LTE Security

Threats, attacks and protection mechanisms

Sony Cherukara

LTE (Long Term Evolution) is the evolution of the UTRAN (Universal Terrestrial Radio Access Network) to E-UTRAN (Evolved UTRAN) to support a high-data-rate, low-latency, packet-optimized radio access technology. This document provides an overview of the security aspects of an LTE implementation.

Palindrome Technologies
100 Village Court
Hazlet, NJ 07730, USA
Tel: +1 (732) 416-7722
www.palindrometech.com

LTE Security – Threats Attacks and Protection Mechanisms

Introduction

LTE (Long Term Evolution) is the evolution of the UTRAN (Universal Terrestrial Radio Access Network) to E-UTRAN (Evolved UTRAN) to support a high-data-rate, low-latency, packet-optimized radio access technology. Long Term Evolution (LTE[1]) 4th generation (4G) data network will provide significantly increased user data throughput in both the downlink (network to mobile) and uplink (mobile to network) direction, decreased latency, and increased total network traffic capacity. Additionally, the LTE network will be deployed with features required for future support of media services, including VoIP, Video, and other enhanced services. . This document provides an overview of the security aspects of an LTE implementation.

Figure 1, depicts the logical structure of a network that implements 3GPP specifications. The core network that supports LTE is called the EPC (Evolved Packet Core). The EPC/LTE architecture comprises a radio domain and a packet core domain which has multiple interfaces to the user management, circuit core and IMS domains. In addition to these interfaces, the packet core may also connect directly to other IP networks.

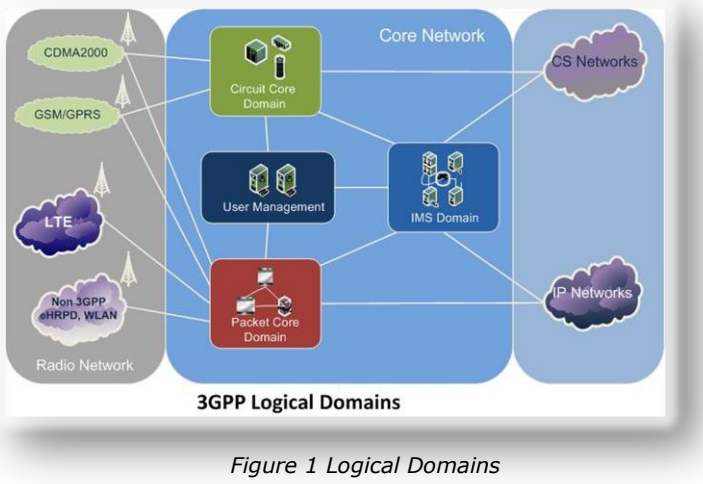


Figure 1 Logical Domains

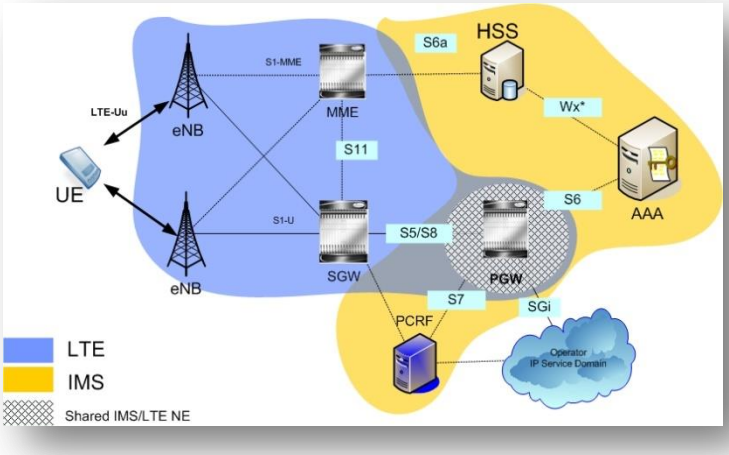
Whereas GSM/UMTS-based operators have a natural evolution to LTE, many CDMA-based mobile operators have also decided to evolve to the LTE specification.

The CDMA operator LTE implementation will support several new capabilities that are not currently present in their current data networks. These new capabilities include:

- Data roaming capabilities with GSM-based data networks
- Support for IPv6 based data connections
- SIM-based device portable user credentials

[1] Also known as evolved Universal Terrestrial Radio Access (eUTRA)

LTE operates in a newly licensed frequency band at 700 MHz and includes certain open access requirements to support "*any device, any application*". This approach requires operators to publish device specifications for suppliers in order to allow any device that meets these requirements to access the network. Furthermore it is expected that the operator will have to allow subscribers (including roaming users) to use any application on their devices as long as it does not impact the network.



LTE provides a new fourth generation data network for Verizon Wireless. LTE will provide users with much higher throughput, up to 12Mbs in the network to mobile direction (downlink) and 5Mbs in the mobile to network direction (uplink). LTE will provide lower data traffic latency. LTE is compatible with the 3GPP standards and provides additional opportunities for roaming with global GSM-based partner networks.

The increased throughput and lower latency combine to make LTE suitable for a variety of advanced features and applications, including VoIP services and multimedia applications. In addition, LTE's increased capabilities allow for a richer experience using existing connected laptop (BBA), PDA and ultimately feature phone applications. LTE Phase 1 is expected to be followed by further development of the LTE Network to support these additional services.

Architecture overview

The EPC architecture is primarily focused on providing IP connectivity over LTE access. The two main principles guiding the design of the EPC architecture are a 'flat' architecture for optimized user traffic and separation of the signaling from the user traffic. A 'flat' architecture implies that a minimal number of nodes are involved in the processing of the user data, thereby reducing costs and increasing efficiency.
The separation of signaling and user traffic was considered necessary due to different scaling concerns. The scaling of signaling data is a function of the number of users accessing the network, whereas the user data scaling typically occurs as a function of new services that are deployed on the network.

The following table provides a list of the LTE/EPC components.

Component	Description/Function
UE	User Equipment, 3G/4G
HSS	Home Subscriber Service
AAA	Authentication, Authorization and Accounting function
PCRF	Policy Control Resource Function
PGW	Packet Data Network Gateway
HSGW	HRPD Serving Gateway
SGW	Serving Gateway
MME	Mobility Management Entity
eNB	E Node B (base station)
FOTA	Firmware Over The Air
DNS	Domain Naming Service

The following subsections provide further details on each element in the LTE/EPC implementation.

UE/UICC

The Universal Integrated Circuit Card (UICC) maintains subscriber and network information (e.g., authentication credentials, encryption keys) to support signaling and data security functions such as authentication and confidentiality. In some cases a one-to-one association between the UICC and the Mobile Equipment (ME) can be established and constitute the User Equipment (UE) (e.g., cell-phone) but in other cases the UICC may not be directly associated with the ME (e.g., laptop using a USB with UICC).

A UICC may include several applications (USIM, ISIM, CSIM and SIM)[2] in order to support access to different networks (e.g., CDMA/GSM). The UICC contains a USIM (Universal Subscriber Identity Module) application which manages the subscriber credentials along with an ISIM (IP multimedia Services Identity Module) to provide access to the IMS core (VoRA services). In addition, it may also contain a CSIM (CDMA SIM) to provide access to the CDMA network. Verizon Wireless has chosen not to implement this feature. This Threat Analysis focused on USIM threats and associated controls.

The USIM holds the master pre-shared key (which is also maintained by the AuC) which is used to derive sub-keys for session integrity, authentication and encryption (e.g., IK and CK).

MME (Mobility Management Entity)

The MME is the primary node that intermediates access to the LTE network by interacting with the HSS and relaying authentication credentials received from the UE. The MME is responsible for idle mode UE tracking and paging procedures including

[2] A UICC which maintains a USIM, SIM and CSIM applications is called R-UIC (removable user identity card).

retransmissions. It is involved in the bearer activation/deactivation process and is also responsible for selecting the corresponding SGW for a UE during the initial attachment and during intra-LTE handover involving Core Network (CN) node relocation. The Non-Access Stratum (NAS) signaling terminates at the MME and it is also responsible for generation and allocation of temporary identities to UEs. It checks the authorization of the UE to camp on the service provider's Public Land Mobile Network (PLMN) and enforces UE roaming restrictions. The MME is the termination point in the network for ciphering/integrity protection for NAS signaling and handles the security key management. Lawful interception of signaling is also supported by the MME. The MME also provides the control plane function for mobility between LTE and 2G/3G access networks with the S3 interface terminating at the MME from the SGSN. The MME also terminates the S6a interface towards the home HSS for roaming UEs.

eNodeB

The evolved RAN for LTE consists of a single node, i.e., the eNodeB (eNB) that interfaces with the UE. The eNB hosts the PHYsical (PHY), Medium Access Control (MAC), Radio Link Control (RLC), and Packet Data Control Protocol (PDCP) layers that include the functionality of user-plane header-compression and encryption. It also offers Radio Resource Control (RRC) functionality corresponding to the control plane. It performs many functions including radio resource management, admission control, scheduling, enforcement of negotiated UL QoS, cell information broadcast, ciphering/deciphering of user and control plane data, and compression/decompression of DL/UL user plane packet headers.

SGW

The SGW (Serving Gateway) routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNB handovers and as the anchor for mobility between LTE and other 3GPP technologies (terminating S4 interface and relaying the traffic between 2G/3G systems and PDN GW). For idle state UEs, the SGW terminates the DL data path and triggers paging when DL data arrives for the UE. It manages and stores UE contexts, e.g. parameters of the IP bearer service, network internal routing information. It also performs replication of the user traffic in case of lawful interception.

HSGW

The HSGW provides interworking between the HRPD access node and the Packet Data Network Gateway (PGW), a key element of the SAE/EPC network. In some network instances, the existing PDSN can be integrated with or upgraded to the HSGW while the existing HA can be integrated with or upgraded to the PGW (or provided as a separate node).

PGW

The PDN GW (Packet Gateway) provides connectivity to the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one PDN GW for accessing multiple PDNs. The PGW performs policy enforcement, packet filtering for each user, charging support, lawful Interception and packet screening. Another key role of the PDN GW is to act as the anchor for mobility between 3GPP and non-3GPP technologies such as WiMAX and 3GPP2 (CDMA 1X and EvDO).

The PGW provides interfaces to Lawful Intercept (CALEA) functionality and unauthorized access to this interface may allow attackers to perform various attacks by manipulating the protocol to obtain traffic, identify intercepted parties among other types of malicious activity. It is therefore critical to protect this interface using authentication and confidentiality.

HSS-AAA

The HSS-AAA (Home Subscriber Server) supports subscriber related functions including, Mobility Management, Call and/or session establishment support and authentication procedures to access the IM subsystem services by storing the generated data for authentication, integrity and ciphering and by providing these data to the appropriate entity in the IMS network (i.e., AAA Server or CSCF).

PCRF

The **PCRF** (Policy Control and Charging Rules Function) supports policy control decision and flow based charging control functionalities. The PCRF also provides network control regarding the service data flow detection, gating, QoS and flow based charging.

FOTA

Firmware Over The Air provides the ability to perform updates and provisioning tasks on the UE/UICC firmware. All control communication and data transfers are expected to be performed over authenticated HTTP(S) sessions. These sessions use PSK-TLS (Pre Shared Key Transport Layer Security). This protocol requires that a TLS key be shared between the UE and the FOTA server and the TLS session is then negotiated based on this key. This scheme provides mutual authentication to ensure that rogue UEs do not get firmware updates and packages.

DNS

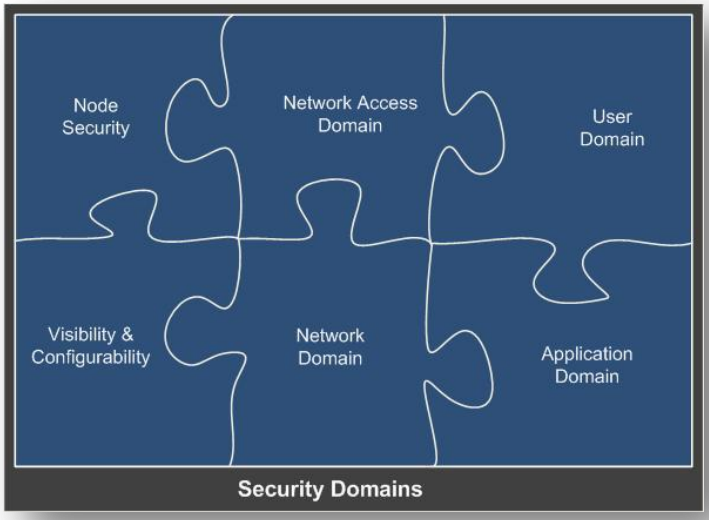
Both the GPRS system (precursor to LTE on GSM networks) and the IP Multimedia Subsystem (IMS) in 3GPP uses DNS extensively. The EPS continues this and expands DNS usage to include node selection. The usage of DNS improves the selection process as various criteria can be used as input to the process while also making inter-operator operations more flexible.

In EPS, the DNS servers are used to store information on the mapping between the APN, the protocol (PMIP/GTP) and PDN GW. It also maps the TAI and Serving GW. The DNS can

also be configured to provide information on collocated nodes and topological and geographical proximity between different nodes.

LTE Security Overview

Security in the EPS is defined within the context of the following groups or domains; Network access security, Network domain security, User domain security, Application domain security and Visibility and configurability of security. In addition to these areas, node/component security is another critical area within the security framework.



Network access security primarily deals with security features that provide secure access to users. This includes mutual authentication and protection of signaling and media traffic (confidentiality and integrity). Network domain security refers to features that ensure secure transfer of data between network elements and protections against attacks on the network that connects these nodes. User domain security relates to the security features of access to terminals (UE), such as PIN codes and passwords. Application domain security references the applications that run on the network including HTTP for web access or IMS. Visibility and configurability is the method by which the UE informs the user whether certain protections are turned on or are configured on the network. Configurability permits the user to configure security features to permit or deny operations by applications. Node security pertains to the security of the underlying operating system and services that are configured on a particular node. This also includes malicious software and physical security (such as access to radio network elements in a remote location).

The different domains within the security framework of the LTE/EPC ensure that proper coverage is provided for different types of attack vectors. A well thought out security architecture emphasizes the concept of defense in depth and the domain model is integral in implementing this concept.

Network Access Security

Network access is a critical component of the security framework within the LTE architecture. The security features supported in E-UTRAN have the following characteristics:

- Mutual authentication between UE and the network.
- Key derivation to create keys for ciphering and integrity protection.
- Encryption, integrity and replay protection of NAS signaling between UE and MME.
- Encryption, integrity and replay protection of RRC signaling between Ue and eNodeB.
- Encryption of the user plane traffic between UE and eNodeB.
- Use of temporary identities to avoid sending the permanent ID (IMSI) over the radio link.

Mutual authentication in E-UTRAN is enabled by to the presence of a secret key K in both the USIM card and the network (specifically the AuC). Once configured, the key never leaves the USIM or the HSS/AuC. The key itself is not used to protect any traffic, rather it is used to generate other keys that provide encryption and integrity for the control plane and user plane traffic.

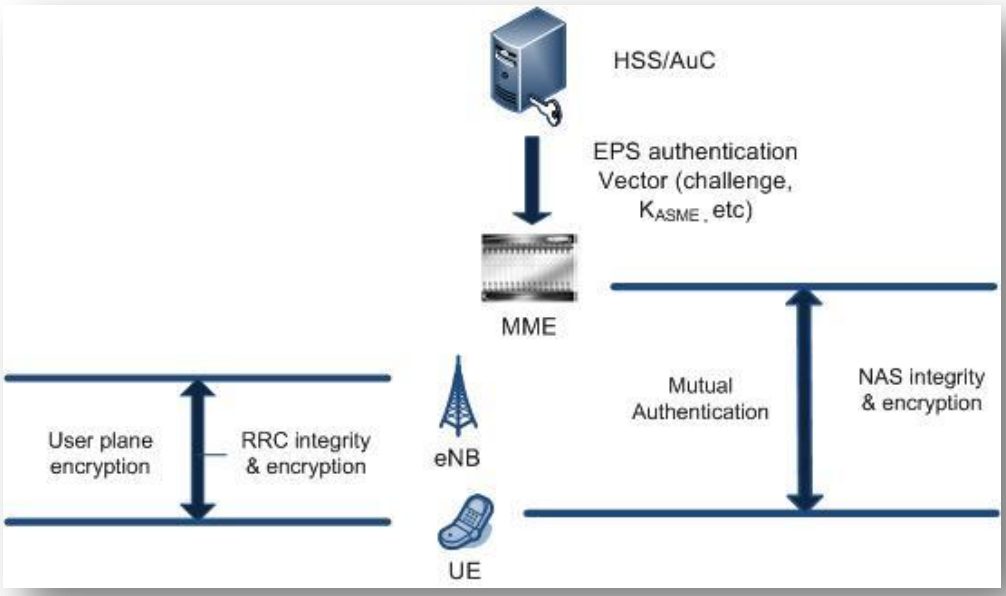


Figure 2 E-UTRAN Security Features

When the UE attaches to the EPS, the UE sends its IMSI to the MME. To mutually authenticate, the MME requests the EPS authentication vector (AV) from the HSS/AuC. The HSS/AuC looks up the shared key (K) and a sequence number (SQN) using the IMSI. The AUC increments the SQN and generated a random challenge (RAND). Taking these parameters and the shared key (K) as input to the cryptographic functions the AV is created. It consists of five values – an expected result (XRES), an authentication token (AUTN), two other keys (CK and IK) and the random challenge (RAND). Subsequently, a new key K_{ASME} is generated based on the CK, IK and the Serving Network identity (SN ID). The SN ID includes the Mobile Country Code (MCC) and the Mobile Network Code (MNC) of the serving network. This provides further key separation so that a key from one serving network cannot be misused in a different network.

The AV that is provided to the MME consists of the K_{ASME} , XRES, AUTN and RAND. Mutual authentication is performed by using the XRES, AUTN and RAND. The MME keeps the K_{ASME} while forwarding RAND and AUTN to the UE. The USIM then computes its own AUTN using the shared key (K) and compares it with the AUTN received from the MME. If they match, the network has authenticated to the USIM. The USIM then computes a response (RES) using the shared key (K) and the challenge (RAND) as parameters. This value is then sent to the MME. If the RES value matches the XRES that the MME received from the HSS/AuC, the UE has authenticated itself to the network, thereby achieving mutual authentication. The UE also computes CK, IK and K_{ASME}.

The following types of traffic are protected between the UE and E-UTRAN:

- RRC (Radio) Signaling between UE and eNodeB
- User plane traffic between UE and eNodeB
- NAS signaling between UE and MME

A number of keys are derived from the K_{ASME} for facilitating encryption and integrity protection for this traffic. Both the UE and the MME compute the keys K_{NASenc} (encryption) and K_{NASint} (integrity) to protect the NAS signaling. The MME also derives the K_{eNB} which is sent to the eNodeB. The eNodeB further derives the key for encryption of the user plane K_{UPenc} and keys to protect the RRC signaling (K_{RRCenc} and K_{RRCint}). The UE derives these same keys as the eNodeB. The key hierarchy is shown in the figure below.

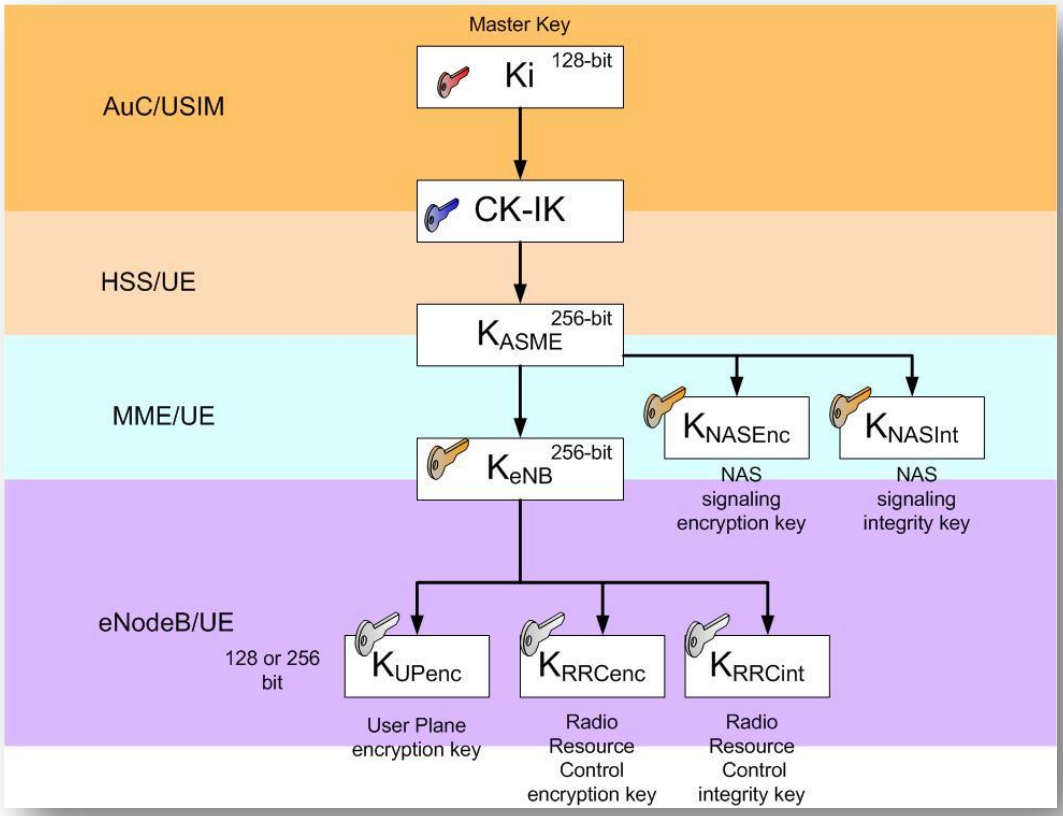


Figure 3 Key Hierarchy

The creation of multiple keys provides key separation, thereby providing better protection of the underlying shared secret K.

To facilitate identity protection, temporary identities are use wherever possible so as to limit the exposure of the IMSI on the radio interface. The GUTI (Globally Unique Temporary ID) is a worldwide unique ID that points to a particular subscriber in a specific MME. The S-TMSI (SAE Temporary Mobile Subscriber Identity) is unique within a particular area of a single network. The GUTI is a long identifier therefore, to save on radio resources, the S-TMSI is often used only within a group of MMEs. The GUTI and S-TMSI constructs and their composition are described in the figure below.

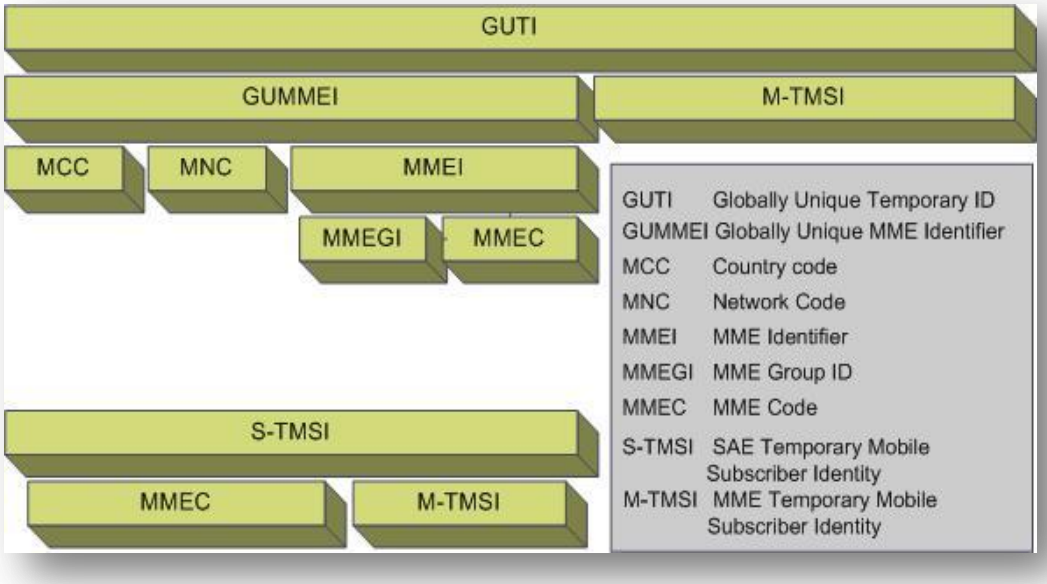


Figure 4 GUTI and S-TMSI Structure

Other network protection mechanisms address the issue of compromised base stations. The 'forward/backward' feature ensures that each time the UE changes its attachment point (due to mobility) or changes from the IDLE state to the ACTIVE state, the air interface keys are updated. This implies that even if the prior keys were compromised, security is still maintained from that point forward.

Network Domain Security

With the advent of IP based transport, the signaling and user plane transport now runs over networks and protocols that are more open and accessible to organizations other than the major telecom institutions. For example, the core network interfaces may traverse third party IP transport networks, or interfaces may cross operator boundaries in cases of roaming.

The specification to protect IP-based control plane traffic is called Network Domain Security for IP-based control planes (NDS/IP) as specified in 3GPP TS 33.210. This specification introduces the concept of security domains, which refer to networks that are managed by a single administrative authority. Security domains may pertain to multiple operators and their networks or a single operator who chooses to segment the network into domains. At the borders of these domains, the operator places Security Gateways (SEGs) to protect the control plane traffic that traverses into and out of the domain. IPSec is used to protect the traffic that passes between the domains, specifically IPSec Encapsulated Security Payload (ESP) in tunnel mode. IKE (Internet Key Exchange) protocol (v1 or v2) is used between the SEGs to set up the security associations.

The S1-U interface between the EPC and E-UTRAN (radio) is of special interest, since user plane data terminates on the eNodeB which may expose sensitive data. This should be

protected either physically or using NDS/IP. IPSec may also be used to protect traffic between entities in the same security domain for further protection. Thus, the end to end traffic between two network entities in different domains is protected in a hop-by-hop fashion.

User Domain Security

Security in the user domain is primarily focused on the secure access to terminals. Most access to terminals may be controlled by using a shared secret such as a PIN code, which is stored inside the USIM. The PIN code provided by the user is validated with the code present in the USIM whereby access is granted. In addition, the security of the UICC/USIM is another aspect of this domain. The protection of the shared key on the USIM is vital for protection against a variety of attacks. The UICC should also be resistant to other attacks such as local exposure of USIM authentication data or connection hijack attacks.

Application Domain Security

Application domain security refers to end-to-end security between the application in the terminal and the entity providing the service. By contrast, other security domains generally refer to security features on a hop by hop basis (single link in the network). This paper focuses primarily on the EPS which provides the transport for the user plane or application traffic, and as such is transparent to application level security.

Visibility and Configurability

This security domain addresses the feedback to users and configuration of settings related to security features available within the network. In most instances, security is transparent to the end user, although in some cases the user should be informed about the operational status. As an example, the usage of encryption in E-UTRAN is dependent on operator configuration and the user should be able to find out whether it is used, perhaps by a symbol displayed on the handset. Configuration of security settings is a property whereby a user can configure whether the use (or provision) of a service should depend on the enablement of a security feature.

Node Security

Node security primarily focuses on threats associated with the network elements in the EPC and LTE. These network elements provide access to the IMS core network and corresponding services such as voice and SMS. Security of these elements involves network services that run on them, malicious software that may be loaded, vulnerabilities in the operating system or use of un-patched software, among other vectors.

Threats

As any carrier grade telecommunications network there are several external and internal threats that need to be managed in order to minimize impact of subscriber communications, revenue assurance, availability and organizational image. The following are some of the most significant threats associated with the LTE/EPC implementation.

Threat Domain	Threats
Fraud	• Subscription sharing • Subscriber impersonation through remote unauthorized access (UICC) • Subscriber impersonation through Trojan Horse/malware
Unauthorized Access	• Exploitation of vulnerable network services • Man-in-the-middle/Connection hijack attacks (UICC) • Attacks on USIM secret key (UICC) • Unauthorized access to management and administrative interfaces • PCRF policy manipulation through vulnerable service • Unauthorized access to the CALEA system via vulnerable network services. • CALEA Wiretap Eavesdropping • Access to subscriber data via backups (HSS) • Access to subscriber profile information through unauthorized DIAMETER requests. • Message eavesdropping (DIAMETER) • Unauthorized access to Backup, recovery and logging data • Unauthorized access to subscriber keys (eNodeB) • Network traffic compromise due to lack of appropriate encryption • System compromise via command injection
Service Disruption	• Signaling message amplification • Resource consumption by mis-configured device • Malformed messages (DIAMETER) • DoS against subscriber availability through spoofed push-profile DIAMETER requests.

	• Service disruption (DoS) via packet flooding • Exploitation of traffic forwarding (HSGW, SGW)
Node Tampering	• Malicious code injection • Unauthorized software modification • Exploitation of operating system vulnerabilities • Manipulation of firmware/package updates (FOTA)

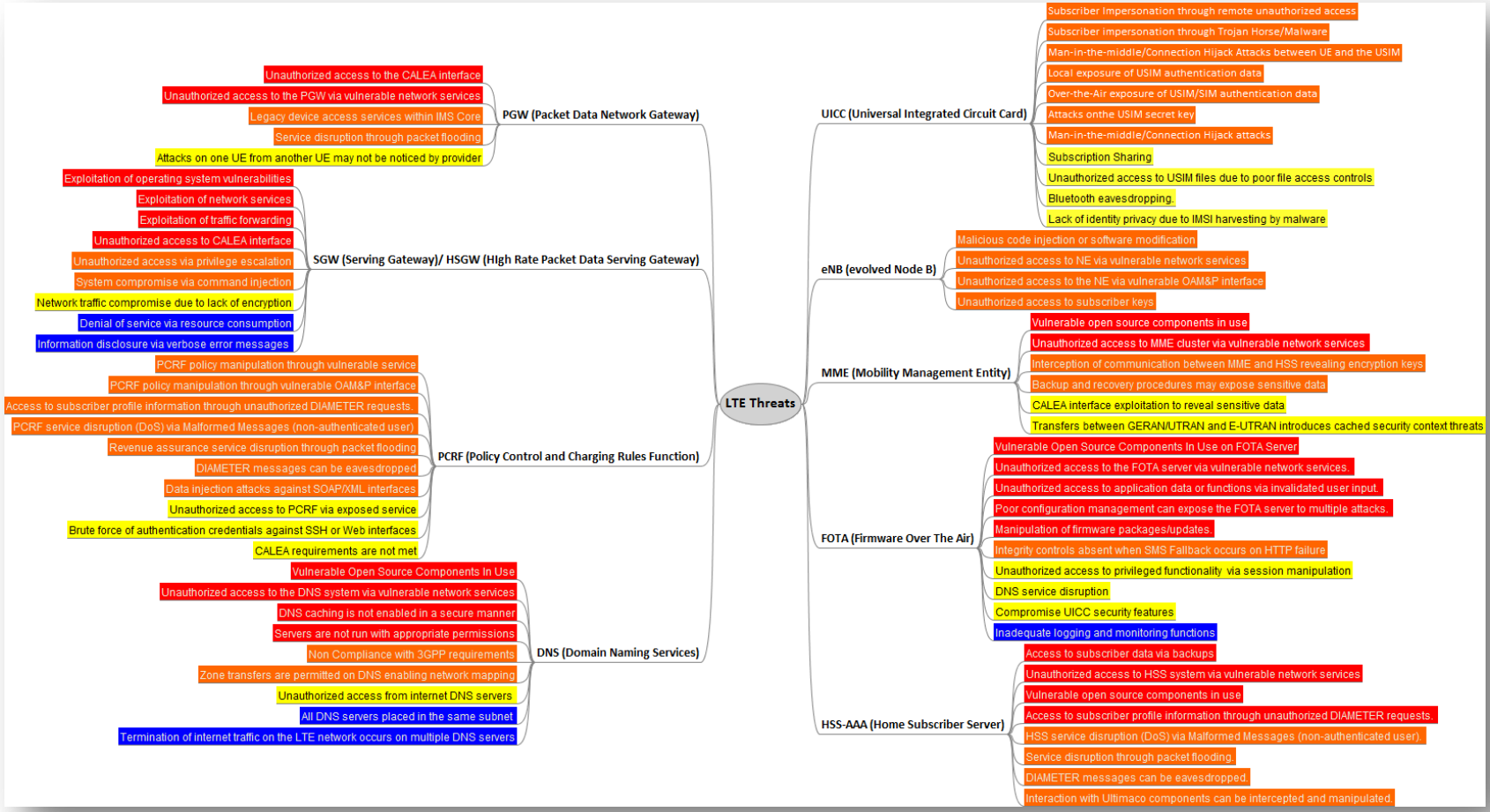


Figure 5 Threat taxonomy visualization

Summary

The LTE architecture implementation is the evolution of UTRAN (for GSM providers) and eHRPD (for CDMA providers) to support high packet rate, low latency communications. A clear understanding of its security requirements and implications is required to address the complexity of the architecture and its deployment.

A holistic approach to security in the LTE implementation will diminish the opportunities for attacks against the infrastructure. The broad areas of focus include:

- Network Access Security
- Network Domain Security
- User Domain Security
- Node Security
- Application Domain Security
- Visibility and Configurability of Security (for users)

In addition to these, traditional security practices such as robust logging, fraud detection monitoring, periodic security evaluations, well-defined security policies among other strategies will help maintain an adequate security posture against internal and external threats without negatively impacting service quality or adversely affecting operations.

For more information contact:

Sony Cherukara
Email: sony.cherukara@palindrometech.com
100 Village Court
Hazlet, NJ 07730, USA
Tel: +1 (732) 416-7722
www.palindrometech.com