Security Analysis of LTE Access Network

Conference Paper · January 2011

CITATIONS
24

READS
2,233

3 authors, including:

Cristina-Elena Vintilă
8 PUBLICATIONS **28** CITATIONS
SEE PROFILE

Victor-Valeriu Patriciu
Technical Military Academy of Bucharest
104 PUBLICATIONS **508** CITATIONS
SEE PROFILE

Security Analysis of LTE Access Network

Cristina-Elena Vintilă, Victor-Valeriu Patriciu, Ion Bica
Computer Science Department
Military Technical Academy - Bucharest, ROMANIA
cristina.vintila@gmail.com, vip@mta.ro, ibica@mta.ro

Abstract: **The latest technological development in mobile telecommunications is the 4G architecture. Developed and standardized by the 3GPP, this technology proposes significant throughput and security enhancements in comparison with its predecessor, 3G – a 3GPP architecture, as well as with the non-3GPP solutions like WiMAX. Besides the enhancements mentioned above, 4G is a simplified network architecture, flat-IP topology and services-oriented. One of the major simplifications is the base-station architecture, called eNodeB in the 4G terminology, which eliminates the need for a radio resource controller and assumes signaling, control-plane and security functions. It is the mobile device connection to the network and the proxy of all its traffic. This is why the access network is one of the most important areas for network design and optimization and also for security in term of access control, authentication, authorization and accounting. This paper reviews the access network components, the eNodeB security requirements, as defined by 3GPP and analyzes two secure access mechanisms to a 4G network, one via eNB (3GPP access type) and the other one via AP (non-3GPP access type). It also proposes an improvement to the AKA protocol in order to obtain better security.**

Keywords-SAE; LTE; EPC; security; eNodeB; shared-secret; HSS; Diameter; EAP; AKA; J-PAKE

I. INTRODUCTION

The most important and influential telecommunications organizations around the Globe are part of the 3GPP society [20]. The latest technological design for mobile telecommunications that appears to be the future communications architectural baseline is the 4G architecture, also called SAE (System Architecture Evolution). SAE comprises the radio access network, usually referred to as LTE (Long Term Evolution) and the EPC (Evolved Packet Core) the core network of this design, a flap-IP network, highly optimized and secure network, oriented on services.

The figure below describes one of the most common architectural design views, a non-roaming architecture with a 4G mobile device and only 4G access to the network. The entities that appear in this case are the UE (User Equipment), the eNodeB (the antenna), the MME (Mobility Management Entity), the SGW (Serving Gateway), PGW (PDN (Packet Data Network) Gateway), HSS (Home Subscriber Server), PCRF (Policy Charging Rules Function) and a 3G access network where the UE can roam to. This also represents the naming of the interfaces that connect these entities.

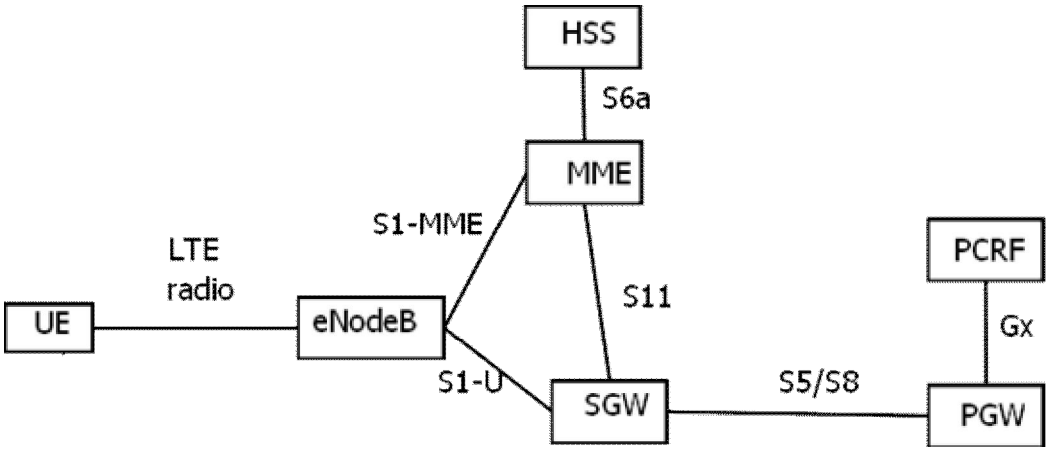

Figure 1. Basic 4G Core Network Architecture

The UE connects to the 4G network by signaling its presence in the eNodeB cell. The cell selection prerequisites are described in [3], [4] and [5]. The process by which an UE chooses a certain antenna (eNodeB) to connect to is called *camping* – the UE *camps* on a cell. The best situation for an UE is to find a so-called *suitable cell* to camp on. This suitable cell is a cell that meets the following requirements: it is part of the selected PLMN (Public Land Mobile Network), part of a registered PLMN or part of the Equivalent PLMN list as per the most recent update from the NAS. Also, the cell should not be barred, not reserved and should not be in the list of forbidden areas for roaming. Once these criteria are met, the UE sends an *Attach Request* message to this eNodeB, asking to attach to the network. This message flows over the LTE

 ISBN:978-1-61208-113-7

radio interface, reaches the eNodeB, and then the eNB sends this message to the MME via the S1-MME interface. The MME verifies the validity of the UE request against the HSS credentials, then selects an appropriate SGW that has access to the PLMN requested by the UE. The PLMN where the UE connects is identified by a string called APN (Access Point Name) preconfigured on the USIM. Once the access request reaches the PGW – which is the UE's anchor point to the desired PLMN, the request is replied with an IP address suitable for this connection and, even more, after interrogating the PCRF about this UE, the PGW may create dedicated bearers for this UE immediately after attach. The decisions on the way are detailed in Section 4.3.8 of [1], which describes the selection functions of each of the core-network entities. Briefly, the HSS drives the selection of the SGW and the SGW on its turn, selects the PGW, based mostly on information already decided upon by the HSS. The MME is selected based on the network topology, the eNB trying to select the MME that minimizes the probability of doing handovers and that provides load balancing with other MMEs.

The Initial Attach process starts with the *Attach Request* message sent by the UE to the eNB selected. This message contains, among other parameters, the IMSI (International Mobile Subscriber Identity) or the old GUTI (Global Unique Temporary Identity), the last TAI (Tracking Area Identifier) if available, PDN Type, PCO (Protocol Configuration Options), Ciphered Options Transfer Flag, KSI-ASME (Key Set Identifier - Access Security Management Entity), NAS (Network Access Server) Sequence Number, NAS-MAC, additional GUTI and P-TMSI (Packet - Temporary Mobile Subscriber Identity) signature.

The PCO means that the UE wants to send some customized information to the network (the PGW may not be in the visited network also), indicating for instance that the UE prefers to obtain the IP address after the default bearer has been activated. If the UE intends to send authentication credentials in the PCO, it must set the Ciphered Options Flag and only send PCO after the authentication and the NAS security have been set up completely. From now on, it is the responsibility of the eNB to proxy the UE's message to the MME. And, once the UE is authenticated, the eNB is also the one responsible of establishing security connections with the UE and the core network in order to protects the UE's traffic at the radio/ethernet border. Being at the border between these two topologies, the eNB is exposed to the security issues arising from both the radio and the IP networks.

II. SECURITY ARCHITECTURE

The 4G architecture defines, in [6], the five main areas concerned with the Security of this design. The first is called Network Access Security and it refers mostly to the radio attacks. The second one is the Network Domain Security and it defines the requirements and rules to prevent attacks over the wire, when exchanging control-plane and user-plane. The third is User Domain Security, dealing with securing the access to mobile terminals, the fourth is the Application Domain Security – which standardizes the set of rules for secure message exchange between applications on clients and servers. The fifth domain defined by this standard is the Visibility and Configurability of Security – set of features that informs the user about a particular security feature and whether this feature is applicable or not to the services this user is trying to access.

The standard [6] describes in Section 5.3 the security requirements necessary for a secure eNB operation environment, as well as for secure eNB functioning. It nevertheless leaves these specifications at a requirements level, permitting the operator to implement the exact protocols he considers for his network; these protocols are compliant to the standard as long as they meet the security requirements defined here, in Sections 11 and 12. The principles are that the eNB should have a mean of securing the cryptographic keys and information inside the device, it should have secure communication links both over the air with the UE and with the MME (via the S1-MME interface), SGW (via the S1-U interface) and other eNBs (via the X2 interfaces, if they exist) for control-plane and user-plane traffic. Also, if the operator has a securely contained environment where these communications happen, he may not implement any precise security measure for the requirements defined here.

The access to a 4G network is done in many ways, most importantly driven by the type of radio medium in place. The most usual procedure is the AKA (Authentication and Key Agreement) Procedure. This happens when the access medium is LTE. The AKA procedure is described in the figure below.

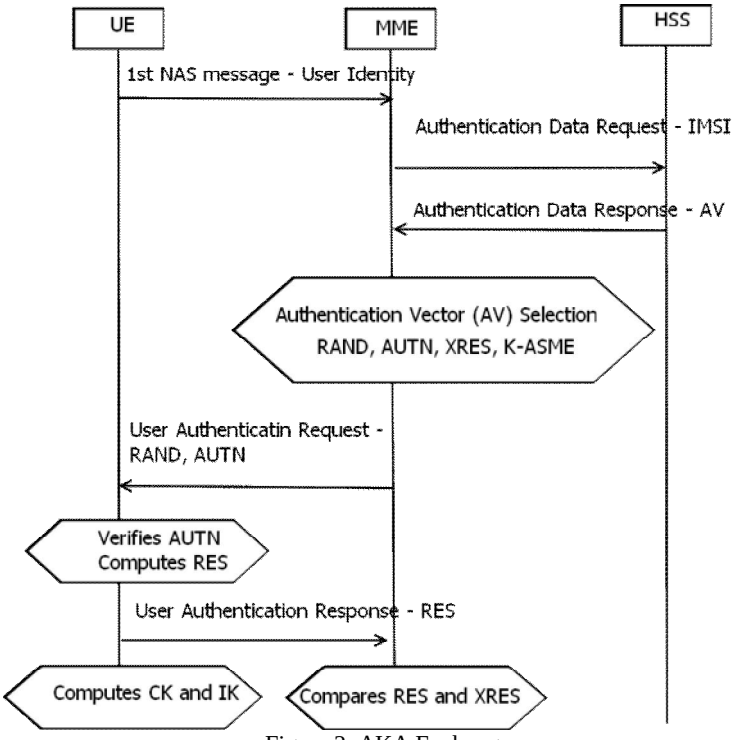

Figure 2. AKA Exchange

The MME here is the authenticator, while the HSS is the authentication server. The communication between the MME and the HSS takes place over S6a and it uses Diameter as a

protocol. The UE (the mobile terminal) has a UICC (Universal Integrated Circuit Card) inside. This circuit stores the K, a shared key located as well on the AuC (Authentication Center) entity part of the HSS. The authentication in 4G is not natively implemented over a PKI infrastructure; it uses the shared-secret symmetric authentication inherited from the 3G UMTS systems, with some improvements.

The purpose of the AKA mechanism is to create keying material for the RRC (Radio Resource Control) signaling, NAS (Non-Access Stratum) signaling and for the user-plane, both ciphering and integrity keys. The first NAS message may be an Attach Request, a Service Request or PDN Connectivity Request message. This message reaches the MME, which should verify the UE's identity. If the UE is new to this network entirely, then the MME asks the UE for its permanent identity – the IMSI. This is considered a security flaw and it is not yet addressed. But, if the UE is not new to this network, but rather reached this MME by means of a TAU (Tracking Area Update) procedure, then this MME should have a GUTI in the message received from the UE. This MME then sends the GUTI and the full TAU message to the previous (old) MME, and this one replies with the actual permanent UE identity – the IMSI and the authentication data for it. The message exchange between the two MME entities takes place over the S10 interface. Also, if the UE roamed to this MME from a 3G network, the current MME tries to connect to the previous management entity of this UE, the (old) SGSN (Serving GPRS Gateway) via the S3 interface and get the IMSI information from there. Otherwise, it tries to derive it and then connects to the HSS via the S6a interface and verifies that the IMSI this UE utilizes is actually valid for this network and may have permission to attach. This message is a Diameter message described in [9].

The HSS gets the AV (Authentication Vector) set and sends it to the MME. This EPS-AV consists of RAND, AUTN, XRES and K-ASME and the HSS, entity that is also called UE's HE (Home Environment) may send multiple sets of AVs to the MME currently serving the UE. The standard recommends that the HSS sends only one set of AVs, but in case it still sends multiple sets, there should be a priority list which the MME should use.

A major improvement when comparing EPS-AKA to UMTS-AKA is that the CK and IK keys never actually have to leave the HSS. The UE signals in its initial message the type of access network he used. If this is E-UTRAN, then a flag called AMF is set to value 1, and this instructs the MME and ultimately the HSS to only send the K-ASME key in the AV reply (along with RAND, AUTN and XRES), but not the CK and IK as well. Also, this K-ASME can be stored in the MME, so, when re-synchronizing the UE's status, the full AKA process may not even have to take place. The MME sends the RAND and AUTN to the UE, then it waits for the response. Here, the eNodeB just forwards these messages back and forth, not participating effectively in the cryptographic exchange. Unlike the GSM, where only the network was authenticating the UE, but not viceversa, the EPS-AKA provides mutual authentication between the UE and the network. Upon receipt of the message, the UE can verify, based on the AUTN, the validity of the reply, computes the RES' and sends this message to the MME. The MME verifies whether XRES equals the RES' and if they are the same, the UE is authenticated. As described, the CK and IK are computed by UICC and HSS independently, they are never sent over the wire in EPS. Also, the HSS sends initial keys to MME and eNB, which are then used by these entities to derive actual keys for NAS, user-plane and RRC traffic.

The figure below depicts two flows: the first one represents the sending of the IMSI in clear-text over the network (the case of the first attach of this UE to the network or when the new MME cannot locate the previous MME) and the second one represents the message exchange between the two MMEs.

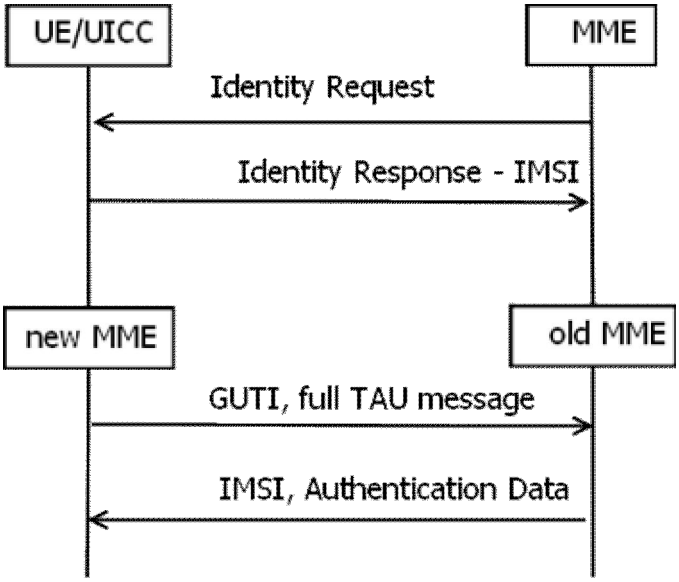

Figure 3. Message exchanges to locate the IMSI

The key hierarchy in 4G is more complicated than in 3G, but it assures this way the protection of the master keys and it also reduces the need for periodic updates, re-generation and transmission of the master keys. There are also special cases for TAU and handover types and also for re-keying that may require special attention, and they are described in [6].

For the non-3GPP access types, the 4G architecture no longer uses the AKA mechanism, but a variation of the EAP with AKA: EAP-AKA (Extensible Authentication Protocol) mechanism. This assumes the presence of a EAP capable phone, the Access Point, which connects to the AAA (Authentication, Authorization, Accounting) server via the Wa interface and the AAA server connects to the HSS via the Wx interface. The EAP-AKA message flow is represented in the picture below. The EAP is a Request/Response type of protocol. When the AP detects the presence of the USIM, it sends this mobile an EAP Identity Request message. The USIM sends back its NAI (Network Address Identifier), which is similar to an e-mail address – RFC 822. The AP forwards this NAI to the 3GPP AAA Server based on the domain name which is part of the NAI – this happens over the Wa interface.

 ISBN:978-1-61208-113-7

Then the AAA server verifies whether it has a valid and unused AV for this USIM. If so, it sends this AV and AKA Challenge for the USIM, back to the AP. If there is no available AV for this USIM, the AAA server contacts the HSS server via the Wx interface, retrieves the AV and then continues to the AKA Challenge. The rest of the process is similar to the EPS-AKA, with the only observation that it takes place over the EAP framework.

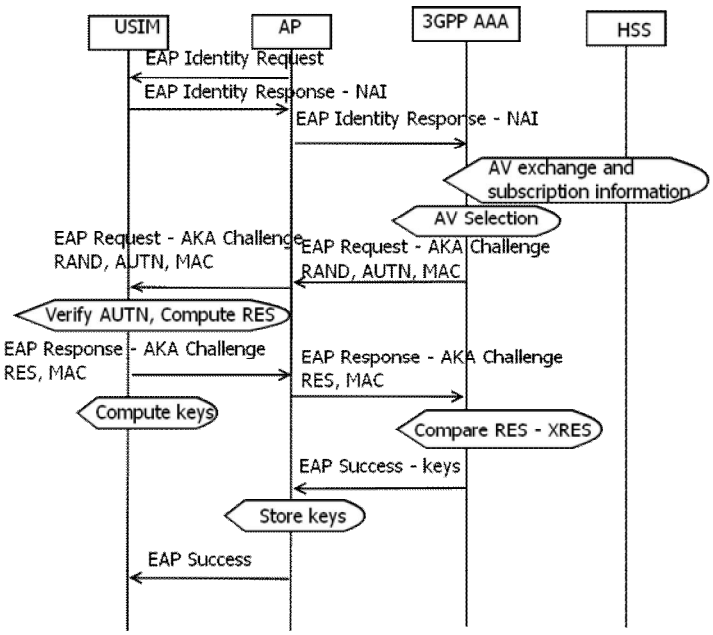

Figure 4. EPS EAP-AKA exchange

When comparing pre-4G authentication methods, there are several aspects that may be observed. One of them is the authentication method. This is very similar for 3G (UMTS), 3.5 G (HSDPA) and 3.75G (HSDPA+), as all of them use the AKA mechanism. The differences appear in the actual implementation: the 3G implementation specifies that the CK and IK keys from the AuC (Authentication Center) part of the HE (Home Environment) are actually being sent to the SGSN at the moment the SGSN downloads the Authentication Vectors from this database. This never happens in 4G, where the key hierarchy is more complicated and the only key downloaded from the HSS to the MME is the K-ASME key. This is also a security improvement in 4G in comparison to 3G, because the CK and IK keys should not leave the AuC, but only be derived independently by the UICC and HSS. In both 3G and 4G security architectures, there are multiple AVs (Authentication Vectors) available in the authentication part of the subscribers database. All these authentication vectors may be downloaded initially by the authentication entity (SGSN, MME respectively), a certain AV being used for a single round of authentication. The order in which these AVs are used is determined in both architectures by a sequence number. The CK||IK pair is derived by the UICC in 3G, and the SGSN only selects this pair from the authentication data received from the AuC. In 4G, the MME receives only its K-ASME from the HSS, and it then derives, together with the UE, the K-NASint and K-NASenc from the K-ASME. The following figure describes the key hierarchy in the 4G architecture.

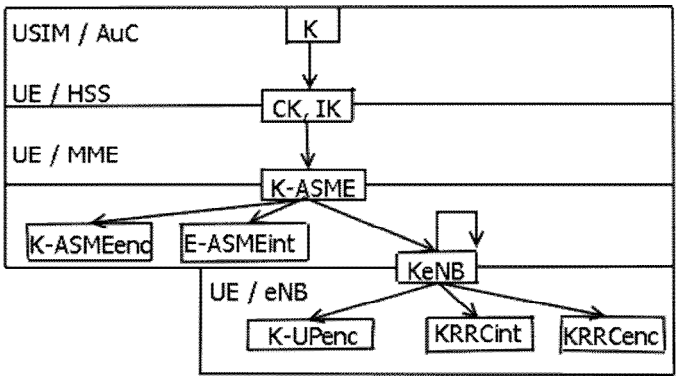

Figure 5. EPS key hierarchy [6]

The keys derived in the classical 4G AKA procedures are the following: K-NASenc (encryption key for NAS traffic), K-NASint (integrity key for NAS traffic), KeNB (derived by MME and eNB), KUPenc (encryption key for the user-plane data, derived by MME and eNB from KeNB), KRRCint and KRRCenc (integrity check, respectively encryption key derived by MME and eNB from KeNB, used for securing the Radio Resource Control traffic).

The sections in this figure describe which entities are involved in a particular key generation process; there are 6 keys derived from the EPS authentication mechanism. This key generation feature introduced in 4G improves the speed of the re-authentication procedures and also the refreshing process of the keys. As the K-ASME may be used a master key in further service requests authentication, the MME no longer has to download the authentication data from the HSS and it can also avoid re-synchronization issues. HSDPA and HSDPA+ follow the 3G procedures and mechanisms.

The entire authentication information that is stored in the UICC and its corresponding associates from the network side is called “security context”; a security context consists of the NAS (Non Access Stratum) and AS (Access Stratum) security contexts. The AS security context has the cryptographic keys and chaining information for the next hop access key derivation, but the entire AS context exist only when the radio bearers established are cryptographically protected. The NAS context consists of the K-ASME with the associated key set identifier, the UE security capabilities and the uplink and downlink NAS count values, used for each EPS security context. The 3G architecture also has the concept of security contexts, and this becomes very important when 3G and 4G devices and network entities interoperate. A 3G device that was initially attached to a 3G network has received a set of security content that is stored in the UICC. This information is considered a partial and legacy security context in the 4G environment. For a security context to be considered full, the MME should have the K-NASenc and K-NASint keys, which are obtained when the 3G device handovers to the 4G network. In this handover case, the legacy security context is

 ISBN:978-1-61208-113-7

referred to as mapped security context. A NAS security context of a mapped security context is always full and it is current (which means it is the most recently activated context). A summary of the types of security contexts that exist in the 3G – 4G interoperation is in the following table.

TABLE I. TYPES OF SECURITY CONTEXTS

AGE/EFFECT	CURRENT	NON-CURRENT
FULL	NATIVE / MAPPED	NATIVE
PARTIAL	X	NATIVE

A native security context is the one established at the EPS-AKA procedure successful completion.

III. SECURITY ISSUES AND ASSESSMENT

The security analysis in a mobile network expands from the radio access network until the core network and services. The most common threats are related to the following security prerogatives:

- authentication: the network must be sure that the person accessing a certain service is the one pretending to be and paying for this service
- confidentiality of data: the user and the network must be sure nobody un-authorized is viewing or accessing the user's data
- confidentiality of location: the user's location must not be known by anybody un-authorized
- denial of service: the user and the network must be sure that nobody interferes with a user's session, nor high-jacks it
- impersonation: the network and the user must be sure that no other user is pretending to be the actual registered user, nor this user can access services available to the actual registered user

The EPS security mechanisms should be able to enforce the above principles, and everything starts with the access level. The NDS (Network Domain Security) enforces these principles as well, but at a different level. When talking about User Domain Security, the Access Level is the first line of defense against attacks. For this, the EPS provides mutual authentication via the EPS-AKA mechanism or EPS-EAP-AKA (for non-3GPP access types). Using the keys generated after the AKA mechanism, all the RRC, NAS and user-plane signaling and data-planes are protected by secure encapsulation and integrity protected. Even though a flaw of the EPS-AKA: the transmission of the permanent identity IMSI over the air at Initial Attach exchange, EPS implements the GUTI value that is sent over the air instead of the IMSI, so that the AKA mechanism also provides identity protection. The only cases that require the transmission of the IMSI are the first Initial Attach and the attach after the core network entities are de-synchronized. This vulnerability opens the door for a man-in-the-middle attack that can take place once the IMSI is captured. Another vulnerability identified within the EAP-AKA, but that manifests in consequence with EPS-AKA also is the lack of PFS support. The PFS – Perfect Forward Secrecy is an attribute of the mechanism's that assures the secrecy of a set of session keys even if a previous set of keys has been compromised.

A solution for the PFS vulnerability can be the use of an algorithm that has the PFS built-in. This algorithm is the Diffie-Hellman key exchange. Still, DH does not provide mutual authentication by itself. Another algorithm, based on the J-PAKE mechanism, can be used. The J-PAKE mechanism has the following properties – as described in [19]:

- off-line dictionary attack resistance – it does not leak any password verification information to a passive attacker
- forward secrecy – it produces session keys that remain secure even when the password is later disclosed
- known-key security – it prevents a disclosed session key from affecting the security of other sessions
- on-line dictionary attach resistance – it limits an active attacker to test only one password per protocol execution

One solution for using the Juggling scheme in the UE's authentication to the network is to replace part of the AKA protocol with the J-PAKE protocol.

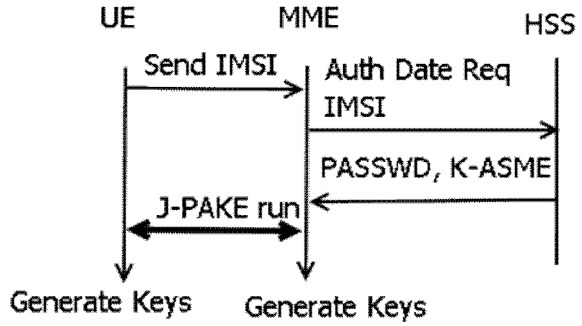

Figure 6. Simplified J-PAKE usage in 4G authentication

This solution does not cover the first security issue present in AKA, the identity protection. This aspect will be debated in a separate article. This solution also assumes the existence of a secure communication channel between the MME and the HSS. Once the IMSI is sent to the HSS by the MME, the HSS will return the shared key it has for this UE, secured via the S6a interface. Having the password, the MME will run the J-PAKE protocol with the UE, the eNB serving as simple relay agent; the UE proves, via the J-PAKE rounds, its knowledge of the password, and at this moment, the UE is considered authenticated by the network and it has also authenticated the network, This is a mutual authentication, resistant to the 4 security aspects listed above. It improves on the AKA algorithm by providing forward secrecy for the keys resulted from this negotiation. The generation of the EPS key hierarchy is not impacted by the authentication mechanism, the generation remains the same as described by the standard.

A more detailed comparison and simulation on the effectiveness of the J-PAKE method versus the AKA method is in progress.

J-PAKE is a password authentication keying agreement protocol, a method to provide zero-knowledge proof using a shared key that is never sent over the transmission medium. One of the first algorithms of this type is the EKE (Encryption Key Exchange) protocol, which has been proved to have many

 ISBN:978-1-61208-113-7

flaws. SPEKE (Simple Password Exponential Key Exchange) is one of the protocols that improved the EKE variant. SPEKE, along with EKE and J-PAKE are all balanced versions of password-authenticated key agreement. This variant uses the same password to authenticate both peers. There is another variant of PAKE, called augmented PAKE. This variant is usable in a client/server environment. Here, a brute-force attack on the connection is more inconvenient and the representative protocols for this variant are B-SPEKE and SRP (Secure Remote Password protocol). J-PAKE improves on the limitations of S-PEKE, limitations that are already observed in the BlackBerry implementation. The actual protocol – level security comparison between J-PAKE and SPEKE are described in the J-PAKE presentation paper. The conclusions are that EKE does not fulfill the off-line dictionary attack resistance requirement, while the SPEKE does not fulfill the on-line dictionary attack resistance requirement.

IV. Conclusions and Future work

This paper presented the basic 4G architecture and reviewed the main security domains used to classify and integrate the security aspects to this design. The paper focused on the access-level security issues that may arise at the eNodeB, UE and MME level. As the connection to the network poses the most issues when talking about User Domain security, this paper analyzed the authentication process of the UE connecting to the 4G network. There are two most common cases when talking about initial attach, the attach of a plain 4G device and the attach of non-3GPP device.

The paper identified two issues that appear almost every time: the lack of identity protection at the first initial attach and the lack of perfect forward secrecy for the AKA mechanism, inherited also in the EAP-AKA mechanism specific to the authentication of the non-3GPP devices. At least for the perfect forward secrecy issue, we have proposed the usage of the J-PAKE protocol in the authentication process, instead of the AKA protocol, which we consider a flexible and lightweight mechanism, suited for use in the mobile device environment.

The future articles will describe the comparison and a possible simulation of the efficiency of J-PAKE in comparison with SPEKE and other similar balanced PEKE algorithms, as well as measure the efficiency of this protocol as the main authentication algorithm in the 4G authentication process.

Further on, this study continues with the analysis of the IMSI identity protection mechanism and proposes a solution for the complete identity protection even for the first initial attach process.

References

[1] TS 23.401, GPRS Enhancements for E-UTRAN access, http://www.3gpp.org/ftp/Specs/archive/23_series/23.401/23401-a10.zip [retrieved: November 2010]
[2] TS 23.122, NAS Functions related to Mobile Stations in idle mode, http://www.3gpp.org/ftp/Specs/archive/23_series/23.122/23122-a10.zip [retrieved: November 2010]
[3] TS 36.300, E-UTRAN Overall Description, http://www.3gpp.org/ftp/Specs/archive/36_series/36.300/36300-a10.zip [retrieved: November 2010]
[4] TS 43.022, Functions of the MS in idle mode and group receive mode, http://www.3gpp.org/ftp/Specs/archive/43_series/43.022/43022-920.zip [retrieved: November 2010]
[5] TS 25.304, UE Procedures in idle mode and procedures for cell reselection in connected mode, http://www.3gpp.org/ftp/Specs/archive/25_series/25.304/25304-930.zip [retrieved: November 2010]
[6] TS 33.401, SAE - Security Architecture, http://www.3gpp.org/ftp/Specs/archive/33_series/33.401/33401-950.zip [retrieved: November 2010]
[7] TS 33.310, Network Domain Security; Authentication Framework, http://www.3gpp.org/ftp/Specs/archive/33_series/33.310/33310-a10.zip [retrieved: November 2010]
[8] TS 33.102, 3G Security Architecture, http://www.3gpp.org/ftp/Specs/archive/33_series/33.102/33102-930.zip [retrieved: November 2010]
[9] RFC 5516, Diameter Command Code Registration for the Third Generation Partnership Project (3GPP) Evolved Packet System (EPS), http://tools.ietf.org/html/rfc5516 , April 2009 [retrieved: November 2010]
[10] TS 29.272, MME related interfaces based on Diameter, http://www.3gpp.org/ftp/Specs/archive/29_series/29.272/29272-a00.zip [retrieved: November 2010]
[11] Tech-Invite, http://tech-invite.com/, [retrieved: March 2010]
[12] TS 29.294, Tunneling Protocol for Control plane (GTPv2-C), http://www.3gpp.org/ftp/Specs/archive/29_series/29.274/29274-a00.zip [retrieved: November 2010]
[13] TS 33.220, Generic Authentication Architecture; Generic Bootstrapping Authentication, http://www.3gpp.org/ftp/Specs/archive/33_series/33.220/33220-a00.zip [retrieved: November 2010]
[14] TR 33.919, Generic Authentication Architecture – System Overview, http://www.3gpp.org/ftp/Specs/archive/33_series/33.919/33919-910.zip [retrieved: November 2010]
[15] TS 33.221, Support for Subscriber Certificates, http://www.3gpp.org/ftp/Specs/archive/33_series/33.221/33221-910.zip [retrieved: November 2010]
[16] Han-Cheng Hsiang and Weu-Kuan Shih, “Efficient Remote Mutual Authentication and Key Agreement with Perfect Forward Secrecy”, Information Technology Journal 8, 2009, Asian Network for Scientific Information [retrieved: November 2010]
[17] RFC 4187, EAP Method for 3GPP AKA, http://tools.ietf.org/html/rfc4187 [retrieved: November 2010]
[18] RFC 2631, Diffie-Hellman Key Agreement Method, http://tools.ietf.org/html/rfc2631 [retrieved: November 2010]
[19] F. Hao and P.Ryan, “Password Authenticated Key Exchange by Juggling”, Proceedings of the 16th International Workshop on Security Protocols,2008, http://grouper.ieee.org/groups/1363/Research/contributions/hao-ryan-2008.pdf [retrieved: November 2010]
[20]3GPP, http://3gpp.org/-partners-, [retrieved: November 2010]
[21] Georgios Kambourakis, Angelos Rouskas, and Stefanos Gritzalis, "Performance Evaluation of Public Key-Based Authentication in Future Mobile Communication Systems", August 2004, EURASIP Journal on Wireless Communications and Networking [retrieved: November 2010]
[22] Qiang Tang and Chris J. Mitchell, “On the security of some password-based key agreement schemes”, 23rd May 2005 [retrieved: November 2010]

 ISBN:978-1-61208-113-7