Network Access Security in Next-Generation 3GPP Systems: A Tutorial

Sankaran C. B., Motorola

ABSTRACT

The 3GPP Release 8 Long Term Evolution/System Architecture Evolution marks the advancement of mobile cellular technology after UMTS-3G. The evolved packet system (EPS) architecture proposed in Release 8 introduces fundamental changes on top of UMTS in several design areas, including security. This article provides a tutorial overview of the proposed security mechanism in EPS. It first gives the background, a brief overview of the overall EPS architecture. It goes on to list the various requirements to be met for EPS security. A description of the EPS security architecture and detailed security procedures are given subsequently. The innovations that have been introduced in EPS, on top of UMTS, are highlighted all through the article. The article concludes by listing some open security issues at the moment.

INTRODUCTION

The Third Generation Partnership Program (3GPP) Long Term Evolution/System Architecture Evolution (LTE/SAE) system seeks to take mobile technology to the next level through the realization of higher bandwidths, better spectrum efficiency, wider coverage, and full interworking with other access/backend systems. LTE/SAE proposes to do all this using an all-IP architecture [1, 2] with well defined interworking with circuit-switched systems. In order to handle future requirements, the system is defined to work across multiple access networks (both 3GPP-defined and non-3GPP-defined). 3GPP access networks include E-UTRAN, UTRAN, and GERAN [1, 3]. Non-3GPP access networks include both trusted and non-trusted networks (CDMA-2000, WiFi, etc.) [4] In this heterogeneous framework, there is a greater risk of unlawful accessing and tampering with information that travels between the various entities. Hence, security functions assume paramount importance to ensure that the setup works as intended and is future proof [5].

The security mechanism in wireless systems has evolved right from the original analog systems through Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS). In GSM the focus of security was largely on the radio path. In UMTS its scope was enhanced to include several network functionalities too. The ever-increasing focus on IP-based mechanisms meant more threats to security; hence, a more robust security architecture is needed in the evolved packet system (EPS). In EPS the 3G security framework has been enhanced to handle the more diverse nature of the architecture and increase robustness. These enhancements include adding security (both integrity protection and ciphering) on the non-access stratum (NAS) plane, additional layers of abstraction to protect important information like keys, security inter-working between 3GPP and non-3GPP networks, and so on. We look at these in detail in later sections.

EPS ARCHITECTURE

The EPS architecture and protocols are given in Fig. 1. The overall architecture has two distinct components: the access network and the core network. The access network is the evolved universal terrestrial radio access network (E-UTRAN), based on orthogonal frequency-division multiplexing (OFDM) and single-carrier frequency-division multiple access (SC-FDMA) technologies [6]. The core network is called the evolved packet core (EPC); it is different from the UMTS core network. E-UTRAN and EPC together constitute the EPS.

Some of the highlights of the LTE and EPC architectures are listed below. For the UMTS architecture, refer to [7], and for the EPS architecture, refer to [1, 2].

E-UTRAN

The E-UTRAN consists of just one node, the eNode-B, which has the functionality of the Node-B and radio network controller (RNC) in UTRAN. The emphasis is on self-configuration and self-optimization of eNodeBs. The eNode-B talks to the mobility management entity (MME) on the signaling plane and directly to the serving gateway (S-GW) on the data plane The eNode-B hosts the physical (PHY), medium access control (MAC), radio link control (RLC), PDCP, and RRC layers. The access stratum (AS) security mechanism consists of ciphering and integrity protection of RRC signaling messages and ciphering of user plane (UP) packets. The base AS security keys are generated using the NAS authentication and key agreement (AKA) proce-

0163-6804/09/$25.00 © 2009 IEEE

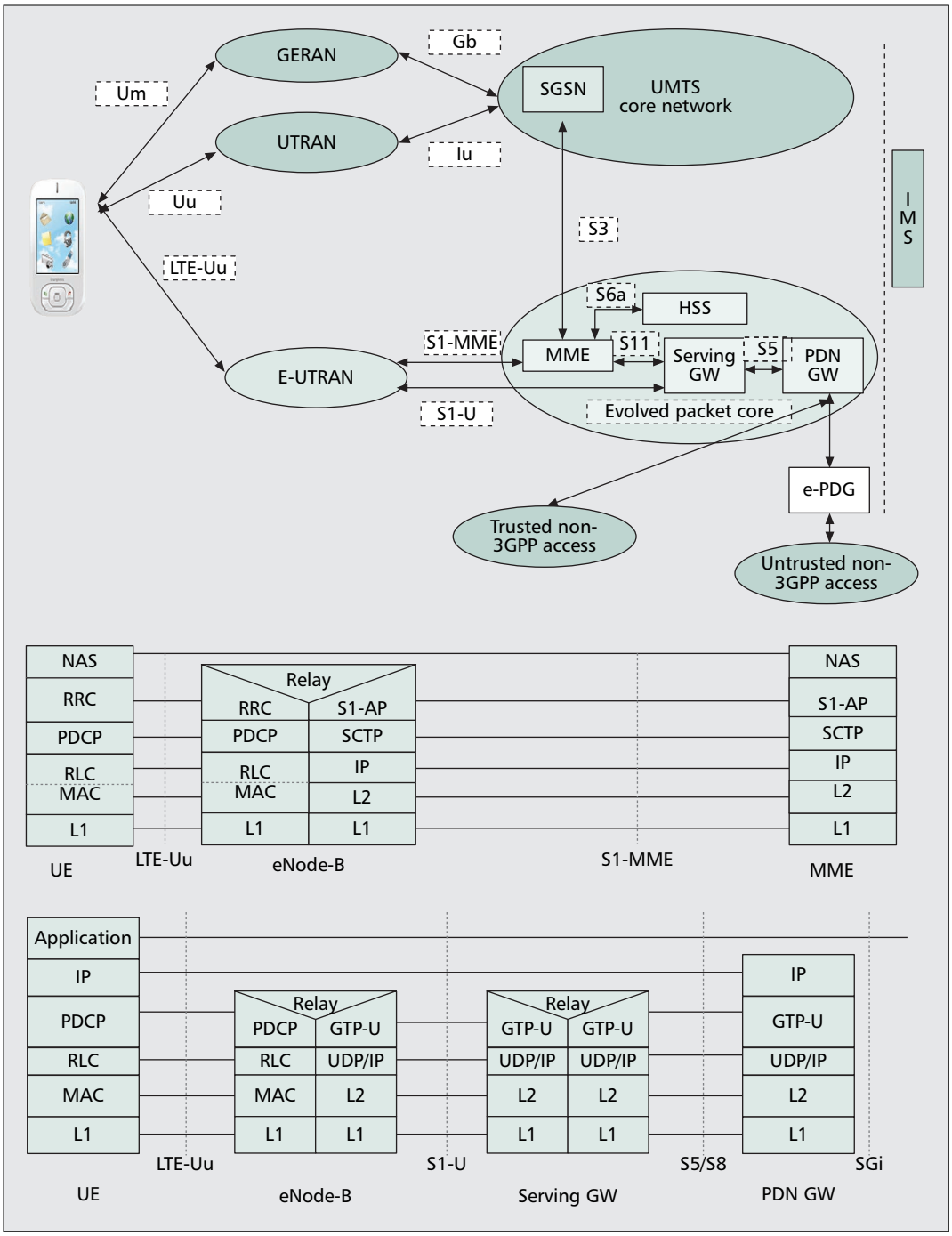

Figure 1. *EPS architecture, signaling, and user plane protocols.*

In GSM, the focus of security was largely on the radio path. In UMTS, its scope was enhanced to include several network functionalities too. The ever-increasing focus on IP based mechanisms meant more threats to security and hence, a more robust security architecture is needed in EPS.

dure. The configuration and activation of AS-level security is done through the AS security mode command (SMC) procedure. The lifetime of an AS security context is tied to the RRC connection; the keys are generated when the UE moves to connected mode and deleted when the UE goes to idle mode.

EPC

The EPC is an all-IP network (AIPN) and is fully packet-switched (PS). Services like voice, which are traditionally circuit-switched (CS), will be handled using the IP multimedia subsystem (IMS) network. Network complexity and latency are reduced as there are fewer hops in both the signaling and data planes. The EPC is designed to support non-3GPP access networks too. A relevant point is that the EPC supports mobile IP. To improve system robustness security, integrity protection, and ciphering have been added at the NAS level also, on top of the security that exists in the access network. Both integrity protection and ciphering will be applicable to all NAS signaling. This would ensure that even if there is a security breach at one level, the other one can ensure that there is no compromise in overall security. The other factor is that the EPC will be in a more controlled environment than

Key requirement	Level I	Level II	Level III
Improve overall robustness over UMTS	Add NAS security, keys and identities are better protected, security association alive through idle	Support IPSec Add NAS security	Same as UMTS
User identity confidentiality	Usage of temporary identities	Support IPSec	Secure storage of IMSI
Mutual authentication of user and network	AKA procedure	N/A	N/A
Data confidentiality	Ciphering at the AS (both signaling and data) and NAS levels (signaling only)	Support IPSec NAS ciphering(signaling only)	N/A
Data integrity	Integrity protection at the AS and NAS levels	Support IPSec NAS integrity protection	N/A
Interworking with GERAN/UTRAN	The specs have defined the gracious handling of security in all the inter-RAT mobility scenarios	The specs have defined the gracious handling of security in all the inter-RAT mobility scenarios	N/A

Table 1. *Summary of LTE security functions and procedures.*

the access network; hence, security at this level becomes a must.

The major EPC elements are:

- **Mobility management entity**The MME is equivalent to the GERAN/UTRAN serving general packet radio service support node (SGSN), and hosts the NAS plane in EPS and interfaces with the home subscriber server (HSS, S6a) to enable the transfer of subscription and authentication data for authenticating/authorizing user access. It terminates the NAS level security.
- **Serving gateway and packet data network gateway**: The S-GW handles the IP data from eNode-Bs directly and terminates the interface towards E-UTRAN. The packet data network gateway (PDN-GW) provides the interface to the PDN.

Major Security Threats and Requirements in LTE/SAE

Some of the key security threats in EPS are:

- Illegal access and usage of the user's and mobile equipment's (ME')s identities — to access network services
- Tracking the user based on the user equipment's (UE's) temporary identity, signaling messages, and so on
- Illegal access and usage of the keys used in security procedures to access network services
- Malicious modification of UE parameters (e.g., failure timers, retry timers) to lock out the phone from normal services either permanently or for an extended period of time
- Willful tampering with the system information broadcast by the E-UTRAN
- Eavesdropping and illegal modification of IP packet contents
- Denial of service to the UE
- Attacks on the integrity of data (signaling or user traffic) by replaying

The key requirements could be summarized as:

- **Improved overall security robustness over UMTS** — to take care of the added/new functionality and the use cases thereof, and work in a secure environment
- **User identity confidentiality** — to ensure that any illegal identification and tracking of any user is not possible
- **Mutual authentication of the user and network** — to ensure that both sides are sure they are communicating with the correct entity, authorized to make that transaction
- **Data confidentiality** — to ensure that any eavesdropping of exchanged data is not possible
- **Data integrity** — to ensure that data received by any entity cannot be tampered with
- **Interworking with GERAN/UTRAN** — to ensure that inter-radio access technology (RAT) procedures work as designed without allowing any security weakness of the other access technologies to compromise LTE/SAE security
- **Replay protection** — to ensure that an intruder is not able to replay control messages already transmitted
- **Allowing/requiring dynamic setup** of all respected security association as much as possible

These are generic high-level requirements that are applicable across multiple entities and interfaces in the LTE/SAE architecture. The specific implementation of the same requirement could be different across these different entities. We look at the detailed architecture below, where we see how these requirements are met.

Security Architecture for EPS

There are four levels of security defined in the specifications. These are:

- **Network access security (level I)**: These are security features that protect the radio link

and provide users with secure access to the EPC and the backend networks. This level has security mechanisms between the USIM, ME, E-UTRAN, and elements in the EPC (both serving and home networks). The integrity protection and ciphering defined in EPC are examples.

- **Network domain security (level II)**: These are security features that protect the wireline networks and enable them to exchange data in a safe manner. This could be, for example, the IPSec used to protect the S1 control plane.
- **User domain security (level III)**: Here the scope is between the USIM and the ME. It would include the mutual authentication of the USIM and the ME before they can access each other, using a secret PIN.
- **Application domain security (level IV)**: The security features that enable applications in the UE and the backend network to exchange information in a secure manner. For example, the IMS architecture provides the framework for this level of security for voice over IP (VoIP).

In Table 1 the different security features and procedures that implement these requirements at each level are summarized. EPS uses the following procedures and mechanisms as effective counter-measures at levels I, II, and III:

- Usage of temporary user identities: Mandating AKA-based mutual authentication during initial attach and as needed before allowing a user to access the network
- Use encryption/ciphering to safeguard the content of user data and signaling messages
- Guarantee signaling messages' integrity using an applicable integrity protection mechanism
- Dynamic key distribution and management in a secure manner using a keying hierarchy based on a preshared master key
- For IP transport (within the network), IPSec with IKE is used for effective protection

Level IV security is out of scope of this article.

Key Management

The various keys play a critical role in the working of the overall security mechanism. Their lifetimes, scope, hierarchy, and properties are clearly defined in the 3GPP Release 8 specifications [8], right from the master key down to the various temporary keys. The E-UTRAN keys are cryptographically separated from the EPC keys used, making it impossible to figure out one from the other. Figure 2 shows the keys' hierarchy and the levels where they are relevant.

The various keys are derived using the Key Derivation Function (KDF) interface defined in [8]. While the inputs are different for the various keys, they are concatenated into a common format S, which is then input to the respective algorithm:

- **KeNB** is a key derived by UE and MME from KASME when the UE goes to connected state or by UE and target eNode-B during eNode-B handover.
- **KNASint** is a key used to protect NAS traffic with a particular integrity algorithm. It is derived by the UE and MME from KASME and an identifier for the integrity algorithm, using the KDF.
- **KNASenc** is a key used to protect NAS traffic with a particular encryption algorithm. It is derived by UE and MME from KASME and an identifier for the encryption algorithm, using the KDF.
- **KUPenc** is a key used to protect UP traffic with a particular encryption algorithm. It is derived by UE and eNode-B from KeNB, and an identifier for the encryption algorithm, using the KDF.
- **KRRCint** is a key to protect RRC traffic with a particular integrity algorithm. It is derived by UE and eNode-B from KeNB and an identifier for the integrity algorithm, using the KDF.
- **KRRCenc** is a key used to protect RRC traffic with a particular encryption algorithm. It is derived by UE and eNB from KeNB and an identifier for the encryption algorithm, using the KDF.

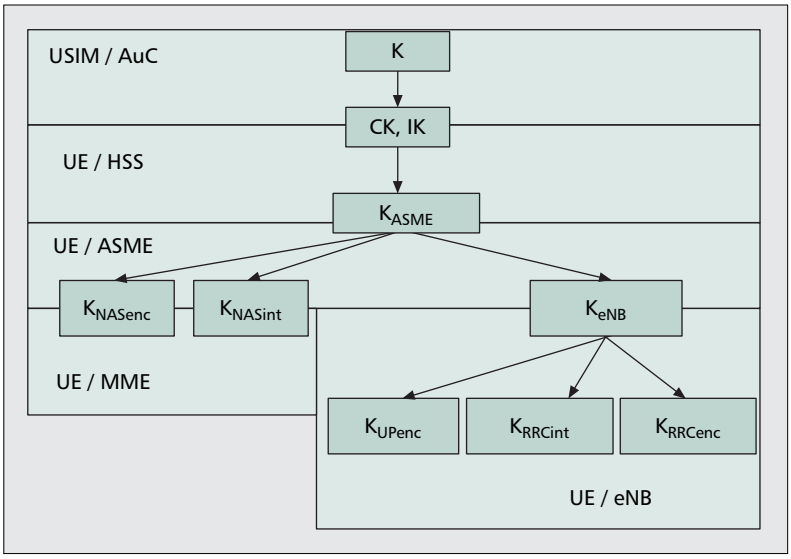

Figure 2. *EPS key hierarchy.*

Security Robustness Improvement over UMTS

The EPC is designed to handle multiple access and backend networks. This means use cases such as eNode-B, where the access network could be unreliable. Also, since all traffic would be wholly IP-based, there is an increased risk of security breach. The major improvement over UMTS is the addition of security functions at the NAS level (between the UE and the MME), on top of the existing ones at the AS level. A separate security sublayer is introduced for doing this and is positioned in between E-MM and RRC in the protocol stack. This sublayer would cipher and integrity protect NAS signaling messages. This would mean that all the NAS signaling (with the exception of a few 3GPP defined messages) would be ciphered and integrity protected twice — once in the NAS security sublayer and once within AS. This adds to the overall

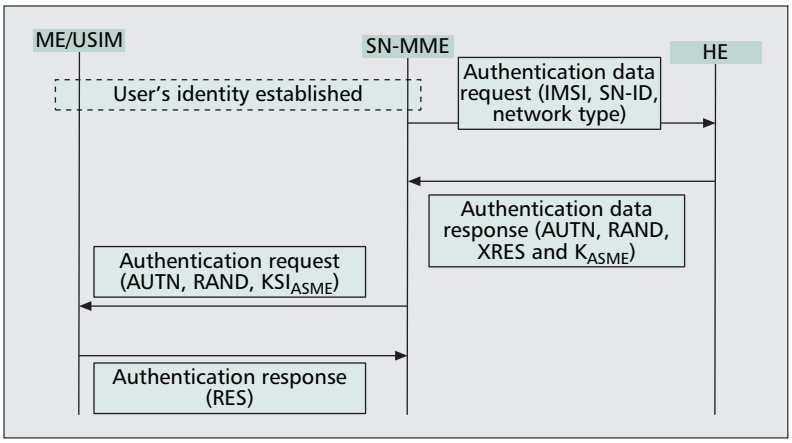

Figure 3. *Message flow for EPS AKA.*

robustness of the architecture; even if one fails, there will be protection from the other.

On the network side, the protection of IP-based internetwork interfaces in EPC and E-UTRAN shall be done using IPSec. This is done for both the signaling and user data planes.

One more improvement is that during the AKA procedure, the ciphering and integrity keys (Ck and Ik) are computed by the HSS in the user's home public land mobile network (HPLMN) when the serving network (SN) queries for the same. While in UMTS these keys are actually communicated back to the SN, it is not so in EPC. Instead, another key, KASME, is computed by the HSS and sent back to the SN. The advantage of KASME is that it is bound to the MS identity and the identity of the SN. Another advantage is that KASME is returned to the SN only after the UE authentication response is validated by the HSS. The NAS security context has a longer lifetime than the AS security context. It can also stay alive when the UE goes to idle.

User Identity Confidentiality

The identity of the user is to be protected to prevent unlawful reading. Threats include tracking and profiling the user's movements, getting information on the network's identity (from the international mobile subscriber identity, IMSI). There are defined countermeasures to prevent these threats. Foremost among these are the usage of temporary identities. Temporary identities are assigned and used wherever possible to avoid unnecessary exchange of permanent identities between entities. Some temporary identities are M-temporary mobile subscriber identity (M-TMSI), which is used to identify the UE within the MME, the S-TMSI, which is constructed from the MME code and the M-TMSI, used for paging the UE, and the globally unique temporary UE identity (GUTI), allocated by the MME with two components, one uniquely identifying the MME that allocated the GUTI and the other uniquely identifying the UE within that MME. GUTI is used to support subscriber identity confidentiality, and, in the shortened S-TMSI form, to enable more efficient radio signaling procedures (e.g., paging and service requests). Apart from the temporary identities, the permanent identities (IMSI and IMEI) shall be stored securely. There is one allowed security breach: if the MME queries for the UE's IMSI in the Identity Request message, the UE should send it, even if security is not configured.

Mutual Authentication of User and Network

The AKA procedure ensures that the serving network (SN) authenticates the user's identity (in the USIM) and the UE validates the signature of the network provided in the authentication token (AUTN). Apart from the authentication itself, this procedure is used to by the HN and UE to generate the Ck and Ik from the same material by the same functions; the KASME is also computed as part of this procedure. The KASME key is subsequently used to derive different session keys for ciphering and integrity protection for AS and NAS.

During the registration, when the UE's identity is established with the MME, it sends a request to the home environment (HE) querying the authentication vector for a specific SN-ID and IMSI. The HE responds with an authentication vector (the use of multiple vectors is part of UMTS and is discouraged for LTE/SAE because there is no need for it with the current keys hierarchy). Each vector has AUTN, RAND (a random value), XRES (which is calculated by the HE using a predefined authentication algorithm using AUTN, RAND, and a master key K unique to each IMSI), and KASME, which is computed from Ck and Ik (these two keys remain in the HSS and are never sent to the MME). There is an additional level of abstraction, where KASME, Ck, and Ik are stored in a key set and identified by a key set identifier (KSIASME). The KSIASME is sent by the MME to the UE in the Authentication Request message along with the AUTN and RAND. The USIM computes the KASME, Ck, Ik, and RES, stores KASME along with the received KSI-ASME, and sends back the calculated RES in the Authentication Response message. The MME compares the RES with the XRES it got earlier and completes the procedure if they are found to be the same. This enables the MME to start ciphering and integrity protection at the next establishment of an NAS signaling connection without executing a new authentication or SMC procedure. It is to be noted that the UE derives the KASME using the SN-ID as a parameter; hence, successful use of the keys derived from KASME implicitly authenticates the network's identity.

Some of the concepts used during the authentication procedure have been described here. The authentication vector has to be *fresh* (i.e., not used before). This is ensured by the sequence numbers exchanged in the messages that serve as an input to the ciphering and integrity algorithms. Also, the algorithms used in the HE and USIM to compute the authentication vectors are largely *one-way* mathematical functions, where an output is gotten given a set of inputs, using a defined algorithm. However, to get back the

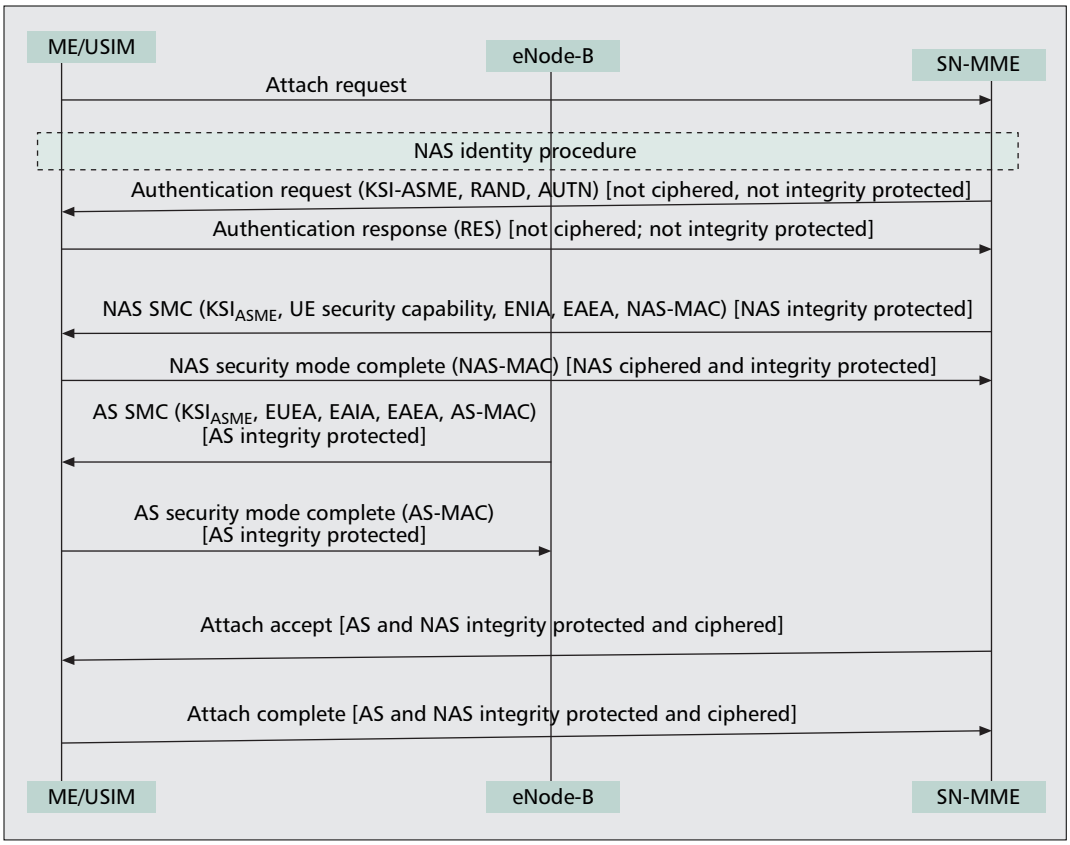

Figure 4. *Establishment of NAS and AS security contexts during initial attach.*

While the Ck and Ik are assigned in the AKA procedure, the ciphering and integrity algorithms and other inputs to these algorithms are communicated in the Security Mode Command (SMC) procedure. There are 2 SMC procedures defined, one at the NAS level and the other one at the AS level.

inputs using the output is extremely complex. This helps in countering security threats. All the different keys used in the AKA and other procedures are interlinked with a defined hierarchy with the single source being the master key K, which is unique to a user and is stored in a secure manner in both the USIM and the HN. Please refer to [1, 8] for more details.

Data Confidentiality: Ciphering and Integrity Protection

Once the UE and network have completed their mutual authentication, they can start communicating in a secure manner, using ciphering and integrity protection. For a detailed description, please refer to [1, 8].

Ciphering is an encryption methodology consisting of adding a random-looking mask bit by bit to the plaintext data to encrypt it. The ciphered message is unintelligible to any third party as the inputs to the algorithm are confidential and protected. On the receiving side the same mask, when added again, retrieves the original plaintext data. This ensures the confidentiality of the data communicated over the radio link. Ciphering is applied on signaling messages (in both NAS and AS) and user plane data (at AS).

Integrity protection ensures that the data received at an entity is what was sent by the sender. In other words, it ensures that the data has not been tampered with midway. This is to ensure protection at the individual message level. Integrity protection is applied to all signaling messages at both the NAS and AS levels. Integrity protection is not applied to user plane data because it would become too much of an overhead at the packet level, impacting the data rates. The basic methodology is computing an integrity tag, which is appended to the message being sent; the same integrity tag is generated on the receiving side too; the message is accepted only when the tags match. Any change in the input parameters (inputs include the original signaling message as well) to the algorithm affect the output in an unpredictable manner; hence, it protects the message from tampering.

While the Ck and Ik are assigned in the AKA procedure, the ciphering and integrity algorithms and other inputs to these algorithms are communicated in the security mode command (SMC) procedure. There are two SMC procedures defined, one at the NAS level and the other one as the AS level.

NAS Security Mechanism

The NAS SMC procedure is triggered by the MME immediately after the AKA — the SMC message contains the replayed security capabilities of the UE, the selected NAS algorithms, and the KSIASME for identifying KASME. This message is integrity protected with an NAS integrity key based on KASME indicated by the KSIASME. The NAS security mode complete message from UE to MME is integrity protected and ciphered with the algorithms indicated by the MME NAS uplink. Downlink ciphering at the MME starts after sending the

3GPP-Rel 8 defines the handshaking between the UE and the different network elements to handle security during mobility within EPS as well as between EPS and UTRAN/GERAN/non-3GPP networks.

NAS security mode command message. NAS uplink and downlink ciphering at the UE starts after receiving the NAS security mode command message.

Once the AKA and SMC procedures are completed, the NAS security context is said to be created and will be applicable during the time the UE is registered. Depending on what triggers a subsequent detach procedure, the context could be maintained or deleted. While the NAS security context exists, all NAS messages shall be integrity protected and ciphered The inputs for the integrity and ciphering algorithms would be the KNASint/KNASenc, NAS COUNT, BEARER identity, and DIRECTION bit.

AS Security Mechanism

The AS SMC procedure is triggered by the eNode-B by sending the AS SMC to the UE; the UE replies with the AS security mode complete message. The SMC contains the selected AS algorithms (for ciphering and integrity protection) and the KSIASME. It will be integrity protected using the KRRCint tied to the KSIASME that comes in the SMC.The AS security mode complete message shall also be integrity protected with the selected RRC algorithm indicated in the AS security mode command message and RRC integrity key based on the equivalent KASME.

RRC and user plane ciphering at the eNode-B shall start after receiving the AS security mode complete message. RRC and UP ciphering at the UE shall start after sending the AS security mode complete message. The input parameters for the ciphering and integrity protection algorithm would be the KRRCenc/KRRCint/KUPenc, the PDCP count, the bearer ID, and a DIRECTION bit.

Refer to Fig. 4 for the case of establishing the AS and NAS security contexts during initial attach.

EPS Security and Mobility

3GPP-Rel 8 defines the handshaking between the UE and the different network elements to handle security during mobility within the EPS as well as between the EPS and UTRAN/GERAN/non-3GPP networks [5, 8]. The major challenge in security during mobility is how the security algorithms, KDFs, and keys are handled. A UE could move either with or without a security context active. Here, we look at the mobility of the UE with the security context active. Some common points are:

- The UE includes its security capabilities, listing the algorithms it can support in E-UTRAN/UTRAN/GERAN, Attach Request (in all the RATs), TAU Request (in E-UTRAN), and RAU Request (in UTRAN/GERAN) in Rel-8.
- The MME and eNode-Bs are configured by the operator with a priority list of algorithms and KDF to use.
- When the AS security context is established in the eNode-B, the MME shall send the UE's security capabilities to the eNode-B, containing the algorithms supported by the UE.

Intra E-UTRAN Mobility in Connected Mode — At the time of a handover (HO), the source eNode-B forwards the UE's security capabilities to the destination eNode-B. The destination eNode-B selects an algorithm to use (based on the priority list), and lets the UE and MME know about it. If the MME also changes during the HO, the source MME shares the UE security capability with the target MME, and the target MME selects a set of algorithms and KDF (based on the priority list) and assigns them to the UE in the TAU Accept message(if the new values are different from the old ones).

Intra E-UTRAN Mobility in Idle Mode — The UE and network use the RAU/TAU signaling to post the mobility to synchronize on the algorithms to use. If there is data to send at the time of the UE movement, the AS keys need to be recomputed. The KeNode-B is computed using the KASME and NAS count; and from the new KeNode-B, the KRRCenc, KRRCint, and KUPenc are derived. An AKA could be either run or not as part of the TAU; key recomputation is different in each case.

Inter-RAT Mobility in Connected Mode — At the time of the HO, the UE's target RAT security capabilities are shared between the MME and the SGSN, and these are further transferred to the eNode-B or RNC. The selected algorithms (in the target RAT) are then conveyed to the UE in the HO command. The keys are recomputed on both the UE and network side at the time of the HO.

Inter-RAT Mobility in Idle Mode — There are two cases here: the UE has a cached security context in the target RAT, or it does not. When the cached context exists, either the old keys are accepted between the UE and the network or a new AKA run is done. In the other case (called the mapped security context), the UE sends KSI or KSIASME or the source RAT in the TAU/RAU request; there is additional signaling between the network elements to set up the security context.

Conclusion

This article has sought to give an introduction to the ideas and concepts that have been used in EPS security. While most of the threats and requirements have been identified, much more remains to be done given the wholly heterogeneous nature of the EPS and the immense possibilities it throws up in applications, network configuration, and so on. Some specific issues being addressed now are:

- Whether or not a single set of high-level security requirements for all types of eNode-B (i.e., femto, pico, and macro) is enough is being discussed. There is a view that the different deployment environments should dictate the requirements.
- Per user activation of UP ciphering is under discussion.
- Negotiation of KDF, used to derive the KASME, and the handling during mobility

(e.g., handover between two eNode-Bs with different KDFs) is under study.
- Key handling during handover is another major area of study.
- It is not yet fully defined which messages should be security protected and which need not be (under certain scenarios). The scenarios and exceptions are being discussed and worked on now.

We conclude that security is one area in 3GPP that needs focus in the coming years to ensure that there is no compromise in security while realizing the potential of the next generation of mobile systems.

REFERENCES

[1] 3GPP Tech. Spec. 23.401 v8.2.0, "General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access," Rel. 8.
[2] 3GPP Tech. Spec. 23.402 v8.0.0, "Architecture Enhancements for Non-3GPP Accesses," Rel. 8.
[3] H. Kaakanen *et al*., *UMTS Network Architecture, Mobility, and Services*, Wiley.
[4] 3GPP2 C.S0024-A v2.0, "CDMA 2000 High Rate Packet Data Air Interface Specification."
[5] 3GPP Tech. Spec. 33.402 V8.1.1, "Security Aspects of Non-3GPP Accesses."
[6] 3GPP Tech. Spec. 36.300 V8.6.0, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall Description," Rel. 8.
[7] E. Dahlman *et al*., "UMTS/IMT-2000 Based on Wideband CDMA," *IEEE Commun. Mag*., vol. 36, no. 9, Sept. 1998.
[8] 3GPP Tech. Spec. 33.401 v8.1.1, "3GPP System Architecture Evolution (SAE): Security Architecture," Rel. 8.

ADDITIONAL READING

[1] 3GPP TS 33.102 V8.0.0, "3G Security; Security Architecture," Rel. 8.
[2] 3GPP TR 33.821 V1.0.0, "Rationale and Track of Security Decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE)," Rel. 8.

BIOGRAPHY

SANKARAN C. B. (sankaran@motorola.com) joined Motorola India in 1997 and is currently working as an engineering manager in the UMTS/GSM handset stack group. His current area of interest is the evolved packet core in LTE. He received his Master's in telecommunications and software engineering from Illinois Institute of Technology, Chicago, in 2001 and his B.Tech. in instrumentation engineering from Madras Institute of Technology, Chennai, in 1996.