11

Potential Applications of IPsec in Next Generation Networks

Cristina-Elena Vintilă
Military Technical Academy, Bucharest, Romania

1. Introduction

IPsec is one of the most secure technologies nowadays. It is used in almost all institutions that are concerned with protecting their communications. Although IPsec is not a very hard set of protocols to understand and use, once you get into its details and try to understand how it works, what is its applicability and what are its limitations, you will find yourself surrounded by mathematics, cryptography and network protocol design challenges. Because IPsec is not just another "encryption" protocol. It is actually an entire stack of protocols, ranging from negotiation protocols, to authentication protocols, to access network technologies, tunnelling protocols, PKI availability, routing and last, but not least, a good deal of cryptography. Companies use IPsec to securely connect their branches to the headquarters or between each other, over the Internet. Just the same, the remote workers have the possibility to securely access their data located at their work place premises no matter where they are. One of the most important aspects of this technology is its authentication role. By itself, IPsec does not provide network authentication. The authentication role of this stack of protocols is reserved for the IKE procedures. Currently at version 2, IKE has managed to simplify the authentication process of a peer and at the same time has managed to increase the security of this process. One of the latest additions to these authentication procedures is the support for mobile subscriber authentication. This functionality is achieved by incorporating the UMTS-SIM and UMTS-AKA key exchange protocols, useful in the NGN world.

Authentication functionality is closely related to identity protection and identification. In a world of mobile devices and wireless communication, the identity theft and impersonation are a continuously raising concern. The NGN technologies require the provisioning of services at an end-to-end guaranteed quality of experience, provided through high data rates and aggressive SLAs. The aim of the future technologies is to provide multimedia services no matter the location of the subscribers, which assumes inter-operator agreements all over the Globe, location and presence services. In order to maintain a high level of quality and availability, proper authentication, correct authorization and detailed and rigorous accounting are essential. Examples of NGN networks range from 4G access networks, like WiMAX and SAE to the converged services core, as it is IMS. These technologies are still under development. Even though there are already a number of production implementations, the technologies are still perfecting; one aspect of this process is security. IPsec is an important part of the design of any NGN system, for its proved security in the wireline industry (Liu, 2010). It supports IPv4 a set of protocols on top of layer 3 design and it is natively integrated into IPv6. The development of IPv6 considered this technology as a native part of the layer 3 design, in order to provide for security mechanism of the future networks. IMS design (TS 24.229) was originally described as running only over IPv6.

This paper does a brief analysis of the security issues faced by the NGN mobile equipment users, as well as the ones faced by the NGN operators. As it describes the security challenges the NGN is going to face, it explores the areas where IPsec has been described as the answer to the question for a secure communication environment in the near future. The paper goes over the IPsec applications in a near future access network as WiMAX and SAE are, as well as the usage of this technology in the IMS world. IPsec integrates technologies like key agreement and management via the EAP and PKI frameworks. One goal of this paper is to identify use cases and scenarios where the IPsec of the future is going to take effect. Even though the NGN mobile terminals are already powerful enough to support the cryptographic computations necessary to function as an IPsec peer, these terminals may make use of the ECC technology to improve their performances. While encrypting the traffic with IPsec is a good security practice, applying this practice to VoIP or Video traffic, sensitive to delays and latencies, poses a number of efficiency challenges. This is when the IKE capabilities come into play; IPsec provides key exchange functionality for SIP negotiation, so that the IMS voice and video traffic is to be protected (RFC4475, 2006; Vrakas, 2010; Wang, 2009). While reviewing the role and capabilities of the IPsec, as well as its possible applications in the next generation architectures, this paper also identifies some of the challenges and limitations this framework faces in the NGN context: mobile IP and mobility management, resistance to denial of service attacks, multimedia protocols, IPv6 control protocols and so on. Though a classic security solution for wireline technologies, IPsec diversifies and evolves, acquires new features and capabilities, while at the same time getting lighter to accommodate the requirements of the mobile subscribers. This paper proposes a journey of understanding how the technology that secures our communications works and how it can be applied in the near-future applications and network design.

2. IPsec technologies

IPsec (Internet Protocol Security) can be defined as a complex set of protocols on top of IP, supported on both IPv4 and IPv6. By itself, IPsec refers to the technology employed in order to secure the transmission of information over an unprotected medium. The security of the transmission may be achieved by using two sets of protocols: ESP (Encapsulated Security Payload) and AH (Authentication Header). In order to be able to use one of these two protocols, or both of them at the same time, security information in the form of encryption and/or authentication keys must be available. This information may be statically pre-configured by a security administrator or it may be dynamically negotiated between the IPsec entities/peer. The first case is referred to as *manual keying*. In this case, the security administrator has already configured security information on both end of the IPsec communication channel; the traffic passing through the IPsec equipment and matching several conditions is to be protected using this information. The second way of achieving the security agreement between the IPsec aware devices is to dynamically negotiate the session information between the IPsec peers. This method has the advantage of dynamic keying, but it may also be susceptible to man-in-the-middle attacks in the first phases of the negotiation. The generic protocol employed to do the negotiation is called ISAKMP (Internet Security Association and Key Management Protocol), represented most commonly by the IKE (Internet Key Exchange) protocol, which has reached its second version. When discussion the use-cases that can take place in an IPsec environment, the IPsec peers may find themselves in one of these two scenarios: one is called *site-to-site* and the other one is called *remote-access*. These two scenarios both refer to the situation where the IPsec computation takes place either between two security gateways or between a security gateway and a stand-alone unit (laptop, pda, smartphone...) called *roadwarrior*; this scenario is also called *dial-up vpn* by some security vendors. There is a separate case where the IPsec peers want to transmit information between each-other in a secure manner, but without the use of an external service provider (as it is a security gateway). This case is called *transport mode*.

2.1 IPsec architecture and traffic logic

The main components of the IPsec architecture are the following:

a. the Policy Agent: this component has the responsibility of negotiating the IPsec cryptographic parameters; these parameters refer to traffic identifiers (also called traffic selectors) that are input as a tuple in the Security Policy Database
b. the Security Policy Database(SPD): this component is a database (considering it as a stand-alone database implementation or part of an operating system kernel); it consists of tuples that represent the traffic selectors of an IPsec agreement: the IP addresses or the subnet which the traffic to be secured belongs to, or, for some of the IPsec equipment on the market, it may also contain port numbers in order to identify the traffic
c. the Security Association Database(SAD): this component is a database as well (stand-alone or part of a kernel implementation); it contains the IKE and IPsec security parameters that are negotiated: cryptographic algorithms, authentication information and identification information

Tuples in both databases are indexed and retrieved at run-time via their index, called SPI (Security Parameter Index), a value transmitted at run-time in each IPsec packet, in order for the receiver to select the proper tuple for decryption of the packet. The traffic logic flow of an IPsec use-case is the following: the Policy Agent is the one to start the IKE negotiation process, which consists of two phases (for each IKEv1 and IKEv2 protocols). The output of the Phase 1 is called ISAKMP SA(Security Association). The output of the Phase 2 is called IPsec SA. The IPsec processing engine adds a new layer of transformation for the actual network traffic; the engine is integrated to the TCP/IP stack of the system and it is called when a particular IP or a layer 4 segment matches the conditions for IPsec. Depending on each implementation, there may be available the configuration of different keys per traffic direction or a single set of keys for each IPsec tunnel. Also, there are ways to configure the Policy Agent to function based on the policy configured for that equipment (*policy-based tunnelling*), or to be triggered by a route utilization (*route-based tunnelling*).

2.2 Secure tunnel negotiation

In order to securely establish a dynamic IPsec tunnel, the ISAKMP – IKE protocol is used, whether its version 1 or version 2. Version 1 is considered less safe than version 2, where multiple security vulnerabilities where covered by safer implementation. IKEv1 is considered more difficult to implement. IKEv1 is described in RFC 2409 and it is currently implemented by all the major security equipment providers. Both IKEv1 and IKEv2 negotiate the IPsec SA in two phases. Phase 1 in IKEv1 can be accomplished in two separate and incompatible flows. One of them is referred to as *Main Mode* and it has 6 messages (or 3 exchanges), and the second one is called *Aggressive Mode* and it consists of 3 messages. Phase 2 of IKEv1 is referred to as *Quick Mode* and it has 3 messages.

The Main Mode messages are the following:

- HDR ISAKMP SAi Proposal – request sent by the Initiator of the tunnel to the Responder, containing the encryption and authentication algorithms
- HDR ISAKMP SAr Response – response sent by the Responder, containing its available encryption and authentication methods
- HDR DH KEi, Ni – message identifying the Diffie-Hellman group and keying material, as well as the Initiator nonce
- HDR DH KEr, Nr – same as the previous message, but identifying the Responder's capabilities
- HDR IDi, Hashi – authenticates the Initiator's Identity
- HDR IDr, Hashr – authenticates the Responder's Identity

Because the 5th and 6th messages are preceded by the exchange of cryptographic information and DH groups, the identities exchanged by them are already encrypted; this makes Main Mode exchange referred to as providing Identity Protection. This protection if identity does not happen for Aggressive Mode, where the phase 1 of IKEv1 has only 3 messages:

- ISAKMP SAi Proposal, DH KEi, Ni, IDi – request sent by the Initiator, containing cryptographic information, Diffie-Hellman material, a nonce and the Identity of the Initiator – in clear
- ISAKMP SAi Response, DH KEr, Nr, IDr, Hashr – same as the proposal, but with the Responder's information
- HDR Hashi2 – the Initiator's hash

In the notations above, the "i" refers to the initiator of the IPsec negotiation, while the "r" refers to the responder of the IPsec negotiation offer.

Phase 1 is followed by Phase 2, also called *Quick Mode*. The purpose of this exchange is to negotiate the traffic selectors and the cryptographic information for the actual data-plane encapsulation. This traffic is referred to as *non-ISAKMP* by RFC 2409. Quick Mode is composed of three messages:

- HDR, Hashi, SA, Ni, [KEi, IDi, IDr] – this message contains the IKE header, hash, SA, nonce and optionally the new DH key, and identities of the parties and it is send by the Initiator
- HDR, Hashr, SA, Nr, [KEr, IDi, IDr] – same as above, but on the Responder side
- HDR, Hashi2 – last message of the Initiator before sending traffic

The second version of IKE, IKEv2 is not fully supported by all equipments on the market, but it is starting to get more and more attention, due to its capabilities: faster tunnel setup, more secure negotiations, more consistent authentication and identification rules, simpler implementation etc. There is only one type of so-called Phase 1 and Phase 2 in IKEv2. The IKEv2 exchange is the following:

- HDR (IKE_SA_INIT), SAi1, KEi, Ni – the initial request coming from the Initiator and containing the cryptographic parameters, DH keys and a nonce
- HDR (IKE_SA_INIT), SAir, KEr, Nr, [CERTREQ] – same as above, the Responder having the possibility to ask for a digital certificate at this point
- HDR (IKE_AUTH), SK {IDi, [CERT,] [CERTREQ,] [IDr], AUTH, SAi2, TSi, TSr} – authentication message, encrypted and authenticated (as in the first exchange there was already sent the DH information), containing the authentication information, ID of the other party, SA and traffic selectors of the Initiator as well as the Responder
- HDR (IKE_AUTH) SK {IDr, [CERT,] AUTH, SAr2, TSi, TSr} – same as above, but from the Responder's side
- HDR (CREATE_CHILD_SA), SK {[N], SA, Ni, [KEi], [TSi, TSr]} – request for creating an SA (IPsec SA) with the nonces, DH keys and traffic selectors indicated
- HDR (CREATE_CHILD_SA) SK {SA, Nr, [KEr], [TSi, TSr]} – same as above, from Responder's side

The first four messages can be assimilated as Phase 1 of the IKEv2, and the last two messages as Phase 2 of the IKEv2. Nevertheless, at tunnel establishment time, only the first four messages appear in the negotiation, as usually the information provided by the last two messages is comprised in messages 3 and 4. The last 2 messages are used for the re-keying process.

2.3 Secure data transmission

After having established the secure parameters to be employed in order to protect the transmission of the data, two protocols can be used to achieved this security, either separate or both at the same time. These protocols are AH (RFC 4302) and ESP (RFC 4303). AH protocol number is 51 and the purpose of this protocol is to ensure protection against replay attacks, due to the integrity check and sequencing it employs. AH method makes a hash of the entire IP packet (both headers and data payload) and adds this has value to the packet sent over the wire. The only fields not taken into consideration when computing the hash value are the ones that are expected to change when routing occurs in a normal network: TTL, TOS, CRC etc. The ESP protocol number is 50 and this method encrypts the data using the material and algorithms negotiated earlier. ESP only encapsulates the payload.

2.4 Authentication and Identification

Two of the most important aspects of the IPsec negotiation are the authentication and identification. Not only do they perform two important functions (authenticating the IPsec peers to each other and identifying the peers to each other), but they are a crucial point for interoperability between different IPsec implementations. Not all networks worldwide happen to use exactly the same equipment as IPsec peers, so interoperability issues arise in many situations. RFC 2409 defines only two types of authentication available for IKEv1: PSK (pre-shared key) and digital certificates/RSA, while RFC 4306 for IKEv2 defines four authentication types: PSK, RSA, DSS and EAP (Extensible Authentication Protocol). The way these options are combined it is a totally different discussion. Most of the site-to-site implementations use a symmetrical authentication scheme (both peers use the same type of authentication for the tunnel being established). On the other hand, the remote-access scenarios many times use a hybrid authentication scheme, where the security gateway authenticates to the road-warriors via a digital certificate, while the clients are authenticated via a password. At the same time, if we are discussing IKEv2, where the EAP method is available, there are many more ways of authentication of the road-warriors.

Configuring PSK on devices is many time straight forward. The RSA configuration tends to be more difficult, as it assume the existence of a PKI infrastructure. As an example, on Strongswan, by default, there is a dedicated directory where the root certificates should reside (*/etc/ipsec.d/cacerts*). In */etc/ipsec.d/certs* the administrator should copy the IPsec certificates for the local machine. All these files paths may be changed from a configuration file (*/etc/ipsec.conf*). The certificates are usually supplied in *pem* format, but they can also be parsed in *der* format (this option is default for Windows CA servers) and the administrator can convert a certificate from one format to another using a tool like *openssl*. When exporting a certificate generated on the CA, both the public and the private keys are downloaded (because the *csr* file has been directly generated on the CA). In this case, the format presented is PKCS12. From PKCS12, the administrator is able to extract both the public key (in a digital certificate) and the private key, in separate files.

- from DER to PEM format:

```
openssl x509 -inform DER -in local.cer -outform PEM -out local.pem
```

- from PKCS12 to PEM format:

```
openssl pkcs12 -in myFile.p12 -out cert.pem -clcerts –nokeys
```

IOS, JunOS or StokeOS network operating systems usually keep the certificate information in their non-volatile memory.

The next step after achieve peer authentication is the proper identification of the peers to each other. This step is very important and it is also very important that the identities of the peers are not disclosed to unauthorized parties. This is one reason why Aggressive Mode method, which does not provide Identity Protection, is no longer included in IKEv2. RFC 2407 identifies the syntax for the identification variables in IKEv1, and RFC 4306 describes this syntax for IKEv2. The identification payload types for IKEv1 are the following: ID_IPv4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV4_ADDR_SUBNET, ID_IPV6_ADDR, ID_IPV6_ADDR_SUBNET, ID_IPV4_ADDR_RANGE, IP_IPV6_ADDR_RANGE, ID_DER_ASN1_DN, ID_DER_ASN1_GN, ID_KEY_ID, and the ones for IKEv2 are the following: ID_IPV4_ADDR, ID_IPV6_ADDR, ID_FQDN, ID_RFC822_ADDR, ID_DER_ASN1_DN, ID_DER_ASN1_GN, ID_KEY_ID.

Identification is one of the major aspects when it comes to interoperability issues, especially when the administrator has to configure a particular type of identification mechanism which is not supported on the peer equipment. Strongswan for instance accepts ID_IP_ADDR (and ID_IP_ADDR_SUBNET for IKEv1), both v4 and v6, ID_FQDN, as in the certificate. The file also permits the configuration of an ID_ASN1_DER_CN, where the administrator can enter the entire subject of the certificate or only certain fields.

```
conn connection1
      left=192.168.0.1
      right=192.168.0.2
      leftid="C=RO, ST=Romania, L=Bucharest, O=Company, OU=Department,
      CN=DebianTest/emailAddress=debian@test.com"
      rightid="C=US, ST=California, L=Calabasas, O=Company, OU=Department,
      CN=Test1"
```

Other equipment has a more or less similar way of defining this set of parameters.

A particular case is IEKv2-EAP. This protocol is described by RFC 3748 and it supports the following internal EAP methods: MD5, TLS, SIM, AKA etc. While MD5 is a simple protocol that can be implemented locally on the IPsec peer, TLS, SIM or AKA usually require an external Radius server, like ACS, FreeRadius or NPS. This is not a mandatory condition, but it is a good practice to have the authentication server separated from the IPsec peer. TLS can be used for almost any type of connection and it may also only authentication the server to the client, as per the TLS specifications. SIM protocol was defined for authentication in 2G networks, used for proving the GSM Subscriber Identity of the client to the 3G access network; this protocol is described in RFC 4186. EAP-AKA (Authentication and Key Agreement) has been defined for authentication of the 3G subscribers to the 3G networks which have a Radius server. Further on, the EAP-AKA is the preferred method of the 4G network authentication procedures, when the mobile equipment to be authenticated is a non-native 4G equipment. LTE uses the native AKA procedure for authenticating the native 4G handset, using the AAA proxy for mobile devices connecting from WiFi or WLAN areas.

An example of an EAP-SIM and EAP-AKA users as they are defined in a FreeRadius implementation is described below.

```
user1 Auth-Type := EAP, EAP-Type := EAP-TLS, Password == "p@ssw0rd"
eapsim1 Auth-Type := EAP, EAP-Type := SIM
EAP-Sim-RAND1 = 0x201112131415161718191a1b1c1d1e1f,
EAP-Sim-SRES1 = 0xd2d2d3d4,
EAP-Sim-KC1 = 0xa0a2a2a3a4a5a6a7,
eapaka1  Auth-Type := EAP, EAP-Type := AKA
EAP-Sim-AUTN  = 0xa0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0,
EAP-Aka-IK    = 0xb0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0,
EAP-Aka-CK    = 0xc0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0,
EAP-Sim-RES   = 0xd0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0,
EAP-Sim-RAND  = 0xe0e0e0e0e0e0e0e0e0e0e0e0e0e0e0e0,
```

As for the moment, the IPsec technology is mature enough and considered stable. Improvements have been made to IKEv2 to support a large range of scenarios. What is of interest in this paper is how much of IPsec can actually be used in the Next Generation Networks, with emphasis on 4G-SAE, the mobile technology that has the greatest area of attention at the moment. We can use IPsec in a peer-to-peer manner for providing hop-by-hop security between core network elements, but we should be able to learn a lot from its authentication and negotiation stages in order to secure the 4G access level, which is of bigger interest due to the large number of devices that will try to connect, as well as due to the large number of connectivity and mobility scenarios employed (Wang, 2008).

There are multiple studies regarding the security of the IPsec, and specially the IKE protocols. One of them (Cremers, 2011) identifies the following vulnerabilities: Reflection attack on IKEv1 Main Mode with digital signatures or pre-shared keys, Reflection attack on IKEv1 Quick Mode, Reflection attack on IKEv1 Main Mode with public key encryption, Authentication failure on IKEv1 Aggressive Mode with digital signatures, Authentication failure on IKEv1 Main Mode with digital signatures that does not require self-communication, Reflection attack on IKEv2 phase 2 exchange. Another important aspect of the IPsec protocol is the computational overhead, described in detail in (Xenakis, 2006). The factors taken into account are the encryption type and the authentication mechanism, and the resultants reflect in the system throughput, total delay and rate increase of the protected data. (Shue, 2007) Overall, the throughput overhead is larger than the overhead brought in by upper layer security protocols, like SSL or TLS, but the security offered by IPsec is also higher and the protocol can tunnel and secure a larger variety of traffic protocols than SSL or TLS can.

3. 4G and services networks technologies

4G is the next generation network technology at the moment. 4G is a generic term that defines a set of features and capabilities for a radio network, as well as for quality of service, mobility and services provided to the customer. It is not strictly related to a particular technology. It has been declared that both WiMAX and LTE are considered 4G technologies. WiMAX is being standardized by the WiMAX forum, being developed from the 802.16 family of wireless standards. The 802.16 is also being called *fixed* WiMAX and was published in 2001. In 2005, the 802.16e family was deployed, called *mobile* WiMAX. In 2011, there have begun to appear implementations of 802.16m. At the same time, the 3GPP forum also worked on improving the UMTS technology, which is considered a 3G generation. This is how the LTE (Long Term Evolution) technology came into existence. LTE is considered a 4G technology and it proposes an all-IP network, simplifying the access level of the network, as well as providing support for higher transmission rates due to improvements on the radio side and dynamic or seamless handover to both 3G networks, as well as to non-3GPP networks, like WiMAX or WLAN. Both 4G technologies are aiming at providing a simple and transparent access to the services network, for their subscribers. One example of services network is the IMS (IP Multimedia Subsystem), developed by 3GPP. IMS supports a large area of services, from simple data, voice and video to sms, mms, push-to-talk, conferencing and presence. A different approach to connecting to an IMS network is the direct access to Internet, where the services accessed may be the same ones as accessed from a wireless connection, without being provided in a unified manner, as in IMS. There is also possible an intermediary solution, where the services network is only referring to the Application Servers (AS) part of the IMS, overlooking the call session functions (Plewes, 2007; Sayyad, 2011).

From now on, the paper will provide a short introduction into the 3GPP LTE technology and discuss the security issues that appear at the access layer of this architecture (Kowtarapu, 2009). We will see what decisions the 3GPP forum has made in terms of protocols to use, their advantages and vulnerabilities and investigate how we can use the lessons learnt from our experience with IPsec.

3.1 3GPP LTE architecture and services network

The 4G-LTE architectures comprises two main components: the radio access network and the EPC (Evolved Packet Core). The radio access network is the eNodeB(the antenna) and the radio medium. The core network contains multiple devices, with roles in signaling, authentication, routing, providing quality of service and so on. The following elements are the most common devices located in the LTE core network (TS 23.203, TS 23.401, TS 29.274, TS 33.401):

a. MME (Mobility Management Entity): it deals with user registration to the network, signalling and mobility management; it can be partially assimilated with the SGSN (Serving GPRS Support Node) from the UMTS architecture, with two major differences: the MME, unlike the SGSN, only does signalling, and, unlike SGSN, additionally has a management position towards the antennas; the MME connects to the database that holds the subscriber authentication information, having a very important role in the user authentication; in 3G, the RNC (Radio Network Controller) had the dedicated function of antenna management;
b. SGW (Serving Gateway): unlike the MME, this entity does both signalling and traffic plane and it is responsible for routing data traffic to a particular set of radio cells (called Tracking Areas);
c. PGW (Packet Data Network Gateway): this component is the one connecting the access network (LTE network) to the services network (IMS, Internet, Intranet etc); it is also one of the QoS enforcement points, together with the antenna; the PGW is connected to the database that holds the subscriber information; this entity may be assimilated to the 3G GGSN (Gateway GPRS Support Node) (Good, 2007);
d. PCRF (Policy Charging and Rules Function): the policy database holding the subscription information material (Yang, 2011);
e. HSS (Home Subscriber Server): the database holding information about the mobile equipment identity and credentials;

The picture below is a schematic representation of a typical 4G network (TS 29.061), where the access side is done via native 4G environment, as well as via 3G and non-3GPP media.

The antenna is the first point of contact of the user to the LTE network. The mobile equipment connects to the network, identifies this network and upon the user signalling to the network, the LTE starts the authentication process. The entities involved in this process are the mobile equipment, as one of the authentication peers (the client), the HSS, as the second authentication peer (the server), the MME as the authenticator and the eNB, as a sort of authentication relay. The MME is the one requesting the UE (User Equipment) its identity information, when downloading credentials from the HSS, in order to start the authentication process and secure key establishment with the mobile. The protocol used for this process is AKA (in native 4G and 3G) and EAP-AKA for the non-3GPP access. Once the authentication is complete, there take place several keys determination, based on mathematical functions defined by 3GPP. The key hierarchy is different for each case: 3G. 4G and non-3GPP. In the 4G case, there are keys for securing and/or authenticating both signalling and data-plane traffic flows, unlike 3G, where only the data-plane was secured. Also, there are specific requirements on how to assure a safe interoperability function between these types of access levels. For instance, the handover from a 4G network to a 3G network is simpler and does not require additional cryptographic computation, while the handover from a 3G network to a 4G network is more cumbersome. In order to achieve authentication for the non-3GPP devices, one or more 3GPP-AAA servers are needed and a ePDG (Evolved Packet Data Gateway). This ePDG entity is the other end of the authentication scenario, the peer the mobile connects to for authentication (Guo, 2010).

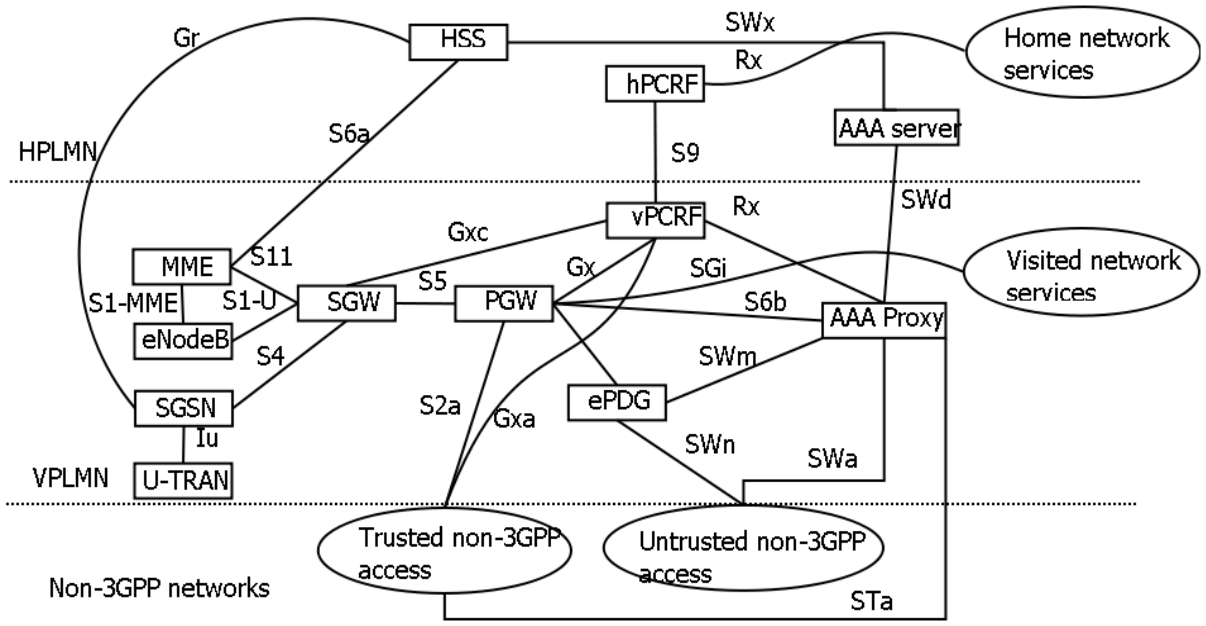


Fig. 1. NGN architecture; local breakout with home & visited network operator's functions

Roaming is an aspect with importance when it comes to security (authentication, authorization as well as accounting and charging). Generically, there are three types of roaming: home routed traffic (the PGW is located in the home network), local breakout with home operator's application functions only (the PGW is located in the visited network, but the services the user accesses are provided by its home network, as it is the example of using an e-mail service) and local breakout with visited operator's application functions only (the PGW is in the visited network as well, but the visited network also provides the services in this case, having a roaming agreement with the home network, in order for that; the home network only serves at assuring the authentication of the user and the policy verification).

Independent of the details of implementation of the access network, the PGW ultimately connects the UE to an APN (Access Point Name) via the SGi interface, an IP-based logical interface. The APN is the services network, no matter the actual format of this network: Internet, Intranet, IMS etc. The typical case considered in this paper is the IMS network. In this case, the PGW connects to the P-CSCF equipment of the IMS core.

The centre of the IMS functionality is the CSCF (Call Session Control Function), provided via three different logical entities: a Proxy (P-CSCF), an Interrogating unit (I-CSCF) and a Serving unit (S-CSCF). The P-CSCF is the first point of contact in the IMS network, staying always in the SIP signalling path and being able to do traffic inspection, SIP header compression (SigComp) and secure tunnelling to the UE: this is the entity the mobile IMS-aware handset establishes and IPsec session with. The P-CSCF can also do media-plane QoS enforcement. The S-CSCF is responsible for registration, message inspection and for selecting the AS (Application Server) that is to serve the subscriber. Assigning a particular S-CSCF to a certain subscriber is the task of the HSS, which is interrogated by the I-CSCF to provide this information. Just as for the 4G network, the IMS relies on the existence of HSS and PCRF databases. The standards move towards a more intimate and efficient integration of the 4G and IMS networks.

3.2 Security aspects

The security aspects in such a complex environment are many and complex. 3GPP has defined five security levels in order to separate the areas that are somehow independent of each other (TS 33.203).

a. Network Access Security: this area deals with granting access to the (core) network only to those users that prove their identity, that identity matching a network's registered user, with valid authentication credentials and with a subscription that allows services to be delivered to this user;
b. Network Domain Security: this area deals with the secure interoperation between the Evolved Packet Core (EPC) network entities; this security is described by the protocols involved in securing the communications between EPC nodes: IPsec (recommended by Specs to take place within an operator's premises) and TLS (usually for inter-operator secure communications);
c. User Domain Security: this area deals with the secure access to the mobile stations;
d. d. Application Domain Security: this area is concerned with how to secure the communication between the applications that reside on the user's mobile device and the core network application servers; as a layer 7 application, this area may implement a large variety of security structures;
e. Visibility and Configurability of Security: this is an informational area, for the user; the subscriber must have constant access to the information concerning the security features available on his device, whether or not they are functioning properly and whether or not they are required for the secure operation of a certain service

When it comes to access to the 4G network, there are two aspects that threaten the security of the model. These aspects are related to the EPS-AKA procedures and there are the lack of identity protection at the first Initial Attach to the network (where the user must send its IMSI over the air, unencrypted) and the lack of the PFS (Perfect Forward Secrecy) property of the AKA algorithm. Sending the IMSI over the air is a problem only for the very first Attach Request, because the subsequent requests are done using a temporary global identity (GUTI).

This attach request message is sent by the UE to the MME; this request may be a TAU (Tracking Area Update), procedure mandatory when moving between areas of radio cells. When the new MME receives this message, it retrieves the identity of the previous MME from the message, and contacts this previous MME. In the message, the new MME requests the IMSI for the GUTI it provides. This way, under the fair assumption that the connection between MMEs is secured (via IPsec for instance), the IMSI identity of the UE is protected.

With regards to the services network, there are a lot of vulnerabilities, some related directly to the security capabilities of the SIP and RTP protocols, while some other to the network design, authentication, authorization and user profile. ETSI has developed the TVRA model in order to organize a table of security vulnerabilities description. The table below proposes a summary of the VoIP networks vulnerabilities, organized on the TVRA model (Edwards 2007; Karopoulos, 2010; VoIPSA, 2011).

No.	Asset	Weakness	Threat	Location	Incident	Objective
1	SIP Session	Signal w/o confidentiality	SIP sniffer	Gm	Loss of privacy	Confidentiality
2	Network topology	Weak authentication and control mechanism	Scan	Gm/Mw	Loss or privacy	Confidentiality
3	SIP Session	Signal w/o confidentiality	SIP Bye attack	Gm	Session damage	Integrity
4	SIP Register	UE configuration	configuration tampering	UE	DoS	Availability
5	SIP Register	DNS reliability	DNS cache attacks	Gm	DoS	Availability
6	SIP Register	Weak authentication and control mechanism	P-CSCF-in-the-middle attack	Gm	Impersonation attack (P-CSCF)	Authentication
7	SIP	Lack of DoS/DDoS prevention	SIP Register flooding	Gm	DoS	Availability
8	SIP Session	Weak authentication and control mechanism	Message Spoofing	Gm	Impersonation attack (user)	Authentication
9	RTP Session	No integrity protection	RTP insert attack	Gm	Session damage	Integrity
10	RTP Session	Weak control of streams	Media theft	UE-UE	Service theft	Accountability
11	RTP Session	Weak authentication and control mechanism	SPIT	UE-UE	User exhaust	Controllability
12	User profile	Weak authentication and control mechanism	SIP SQL injection	HSS	DoS	Availability

Table 1. VoIP TVRA model example

Along with the list of vulnerabilities, there are organizations that discuss these security issues in more details and also present the current status of the security tools available for assessing the level of security of this type of networks (Plewes, 2007).

4. Security solutions and alternative models

4.1 4G GAA security solution

The 3GPP forum defines a generic authentication scheme, named GAA (Generic Authentication Architecture), which as two main components: the component responsible for authentication via shared secrets, GBA (Generic Bootstrapping Authentication) and the component responsible for authentication via digital certificates, SSC (Support for Subscriber Certificates). There are six entities as defined by the GAA: HSS, BSF, NAF, ZnProxy, SLF and UE. The figure below describes an authentication scenario where the UE is located in roaming, and there is a third, untrusted, network between the visited and the home network.

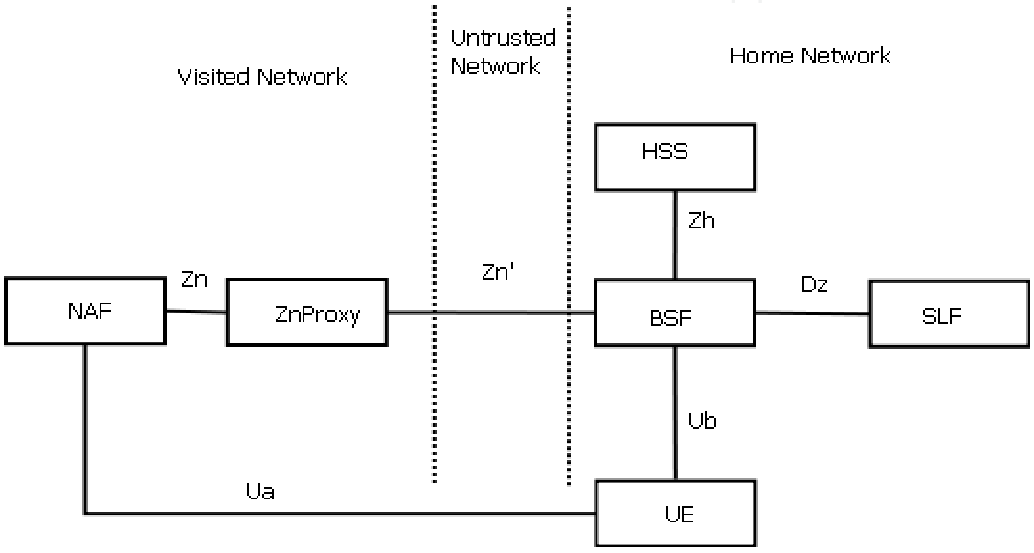


Fig. 2. GBA simplified architecture

The HSS is the database holding the USS (User Security Settings). It has the purpose of mapping the USS to one or more private user identities, which in IMS is called IMPI (IP Multimedia Private Identity). An example of USS is the GUSS (GBA User Security Settings), which may contain the following parameters: type of UICC, lifetime of the subscriber's key, timestamp etc. The BSF (Bootstrapping Server Function) has the role to authenticate the UE, via the AKA method. Before that, it communicates to the HSS in order to download AV (Authentication Vector) parameters used to derive the keying material for AKA. A native 4G handset should support discussion EPS-AKA with the BSF. The NAF (Network Application Function) is a generic server that the UE tries to connect to. The BSF derives the Ks_NAF key and sends it to the NAF. The UE also generates also a Ks_NAF key. For this procedure to function properly, the BSF should have connectivity to the NAF the user connects to. The BSF should keep a list of NAFs and a list of groups of NAFs, in order to be able to identify at any given moment which NAF should be chosen if an application-specific USS appears. (Aiash, 2010; Keromytis, 2010) The ZnProxy appears in the roaming cases, and it may be a stand-alone device or part of the functionality of an existing device, like the visited NAF, visited AAA server or an application server. This entity has the role of locating the user's home BSF device. In cases where there are multiple HSS databases, the SLF (Subscriber Location Function) is the entity queried by the BSF in order to locate the HSS containing the authentication information. The following steps describe the bootstrapping procedure:

1. UE sends the HTTP request to the BSF, inserting an user identity, either its IMPI or its TMPI, if it has a temporary ID available;
2. The BSF identifies whether it received a TMPI or an IMPI; if it was a TMPI, it looks for the corresponding IMPI in its cache, and if it's not found, it gives an error to the UE, requesting the IMPI, otherwise it continues authenticating the UE to the HSS.

Then the BSF tries to locate the HSS and retrieve the GUSS and the AV from it, where AV=(RAND||AUTN||XRES||CK||IK), over Zh;

3. BSF forwards the RAND and AUTN to the UE, in order to authenticate it;
4. The UE uses AUTN to authenticate the network, then computes the XRES, CK and IK and
5. sends the XRES to the BSF, in order to be authenticated by this entity and

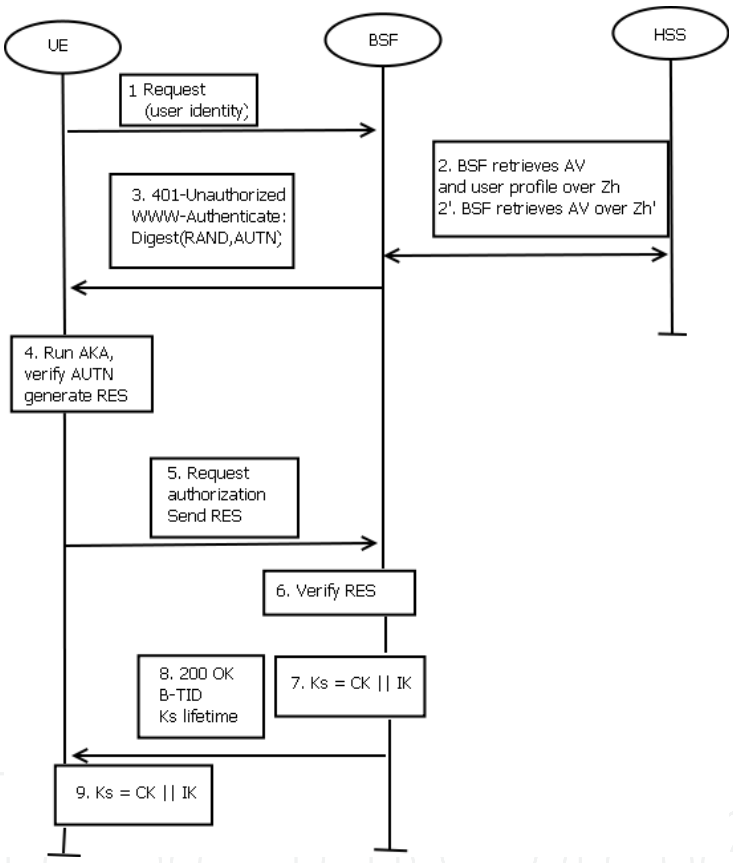


Fig. 3. GBA procedure

1. the BSF verifies the XRES against its already computed RES; if they match, the UE is authenticated;
2. The BSF obtains the Ks by concatenating CK and IK, same as the UE and
3. replies to the UE with a B-TID in the 200 OK message;
4. The UE also obtains the Ks by concatenating its CK and IK

At this point, both the UE and the BSF derive the Ks_NAF key, the actual key that will be used to secure the communication between the UE and the NAF.

Ks_NAF = KDF (Ks, "gba-me", RAND, IMPI, NAF_Id), where KDF is the key derivation function and the NAF_Id looks like this: NAF_Id = FQDN of the NAF || Ua security protocol identifier. All the values possible and structure of these components are defined in references.

4.2 IMS AKA procedure

The IMS network is the NAF server from the above topology (more exactly, the P-CSCF plays the role of the NAF server). Another method to do subscriber authentication is the SIP-AKA procedure. The purpose of this procedure is to authenticate the user and exchange keying material for IPsec (Chen, 2008; MSF, 2011; Nasser, 2009; TR 33.978).

I have executed several tests, using an IMS client and an IMS CSCF solution. The figure below describes the theoretical exchange, while some of the traffic captures are included following the theoretical description.

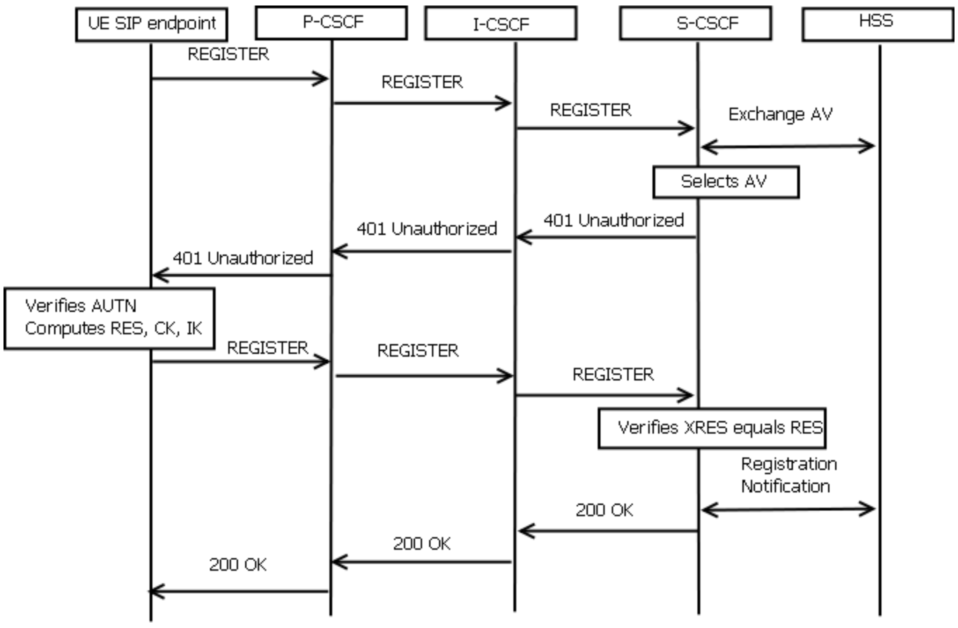


Fig. 4. SIP-IMS-AKA authentication procedure

The first packet of the conversation is the SIP REGISTER, which at first does not contain any authentication methods, nor information.

```
Request-Line: REGISTER sip:open-ims.test SIP/2.0
Method: REGISTER
Request-URI: sip:open-ims.test
[Resent Packet: False]
Message Header
Via: SIP/2.0/UDP 172.20.1.1:1143;rport;branch=z9hG4bK1275411663890
From: <sip:11111@open-ims.test>;tag=6334
        To: <sip:11111@open-ims.test>
Call-ID: M-50a5456166f246b78f081ac2453ee4ea
        CSeq: 901 REGISTER
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, BYE, MESSAGE, OPTIONS, NOTIFY, PRACK, UPDATE,
REFER
```

```
Contact: <sip:11111@172.20.1.1:1143;transport=udp>;expires=600000;+deviceID="3ca50bcb-
7a67-44f1-afd0-994a55f930f4";mobility="fixed"
User-Agent: IM-client/OMA1.0 Mercuro-Bronze/v4.0.1624.0
P-Preferred-Identity: <sip:11111@open-ims.test>
Supported: path
P-Access-Network-Info: ADSL;eutran-cell-id-3gpp=00000000
Privacy: none
Content-Length: 0
```

The P-CSCF locates the S-CSCF assigned by the HSS and collects the AKA information from there, one or more AVs, containing the following parameters: RAND, AUTN, XRES, IK, CK. The RAND and AUTN are passed on to the UE, via the 401 Unauthorized SIP message, while the XRES is kept for comparison.

```
Status-Line: SIP/2.0 401 Unauthorized - Challenging the UE
Message Header
Via: SIP/2.0/UDP 172.20.1.1:1143;rport=1143;branch=z9hG4bK1275411663890
From: <sip:11111@open-ims.test>;tag=6334
    SIP from address: sip:11111@open-ims.test
    SIP from address User Part: 11111
    SIP from address Host Part: open-ims.test
    SIP tag: 6334
To: <sip:11111@open-ims.test>;tag=925746a962736b96138042b427df6549-2212
    SIP to address: sip:11111@open-ims.test
    SIP to address User Part: 11111
    SIP to address Host Part: open-ims.test
    SIP tag: 925746a962736b96138042b427df6549-2212
Call-ID: M-50a5456166f246b78f081ac2453ee4ea
CSeq: 901 REGISTER
Path: <sip:term@pcscf.open-ims.test:4060;lr>
Service-Route: <sip:orig@scscf.open-ims.test:6060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH,
MESSAGE, INFO
Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))
Content-Length: 0
Warning: 392 172.21.119.1:6060 "Noisy feedback tells:  pid=2028 req_src_ip=172.21.118.1
req_src_port=5060 in_uri=sip:scscf.open-ims.test:6060 out_uri=sip:scscf.open-ims.test:6060
via_cnt==3"
WWW-Authenticate: Digest realm="open-ims.test", nonce = "qxZ3KUqjXlvgogK8aNtyH
L4yoDzYBwAAFNpK0YllC1w=", algorithm = AKAv1-MD5, qop="auth,auth-int"
Authentication Scheme: Digest
realm="open-ims.test"
nonce="qxZ3KUqjXlvgogK8aNtyHL4yoDzYBwAAFNpK0YllC1w="
algorithm=AKAv1-MD5
qop="auth
```

SIP-AKA provides mutual authentication. The UE uses the AUTN to authenticate the network and if this authentication is successful, it then computes the RES (response) and sends it to the P-CSCF. It also derives the CK and IK keys.

```
Request-Line: REGISTER sip:open-ims.test SIP/2.0
Message Header
Via: SIP/2.0/UDP 172.20.1.1:1143;rport;branch=z9hG4bK1275411663891
From: <sip:11111@open-ims.test>;tag=6334
To: <sip:11111@open-ims.test>
Call-ID: M-50a5456166f246b78f081ac2453ee4ea
CSeq: 902 REGISTER
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, BYE, MESSAGE, OPTIONS, NOTIFY, PRACK, UPDATE,
REFER
Contact:  <sip:11111@172.20.1.1:1143;transport=udp>;expires=600000;+deviceID="3ca50bcb-
7a67-44f1-afd0-994a55f930f4";mobility="fixed"
User-Agent: IM-client/OMA1.0 Mercuro-Bronze/v4.0.1624.0
Authorization: Digest algorithm=AKAv1-MD5,username="11111@open-
ims.test", realm= "open-
ims.test",nonce="qxZ3KUqjXlvgogK8aNtyHL4yoDzYBwAAFNpK0YllC1w=",uri="sip:open-
ims.test",response="974679fa1f988670b52ebd3b058cf42a",qop=auth-in
    P-Preferred-Identity: <sip:11111@open-ims.test>
    Supported: path
    P-Access-Network-Info: ADSL;eutran-cell-id-3gpp=00000000
    Privacy: none
    Content-Length: 0
```

Upon the receipt of this message, the P-CSCF authenticates the user by comparing the RES and XRES values, and sends a reply back to acknowledge this fact.

```
Status-Line: SIP/2.0 200 OK - SAR successful and registrar saved
Message Header
Via: SIP/2.0/UDP 172.20.1.1:1143;rport=1143;branch=z9hG4bK1275411663891
From: <sip:11111@open-ims.test>;tag=6334
To: <sip:11111@open-ims.test>;tag=925746a962736b96138042b427df6549-5b6b
Call-ID: M-50a5456166f246b78f081ac2453ee4ea
CSeq: 902 REGISTER
P-Associated-URI: <sip:11111@open-ims.test>
Contact: <sip:11111@172.20.1.1:1143;transport=udp>;expires=600000
Path: <sip:term@pcscf.open-ims.est:4060;lr>
Service-Route: <sip:orig@scscf.open-ims.test:6060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH,
MESSAGE, INFO
Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))
Content-Length: 0
Warning: 392 172.21.119.1:6060 "Noisy feedback tells:  pid=2027 req_src_ip=172.21.118.1
req_src_port=5060  in_uri=sip:scscf.open-ims.test:6060  out_uri=sip:scscf.open-ims.test:6060
via_cnt==3"
```

The two parties (the UE and the P-CSCF) may use the CK and IK keys to establish an IPsec tunnel.

4.3 IPsec in end-to-end security

The most common case of the IPsec usage in a 4G network is the simple end-to-end implementation of the protocol between the mobile device and the services network peer (a security gateway, server or another peer) (Vintilă, 2010). A representation of this scenario is pictured in the figure below.

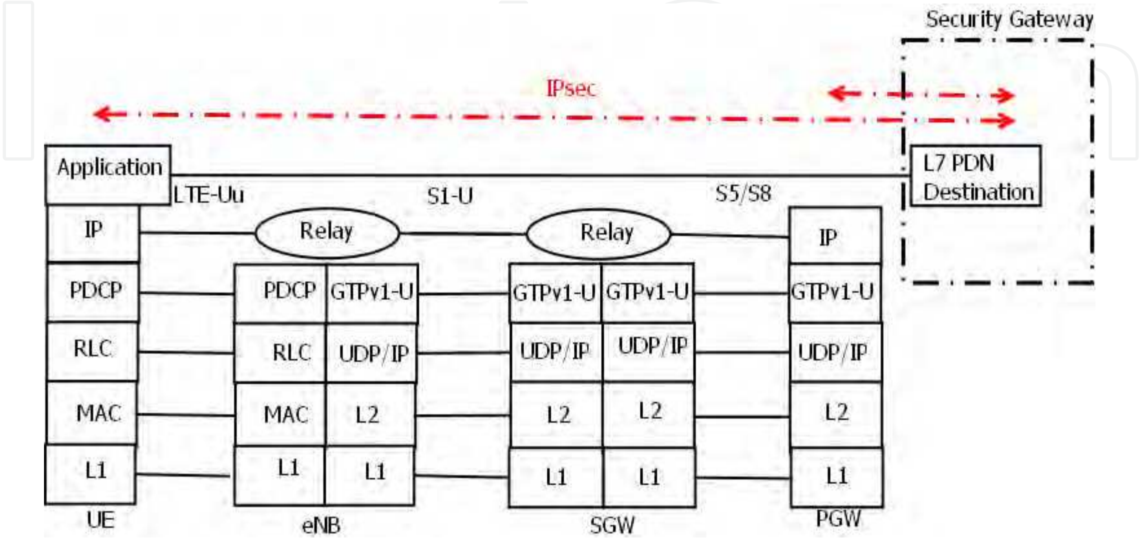


Fig. 5. IPsec scheme in LTE topology

The ends of the IPsec tunnels are the UE and the P-CSCF. The IMS negotiation messages would look the following. The first REGISTER message contains the IPsec declaration. Some of the headers have been excluded to save editing space.

Request-Line: REGISTER sip:open-ims.test SIP/2.0
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=666; spi-s=777; port-c=1234; port-s=5678
Require: sec-agree
Proxy-Require: sec-agree
The reply from the P-CSCF is initially a 401 Unauthorized.
Status-Line: SIP/2.0 401 Unauthorized - Challenging the UE
Message Header
Security-Server: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96;spi-c=222;spe-s=333;port-c=2345;port-s=3456

The second REGISTER message looks like this:

Request-Line: REGISTER sip:open-ims.test SIP/2.0
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=666; spi-s=777; port-c=1234; port-s=5678
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96;spi-c=222;spe-s=333;port-c=2345;port-s=3456
Require: sec-agree
Proxy-Require: sec-agree

The IPsec tunnel is thus negotiated.

For the VoIP networks, there can be used up to five different security mechanisms: digest, TLS, IPsec-IKE, IPsec-man and IPsec-3gpp, the latter being specified by 3GPP. This end-to-end security mechanism should not be influenced by the handover scenarios. This is because the local security association between the UE, the MME and eNB are refreshed during handover and/or TAU procedures, while the "application" security associations are maintained. This assumption holds as long as the UE is attached to a particular PGW. If the UE detaches, there is no guarantee it will get the same IP the next time it attaches and even in that case, the IPsec tunnel is torn down.

In the NAT scenarios, the issues that impact the wireline IPsec are the same in the NGN case.

The mobile device has to follow specific steps to get authenticated in the 4G network. Similar or totally different steps must be taken to authenticate to each services network. The process for 4G is EPS-AKA or EAP-AKA. In the IMS network it can authenticate via IMS-AKA and secure the traffic via TLS or IPsec. But, because IMS is a special kind of services network, being closely described by 3GPP in conjunction with the access network, some part of the security weight already established can be used to secure the access to the services network. The following scheme tries to lessen the cryptographic and message exchange burden of the UE to IMS authentication process, by using the PGW as an authentication proxy. This happens because the PGW is the closest 4G entity to the IMS network. It should be in direct connection to the P-CSCF. The PGW unpacks both the signaling GTPv2-c packets as well as the GTPv1-u data-plane packets that arrive on the S5/S8 interface. Being at the edge of the 4G network, it is also able to inspect the content of these message or forward packets that match some particular criteria (port number, protocol number, ToS value etc) to a separate, dedicated, inspection entity. It is fairly simple to identity the IMS SIP packets (for instance by the port number, usually 5060). In the classic model, the SIP packets would simply be forwarded to the P-CSCF, as the PGW (GGSN) has no specific IMS-aware functionality (Vintilă, 2011).

In the proposed scheme, before the Initial Attach procedure, the UE selects 'p' and 'g' primes non-null and a secret 'a', then uses these values to derive value A from the Diffie-Hellman procedure: A=g^a mod p. Then the UE inserts value A, p and g (or only A if p and g are somehow agreed upon from a pre-configured setting), then adds them to the PCO (Protocol Configuration Options) IE in the Attach Request message to the MME, PCO IE that propagates to the PGW in the Create Session Request message. This entity looks at the values received and computes value B=g^b mod p, where b is its key. After it verifies that the UE is valid and sends it an IP (or an empty IP, if it is to be configured later dynamically), and includes also the B value in the PCO from the Create Session Response. The response gets back to the UE in the Attach Accept message. At this moment, the UE and the PGW derive a common Diffie-Hellman key K, which they can use as a symmetrical encryption key or as a master key to derive further key for securing traffic between them. The UE sends the SIP Register message and includes its secret key SIP-K, encrypted with K. This message arrives at the PGW.

The P-CSCF discovery procedure follows next, while the PGW acts on behalf of the UE during the IMS authentication. If the authentication is successful, the PGW will announce the UE (via a 200 OK message) that the UE is connected to the IMS core.

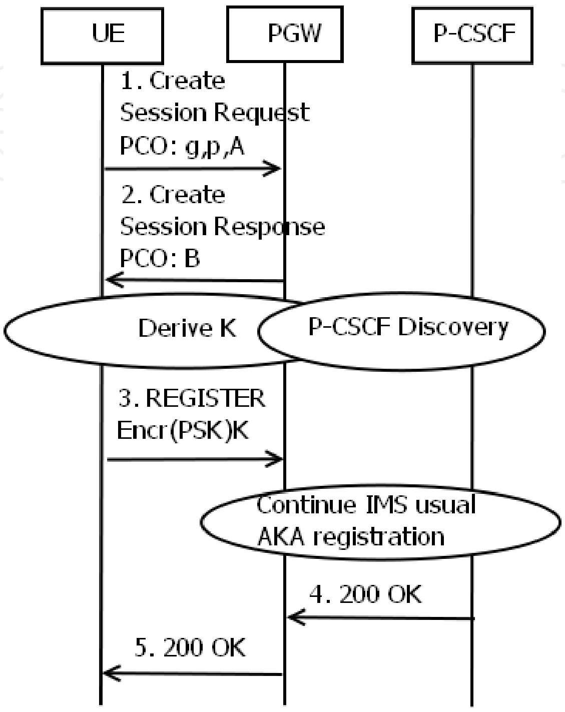

UE
PGW
P-CSCF
1. Create Session Request PCO: g,p,A
2. Create Session Response PCO: B
Derive K
P-CSCF Discovery
3. REGISTER Encr(PSK)K
Continue IMS usual AKA registration
4. 200 OK
5. 200 OK

Fig. 6. Proposed scheme

Although it saves only a few messages, this scheme has the main advantage of decreasing both the network load, as well as the cryptographic computation on the UE. One of the disadvantages of this scheme is that the cryptographic computation actually increases in the beginning, due to the DH procedure. The advantage is that the DH key can be used as a master key for further exchanges and this key remains valid for duration of the attach. Another disadvantage is that the model produces small functionality changes in the UE functionality. The SIP implementation will need to store the secret key in a dedicated header. This should not be a great impediment in the implementation of this feature, as the SIP protocol is highly flexible and there is no 100% agreed implementation in the industry, at this moment. Another advantage is that the IMS model, being relatively mature and stable, is not needed to implement this mode. The internal IMS-AKA procedure remains unchanged. The PGW replies to the 401 Unauthorized message; it verifies the AUTN, computes the RES and replies to P-CSCF. A secondary benefit is the generation of a secret key which can be used as a master key to derive cryptographically resistant session keys for later use.

5. Conclusion

IPsec is considered one of the most secure protocols in the Internet. It is being successfully used in securing traffic all over the Internet, in the wireline technologies. Whether the use case involves companies trying to secure traffic between their branches or trying to assure a secure remote connection for its mobile workers, the IPsec is one of the preferred protocols. IPsec is a complex set of protocols, and none of the solutions right now on the market actually implement all of it. This situation leads to many incompatibility cases between different IPsec implementations. Nonetheless, IPsec is widely implemented and the differences in implementation many times constitute market differentiators.

As it is so popular in wireline technologies, industry and researchers investigate ways to implement IPsec or parts of it in the wireless technologies, as well, in order to export its benefits to the telecommunications world. Protocols used in IPsec are already implemented in technologies like WiMAX and UMTS: AKA, used as an EAP method in IPsec – IKEv2 authentication procedures. In 4G, the 3GPP forum looks into the EAP-AKA procedure for authenticating mobile handsets that attach to the 4G network from non-3GPP access radio networks. 3GPP also makes use of the IPsec in the IMS security: IPsec-3GPP, negotiated not via IKE, but via SIP signaling. Other IPsec alternatives appear as IPsec-man and IPsec-IKE in the SIP negotiation, along with digest and TLS.

The examples provided using open-source implementations in tools like OpenIMSCore, Strongswan or FreeRadius demonstrate how the IPsec protocols can be configured. Although different security equipment producers provide alternative configuration methods, the overall input aspect is similar, according to the purpose served. Adapting IPsec onto mobile devices would mean a significant work on improving its computational overhead and also some of the security aspects. One idea would be to use elliptic curve cryptography, used already in IPsec, but not implemented extensively in the industry so far.

The model proposed in this paper does a very short incursion in a scenario where the PGW, a very powerful device of the LTE core network, takes up part of the cryptographic burden of the authentication process of a mobile device to an IMS network. There is no doubt IPsec has gained a powerful sit in the NGN world and there are to be expected many improvements that address the shortcomings of its implementation in the mobile world.

6. References

Mahdi Aiash, Glenford Mapp, Aboubaker Lasebae, Raphael Phan, Providing Security in 4G Systems: Unveiling the Challenges, *AICT '10 Proceedings of the 2010 Sixth Advanced International Conference on Telecommunications*, ISBN: 978-0-7695-4021-4 [last access: June 2011]

Chi-Yuan Chen, Tin-Yu Wu, Yueh-Min Huang, Han-Chieh Chao, An efficient end-to-end security mechanism for IP multimedia subsystem, *Computer Communications*, Volume 31 Issue 18, December, 2008 [last access: June 2011]

Cas Cremers, Key Exchance in IPsec revisited: Formal Analysis of IKEv1 and IKEv2, ETH Zurich, Switzerland, *ESORICS 2011, Leuven, September 2011*

John Edwards, A Guide to Understanding the VoIP Security Threat, February 2007, http://www.voip-news.com/feature/voip-security-threat-021407/ [last access: June 2011]

Richard Good, Fabricio Carvalho Gouveia, Shengyao Chen,Neco Ventura, Thomas Magedanz, Critical Issues for QoS Management and Provisioning in the IP Multimedia Subsystem, *Journal of Network and Systems Management*, Volume 16 Issue 2, June 2008 [last access: June 2011]

Xiaogang Guo, Hao Xue, Shuguang Chen, The optimized data network security system based on 4G system for power grid system, *GMC '10 Proceedings of the 2010 Global Mobile Congress*, ISBN: 978-1-4244-9001-1 [last access: June 2011]

Giorgos Karopoulos, Georgios Kambourakis, Stefanos Gritzalis, Elisavet Konstantinou, A framework for identity privacy in SIP, *Journal of Network and Computer Applications*, Volume 33 Issue 1, January, 2010 [last access: June 2011]

Angelos D. Keromytis, Voice over IP: Risks, Threats and Vulnerabilities, *5th Ph.D. School on Security in Wireless Networking (SWING),* Bertinoro, Italy, June/July 2010 [last access: June 2011]

Chakravarthy Kowtarapu, Chetan Anand, Guruprasad K.G., Shishir Sharma, Network separation and IPsec CA certificates-based security management for 4G networks, *Bell Labs Technical Journal - 4G Wireless Technologies*, Volume 13 Issue 4, February 2009 [last access: June 2011]

Yang Liu, Zhikui Chen, Feng Xia, Xiaoning Lv, Fanyu BuA, Trust Model Based on Service Classification in Mobile Services, *GREENCOM-CPSCOM '10 Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*, ISBN: 978-0-7695-4331-4 [last access: June 2011]

MSF forum – VoLTE seminar
http://www.msforum.org/interoperability/MSF-VoLTE-SCN-001-FINAL.pdf
[last access: June 2011]

Nidal Nasser, Ming Shang, Policy control framework for IP Multimedia Subsystem, *ISTA '09 Proceedings of the 2009 conference on Information Science, Technology and Applications*, ISBN: 978-1-60558-478-2 [last access: June 2011]

Anthony Plewes, The biggest VoIP security threats - and how to stop them, March 2007, http://www.silicon.com/legacy/research/specialreports/voipsecurity/0,3800013656,39166479,00.htm [last access: June 2011]

Anthony Plewes, VoIP threats to watch out for, March 2007, http://www.silicon.com/special-features/voip-security/2007/03/09/voip-threats-to-watch-out-for-39166244/ [last access: June 2011]

M. Sayyad, N. Ansari, S. Burli, H. Shah Thakur, A. Khatanhar, Review of IP multimedia subsystem, *ICWET '11 Proceedings of the International Conference & Workshop on Emerging Trends in Technology*, ISBN: 978-1-4503-0449-8 [last access: June 2011]

Craig A. Shue, Minaxi Gupta, Stefan A. Myers, IPSec: Performance Analysis and Enhancements, CiteSeer, http://www.cs.indiana.edu/cgi-pub/cshue/research/icc07.pdf [last access: September 2011]

SIP Torture Test Messages
http://www.ietf.org/rfc/rfc4475.txt [last access: June 2011]

TS 23.203, Policy and Charging control architecture,
http://www.3gpp.org/ftp/specs/archive/23_series/23.203/ [last access: June 2011]

TS 23.401, GPRS enhancements for E-UTRAN access,
http://www.3gpp.org/ftp/specs/archive/23_series/23.401/ [last access: June 2011]

TS 24.229, IMS Call Control based on SIP and SDP,
http://www.3gpp.org/ftp/specs/archive/24_series/24.229/ [last access: June 2011]

TS 29.061, Interworking between PLMN supporting packet-based services and PDN,
http://www.3gpp.org/ftp/specs/archive/29_series/29.061/ [last access: June 2011]

TS 29.274, EPS – GTPv2-C
http://www.3gpp.org/ftp/specs/archive/29_series/29.274 [last access: June 2011]

TS 33.203, 3G security,
http://www.3gpp.org/ftp/specs/archive/33_series/33.203/ [last access: June 2011]

TS 33.401, SAE – Security Architecture,
http://www.3gpp.org/ftp/Specs/archive/33_series/33.401/ [last access: June 2011]

TR 33.978, Security Aspects of Early IMS,
http://www.3gpp.org/ftp/specs/archive/33_series/33.978/ [last access: June 2011]

Cristina-Elena Vintilă, A solution for secure SIP conferencing over IMS and SAE, *WSEAS TRANSACTIONS on COMMUNICATIONS*, Volume 9 Issue 7, July 2010 [last access: June 2011]

Cristina-Elena Vintilă, Victor-Valeriu Patriciu, Ion Bica, A J-PAKE based solution for secure authentication in a 4G network, *NEHIPISIC'11 Proceeding of 10th WSEAS international conference on electronics, hardware, wireless and optical communications*, and *10th WSEAS international conference on signal processing, robotics and automation*, and *3rd WSEAS international conference on nanotechnology*, and *2nd WSEAS international conference on Plasma-fusion-nuclear physics*, 2011 ISBN: 978-960-474-276-9 [last access: June 2011]

VoIPSA – Voice over IP Security Alliance
http://www.voipsa.org/ [last access: June 2011]

N. Vrakas, D. Geneiatakis, C. Lambrinoudakis, A Call Conference Room Interception Attack and Detection, *Proceedings of the 7th International Conference on Trust, Privacy & Security in Digital Business* (TrustBus 2010), Bilbao, Spain, 2010, Lecture Notes in Computer Science LNCS, Springer

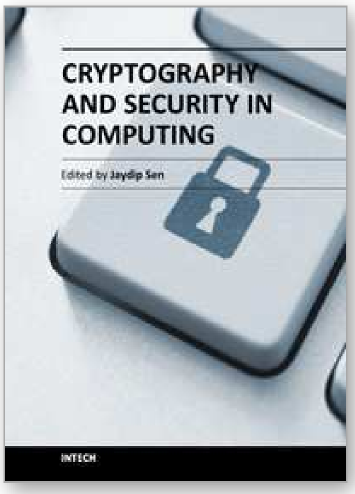
Dong Wang, Chen Liu, Model-based Vulnerability Analysis of IMS Network, *Journal of Networks*, Vol. 4, No. 4, June 2009 [last access: June 2011]

TS 23.228, IMS Release 8,
http://www.3gpp.org/ftp/specs/archive/23_series/23.228/ [last access: June 2011]

Christos Xenakis, Nikolaos Laoutaris, Lazaros Merakos, Ioannis Stavrakakis, A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms, *Computer Networks*, Volume 50, Issue 17, 5 December 2006, Pages 3225-3241 [last access: September 2011]

Yong Yang, Fernandez Alonso, Charging correlation for dedicated bearers, WIPO Patent Application WO/2011/039348 [last access: June 2011]

Yu-mei Wang, Jian Qin, Rong-jun Li,Jia-Jia Wen, Managing feature interaction based on service broker in IP multimedia subsystem, *Proceeding Mobility '08 Proceedings of the International Conference on Mobile Technology, Applications, and Systems*, ISBN: 978-1-60558-089-0 [last access: June 2011]



Cryptography and Security in Computing

Edited by Dr. Jaydip Sen

ISBN 978-953-51-0179-6
Hard cover, 242 pages
Publisher InTech
Published online 07, March, 2012
Published in print edition March, 2012

The purpose of this book is to present some of the critical security challenges in today's computing world and to discuss mechanisms for defending against those attacks by using classical and modern approaches of cryptography and other defence mechanisms. It contains eleven chapters which are divided into two parts. The chapters in Part 1 of the book mostly deal with theoretical and fundamental aspects of cryptography. The chapters in Part 2, on the other hand, discuss various applications of cryptographic protocols and techniques in designing computing and network security solutions. The book will be useful for researchers, engineers, graduate and doctoral students working in cryptography and security related areas. It will also be useful for faculty members of graduate schools and universities.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Cristina-Elena Vintilă (2012). Potential Applications of IPsec in Next Generation Networks, Cryptography and Security in Computing, Dr. Jaydip Sen (Ed.), ISBN: 978-953-51-0179-6, InTech, Available from: http://www.intechopen.com/books/cryptography-and-security-in-computing/potential-applications-of-ipsec-in-next-generation-networks

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821