IEEK Transactions on Smart Processing and Computing

Overview of SAE/LTE security

Anand R. Prasad and Xiaowei Zhang

NEC Corporation / Kanagawa 211-8666, Japan {anand@bq, x-zhang@cq}.jp.nec.com

***** Corresponding Author: Anand R. Prasad

Received December 26, 2012; Revised January 22, 2013; Accepted February 10, 2013; Published February 28, 2013

Abstract**:** This paper provides an overview of the security in the System Architecture Evolution (SAE) / Long-Term Evolution (LTE) system. Security is an integral part of SAE/LTE with improvements over the Third Generation (3G) system. This paper reviews the SAE/LTE system architecture, and discusses the security requirements, algorithms, Authentication and Key Agreement (AKA), Security Mode Command (SMC), key hierarchy and security for mobility.

Keywords**:** SAE/LTE, EPS, security, key management, AKA, mobility security

1. Introduction

System Architecture Evolution (SAE) / Long-Term Evolution (LTE) is the first mobile communications system that is based entirely on IP and provides a higher data-rate with improved security compared to the previous system [1]. SAE/LTE was specified by the Third Generation Partnership Project (3GPP) in 2009 as “Release 8”. The 3GPP specifications are developed in releases where each release fulfills certain requirements. In the case of SAE/LTE, the system went through several changes compared to 3G. These include the following: (a) the base station or eNodeB (eNB) has enhanced functionality, (b) eNB is the end-point for the user traffic, (c) there is a key hierarchy allowing for key separation depending on the purpose, and (d) forward security is provisioned.

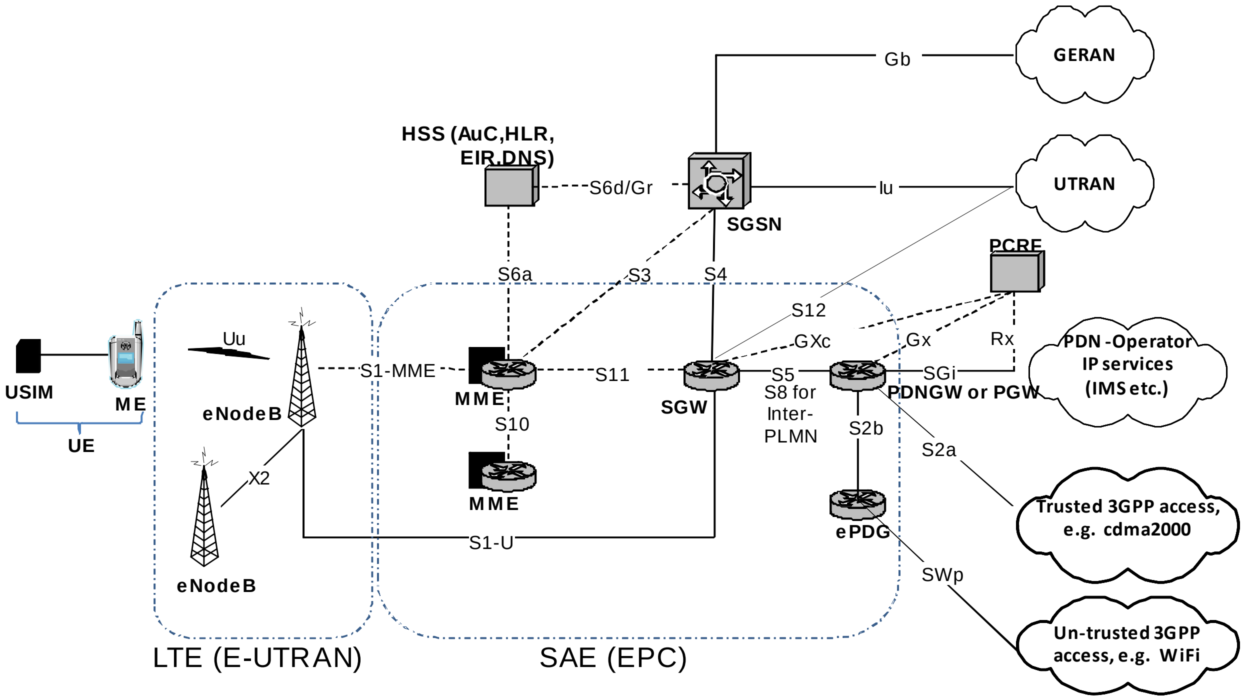
As with earlier specifications from 3GPP, in the mobile device side (known as User Equipment or UE) the core of the security lies in the Universal Subscriber Identity Module (USIM), which is used to authenticate the subscriber. After authentication, the mobile device and the network generate the key material for securing the communication. Communication between the network and UE is in the form of signaling (control plan in 3GPP terminology) and user data (user plane in 3GPP terminology). Signaling traffic is integrity protected against modification and is recommended to provide confidentiality for both signaling and user data. The user data security ends at the eNB, whereas that of signaling, depending on the type, ends at the eNB or core network. SAE/LTE security is also provisioned between all network elements using IP Security (IPsec). Another feature of SAE/LTE security is secure mobility within the SAE/LTE network as well as with other networks, such as like Universal Mobile Telecommunications System (UMTS) or non-3GPP networks. Mechanisms were developed such that neither the security of UMTS or non-3GPP nor the security of SAE/LTE is compromised.

This tutorial paper provides an overview of SAE/LTE security. For a better understanding of security, Section 2 provides a SAE/LTE system overview followed by detailed discussion on SAE/LTE security in Section 3 including security requirements, algorithms, Authentication and Key Agreement (AKA), Security Mode Command (SMC), key hierarchy and mobility security in SAE/LTE. Section 4 concludes the paper with a discussion on future topics.

2. SAE/LTE System Architecture Overview

Fig. 1 presents the SAE/LTE system architecture [1, 2]. SAE/LTE is also referred to as the Evolved Packet System (EPS) consisting of the core network or SAE, also known as the Evolved Packet Core (EPC), and the radio access network or LTE, also known as Evolved-UMTS Terrestrial RAN (E-UTRAN). The User Equipment (UE) is connected to the EPC over E-UTRAN. The UE constitutes of the Universal Subscriber Identity Module (USIM) and Mobile Equipment (ME).

When defining the SAE/LTE system architecture, 3GPP paid particular attention to supporting flexible network configurations and providing high service availability. In the core network, for example, separation of the control functionality (MME) from the user plane



X2, S1-U, S2a, Rx etc. are reference points between network elements. Protocols are defined for each reference point.
Solid lines between network elements are mainly for user plane traffic as defined by 3GPP while dashed lines are mainly for control plane.

Fig. 1. SAE/LTE system architecture.

handling increases the flexibility when deploying the network.

SAE is an all-IP core network with a flattened architecture that is capable of catering to different types of radio networks including LTE, Wi-Fi, WiMAX or 3GPP2 based technologies. The SAE constitutes the Home Subscriber Server (HSS), Mobility Management Entity (MME), Packet Data Network (PDN) Gateway (PDN GW or PGW), Serving Gateway (SGW), and Policy and Charging Rules Function (PCRF). This paper focuses mainly on HSS and MME because they are involved in security (see details in next section).

MME plays a key role on the control plane signaling (Non-Access Stratum (NAS) signaling, i.e. core network-related signaling) operations of SAE, and is the termination point of NAS security. MMEs also perform NAS key handling, algorithm negotiation and MMEs participate in key handling of AS security. The connectivity between eNB and MME is secured using IP security (IPsec) [3]. MME is involved in the handover of an UE within EPS, particularly inter-MME, and also during inter-radio access technology (RAT) handover, e.g. to/from UMTS. MME also performs the selection of PGW and SGW for the UE. The MME interfaces to the home subscriber subsystem (HSS) and participates in the Authentication and Key Agreement (AKA) of an UE. A MME also takes care of the UE reachability, even when the UE is idle.

LTE with an evolved-NodeB (eNodeB or eNB) operates Radio Resource Management (RRM), has the job of selecting a MME and routing capability of the User Plane (UP) data towards the SGW, and carries the transmissions of the signaling messages. The eNB is a radio interface to the mobile network. The integrity and confidentiality protection of Access Stratum (AS), i.e. the Radio Resource Control (RRC) – the radio level control plane – and the UP, terminates at the eNB. Therefore, eNBs also perform AS security-related key handling and algorithm negotiation. For efficient use of the air interface, the eNB performs IP header compression. The eNBs also perform handover, where intra-eNB does not need to involve the MME, whereas inter-eNB handover may involve the MME.

Some of the protocols of SAE/LTE are suggested in the text above, the protocol stack itself is depicted in Fig. 2. As said earlier, the mobile network constitutes the control plane and user plane protocols. The Packet Data Control Protocol (PDCP) and Radio Resource Control (RRC) are summarized because they are related to the discussion in this paper.

The PDCP [4] performs an integrity protection and confidentiality for the control plane of E-UTRAN, i.e. RRC, it also provides confidentiality for UP. RRC and UP together form the AS. RRC controls the security context in the PDCP. The PDCP also provides duplicate detection, retransmission and in-sequence delivery of packets to a higher layer for user plane data. The RRC [5] layer provides several major functions, such as connection management, resource release etc. For security, RRC takes care of the key management of the AS. Some RRC messages are not security protected. The NAS is the control plane of EPC and provides mobility management, session management etc. For security, NAS is the layer where the Authentication and Key Agreement (AKA)

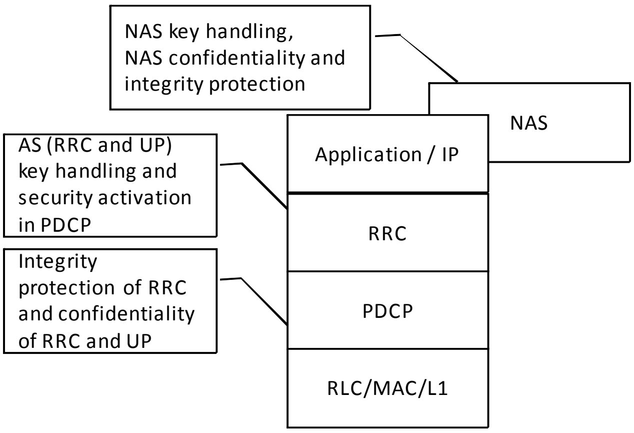

NAS key handling, NAS confidentiality and integrity protection
NAS
Application / IP
AS (RRC and UP) key handling and security activation in PDCP
RRC
Integrity protection of RRC and confidentiality of RRC and UP
PDCP
RLC/MAC/L1

Fig. 2. SAE/LTE protocol stack.

takes place; it also manages the keys for the integrity and confidentiality protection of NAS messages.

3. SAE/LTE Security

This section presents SAE/LTE security. The section starts with a discussion of security issues and requirements followed by a discussion on security requirements, algorithms, AKA and SMC, key hierarchy and security for mobility.

3.1 Security Requirements

The basic security requirements of SAE/LTE are (1) Continued usage of current USIM for the SAE/LTE network and (2) Security should be at least of the same level or better than that compared to UMTS. Further details of the requirements are discussed below and more detail is provided in Fig. 3 [1, 2].

To fulfill the first basic requirement, the AKA used in 3G is maintained mostly with slight enhancements such that older releases of USIM can be reused. This provides comparable security to UMTS thereby taking care of the second basic requirement. Several other enhancements were done, some of which arise from the new architecture. Compared to the earlier generation of mobile systems (1) SAE/LTE requires forward security. Therefore, a successful attack at a given time should not lead to an attack on future communication after a change in the security context (in fact an attack on earlier communication is also not possible. Hence, SAE/LTE also provides backward security). (2) Key separation for every purpose is required (integrity and confidentiality in RRC, UP and NAS), which means that, for example, a compromise of integrity key of RRC should not lead to a successful attack on the confidentiality of RRC or UP and NAS. (3) Integrity is mandatory for RRC and NAS but there is no integrity for UP data; confidentiality is optional for both AS, i.e. RRC & UP, and NAS. From this the control plane of SAE/LTE can be authenticated on a per packet basis and is secure against a man-in-the-middle attack.

As described in Section 2, eNB is the end-point for AS security in the network side. The eNB manages the AS security context and initiates AS security towards UE. Therefore, the eNB configuration should be authenticated and authorized. Security context and keys should be stored in a secure environment within the eNB.

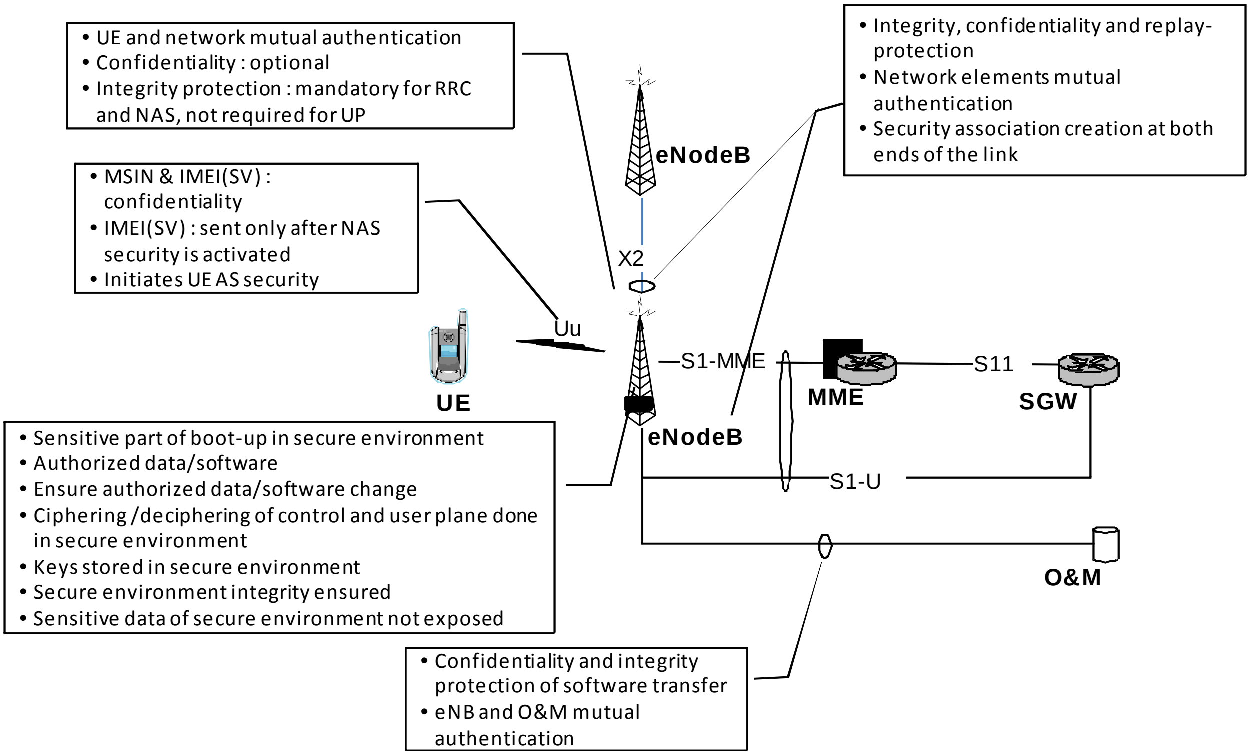

• UE and network mutual authentication
• Confidentiality : optional
• Integrity protection : mandatory for RRC and NAS, not required for UP
• MSIN & IMEI(SV) : confidentiality
• IMEI(SV) : sent only after NAS security is activated
• Initiates UE AS security
• Integrity, confidentiality and replay-protection
• Network elements mutual authentication
• Security association creation at both ends of the link
eNodeB
X2
Uu
UE
S1-MME
S11
MME
SGW
eNodeB
S1-U
O&M
• Sensitive part of boot-up in secure environment
• Authorized data/software
• Ensure authorized data/software change
• Ciphering /deciphering of control and user plane done in secure environment
• Keys stored in secure environment
• Secure environment integrity ensured
• Sensitive data of secure environment not exposed
• Confidentiality and integrity protection of software transfer
• eNB and O&M mutual authentication

Fig. 3. SAE/LTE security requirements.

MME is the end-point for integrity and confidentiality protection of NAS signaling; it manages the NAS keys and participates in AS key handling. MME retrieves Authentication Vectors (AVs) from the HSS, where it verifies UE authentication. The home network element HSS performs authentication with UE and generates AVs.

3.2 Algorithms

The algorithms for confidential and integrity protection are known as the EPS Encryption Algorithm (EEA) and EPS Integrity Algorithm (EIA). Three cryptographic algorithms were standardized for EEA and EIA: SNOW 3G, AES and ZUC.

SNOW 3G is defined in the SAGE Specifications [1, 2, 6], which is a word-oriented stream cipher. This algorithm was designed as a cryptographic solution to tackle algebraic attacks. AES (Advanced Encryption Standard) uses the core function of a block cipher. The latest agreed algorithm, ZUC, is a new stream cipher, which was standardized to fulfill the Chinese regional requirement. SNOW 3G and AES are mandatory algorithms for SAE/LTE, whereas ZUC is optional.

Although the same algorithms are implemented on both the UE and network (eNB and MME), the UE and network element still require a mechanism to negotiate which algorithm should be used when a key is to be derived. In 3GPP, a security mode command (SMC) is defined for algorithm selection and negotiation. The serving network will select the algorithm depending on the priority set by the mobile operator and UE capability. The selected algorithm will be indicated to the UE with integrity protection. SMC exists for both NAS and AS security [1, 2, 7]; see Section 3.3 for details. Having two algorithms, which are essentially different from each other, ensures that the network has a backup algorithm to work securely in the case of failure (hacked or cracked algorithm) in one of the algorithms.

3.3 Authentication and Key Agreement and Security Mode Command

The 3GPP Authentication and Key Agreement (AKA) procedure is for mutual authentication between the UE and network as well as for the generation of an initial key, K_{ASME}, between the UE and MME of the serving network [1, 2]. Using K_{ASME}, the UE and MME can derive the NAS keys and AS keys. The NAS and AS keys are derived and activated using the Security Mode Command (SMC) procedure, which provides algorithm negotiation, see Section 3.2. This section discusses the AKA, NAS SMC and AS SMC.

3.3.1 3GPP AKA Procedure

3GPP AKA is designed for mutual authentication between the UE and network (HSS and MME), which results in the derivation of same / agreed key (K_{ASME}) between the UE and MME. The 3GPP AKA procedure can be initiated by the network anytime, which also ensures the freshness of key K_{ASME}. The AKA procedure uses a challenge-response protocol; it also contains a sequence number-based protocol against a replay attack. Fig. 4 provides an overview of the 3GPP AKA procedure.

The 3GPP AKA procedure can be divided into two phases: (1) distribution of Authentication Vector (AV) from the HSS to serving MME (as in steps 4, 5 in Fig. 4), where the AV constitutes of RAND, AUTN, XRES and K_{ASME}; and (2) the authentication and key agreement procedure between the UE and serving MME (step 6 to 12

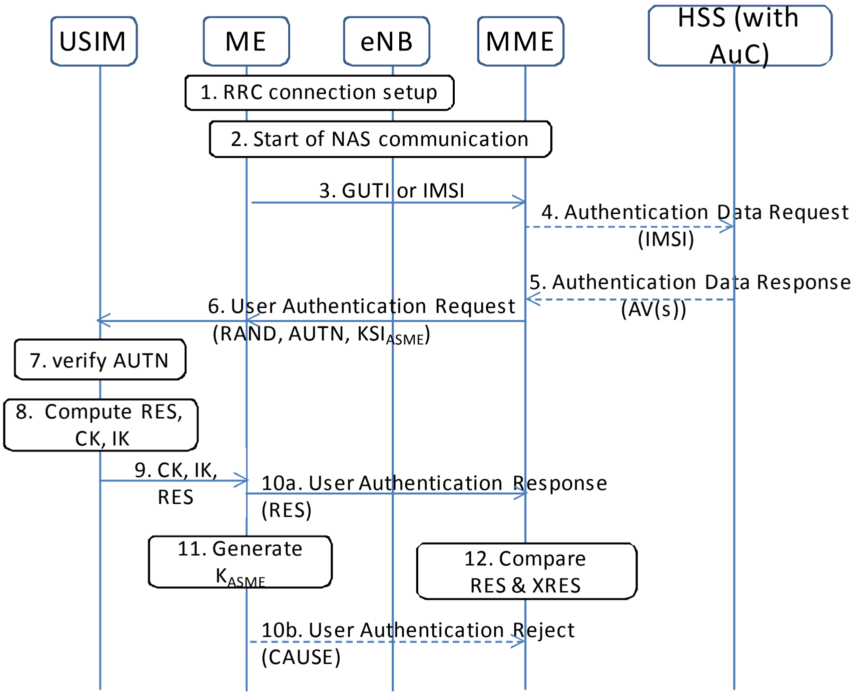

USIM
ME
eNB
MME
HSS (with AuC)
1. RRC connection setup
2. Start of NAS communication
3. GUTI or IMSI
4. Authentication Data Request (IMSI)
5. Authentication Data Response (AV(s))
6. User Authentication Request (RAND, AUTN, KSI_ASME)
7. verify AUTN
8. Compute RES, CK, IK
9. CK, IK, RES
10a. User Authentication Response (RES)
11. Generate K_ASME
12. Compare RES & XRES
10b. User Authentication Reject (CAUSE)

Fig. 4. 3GPP AKA procedure.

in Fig. 4). The first phase can be omitted if the serving MME already has a valid authentication vector. The two phases are explained below based on the steps in Fig. 4. Note that the two phase concept is only being used for explanation.

Phase (1) Authentication Vector distribution (HSS – MME): This phase begins after the UE initiates radio communication. Therefore, Radio Resource Control (RRC) is setup (Step 1), and NAS connectivity (Step 2) and the UE has sent its identity to the MME. The identity is either International Mobile Subscriber Identity (IMSI) or Globally Unique Temporary Identity (GUTI) a temporary identity at the given MME (Step 3). The serving network element MME invokes the procedure by sending an Authentication Data Request message to the HSS, which includes IMSI of UE so the HSS can fetch data related to the given subscription (Step 4). The HSS sends Authentication Data Response message to the MME with AV for a given UE, Therefore the MME can perform user authentication (Step 5). The HSS can send more than one AV to the MME. Each AV contains a challenge of RAND and AUTN for the UE to authenticate the MME, the key K_{ASME} and a challenge response XRES computed with K_{ASME}.

Phase (2) authentication and key agreement (MME – UE): This procedure is also invoked by a serving network element MME by sending a User Authentication Request to UE (Step 6). MME inserts the RAND, AUTN and key identifier, KSI_{ASME}, in the authentication request. Upon receiving the message, USIM in UE will verify the AUTN (Step 7) and calculate the CK, IK and RES if the AUTN is acceptable (Step 8). The CK, IK and RES are sent to the ME from USIM (Step 9). The RES is inserted in the User Authentication Response message and sent to the MME from E (Step 10a). The ME generates K_{ASME} (Step 11). The MME compares the RES and the expected value, XRES (Step 12). The UE is authenticated if they are a match. Key K_{ASME} is calculated at the UE side. Therefore, it can share the same key with MME. If the AUTN is not verified at Step 7, UE sends a User Authentication Reject message to the MME with a proper cause.

3.3.2 NAS SMC Procedure

After 3GPP AKA, the UE and network can establish the NAS security context for a given KSI_{ASME}. The NAS security context is established using NAS SMC, see Fig. 5.

The serving network MME selects the highest priority algorithm for the NAS communication, derives the NAS keys and starts NAS integrity protection. The MME then informs the UE as to which confidentiality and integrity algorithm and K_{ASME} to use for NAS key derivation in the NAS Security Mode Command. The NAS Security Mode command is integrity protected, and the UE security capabilities are also included in the message. Initially, the UE sends UE security capabilities to the MME without integrity protection. Therefore, the MME sends the UE security capabilities back to UE in an integrity protected message so that the UE can verify its correctness. The MME starts integrity protection after sending the NAS Security Mode Command to the UE.

The UE verifies the integrity of the NAS Security Mode Command. If the check is successful, the UE begins ciphering, deciphering and integrity protection, and responds to the MME with a NAS Security Mode Complete message. When the integrity check fails at UE, it sends the MME a NAS Security Mode Reject with a proper cause. After a successful NAS SMC procedure, the AS security context can be established; see Section 3.3.3.

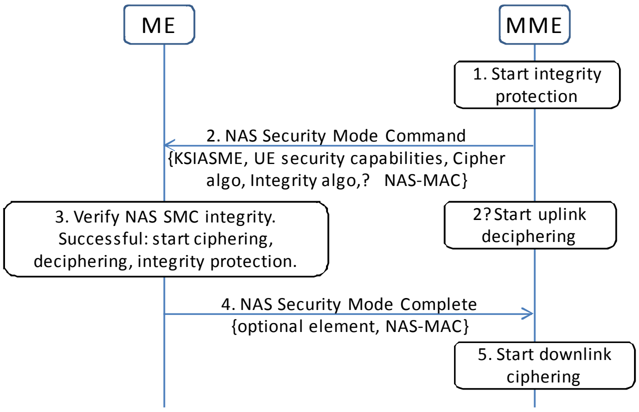

ME
MME
1. Start integrity protection
2. NAS Security Mode Command {KSIASME, UE security capabilities, Cipher algo, Integrity algo,?   NAS-MAC}
3. Verify NAS SMC integrity. Successful: start ciphering, deciphering, integrity protection.
2?Start uplink deciphering
4. NAS Security Mode Complete {optional element, NAS-MAC}
5. Start downlink ciphering

Fig. 5. 3GPP NAS SMC procedure.

3.3.3 AS SMC Procedure

The basic purpose of the AS SMC procedure is the same as that for NAS SMC but it is run between the UE and eNB, see Fig. 6. AS SMC begins after receiving a message by eNB from the MME. The eNB chooses the algorithm from the priority list, starts RRC integrity protection and initiates the SMC procedure by sending an integrity protected AS Security Mode Command to the UE, indicating the integrity and ciphering algorithms for the AS. The UE first verifies the message from the eNB, starts integrity and confidentiality of the AS messages and then responds with an integrity protected AS Security Mode Complete. The UE replies with an unprotected Security Mode Failure message if the integrity check fails.

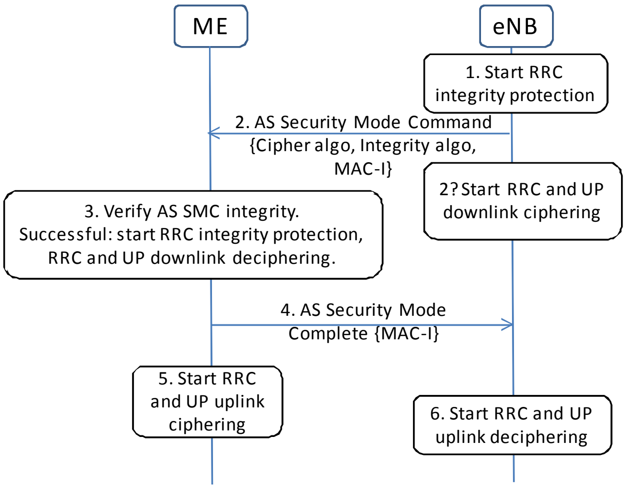

ME
eNB
1. Start RRC integrity protection
2. AS Security Mode Command {Cipher algo, Integrity algo, MAC-I}
2?Start RRC and UP downlink ciphering
3. Verify AS SMC integrity. Successful: start RRC integrity protection, RRC and UP downlink deciphering.
4. AS Security Mode Complete {MAC-I}
5. Start RRC and UP uplink ciphering
6. Start RRC and UP uplink deciphering

Fig. 6. 3GPP AS SMC procedure.

As stated above, the AS is made from the RRC and UP, where the RRC is mandatorily integrity protected and optionally confidentially protected, whereas the UP is optionally confidentiality protected. Note that UP is never integrity protected because any error in a wireless channel can lead to the discarding of the message due to an integrity check failure, leading to a degradation of the service.

3.4 Key Hierarchy

Fig. 7 shows the SAE/LTE key hierarchy. The hierarchy follows key separation required for confidentiality and integrity protection for NAS, AS and UP. This section provides an overview of the SAE/LTE keys.

- K: This is the root key that is shared between the USIM and Authentication Centre in the home network (AuC). This key is used for mutual authentication, i.e. AKA. K is 128 bits and never leaves the USIM and AuC.
- CK, IK: These keys are computed from K and are used for confidentiality, CK, and integrity, IK, in 3G. At the home network, AuC computes the CK, IK and sends them to the HSS. At the UE, the USIM computes the CK, IK and sends them to ME.
- KASME: A 256 bits key is derived from CK, IK and is bound to the serving network identity (SNID). KASME is only created by either a successful AKA or by the inter-Radio Access Technology (RAT) procedures towards E-UTRAN.
- NAS keys: NAS keys contain a pair of keys, KNASenc and KNASin, for NAS signaling encryption and integrity protection separately. The NAS keys are derived and shared between the MME and UE.

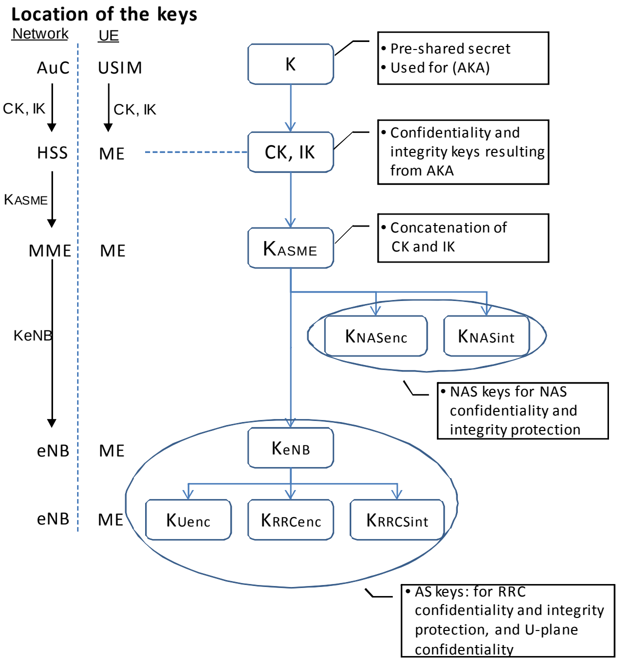

Location of the keys
Network
UE
AuC
USIM
CK, IK
CK, IK
HSS
ME
KASME
MME
ME
KeNB
eNB
ME
eNB
ME
K
• Pre-shared secret
• Used for (AKA)
CK, IK
• Confidentiality and integrity keys resulting from AKA
KASME
• Concatenation of CK and IK
KNASenc
KNASint
• NAS keys for NAS confidentiality and integrity protection
KeNB
KUenc
KRRCenc
KRRCSint
• AS keys: for RRC confidentiality and integrity protection, and U-plane confidentiality

Fig. 7. Key hierarchy.

- AS keys: AS keys contains a pair of keys KRRCenc and KRRCint for the AS control plane, i.e. RRC, encryption and integrity protection respectively, and K_{UPenc} for UP encryption. The root for AS keys is K_{eNB}, which is derived at every handover and is associated with a given cell of the eNB.

3.5 Security in Mobility

SAE/LTE, being a mobile system, certainly supports different types of mobility. Mobility with itself brings several security issues compared to communication with a static device. This section is started with an overview of mobility, followed by security in the mobility for SAE/LTE.

3.5.1 Overview

Mobility can occur when the UE is in an on-going session, i.e. active, or the UE is idle. Handover is the mode of mobility when the UE is active. Different types of handover, both for an active and idle UE, can be categorized as follows, see Fig. 1 regarding the X2 and S1 interfaces:

- Intra-SAE/LTE
  - X2 handover: The UE moves from one eNB to other
  - S1 handover: Handover leads to change in MME
  - Intra-eNB handover: The UE moves from one cell of a given eNB to other
- Inter- RAT handover: Our focus in this paper is on handover between SAE/LTE and UTRAN

In SAE/LTE handover begins with preparation followed by execution and finally completion. All phases must be secured where secured means (i) source authenticity, (ii) message integrity, (iii) replay protection and (iv) provision for forward (as well as backward) security. Requirements (i) – (iii) can be fulfilled using the appropriate keys associated with a given UE and cell of eNB, which is achieved in SAE/LTE by authentication and key derivation. The open point is the fulfillment of requirement (iv), which will be covered in the following sub-sections.

To fulfill the requirement for forward security, it is essential to re-key at every handover and the new key should be independent of the previous key. Re-keying requires that a common random value be available at the network and the UE, which can be made available by different means. As discussed in Section 3.1, the eNodeB can be located in easily accessible place and can be attacked easily. With this in mind, 3GPP solution development begins with the assumption that an UE is connected to a eNB that is compromised. This means that (a) the random value for re-keying must not be generated at the eNB, and (b) the random value must be given to the target eNB (eNB where the UE will move to from the current, source, eNB) and not to the source eNB.

3.5.2 Intra-SAE/LTE

This section discusses the X2 and S1 handover, see Section 2 and Fig. 1 regarding the X2 and S1 interfaces.

The discussion in this section is not applicable to an idle UE because such UE only has a NAS context.

X2 Handover

X2 handover occurs when UE moves between the eNBs connected to the same MME. The random value at the UE and eNB is called the Next Hop (NH) parameter that is sent to the target eNB by the MME. A attacker that has compromised the source eNB will also be able to impact (perform attack of any form) the services of the given UE at the target eNB (the first hop) but the UE services will be secured from the next handover onwards; assuming that the target eNB is not compromised. With this background, this section explains the details of X2 handover.

Referring to Fig. 8, each K_{eNB} is associated with a NH value and a counter, NH Chaining Counter (NCC). Upon handover, an intermediary key K_{eNB}* is derived by the source eNB from NH and is sent to the target eNB after binding it to the cell identity (Physical Cell Identity, PCI) and frequency of the target eNB (EARFCN-DL or E-UTRAN Absolute Radio Frequency Channel Number-Down Link); the target is always one of the cells of the target eNB. Sometimes, depending on deployment or failure of connectivity to the MME, which leads to a lack of new NH parameter, K_{eNB}* might be derived directly from K_{eNB} at the source eNB. K_{eNB}* received from the source eNB is used as K_{eNB} at the target eNB. The first K_{eNB} is derived from K_{ASME}, no NH is associated with this key and the NCC is set to 0. The first K_{eNB} is sent to the eNB by MME along with the next NH and NCC (NCC=1). Upon handover, the MME increments NCC by 1 and sends a new NH and NCC value to the target eNB. Hence, NCC=1 is never used.

S1 Handover

S1 handover, in simple terms, occurs when the S1 interface is involved in handover key management. Such handover occurs when both the source and target eNBs are connected to different MMEs but it can also occur when both eNBs are under the same MME. In the case of S1 handover, the communication from the "next hop" is secured even if the source eNB is compromised. This happens because the source MME sends a new NH with the NCC incremented by 1 to the target MME, which in turn forwards a new NH, NCC pair to the target eNB. The target eNB derives K_{eNB} from the new NH, NCC pair. The UE is informed of the NCC used for key derivation. Therefore, the UE and target eNB use a NH value that is unknown to the source eNB leading to a K_{eNB} that cannot be known to an attacker of the compromised source eNB.

3.5.3 Inter-RAT

Inter-RAT, or I-RAT, handover occurs whenever the UE moves between SAE/LTE and different technology. To achieve secure communication in the target serving network, the UE and the target network should share a valid security context. This section briefly discusses the mobility between E-UTRAN and UTRAN.

When an UE transits from E-UTRAN to UTRAN, both UE and MME generate a key CK' and IK', which are called the mapped UTMS security context because they are derived (or mapped) from K_{ASME}. Similarly, when an UE performs handover from UTRAN to E-UTRAN, both UE and MME derive K'_{ASME} from the CK and IK; there are rules on when this is not required. The NAS and AS keys are derived from the K'_{ASME}. After handover, the MME can decide to invoke the AKA procedure.

4. Current Trend and Future Topics

This paper presented an overview of SAE/LTE security. Some of the new security features developed in the SAE/LTE system that differ from UMTS are: 1) key

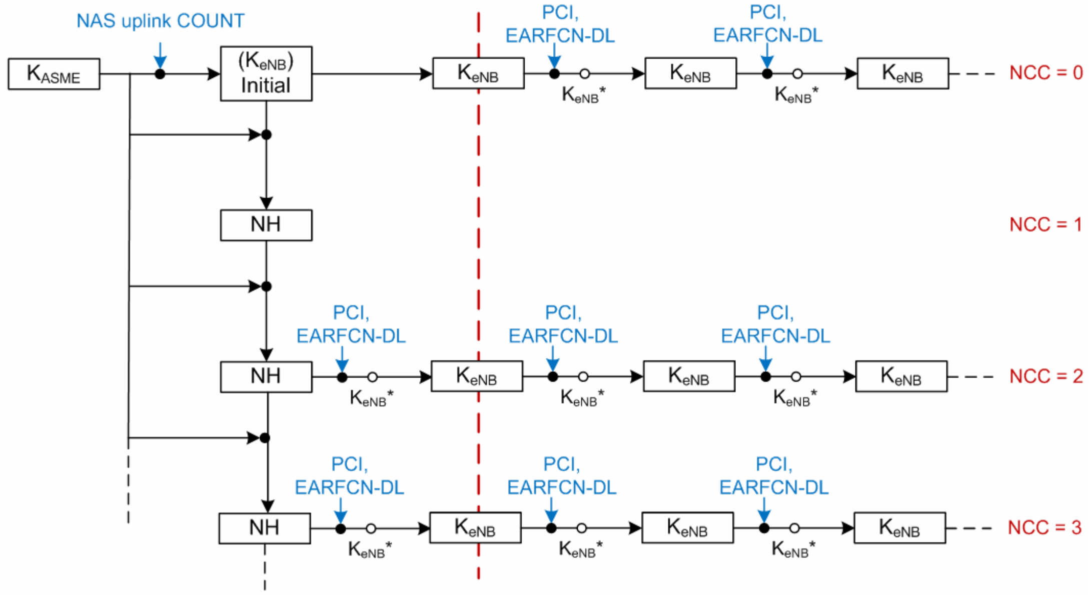


Fig. 8. Handover key chaining

hierarchy is introduced, 2) eNB is the end-point for user plane security, 3) key separation depending on use (NAS, AS – UP and RRC), 4) forward security and (5) inter-RAT mobility security.

Currently, SAE/LTE is widely adopted around the world with deployment existing in several countries. While moving towards SAE/LTE, operators have been experiencing increasing traffic over their network coming from the Internet, which is known as over the top (OTT) services. Mobile operators cannot benefit a great deal from the OTT services while at the same time there is the potential for an increase in cyber attacks. Therefore, it is important to work on services for operators to increase their revenue and develop solutions against cyber attacks in mobile networks.

SAE/LTE provisions voice service using an IP Multimedia Subsystem (IMS) that is based on Session Initiation Protocol (SIP) used for Voice over IP (VoIP). Therefore, spam over IP telephony (SPIT) can be expected in mobile networks when IMS is used. Some study is done in 3GPP regarding SPIT under the study known as Protection for Unsolicited Communication in IMS [8].

Another topic in 3GPP of prime importance is Machine Type Communication (MTC) [9] or Machine-to-Machine (M2M) system. M2M is a type of service that the operator provides for machine type devices. MTC devices are different from normal UE in the sense that there is no human interface, communication is triggered by an external server, devices might be required to run on battery for long time, and the amount of data communicated is expected to be very small. Therefore, MTC raises new security and privacy concerns.

References

[1] Anand R. Prasad and Seung-Woo Seo, Security in Next Generation Mobile Networks: SAE/LTE and WiMAX, River Publishers, August 2011, Denmark.

[2] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[3] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[4] 3GPP TS 36.323: "Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification".

[5] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC); Protocol specification".

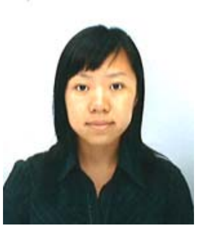
[6] http://www.etsi.org/index.php/services/security-algorithms/3gpp-algorithms. Article (CrossRef Link)

[7] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[8] 3GPP TR 33.937: "Study of mechanisms for Protection against Unsolicited Communication for IMS (PUCI) ".

[9] 3GPP TR 33.868: "Security aspects of Machine-Type Communications".

Anand R. Prasad, Dr. & Ir. (MScEngg), Delft University of Technology, The Netherlands, Certified Information Systems Security Professional (CISSP), Fellow IETE and Senior Member IEEE, is a NEC Certified Professional (NCP) and works as a Senior Expert at NEC Corporation, Japan, where he leads the mobile communications related security activity. Anand is a vice-chairman of 3GPP SA3 (mobile communications security standardization group). He is a Member of the Governing Body of Global ICT Standardisation Forum for India (GISFI) where he is founder chairman of the Security & Privacy working group and was chairman of the Green ICT working group. Before joining NEC, Anand led the network security team in DoCoMo Euro-Labs, Munich, Germany, as a manager. He started his career at Uniden Corporation, Tokyo, Japan, as a researcher developing embedded solutions, such as medium access control (MAC) and automatic repeat request (ARQ) schemes for wireless local area network (WLAN) product, and later he was a project leader of the software modem team. Subsequently, he was a systems architect (as distinguished member of technical staff) for IEEE 802.11 based WLANs (WaveLAN and ORiNOCO) in Lucent Technologies, Nieuwegein, The Netherlands, during which period he was also a voting member of IEEE 802.11. After Lucent, Anand joined Genista Corporation, Tokyo, Japan, as a technical director with focus on perceptual QoS. Anand has provided business and technical consultancy to start-ups, started an offshore development center based on his concept of cost effective outsourcing models and is involved in business development. Anand has applied for more than 40 patents, has published 6 books and authored more than 50 peer reviewed papers in international journals and conferences. His latest book is on "Security in Next Generation Mobile Networks: SAE/LTE and WiMAX", published by River Publishers, August 2011. He is a series editor for standardization book series and editor-in-chief of the Journal of ICT Standardisation published by River Publishers, an Associate Editor of IEEK (Institute of Electronics Engineers of Korea) Transactions on Smart Processing & Computing (SPC), advisor to Journal of Cyber Security and Mobility, and chair / committee member of several international activities. He is a recipient of the 2012 (ISC)² Asia Pacific Information Security Leadership Achievements (ISLA) Award as a Senior Information Security Professional.



Xiaowei ZHANG received her PhD in Information Science from Chiba University, Japan. She is currently working as Assistant Manager in NEC Corporation, Japan. Her recent activity has been on mobile network security. Her interests also includes M2M communication and security, smart phone security. She is a member of IEEE and has applied for more than 20 patents.