by a correctly configured IPSec implementation is not equivalent to and cannot be translated to authentication in the LTE network. A single compromised IPSec connection might allow an attacker to impersonate other nodes in the network and would expose systems to attacks at the level of the protocols that are otherwise protected within the IPSec tunnel.