A SECURITY PROTOCOL FOR MUTUAL AUTHENTICATION AND MOBILE VPN DEPLOYMENT IN B3G NETWORKS

Christoforos Ntantogian
Department of Informatics and Telecommunications
University of Athens, Greece
ntantogian@di.uoa.gr

Christos Xenakis
Department of Technology Education and Digital Systems
University of Piraeus, Greece
xenakis@unipi.gr

ABSTRACT

This paper proposes a security protocol that provides mutual authentication between a user and a WLAN that the first tries to connect to, and deploys a mobile Virtual Private Network (VPN) that protects the user's data conveyed over the wireless network. For the user authentication as well as for the initialization of the VPN and the related key agreement, the EAP-SIM encapsulated within the Internet Key Exchange version 2 (IKEv2) is proposed. The deployed VPN, which is based on IPsec, ensures confidentiality, source authentication and integrity of the data exchanged over the WLAN. At the same time, the user has been subscribed to the 3G-network for charging and billing purposes using the legacy EAP-SIM authentication protocol. The established VPN can seamlessly operate and continuously provide security services as the mobile user moves and roams, materializing the notion of mobile VPN. The proposed security protocol eliminates the required enhancements to the current network infrastructure and operates transparently to the existing network functionality

I. INTRODUCTION

The evolution and successful deployment of Wireless Local Area Networks (WLANs) worldwide has yielded a demand to integrate them with third-generation (3G) mobile networks. The effort to develop 3G-WLAN integrated networks, also referred as Beyond 3G (B3G) networks, materializes the vision for the next generation mobile/wireless systems, which promise to provide high quality services and anywhere-anytime connectivity to mobile users.

An attempt to integrate the two incompatible technologies (i.e., WLAN and 3G) and ensure cooperation at the level of security is the EAP-SIM protocol [3]. EAP-SIM provides authentication and session key agreement to users that try to connect to a WLAN by employing the users' subscription in the Global System for Mobile communications (GSM)/General Packet Radio Services (GPRS). However, as the relative specifications document acknowledges, EAP-SIM presents some fundamental security flaws that may allow an attacker to compromise the integrity of EAP-SIM transactions [4]. In addition, the currently deployed confidentiality mechanisms, which protect data conveyance over the WLAN, do not adequately satisfy the explicit requirements of B3G networks and their users for high level security services and minimum enhancements to the existing network infrastructure. More specifically, the Wired Equivalent Privacy (WEP) protocol and the Temporary Key Integrity Protocol (TKIP) suffer from certain security flaws [8], [10], while the deployment of the Counter Mode CBC-MAC protocol (CCMP) may arise several compatibility issues, since it requires considerable changes to the existing WLAN infrastructure [9], since the wireless Access Points (APs) must incorporate additional software and hardware for implementing the Advanced Encryption Standard (AES) security algorithm. Moreover, all the aforementioned security mechanisms apply encryption over the radio interface, leaving unprotected the fixed part of the WLAN.

To overcome the above deficiencies, this paper proposes a security protocol that provides secure authentication between a user and a WLAN that the first tries to connect to, and deploys a mobile Virtual Private Network (VPN) that protects the user's data conveyed over the wireless network. The proposed security protocol is carried out in two distinct phases. In the first phase, an EAP-MD5 authentication takes place, which authenticates the user to a wireless AP, protecting the latter from blind Denial of Service (DoS) attacks at the network layer. In addition, WEP encryption is activated over the radio interface protecting the latter from traffic analysis and the IP address assigned to the user from being disclosed. Although the EAP-MD5 authentication and the WEP encryption are considered that they do not provide an adequate level of security for WLANs, in the proposed security protocol these measures are employed as complementary security measures focusing on the protection of the WLAN against certain security threats and not protecting it in general. After the initial EAP-MD5 authentication, the proposed security protocol employs the Internet Key Exchange version 2 (IKEv2) [2] that encapsulates EAP-SIM messages for "strong" mutual authentication between the user and the network (second phase). In this way the weaknesses of the legacy EAP-SIM authentication method are eliminated, and the level of authentication provided in B3G networks is enhanced. Then, the Security Associations (SAs) that have been established by IKEv2 are used for the deployment of a VPN between the user and the WLAN. The deployed VPN, which is based on IPsec [6], ensures confidentiality, source authentication, and integrity of the data exchanged over the WLAN. At the same time, the user has been subscribed to the 3G-network for charging and billing purposes using the legacy EAP-SIM authentication protocol. To support VPN mobility, in cases that the involved user moves, the security protocol incorporates the Mobility and Multihoming IKE (MOBIKE) functionality [5], which provides mobility management to the deployed SAs. The proposed security protocol eliminates the required enhancements to the current network infrastructure and operates transparently to the existing network functionality.

1-4244-1144-0/07/$25.00 ©2007 IEEE.

The rest of this paper is organized as follows. Section 2 briefly introduces the B3G network architecture, as well as the security weaknesses of the currently deployed protocols and mechanisms that provide authentication and data protection over the WLAN in this architecture. Section 3 presents the proposed security protocol that provides mutual authentication and deploys an IPsec-based mobile VPNs for data protection over the WLAN. Section 4 elaborates on a security analysis of the proposed security protocol focusing on the specific advantages and the potential drawbacks. Finally, section 5 contains the conclusions.

II. BACKGROUND

A. *B3G Network Architecture*

As shown in Fig. 1 the B3G network architecture [1] consists of two main parts: the visited WLAN-Access Network (AN) and the 3G home network. The WLAN-AN consist of the wireless APs, which act like AAA (Authentication, Authorization and Accounting) clients that forward security related messages to the AAA server, and the Network Access Server (NAS) that provides to the mobile users access to the public Internet. Note that the AAA protocol is based on Diameter. On the other hand, the main components of the 3G home network are: the AAA server that provides authentication services to the WLAN, the Home Location Register (HLR), which is a database used for the management of permanent data of the mobile users, and the Authentication Center (AuC) that maintains security information related to the mobile subscribers. To provide authentication services, the AAA server contains all the information required for the service handling of the mobile users through the WLAN, and communicates with the HLR and the AuC using the Mobile Application Part (MAP) protocol.

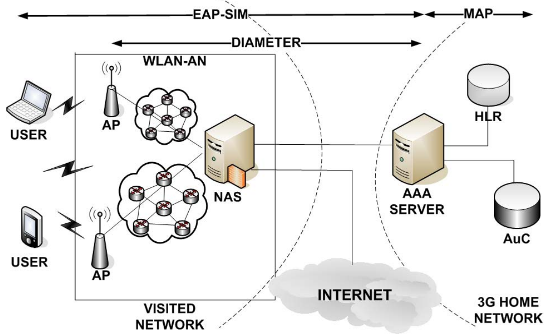

Fig. 1 The B3G network architecture

B. *EAP-SIM*

As mentioned previously, EAP-SIM [3] is designed to provide mutual authentication and session key agreement in the forthcoming B3G network architecture. EAP-SIM incorporates two basic enhancements that eliminate known security weaknesses of the authentication and key agreement procedure of GSM/GPRS. First, the keys in EAP-SIM are enhanced to have 128-bits security, in contrast with the 64-bit security of the initial GSM keys. Second, EAP-SIM supports mutual authentication in contrast to the GSM/GPRS authentication that performs only user to network authentication. EAP-SIM uses two or three Kc keys of several authentication triplets to generate a Master Key (MK). From the MK key several keys are generated: Important here are (a) the Master Session Key (MSK) for encryption purposes and (b) the K_auth key that is used for the calculation of a keyed Message Authentication Code (MAC) over the RAND parameters of the GSM/GPRS authentication triplets. The AAA server generates this keyed MAC, in order to authenticate itself to the mobile user. On the other hand, the user is authenticated to the AAA server using the SRES parameter of the authentication triplets [3].

Although EAP-SIM was designed as an advanced authentication protocol, it does not meet its security goals. An essential drawback of the EAP-SIM authentication procedure is related to the fact that its sessions are not independent [4]. Specifically, if some authentication triplets of a user are compromised, then, an adversary may use them to authenticate himself to the user as a valid network. The ways in which the adversary can obtain authentication triplets are: (a) having physical access to the SIM-card of the user; (b) using a malicious piece of software that attacks against the user platform; (c) performing attacks on the 3G network (it is assumed that the same authentication triplets are used for both 3G and WLAN access); and (d) getting access to the communication between the HLR/AuC and the AAA server that exchange authentication information. Obtaining authentication triplets the adversary may impersonate a valid network and calculate valid keys, as he possesses valid authentication triplets. Thus, he is authenticated to the user as a legitimate AAA server, since there is no way for the former to understand that there is a replay attack. Although EAP-SIM mandates the use of fresh authentication triplets, there is no mechanism that enables the user to check whether the authentication triplets, received from the AAA server, are fresh. The adversary may use the compromised triplets as long as the secret key, Ki, which is included in the SIM-card and uniquely, identifies the user’s subscription in the network, remains the same and this could be for years.

Except for the above deficiency, many EAP-SIM messages (e.g., EAP-Request/Notification, EAP-Response/Notification, EAP-Success and EAP-Failure) are exchanged unprotected enabling the attacker to send false notifications to the peers and mount denial of service attacks.

III. PROPOSED SECURITY PROTOCOL

A. *Protocol Outline*

The proposed security protocol involves two separate security domains (i.e., the visited WLAN and the home 3G network) with an explicit level of trusted relations between the network entities that are responsible for the interworking between the WLAN and the 3G-network (i.e., the NAS and the AAA server). It is worth noting that, since the communication link between the NAS and the AAA sever is based on Diameter, there is a pre-established IPsec tunnel between them that protects the Diameter message exchange, enhancing the level of trust between the two separate security domains.

When a mobile user is associated to a wireless AP, they perform the first phase of the proposed security protocol, which is based on the EAP-MD5 method (see Fig. 2). This phase authenticates the user to the wireless AP, protecting the latter from blind DoS attacks at the network layer. After authentication completion, the wireless AP assigns to the user an IP address that is required for the execution of IKEv2 (i.e., phase 2 of the proposed security protocol). In addition, the WEP encryption is activated over the radio interface using a WEP key, which is generated and maintained in as described in section 3.3 below. This encryption is employed to protect the radio interface from traffic analysis and the privacy of the assigned IP address. Although the EAP-MD5 authentication and the WEP encryption are considered that they do not provide an adequate level of security for WLANs, in the proposed security protocol these measures are employed as complementary security measures focusing on the protection of the WLAN against certain security threats and not protecting it in general.

After the initial EAP-MD5 authentication, the proposed security protocol employs IKEv2 for mutual authentication between the mobile user and the network (second phase) (see Fig. 2). IKEv2 is a component of IPsec used for performing authentication and establishing and maintaining SAs. The proposed security protocol encapsulates EAP-SIM messages within IKEv2 protecting them during negotiation and thus, enhancing the related authentication procedure. After the completion of IKEv2, two IPsec SAs (i.e., one for each direction) are established between the mobile user and the NAS that are used for the deployment of a bi-directional mobile VPN over the WLAN-AN.

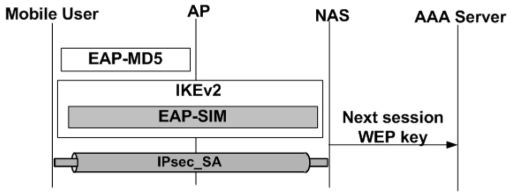

Fig. 2 Outline of the proposed security protocol

B. Initial Phase

To initiate the EAP-MD5 authentication, the AP sends an EAP-Request/Identity (see Fig. 3) to ask from the mobile user its identity. The mobile user replies with its identity in a Network Access Identifier (NAI) format, which is included in an EAP-Response/Identity message. Note that this identity is used only in this initial phase in order to enable the AAA server to retrieve the user's WEP key. By receiving this message, the AP forwards it to the AAA server to retrieve the WEP key of the user from the related list. The WEP key of each user is not static, but it changes dynamically every time the user is authenticated to the network. Initially, the home network assigns to each subscribed user a secret WEP key that will be used in the first authentication attempt. After the completion of the EAP-MD5 authentication, both the user and the NAS (during the IKEv2 negotiation) generate a new secret WEP key. The user stores the generated WEP key in his device and the NAS forwards it to the AAA server, in order to be used in the next authentication attempt (see section 3.3).

After retrieving the WEP key, the AAA server sends a challenge (i.e., a random number) to the user. The latter answers by returning to the AP a hashed value ($H_{challenge}$) calculated over the challenge and the WEP key using the MD5 hash algorithm. The AP forwards this value to the AAA server. The latter computes its own hashed value of the challenge using the WEP key of the user and compares it with the hashed value sent by the user. If the two hashed values match then, the mobile user is authenticated and the AAA server sends an EAP-Success message together with the WEP key to the AP. After authentication, the mobile user obtains an IP address and he is able to execute the IKEv2 negotiation.

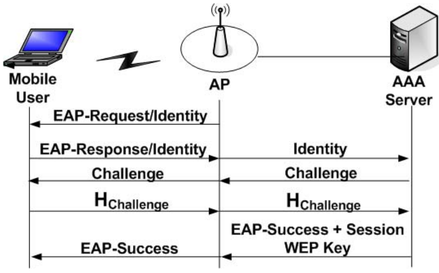

Fig. 3 The initial phase of the proposed security protocol

C. Second Phase

At the beginning of the IKEv2 negotiation (step 1 in Fig. 4), the user sends to the NAS the *SAi1* payload, which denotes the set of cryptographic algorithms that it supports for the IKE SA, the *KEi*, which is the Diffie-Hellman value, and a *Ni* value that represents the nonce. The nonce (i.e., a random number of at least 128 bits) is used as input to the cryptographic functions employed by IKEv2 to ensure liveliness of the keying material and protect against replay attacks. The NAS answers with a message that contains its choice from the set of cryptographic algorithms for the IKE SA (*SAr1*), its value to complete the Diffie-Hellman exchange (*KEr*) and its nonce (*Nr*). At this point, both the user and the NAS can calculate the SKEYSEED value as follows:

$$\mathrm{SKEYSEED} = \mathrm{prf}((\mathrm{Ni} \mid \mathrm{Nr}), \mathrm{g}^{\wedge}\mathrm{ir}) \quad (1)$$

where prf is the pseudorandom function negotiated in the previous messages and g^ir is the shared secret key that derives from the Diffie-Hellman exchange. The SKEYSEED value is used to calculate various secret keys: The most important are: the SK_d used for providing the keying material for the IPsec SA; SK_ei and SK_ai used for encrypting and providing integrity services, respectively, to the IKEv2 messages from the user to the NAS (IKE SA); and, finally, SK_er and SK_ar that provide security services in the opposite direction (IKE SA).

Finalizing the IKE_SA_INIT exchange, the IKE_AUTH exchange can start. It is worth noting that from this point all the following IKEv2 messages are encrypted and integrity protected using the IKE_SA, as shown in Fig. 4. The IKE_AUTH exchange of messages starts when the user sends to the NAS a message (step 2 in Fig. 4) that includes his identity (*IDi*), the *CERTREQi* payload (optionally), which is a list of the CAs whose public keys the user trusts, the traffic selectors (i.e., *TSi* and *TSr*), which allow the peers to identify the packet flows that require processing by IPsec, the Configuration Payload Request (*CP-Request*), which is used to obtain a remote IP address from the NAS and get access to the public internet, and the *MOBIKE_SUPPORTED* payload. The latter denotes that the user supports the MOBIKE functionality [5], which provides mobility management for the deployed IPsec SAs and is analyzed in the next section.

Upon receiving this message, the NAS forwards the identity of the user (*IDi*) to the AAA server and the latter initiates an EAP-SIM dialogue by sending to the NAS an EAP-Request/SIM/Start message encapsulated in a Diameter message (step 3 in Fig. 4). The NAS forwards to the user the EAP-Request/SIM/Start message encapsulated in an IKEv2 message, which also includes the identity of the NAS *(IDr*), its certificate (*CERTr*), the *AUTHr* payload, and the *MOBIKE_SUPPORTED* payload, which denotes that the NAS also supports MOBIKE. The AUTHr payload contains signed data used to authenticate the *NAS* to the mobile user. Upon receiving the EAP-Request/SIM/Start message, the user verifies the *AUTHr* field by using the public key of the NAS included in the certificate of the *CERTr* payload and answers by sending an EAP-Response/SIM/Start message encapsulated in an IKEv2 message. From this point, the IKEv2 messages contain only EAP-SIM payloads, which are encrypted and integrity protected using the IKE SA just like the previous IKEv2 messages. The EAP-SIM authentication protocol [3] proceeds, normally, and the AAA server communicates with the HLR/AuC to obtain the authentication triplets of the user (step 4 in Fig. 4). The EAP-SIM authentication dialogue ends when the AAA server sends an EAP-Success (or an EAP-Failure in case of a failure) to the NAS. In case of a successful authentication together with the EAP-Success message the AAA server sends to the NAS the MSK, which is generated by the execution of EAP-SIM (see section 2.2), as shown in Fig. 4 (step 5).

After the completion of the EAP-SIM negotiation, the last step (step 6) of IKEv2 creates an IPsec SA. In this step, both the NAS and the mobile user generate the *AUTHr* and *AUTHi* payloads, respectively, using the generated MSK of EAP-SIM, in order to avoid man-in-the-middle attacks. The NAS together with the *AUTHr* payload also sends its traffic selector payloads (*TSi* and *TSr*), its choice from the supported set of cryptographic algorithms that will be used in the IPsec SA (*SAr2* payload) and the assigned user's remote IP address in the Configuration Payload Reply (*CP-REPLY*) payload. It must be noted that the deployed IPsec SA protects the one-way communication between the user and the NAS.

For bi-directional secure communication one more IPsec SA needs to be established between the NAS and the mobile user, by executing the Create_Child_SA exchange of IKEv2 [2] over the established IKE SA. After the establishment of the IPsec SA, the related keying material (KEYMAT) is generated as follows:

$$\text{KEYMAT} = \text{prf}(\text{SK\_d}, \text{Ni} \mid \text{Nr}) \quad (2)$$

where Ni and Nr are the nonces from the IKE_SA_INIT exchange, and SK_d is the key that is generated from SKEYSEED. The KEYMAT is also used to generate the next session WEP key that will be used in the next EAP-MD5 authentication of the user, since IKEv2 has the flexibility of generating several keys from the KEYMAT value [2]. The mobile user stores this WEP key and at the same time the NAS transfers it to the AAA server of the user's home network.

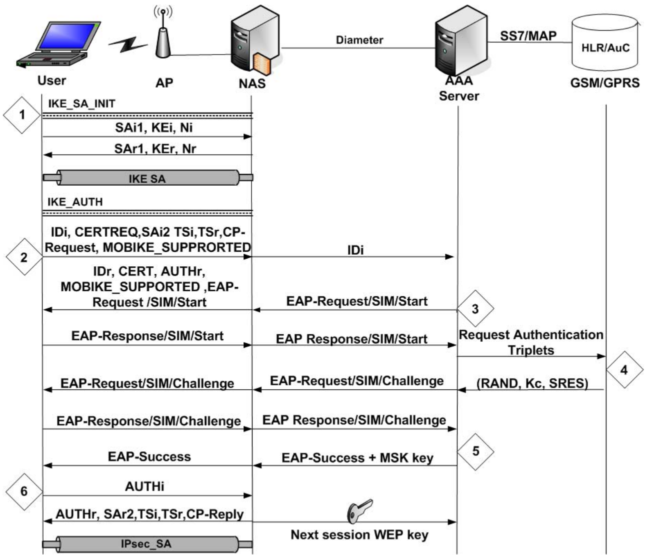
User
AP
NAS
Diameter
AAA Server
SS7/MAP
HLR/AuC
GSM/GPRS
1
IKE_SA_INIT
SAi1, KEi, Ni
SAr1, KEr, Nr
IKE SA
IKE_AUTH
IDi, CERTREQ,SAi2 TSi,TSr,CP-Request, MOBIKE_SUPPRORTED
2
IDi
IDr, CERT, AUTHr, MOBIKE_SUPPORTED ,EAP-Request /SIM/Start
EAP-Request/SIM/Start
3
EAP-Response/SIM/Start
EAP Response/SIM/Start
Request Authentication Triplets
4
EAP-Request/SIM/Challenge
EAP-Request/SIM/Challenge
(RAND, Kc, SRES)
EAP-Response/SIM/Challenge
EAP Response/SIM/Challenge
5
EAP-Success
EAP-Success + MSK key
6
AUTHi
AUTHr, SAr2,TSi,TSr,CP-Reply
Next session WEP key
IPsec_SA

Fig. 4 The second phase of the proposed security protocol

D. *IPsec VPN Deployment*

After the completion of the authentication procedure and the establishment of the pair of IPsec SAs between the user and the NAS, a bi-directional VPN that allow secure data exchange over the WLAN-AN, is deployed. At the same time, the mobile user has been subscribed to the 3G-network for charging and billing purposes using the legacy EAP-SIM authentication protocol. The deployed VPN tunnel runs on top of the wireless link and is based on IPsec [6], which is one of the strongest security framework available in networking.

In case that the user moves and is associated to a new wireless AP, then, the latter will assign to him a new IP address and thus, the established IPsec SAs must be re-negotiated using IKEv2. However, creating new SAs implies a repetition of expensive calculations and IKEv2 messages exchange. To avoid this iterative overhead, a mechanism for updating the new IP address in the context of the established SAs is needed. Such a mechanism is provided by the MOBIKE protocol [5], which enables a user with established IPsec SAs to move from one AP to another, without re-establishing them. MOBIKE runs on the top of IKEv2 and facilitates the deployment of mobile VPNs. For the application of MOBIKE in the considered network environment, the mobile users and the NAS have to incorporate the related functionality and execute it in cases that the user moves.

IV. Security Analysis

A. *Advantages*

The main advantage of the proposed security protocol is that it enhances the authentication procedure of EAP-SIM by employing the "strong" authentication mechanism of IKEv2. Thus, the identified security weaknesses of EAP-SIM and the accompanied vulnerabilities described before are eliminated. More specifically, the mobile user and the AAA server are authenticated each other using protected EAP-SIM messages by IKEv2. In addition, the NAS is authenticated to the user by using its certificate within the secure IKEv2 negotiation.

Therefore, an adversary cannot mount a replay attack by stealing the authentication triplets of the user and impersonate a valid network, since he doesn't possess a valid certificate. Moreover, encapsulating EAP-SIM messages within IKEv2 ensures confidentiality and integrity of the critical data (such as the user identity, etc) conveyed by EAP-SIM, eliminating the possibility to be disclosure and exploited by an adversary. Except for improving the level of security supported, the proposed security protocol defeats certain attacks that threaten the wireless link. More specifically, since the IKEv2 does not support a username password mechanism, it is not vulnerable to dictionary or social engineering attacks. The user and the NAS may refresh the keying material used in case that they wish to or it is necessary (i.e., they want to exchange critical data) by initiating a new IPsec SA exchange. They may also exchange new Diffie-Hellman values, in order to exploit the advantages of "Perfect Forward Security" (PFS). PFS forces the communicating endpoints to forget the keys used by a connection between them and the related data that are used to compute these keys. Additionally, the proposed security protocol offers protection against DoS attacks by employing the EAP-MD5 authentication (first phase). This mechanism authenticates the users at the layer 2, restricting the fraudulent users to perform blind DoS attacks at the network layer to the wireless APs. A user cannot obtain an IP address without being authenticated. In addition, the encryption at the layer 2 using WEP protects the IKEv2 messages and the IP headers of the packets exchanged between the users and the APs. Thus, an adversary cannot spoof the IP headers of the packets sent over the air performing traffic analysis or DoS attacks.

Finally, after the establishment of a pair of IPsec SAs between the user and the NAS, an IPsec-based VPN tunnel has been deployed between them that protects data sent over the radio access network and the fixed part of the WLAN-AN. IPsec provides security at the network layer and thus, offers many advantages and a remarkable flexibility compared to other security mechanisms. The details of network security are usually hidden from applications, which therefore automatically and transparently take advantage of whatever network-layer security services the environment provides. A reasonable question is that whether IPsec can be applied on mobile devices and over wireless links, which are characterized by limited resources. Xenakis et al. [7] examine the processing and the communication overheads of IPsec, evaluate the feasibility of deploying it on handheld devices and wireless networks, and give a positive answer to the previous question.

B. *Drawbacks*

The main drawback of the proposed security protocol is related to the fact that the existing network infrastructure, which supports EAP-SIM authentication, should be enhanced. Specifically, the mobile devices and the NAS should be enhanced to support IKEv2. In addition, both of them must incorporate IPsec in order to provide network layer VPNs. Finally, the proposed security protocol requires the deployment of Public Key Infrastructure (PKI), which facilitates the authentication of the NAS to mobile users. However, these enhancements do not refer to the wireless APs, as happens with other security protocols, which are widely deployed and their replacement-enhancement costs. On the other hand, the mobile devices that are laptops or PDAs, and the NAS, which is a central network entity of B3G infrastructure can be enhanced easier reducing the overall cost.

Regarding network performance, the execution of IKEv2 and the encapsulation of EAP-SIM within IKEv2 messages increases the time required for user authentication, compared to the pure EAP-SIM authentication scheme. However, since the user authentication procedure does not take place, frequently, the increased time delay is not expected to cause problems to the involved users. On the contrary, this is the price of the improved security services that the proposed security protocol supports.

V. Conclusions

This paper has proposed a security protocol that enhances the authentication procedure of EAP-SIM by employing the "strong" authentication mechanism of IKEv2. Thus, the identified security weaknesses of EAP-SIM and the accompanied vulnerabilities described above are eliminated. The mobile user and the AAA server are authenticated each other using protected EAP-SIM messages by IKEv2. In addition, the NAS is authenticated to the user by using its certificate within the secure IKEv2 negotiation. On the other hand, the main drawback of the proposed protocol is that its deployment may increase the computational overhead of the involved entities compared to the pure EAP-SIM.

References

[1] 3GPP TS 23.234 (v 7.3.0), "3GPP System to WLAN Interworking; System Description", Release 7, Sep. 2006.

[2] C. Kaufman, "The Internet Key Exchange (IKEv2) Protocol", RFC 4306, Dec 2005.

[3] H. Haverinen, J. Saloway "EAP-SIM Authentication", RFC 4186, Jan 2006.

[4] S.Patel, "Analysis of EAP-SIM Session Keys Agreement", Lucent Technologies.

[5] P.Eronen, "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, Jun 2006.

[6] S. Kent R. Atkinson, "Security Architecture for Internet Protocol", RFC 2401, Nov 1998.

[7] C. Xenakis, N. Laoutaris, L. Merakos, I. Stavrakakis, "A Generic Characterization of the Overheads Imposed by IPsec and Associated Cryptographic Algorithms", Computer Networks, Elsevier Science, Vol. 50, No. 17, Dec 2006, pp. 3225-3241.

[8] N. Borisov, I. Goldberg, D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", Proc of the 7th annual International Conference on Mobile Computing and Networking", 2001, ACM MOBICOM, pp.180-188.

[9] J. Cheng Chen, M. Chia Jiang, Y.Wen Liu, "Wireless LAN Security and 802.11i", IEEE Wireless Communications", Vol. 12, No 1, Feb. 2005 pp.27-36.

[10] N. Ferguson, "Micheal: an improved MIC for 802.11 WEP", IEEE 802.11i Working Group IEEE 802.11-02/020r0, Jan 2002.

Acknowledgement

Work supported by the project CASCADAS (IST-027807) funded by the FET Program of the European Commission.