A Secure One-Way Authentication Protocol in IMS Context

Mohamed Maachaoui[1,2], Anas Abou El Kalam[1,2], and Christian Fraboul[1]

[1] Université de Toulouse, IRIT-ENSEEIHT. Toulouse, France
[2] Université Cadi-Ayyad, ENSA. Marrakesh, Morocco
{mohamed.maachaoui,anas.abouelkalam,
christian.fraboul}@enseeiht.fr

Abstract. The IMS (IP Multimedia Subsystem) architecture is the key control for next generation networks (NGN). IMS gives network operators the opportunity to extend their services, including voice and multimedia communications and deliver them in new environments with new goals. Its security is paramount, especially authentication. In IMS, authentication is divided into two phases a PS (Packet-Switch) domain-level with the 3GPP-AKA protocol, and a second at IMS level using the IMS-AKA protocol. The latter is based on 3GPP-AKA, which leads to a large duplication of steps between the two phases. Some Works have tried to reduce this duplication and increase the IMS-AKA efficiency, but they add new vulnerabilities to IMS-AKA. The aim of this paper is to solve the security problems of IMS-AKA while maintaining good efficiency.

Keywords: Authentication, IMS, IMS-AKA, 3GPP-AKA, SIP, Diffie-Hellman.

1 Introduction

The move toward an all IP architecture for service delivery appears to be a strong trend. In this context, customers seem to desire an access to personalized interactive, multimedia services, on any device, and anywhere. This trend introduces new requirements for network infrastructures. The IP Multimedia Subsystem (IMS) is seen as a promising solution for fulfilling these expectations. IMS refers to a functional architecture for multimedia service delivery, based upon Internet protocols. Its aim is to merge Internet and cellular worlds, in order to enable rich multimedia communications [1, 2]. It is specified in the 3rd Generation Partnership Project (3GPP). IMS is intended to be "access agnostic", which means that service delivery should be independent of the underlying access technology. Thus, the use of open Internet Protocols is specified in IMS for better interoperability.

In Next Generation Network (NGN), IMS has become the core of control and fused multi-access modes. Based on IMS, ubiquitous services will be implemented easily. Therefore, IMS is supposed to become the favorite solution for fixed and mobile multimedia providers, but also one of the favorite attackers target. Consequently, strong and complex security services and mechanisms are needed to implement a robust security framework.

B. de Decker et al. (Eds.): CMS 2011, LNCS 7025, pp. 222–231, 2011.

One of the important needs and requirements is to ensure mutual authentication between users and the network. To do this, IMS defines the authentication protocol AKA (Authentication and Key Agreement) [3], which is based on the 3GPP-AKA protocol [4] and has a similar security level. IMS-AKA is based on SIP (Session Initiation Protocol) [5] and Diameter [6, 7, 8]. When a User Equipment (UE) wants to access IMS services, it must pass two authentications: (1) Packet-Switch (PS) level authentication using the 3GPP-AKA protocol, called the packet-switch domain authentication. (2) IMS level authentication using the IMS-AKA protocol. IMS-AKA reuses the same concept and principles of 3GPP-AKA. Both the PS and IMS authentications are necessary for IMS subscriber. If only the PS domain authentication is used, an attacker can impersonate other IMS subscribers in IMS, so-called fraudulent IMS usage [9]. However, since IMS-AKA is based on 3GPP AKA, it is inefficient that almost all involved steps in the two-pass authentication are duplicated.

In This paper we propose a new IMS authentication mechanism that improves the IMS-AKA in terms of security and efficiency. Actually, the proposed AKA does not need the duplicated AKA operations. Besides, it can withstand IMS-AKA security attacks, and keep the mutual authentication and key agreement capabilities.

The remainder of this paper is thus organized as follows. We briefly introduce the IMS architecture and its security mechanisms in Section 2. Section 3 presents the related works and discusses their common security problems. Subsequently, in section 4 we give details of the proposed protocol and we provide our analysis in terms of security and performance. Finally, we draw our conclusions in Section 6.

2 Security in IMS

The main components of this architecture are CSCF (Call Session Control Function) and HSS (Home Subscriber Server). HSS (Home Subscriber Server) contains subscriber databases, e.g., user identity and registration information. HSS entity interacts with other network entities via the Diameter protocol. CSCF (Call Session Control Function), which is a SIP server, is an essential node in IMS. CSCF processes SIP signaling in IMS. There are three types of CSCF, (1) A proxy-CSCF (P-CSCF), (2) A serving-CSCF (S-CSCF) and, (3) An interrogating-CSCF (I-CSCF).

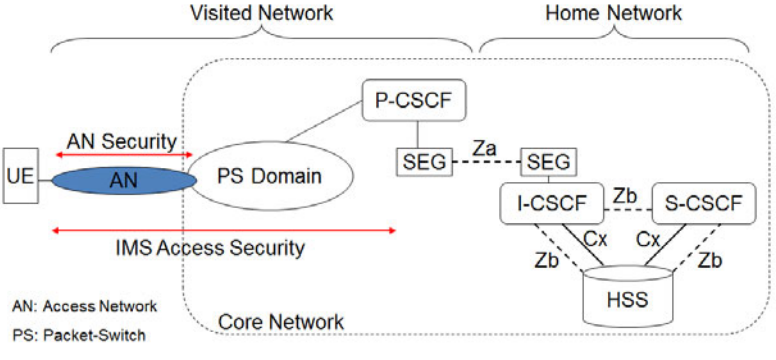

Fig. 1. Network domain Security in IMS

IMS security is divided into access security specified in 3GPP TS 33.203 [10] and network security specified in 3GPP TS 33.210 [11]. Network security deals with securing traffic within one security domain or between different security domains. A security domain is a network that is managed by a single administrative authority. Traffic between SEGs is protected using IPsec ESP (specified in RFC 2406 [12] and RFC 4303 [13]) running in tunnel mode. The interface used between entities in the same security domain is called Zb interface. The interface between SEGs from different domains is called Za. Figure 1 illustrates this point. Authentication, integrity protection, and encryption are mandatory in the Za interface. As the interface Zb only carries intra-operator traffic, it is up to the operator to decide whether to deploy the interface. Cx is a reference points for S-CSCF and I-CSCF to acquire subscriber information from HSS, in which the employed protocol is the diameter protocol.

Access security includes authentication of users and the network, and protection of the traffic between the IMS terminal and the network. In this article we are interested to this type of security mainly the IMS authentication.

3 Related Work

Assume that the user has been well authenticated at the PS-domain. The IMS terminal can begin registration/authentication at IMS-level. IMS-level registration / authentication procedure uses the IMS-AKA [3] (Authentication Key Agreement) protocol and it is accomplished by a SIP Register request. Registration with the IMS is mandatory before the IMS terminal can establish a session. In this section we will present the authentication process in IMS network with the IMS-AKA protocol as well as two proposals that reduce redundant steps in IMS-AKA and then increase the efficiency of the protocol in terms of number of messages exchanged, after that we provide our security analysis for the three mechanisms.

3.1 IMS Authentication: IMS-AKA Protocol

Assume that the user has been well authenticated at the PS-domain. The process of IMS-AKA uses two successive SIP Register requests and responses. It can be divided as shown in Figure 2 to the following steps:

I1: The UE sends a SIP Register message to S-CSCF (with the parameter) through the P-CSCF and I-CSCF.
I2: If S-CSCF does not have a valid authentication vector (AV) array for UE, S-CSCF sends a Multimedia Authentication Request (MAR) over Cx interface to HSS for obtaining an AV array. Otherwise, this Step and Step I3 can be skipped. Note that an AV contains (1) a random number RAND, (2) an expected response XRES, (3) a cipher key CK, (4) an integrity key IK, and (5) an authentication token AUTH.
I3: HSS generates an ordered array of n AVs. HSS sends the AV array over Cx interface to S-CSCF via a Multimedia Authentication Answer (MAA) message.
I4: S-CSCF selects the next unused authentication vector from the ordered AV array and sends the parameters RAND and AUTH (from the selected authentication vector)

to the UE through a SIP 401 Unauthorized message. This message contains also the keys CK and IK which are kept by P-CSCF.

I5: The UE verifies the received AUTN. If the result is positive, UE derives RES, CK and IK. Both IK and CK are used for IP security (IPsec) security association between UE and P-CSCF. Then, UE sends RES to S-CSCF through P-CSCF and I-CSCF. This response is generated in a new registration SIP Register request.

I6: S-CSCF verifies the user response XRES, If the result is positive, the authentication and key agreement exchange is successfully completed. S-CSCF sends a Server Assignment Request (SAR), over the Cx interface, to inform HSS about which S-CSCF will serve the UE.

I7: HSS stores the name of S-CSCF and sends the user's profile through a Server Assignment Answer (SAA) message over the Cx interface.

I8: Finally, S-CSCF sends a SIP 200 OK message to UE to notify him of the success of the registration process.

Note that in the second phase (second SIP Register) messages between the UE and P-CSCF are protected by an IPsec security association. This session is negotiated during the first phase through the two fields Security-Client (message 1) and Security-Server (message 10). The terminal includes a Security-Verify (message 11) header field in this Register mirroring the contents of the Security-Server header field received previously to withstand a man-in-the-middle attack.

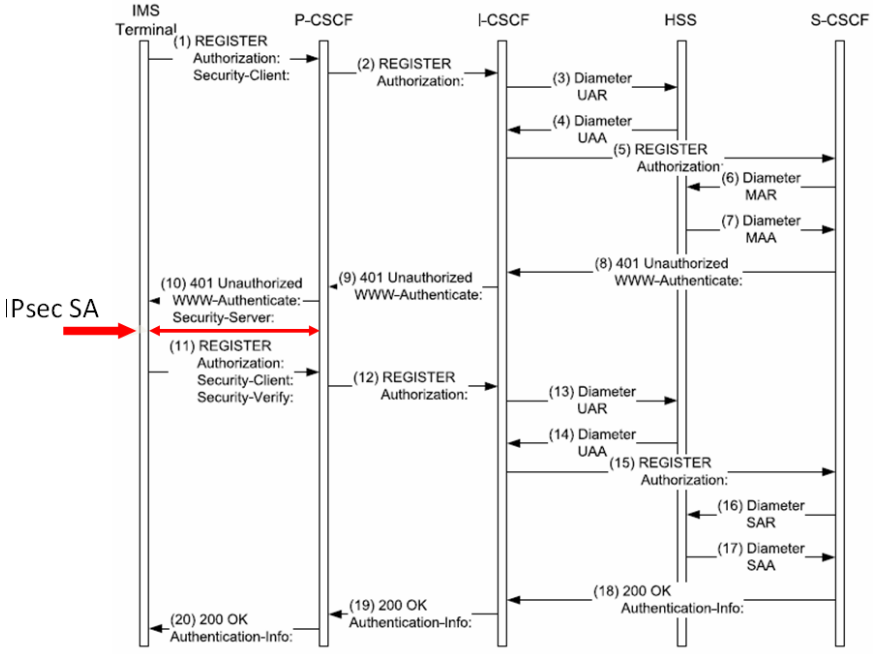

Fig. 2. IMS authentication/registration with IMS-AKA protocol

3.2 One-Pass GPRS and IMS Authentication Procedure for UMTS

This approach [9] proposes a one-pass authentication (performed at the PS level) that can authenticate an IMS user without explicitly performing the IMS-level authentication. To achieve this, it relies on the IMSI (International Mobile Subscriber Identity) parameter that the PS Domain previously stored while authenticating the UE, by adding it to the SIP message. The authentication is successful if the IMSI stored by the HSS equals the one sent by the PS Domain. This eliminates the use of authentication vectors (AV).

3.3 One-Pass Authentication and Key Agreement Procedure in IP Multimedia Subsystem for UMTS

This proposal [14] analyzes security issues in the previous approach, and improves the authentication process without losing efficiency (one-way). In contrast to IMS AKA, the UE starts with the challenge by sending a "digest-response" message with an authentication request header and a timestamp. Then, The S-CSCF verifies the message; if correct it authenticates the UE and replies with the authentication vector and a "response-auth" message. After that, the UE verifies the "response-auth" message, if it is valid; the UE assumes that the S-CSCF is legal, so it calculates the encryption and integrity keys that will be shared with the P-CSCF for data protection.

3.4 Security Analysis

In the first approach Lin et al. [9] may save up to 50% of the IMS registration/authentication traffic, as compared with the 3GPP two-pass procedure. However, this proposal adds new security issues to the authentication procedure.

In the Chung-Ming et al. approach (second solution) [14] the main objective is to keep the one-way proposed in Lin et al's scheme with an improvement in security. Despite that all three mechanisms are still suffering from the following vulnerabilities:

- No mutual authentication: in the first approach S-CSCF only verifies UE's identities (Private identities in PS domain and IMS level). UE does not authenticate S-CSCF and so it cannot be sure of whom is it exchanging information with. In this way, UE may have potential security problems, i.e., fake S-CSCF.
- Loss of key agreement capability: CK and IK are agreed for IPsec security association as explain in I4 and I5 in the sub-section 3.1. Unfortunately, in Lin et al.'s one-pass authentication proposition the encryption key CK and integrity key IK are not used. It results that confidentiality and integrity are not ensured for the exchanged messages between UE and P-CSCF.
- No guarantee of integrity and confidentiality: again, on Lin et al.'s schema, information does not travel through a secure channel since the protocol does not negotiate the IPsec security association. IMS-AKA and Chung-Ming et al. approaches are similarly vulnerable, since the traffic transmitted during the session initialization travels in plaintext, allowing an attacker to read or alter such information.

- In the core network, for the three schemas, there is no secure channel that prevents register data manipulation, since the implementation of the interface Zb is optional. It may not be implemented by the network administrator. Moreover, in IMS-AKA and Chung-Ming et al. approaches, the keys CK and IK could be captured by attackers inside the network.

4 The Proposed Authentication Protocol

4.1 Principle

Assume that UE shares with the IMS network (HSS) the algorithms to use for encryption and hashing, and we also assume that CSCFs and HSS share, in addition to encryption algorithms (such as AES [15] for example) and hashing (SHA-1 as [16] for example), a prime number *p* and a base *g*. The operations and mechanisms used are based on cryptographic functions contained in IMS-AKA's specification, in order to minimize the changes to system architecture. The aim of our proposal is to keep the one-way proposed by Lin et al. and at the same time resolve security issues already discussed. In order to transfer sensitive data we propose to use a secure channel based on Diffie-Hellman for the key exchange. The proposed mechanism illustrated in Figure 3 can be decomposed into the following steps:

S1: In the *ith* authentication with the proposed protocol, UE derives a random RANDi from a vector RAND as:

$$RANDi = RAND\ [i] \tag{1}$$

Where RAND is a random vector that UE has generated at the first authentication, if UE does not have a RAND vector it generates a new one and in this case i=0 i.e. RANDi = RAND [0]. After that, UE computes the RESi and derives the CKi and IKi keys as follows:

$$RESi = f2k(RANDi),\ CKi = f3k(RANDi),\ IKi = f4k(RANDi) \tag{2}$$

Where: *k* is the shared secret key between UE and HSS.
fi are the cryptographic algorithms shared between UE and HSS. *f2* is a message authentication codes, *f3* and *f4* are key generation functions.

Next, UE sends a SIP Register request with the IMPI (IP Multimedia Private Identity), RANDi and the RESi to S-CSCF via the P-CSCF. Moreover in our protocol CKi and IKi are also used to secure the SIP Register request between UE and S-CSCF. Actually, to ensure data confidentiality and integrity, we propose to encrypt the critical information and authenticate all information that will not be modified during the transmission.

S2: P-CSCF forwards the request to S-CSCF via I-CSCF. In addition, P-CSCF begins a Deffie-Hellman negotiation with S-CSCF. P-CSCF adds a value α to the message before transmission to S-CSCF where: $\alpha = g^a \bmod p$, with *a* is a random number.

S3: Assume that S-CSCF does not have the AVs for this UE; otherwise this step and step S4 can be skipped. S-CSCF invokes the authentication vector distribution

procedure by MAR message with HSS over the cx interface. In order to secure the HSS response containing the AV information S-CSCF performs a key exchange with HSS. Therefore, S-CSCF adds a value $\beta = g^b \bmod p$ where b is a random value.
S4: HSS uses RAND and IMPI, to find the pre-shared secret key k with this user, to derive AV. Then, it calculates $\chi = g^c \bmod p$ with c is a random number. Next, HSS encrypts MAA message using the negotiated key $DH(\beta\chi)$ (DH for Diffie-Hellman [17]). χ value is sent in clear.
S5: Upon receipt of the message MAA, S-CSCF retrieves χ and calculates $DH(\beta\chi)$ to decrypt the message and extract AV. Then, S-CSCF checks the hash value received in step S2 to verify the integrity of the request, if the result is positive S-CSCF decrypts the message. After that, S-CSCF extracts RESi. RESi is compared with XRESi contained in AVi. If they are equal, it means that UE is a legal user.
S6: S-CSCF sends a SIP OK message with AUTNi, CKi and IKi to P-CSCF with the value $\beta' = g^{b'} \bmod p$. β' value is used with the value α to build a shared key between S-CSCF and P-CSCF. The β' value is sent in clear.
S7: P-CSCF decrypts the message using the key DH ($\alpha\beta'$), stores CKi, IKi, and forwards the SIP OK message with AUTNi to UE. This message is encrypted and authenticated by CKi and IKi (as in step S1).
S8: UE calculates AUTNi and compares it with the one received from S-CSCF. S-CSCF is considered well authenticated if the result is positive.

To establish an IPsec security association between UE and P-CSCF, we use as in IMS-AKA the two fields “Security_Client” and “Security_Server”.

4.2 Security Analysis

In this section we will analyze the proposed mechanism in terms of security. The security properties in the proposed mechanism are presented as follows:

- *Mutual authentication between UE and S-CSCF (IMS Network):* The proposed protocol allows mutual authentication between UE and the S-CSCF. In the network side, S-CSCF retrieves AV from the HSS and verifies UE by comparing the XRESi with the RESi sent by UE. In the user side, to authenticate the network UE compares the AUTNi received from S-CSCF with the one that it calculates.
- *Using key CK & IK (key agreement property insured):* CK and IK are used to establish an IPsec session between UE and P-CSCF after authentication. Moreover, in our approach these two keys are used during the authentication/ registration procedure between UE, S-CSCF and P-CSCF (step S1 and S7).
- *Replay Attack:* To prevent replay attacks, RAND is a vector RAND. RANDi values are thus defined according to a specific order between UE and HSS. Moreover, the response AUTNi is calculated using a sequence number SQN (same as IMS-AKA).
- *Data Confidentiality and Integrity:* Confidentiality and integrity of data travelling between UE and the network is secured by encryption and hashing SIP messages using the keys CK and IK with encryption / hash algorithms pre-shared. At the core network, information exchanged is encrypted and authenticated using the keys negotiated with Deffie-Hellman between CSCF.

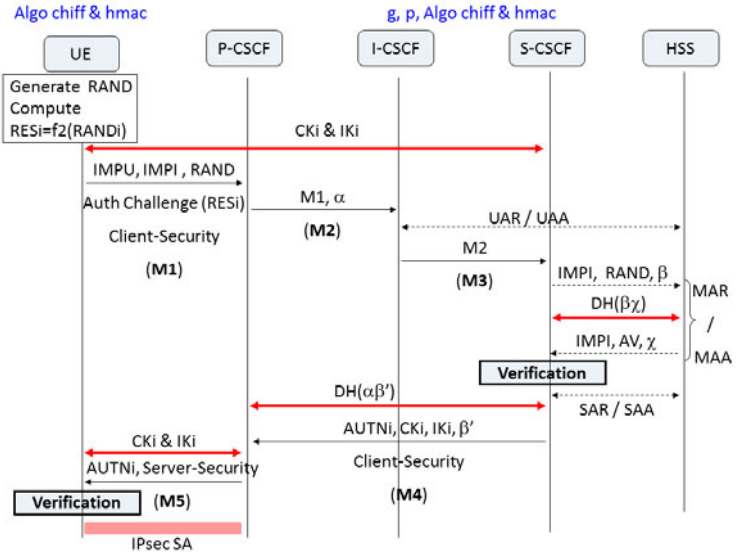

Fig. 3. The proposed one-way AKA protocol

4.3 Performance Analysis

In this section we evaluate our protocol in terms of performance, and then we will compare it with the IMS-AKA and Lin et al's solution. The comparison is based on the number of exchanged messages as they are transmitted across an air interface. We adopt the assumption depicted in [9]. The assumption is as follows, suppose that the expected SIP message delivery cost between UE and S-CSCF is one unit, and the expected Cx message delivery cost between the CSCF and the HSS is α units. It is anticipated that $\alpha<1$ for the following two reasons: (1) CSCFs and HSS exchange the Cx messages through IP network. (2) Besides the IP network overhead, SIP communications between UE and S-CSCF involves PS domain core network and access radio network. (3) CSCFs and HSS are typically located at the same location, while UE is likely to reside at a remote location.

Let C: be the total cost of IMS AKA, and C_P: The total cost of the proposed protocol.

If S-CSCF does not have valid AVs, the delivery cost of IMS-AKA is expressed by C_1. Otherwise, if the messages MAR/MAA are not executed in IMS-AKA, the delivery cost of IMS-AKA is expressed by C_2:

$$C_1 = 4 + 6\alpha. \qquad C_2 = 4 + 4\alpha. \tag{3}$$

IMS registration is periodically performed. In Steps I2 and I3 of the IMS-AKA procedure, an AV array of size n is sent from HSS to S-CSCF. Assume that the number of operations (authentication/registration) that the same S-CSCF performs is m. Therefore, only *ceilling (m/n)* messages MAA/MAR are executed. With *ceilling (x)* is the upper integer part. From (3), and let x = *ceilling(m/n)*, the average delivery cost of IMS-AKA C can be expressed as:

$$C = x/m\ C_1 + (m - x)/m\ C_2 = 4 + (2x/m + 4)\alpha \quad (4)$$

Similar to IMS-AKA, the average delivery cost of the proposed AKA Cp is:

$$C_P = x/m\ C_{P1} + (m - x)/m\ C_{P2} = 2 + (2x/m + 4)\alpha \quad (5)$$

From (4) and (5), the improvement *I* of the proposed protocol over the IMS-AKA is expressed as:.

$$I = (C - C_P)/C = m/(x\alpha + 2m(1 + \alpha)) \quad (6)$$

Similarly, the improvement *I'* of the Lin et al.'s solution over the IMS-AKA is:

$$I' = (C - C_L)/C = (m + x\alpha)/(x\alpha + 2m(1 + \alpha)) \quad (7)$$

Figures 4 and 5 plot I and I' as a function of α and m when m = 10.

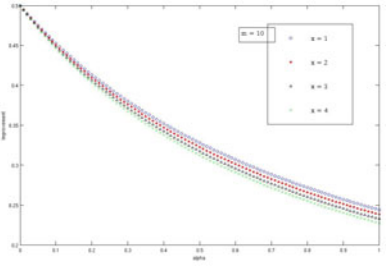

Fig. 4. Improvement of the proposed protocol over the IMS-AKA

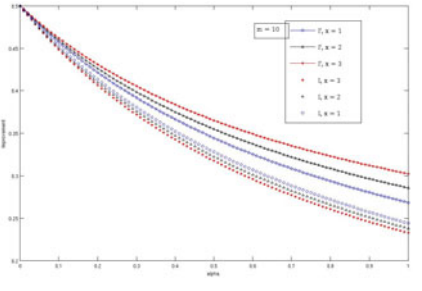

Fig. 5. A comparison of the two improvements I (proposed solution) and I' (Lin et al. solution)

As Figure 4 illustrates, the proposed one-pass AKA can save up to 50% of the SIP/Cx traffic over the IMS-AKA. When α approximates to 1, i.e. all of the network elements are located within the same network, *I* is lower than *I'*, which difference is less than 10% (Figure 5). This difference is due to the fact that in our proposal S-CSCF needs to retrieve AVs from HSS. However, according to the security analysis Lin et al.'s solution has some security problems and loses the mutual authentication and key agreement capabilities.

5 Conclusion

In this paper we proposed a new protocol for authentication in IMS. This proposal resolves the IMS-AKA security issues protocol; in addition our protocol keeps the one-way proposed by Lin et al. The performance analysis shows that the efficiency of the proposed protocol is comparable to that provided by the scheme of Lin et al. Table 1 shows a comparison between the different solutions discussed in this article.

Table 1. Comparison between the proposed protocol and the discussed solutions

	IMS-AKA	One-Pass Authentication	Proposed One-Pass AKA	Proposed protocol
Mutual Authentication	Yes	No	Yes	Yes
One-way	No	Yes	Yes	Yes
Key Agreement	Yes	No	Yes	Yes
Efficiency	---	Very good	Good	Good
Confidentiality	Yes (*)	No	No	Yes
Integrity	Yes (*)	No	No	Yes

In future works we expect to specify our protocol with appropriate formalisms (UML, Petri nets, etc.), in order to check various aspects of its behavior. The main goal is to validate the security aspects of the proposed protocol based on rigorous analysis of its vulnerabilities.

References

1. Camarillo, G.: Introduction to TISPAN NGN. Ericsson, Tech. Rep. (2005)
2. Tadault, M., Soormally, S., Thiebault, L.: Network evolution towards IP multimedia subsystem. Alcatel, Tech. Rep. (2003), http://www.alcatel.com/doctypes/articlepaperlibrary/pdf/ATR2003Q4/T0312-IP-Multimedia-EN.pdf
3. 3GPP TS 33.102: Security architecture. V8.4.0 2009-10
4. 3GPP TS 33.105: Cryptographic algorithm requirements. s.l. : ETSI, 2009-02. vol. 8
5. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Spark, R., Handley, M., Schooler, E.: Session Initiation Protocol. RFC 3261 (June 2002)
6. Calhoun, P., Loughney, J., Guttman, E., Zorn, G., Arkko, J.: Diameter Base Protocol RFC 3588 IETF (2003)
7. 3GPP TS 29.228. Technical Specification Core Network; IP Multimedia Subsystem Cx and Dx Interfaces; Signaling Flows and Message Contents (Release 5)
8. 3GPP TS 29.229. Technical Specification Core Network; Cx and Dx Interfaces Based on the Diameter Protocol; Protocol Details
9. Lin, Y.-B., Chang, M.-F., Hsu, M.-T., Wu, L.-Y.: One-pass GPRS and IMS authentication procedure for UMTS. IEEE Journal on Selected Areas in Communications 23(6), 1233–1239 (2005)
10. 3GPP TS 33.203: Access security for IP-based services. V8.6.0 s.l. : ETSI, 2009-07
11. 3GPP TS 33.210: 3G security; Network Domain Security (NDS); IP network layer security. V8.3.0 s.l.: ETSI, 2009-07
12. Kent, S., Atkinson, R.: IP Encapsulating Security Payload (ESP). RFC 2406, Internet Engineering Task Force (November 1998)
13. Kent, S.: IP Encapsulating Security Payload (ESP). RFC 4303, Internet Engineering Task Force (December 2005)
14. One-Pass Authentication and Key Agreement Procedure in IP Multimedia Subsystem for UMTS. Chung-Ming, Huang y Jian-Wei, Li. s.l.: IEEE (2007)
15. Frankel, S., Glenn, R., Kelly, S.: The aes-cbc cipher algorithm and its use with ipsec, ietf, rfc3602 (2003)
16. Madson, C., Glenn, R.: The use of hmac-sha-1 within esp and ah. ietf, rfc2404 (1998)
17. Rescorla. Diffie-Hellman Key Agreement Method. RFC 2631 (June 1999)