An Enhanced EAP-SIM Authentication Scheme for Securing WLAN

Christoforos Ntantogian, Christos Xenakis, and Lazaros Merakos.
Communication Networks Laboratory, Department of Informatics & Telecommunications, University of Athens, Greece. e-mail: {ntantogian,xenakis ,merakos}@di.uoa.gr

Abstract— **This paper presents an enhanced EAP-SIM authentication scheme for securing WLAN. The proposed scheme uses the Internet Key Exchange version 2 (IKEv2) protocol to protect the authentication procedure of EAP-SIM by encapsulating its packets. In this way the vulnerabilities of EAP-SIM authentication method are eliminated. After the employment of IKEv2, a Virtual Private Network (VPN) tunnel is established that protects data transferred over the air interface. The tunnel, which is based on IPsec, ensures confidentiality, authentication and integrity of the data exchanged in the WLAN environment. The proposed scheme has minimal impact on the existing network infrastructure. The user is still authenticated by proving the possession of a SIM card, in order to get subscribed in his home network for billing and charging purposes. The proposed scheme requires only that each end-point of the established VPN tunnel must have the appropriate IPsec software.**

Index Terms— **Authentication, WLAN, EAP-SIM, IKEv2, IPsec-based VPN.**

I. Introduction

THE convergence of Wireless Local Area Networks (WLANs) and 3G systems is currently being deployed from the Third Generation Partnership Project (3GPP), which provides an interworking architecture as an add-on to the 3GPP cellular system specification. The integration of the two systems aims at combining them in such a way that brings out the functional advantages of each technology in a smooth way. The advantages of the cellular technology are related to the roaming capability, the subscription management and the authentication and key agreement procedure. On the other hand, WLANs provide better bandwidth and processing capabilities. To materialize this integration and ensure cooperation at the level of security, the EAP-SIM authentication and session key agreement protocol has been designed for the Global System for Mobile communications (GSM)/General Packet Radio Services (GPRS) network.

EAP-SIM [2] developed by 3GPP, is one of the various authentication methods that the Extensible Authentication Protocol (EAP) supports. It provides Authentication and session Key Agreement using the GSM/GPRS Subscriber Identity Module (SIM). However, as the relative specification document acknowledges [2] EAP-SIM does not provide an adequate level of security, since it has some fundamental flows that may allow an attacker to compromise the integrity of its transactions [4].

In this paper, an enhanced EAP-SIM authentication scheme for securing WLAN is proposed and analyzed. This scheme uses the Internet Key Exchange version 2 (IKEv2) [1] protocol to protect the authentication procedure of EAP-SIM by encapsulating its packets. In this way the vulnerabilities of the EAP-SIM authentication method are eliminated. After the employment of IKEv2, a Virtual Private Network (VPN) tunnel is established that protects data transferred over the air interface. The tunnel, which is based on IPsec [11], ensures confidentiality, authentication and integrity of the data exchanged in the WLAN environment. The proposed scheme has minimal impact on the existing network infrastructure. The user is still authenticated by proving the possession of a SIM card, in order to get subscribed in his home network for billing and charging purposes. The proposed scheme requires only that each end-point of the established VPN tunnel must have the appropriate IPsec software.

The rest of this paper is organized as follows. In section 2, the EAP-SIM protocol is, briefly, analyzed presenting its vulnerable points as well as the identified risks from its use. Section 3 depicts the proposed security scheme that uses the IKEv2 protocol to carry EAP-SIM messages and the deployment of an IPsec-based VPN tunnel. Section 4 elaborates on a security analysis of the proposed scheme pointing its advantages. Finally, Section 5 contains the conclusions.

II. Background

A. *EAP-SIM protocol*

EAP-SIM incorporates two basic enhancements that eliminate known security weaknesses of the GSM/GPRS authentication and key agreement procedure. 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 authentication, which performs only user to network authentication. The authentication procedure of EAP-SIM involves the following functional entities: a mobile user, a wireless access point which acts like an Authentication Authorization Accounting (AAA) [10] client, an AAA server and the GSM/GPRS network. EAP-SIM uses two or three Kc keys of the GSM authentication triplets to generate a Master

Key (MK). From the MK key two other keys are generated: (a) the Master Session Key (MSK) for encryption purposes and (b) the K_auth key that is used for the derivation of a keyed Message Authentication Code (MAC) [9] over the RAND parameters of the GSM triplets. The AAA server generates this keyed MAC in order to authenticate itself to the mobile user.

B. EAP-SIM Weaknesses

Although EAP-SIM was designed to provide security enhancements to the GSM authentication, it does not meet its security goals [4]. If an attacker wants to authenticate himself to a mobile user and impersonate an AAA server, the only thing that he has to do is to generate a valid keyed MAC using a K_auth key. A valid MAC can be generated by possessing two or three Kc keys and the related RAND parameters of GSM authentication triplets, which can be obtained with one of the following ways:

1. Having physical access to a SIM card, it is easy to obtain any parameter of GSM triplets.
2. Using virus or other malicious piece of software, an adversary may mount an attack on the user platform in order to obtain triplets.
3. If the same SIM credentials are also used for GSM traffic, the triplets could be revealed in the GSM network.
4. An attacker could gain access to the communication between the AuC and the AAA server in the EAP-SIM authentication dialogue.

Thus, if eventually multiple GSM triplets are compromised; then, an adversary may impersonate a valid network and start an authentication session with the mobile user. The attacker can calculate a valid hashed MAC, as he possesses the RAND parameters, and he can generate the K_auth from the encryption keys Kc. Since there is no way for the user to understand that there is an attack, he authenticates the attacker as a legitimate network, based on the received valid MAC. The compromised GSM triplets can be used by an adversary to perform attacks as long as the permanent key Ki, which is employed to produce the triplets, remains the same and this could be for years.

Except for the above serious deficiency, there are still a lot of more that a malicious can exploit to attack to EAP-SIM. First, the mobile user is obligated to send his permanent identity IMSI (International Mobile Subscriber Identity) in clear text on the first connection with the authentication server. In such cases, the identity privacy feature can easily be compromised, since passive eavesdroppers may steal the identity of the user. In addition, due to the fact that EAP-SIM supports version negotiation, it is possible to downgrade the EAP-SIM version because EAP-SIM does not protect the messages that include the payloads for EAP-SIM method negotiation. Furthermore, the EAP-Request/Notification, EAP-Response/Notification (see [2]), EAP-Success and the EAP-Failure messages are not protected, enabling an attacker to send false notifications to the peer and mount denial of service attacks by spoofing these messages. Finally, EAP-SIM doesn’t offer ciphersuite negotiation.

III. PROPOSED SECURITY SCHEME

The identified weaknesses of the EAP-SIM authentication procedure may compromise end-users and network security, and threaten 3G-WLAN interworking architecture. To overcome these security weaknesses, an enhanced EAP-SIM authentication protocol, which is based on IKEv2, is proposed and the deployment of an IPsec-based VPN over the wireless environment is introduced. In the following, the proposed enhancements as well as the deployment of the enhanced protocol are described and analyzed.

A. Protocol Enhancements

IKEv2 [1] is a component of IP Security Protocol (IPsec) used for performing mutual authentication, and establishing and maintaining a Security Association (SA), which is a one-way relationship between a sender and a receiver that affords security services. A basic difference between IKEv2 and IKEv1 [7] is that the first supports legacy authentication methods, which enables the conveyance of the EAP-SIM messages in IKEv2 payloads. In other words, IKEv2 has the ability of using an EAP method, like EAP-SIM, for authentication purposes. In the proposed scheme, IKEv2 is used to encapsulate EAP-SIM messages protecting them during negotiation. The derived MSK key from the EAP-SIM procedure is used to authenticate the peer entities of the IKEv2 procedure. After a successful EAP-SIM authentication, the established IPsec_SA is used to deploy an IPsec-based VPN tunnel that protects users data.

Based on the 3G-WLAN networking architecture, the proposed mechanism involves the following functional entities: a mobile user, a NAS, a Certification Authority (CA), an AAA server, and, finally, the GSM/GPRS network (see figure 1). The mobile user is an EAP-SIM client and at the same time an IKEv2 client. On the other hand, the NAS must incorporate VPN server capabilities (for that reason it is called VPN enabled NAS) and must reply to the IKEv2 requests of the mobile user. The VPN enabled NAS is authenticated to the mobile user by using a certificate provided from the CA. Additionally, the VPN enabled NAS acts like an AAA client that transfers the EAP-SIM messages using the Radius protocol to the AAA server (see figure 1). Finally, the AAA server communicates with the GSM/GPRS network to obtain the GSM authentication triplets.

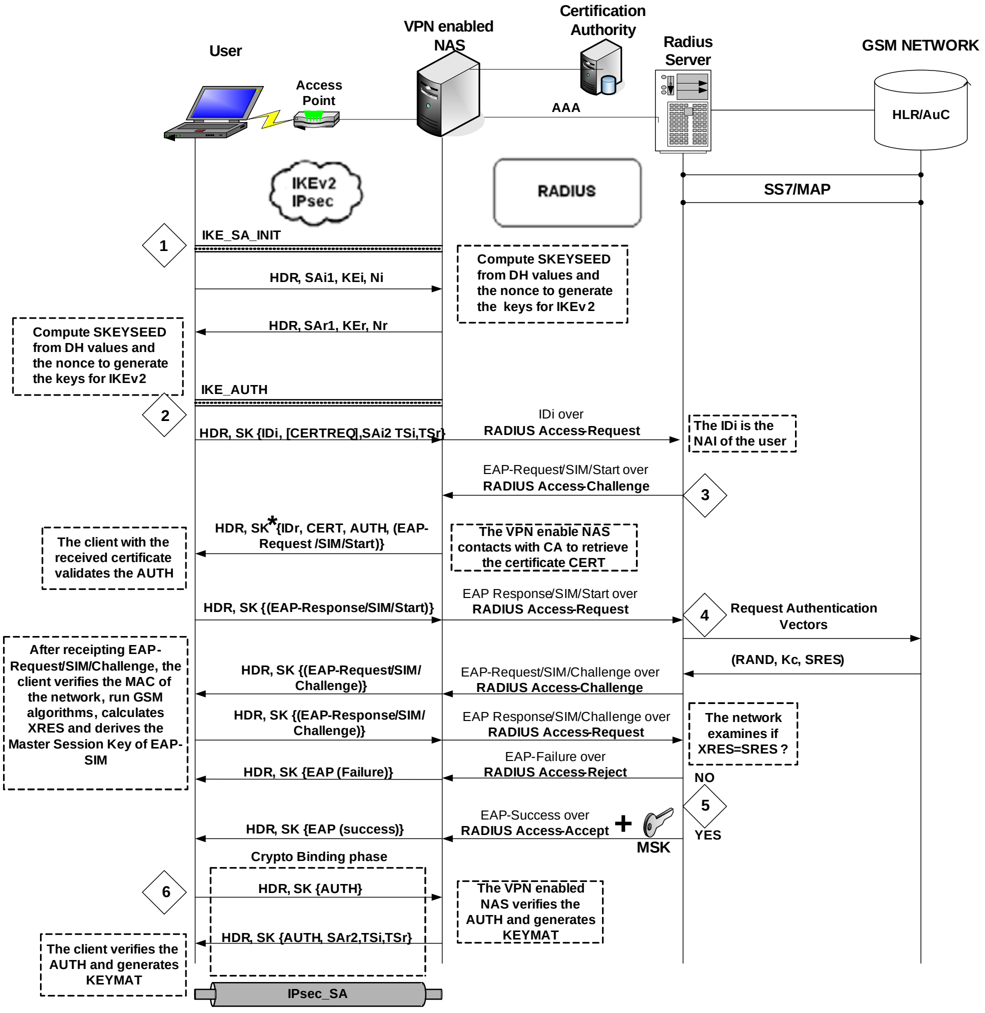
Since the IKEv2 is an application layer protocol, in contrast to EAP-SIM, which is a layer two protocol, the mobile user must initially obtain a temporary IP address, which can be used only for authentication purposes. In the sequel, whether the user is authenticated as a legitimate, he will be assigned from the VPN enabled NAS a permanent IP address that is used for Internet access. The permanent IP address is exchanged in an encrypted form within the configuration payload [1] of IKEv2. For the effective management of the IP addresses (temporary and permanent), the VPN enabled NAS has to maintain an Access Control List (ACL). This list defines the access privileges that each user obtains to the network, separating the users with temporary and privileged

IP addresses.

Except for the ACL, the VPN enabled NAS must also maintain a list that stores all the previously used RANDs. The existence of such a list may prevent an adversary to mount a replay attack by impersonating a rogue network. Although EAP-SIM does not allow reusing the RAND challenges in consecutive authentication exchanges and the AAA server is mandated to use fresh triplets, the user cannot check whether the triplets are fresh, since there is no practical mechanism that does this check. Therefore, the VPN enabled NAS should be enhanced to store and check the previously used RANDs. If a RAND parameter has been re-used, the VPN enabled NAS aborts the IKEv2 authentication procedure. The probability of a vector being accidentally repeated is practically negligible, because an individual RAND is 128-bits long.

B. *Authentication Procedure*

The authentication procedure of IKEv2, which creates an IPsec_SA, consists of two phases: (a) the IKE_SA_INIT and (b) the IKE_AUTH exchange, as shown in figure 1. The IKE_SA_INIT exchange (noted as step 1 in figure 1) consists of a single request and reply messages, which negotiate cryptographic algorithms, exchange nonces, and do a Diffie-Hellman exchange. In the context of this phase, four cryptographic algorithms are negotiated: (a) an encryption algorithm, (b) an integrity protection algorithm, (c) a Diffie-Hellman group, and (d) a pseudo-random function (prf). The prf is employed for the construction of keying material for all of the cryptographic algorithms used. The second phase, (i.e, IKE_AUTH exchange) authenticates the previous messages, exchanges identities and certificates, encapsulates EAP-SIM messages, and establishes an IPsec_SA (step 2-6 of figure 1). All the messages of IKEv2 include a header payload (HDR), which contains a Security Parameter Index (SPI), a version number, and security related flags. The SPI is a value chosen by the user and the VPN enabled NAS to identify a unique SA.


User
Access Point
VPN enabled NAS
Certification Authority
Radius Server
GSM NETWORK
HLR/AuC
AAA
IKEv2 IPsec
RADIUS
SS7/MAP
1
IKE_SA_INIT
HDR, SAi1, KEi, Ni
Compute SKEYSEED from DH values and the nonce to generate the keys for IKEv2
HDR, SAr1, KEr, Nr
Compute SKEYSEED from DH values and the nonce to generate the keys for IKEv2
IKE_AUTH
2
HDR, SK {IDi, [CERTREQ],SAi2 TSi,TSr}
IDi over RADIUS Access-Request
The IDi is the NAI of the user
EAP-Request/SIM/Start over RADIUS Access-Challenge
3
HDR, SK*{IDr, CERT, AUTH, (EAP-Request /SIM/Start)}
The VPN enable NAS contacts with CA to retrieve the certificate CERT
The client with the received certificate validates the AUTH
HDR, SK {(EAP-Response/SIM/Start)}
EAP Response/SIM/Start over RADIUS Access-Request
4
Request Authentication Vectors
(RAND, Kc, SRES)
After receipting EAP-Request/SIM/Challenge, the client verifies the MAC of the network, run GSM algorithms, calculates XRES and derives the Master Session Key of EAP-SIM
HDR, SK {(EAP-Request/SIM/ Challenge)}
EAP-Request/SIM/Challenge over RADIUS Access-Challenge
HDR, SK {(EAP-Response/SIM/ Challenge)}
EAP Response/SIM/Challenge over RADIUS Access-Request
The network examines if XRES=SRES ?
HDR, SK {EAP (Failure)}
EAP-Failure over RADIUS Access-Reject
NO
5
YES
HDR, SK {EAP (success)}
EAP-Success over RADIUS Access-Accept
+
MSK
Crypto Binding phase
6
HDR, SK {AUTH}
The VPN enabled NAS verifies the AUTH and generates KEYMAT
HDR, SK {AUTH, SAr2,TSi,TSr}
The client verifies the AUTH and generates KEYMAT
IPsec_SA

*The notation SK{ … } indicates that the content between brackets is encrypted and integrity protected

Figure 1 The enhanced EAP-SIM authentication scheme using IKEv2

At the start of the proposed mechanism (step 1 in figure 1), the user sends the SAi1, which denotes the set of cryptographic algorithms for the IPsec_SA that he supports, the KEi that is the Diffie-Hellman value, and a Ni value that represents the nonce (a random number at least 128 bits). The VPN enabled NAS responds with a message that contains its choice of cryptographic suite (SAr1), its value to complete the Diffie-Hellman exchange (KEr), and its nonce (Nr). At this point, both the user and the VPN enabled NAS can calculate the SKEYSEED value as follows:

$$SKEYSEED = prf((Ni \mid Nr), g \wedge ir)\ [1] \qquad (1)$$

where prf is the pseudorandom function negotiated in the previous messages, and g^ir is the shared secret key from the Diffie-Hellman exchange. The SKEYSEED value is used to calculate five other secret keys: SK_d used for deriving the keying material for IPsec_SA; SK_ai and SK_ar used as keys to the integrity protection algorithm of IKEv2; and, finally, SK_ei and SK_er used for encrypting all subsequent exchanges (see table 1). From these keys the mobile user uses the SK_d, the SK_ai and the SK_ei key, while the VPN enabled NAS uses the SK_d, the SK_ar and the SK_er key.

Table 1 The keys generated for IKEv2

SK_d = prf(SKEYSEED, Ni | Nr | SPIi | SPIr)
SK_ai = prf(SK_d, Ni | Nr | SPIi | SPIr)
SK_ar = prf(SK_ai, Ni | Nr | SPIi | SPIr)
SK_ei = prf(SK_ar, Ni | Nr | SPIi | SPIr)
SK_er = prf(SK_ei, Ni | Nr | SPIi | SPIr)

Finalizing the IKE_SA_INIT exchange, the IKE_AUTH exchange starts. As shown in the step 2 of figure 1, the user sends his identity (IDi), which could be in a Network Access Identifier (NAI) format, optionally, the CERTREQ payload, which is a list of its ”trust anchors”, i.e. the names of the CAs whose public keys he trusts, and the traffic selectors (i.e. TSi and TSr) to the VPN enabled NAS. These selectors allow the peers to identify the packet flows that require processing by IPsec. Additionally, the user indicates to the VPN enabled NAS that desires to use EAP-SIM authentication, by intentionally omitting the AUTH payload that regularly must send in this message. It is worth noting that the payload of this message is encrypted with the SK_ei key and integrity protected with the SK_ai key excluding the message header (HDR), as shown in figure 1. Next, the VPN enabled NAS forwards the user identity (IDi) to the Radius server.

Upon receiving the IDi, the Radius server initiates an EAP-SIM dialogue by sending to the VPN enabled NAS an EAP-Request/SIM/Start message encapsulated in a Radius packet (step 3 of figure 1). The VPN enabled NAS forwards to the mobile user the EAP-Request/SIM/Start message encapsulated in an IKEv2 message, which also includes the VPN enabled NAS id (IDr), its certificate (CERT), and the AUTH payload. The latter contains signed data and is used to authenticate the VPN enabled NAS to the mobile user. Similarly to the previous message, the payload of this IKEv2 message is encrypted with SK_er key and integrity protected with the SK_ar key except for the message header. The mobile user upon receiving the EAP-Request/SIM/Start message, he verifies the AUTH field by using the public key included in the certificate of the CERT payload, and answers by sending an EAP-Response/SIM/Start message encapsulated again in an IKEv2 message. From this point the IKEv2 messages contain only EAP-SIM payloads and they are encrypted and integrity protected just like the previous messages. The EAP-SIM exchange continues, normally, and the Radius server communicates with the HLR to get the GSM triplets (step 4 of figure 1). The authentication procedure proceeds until an EAP-SUCCESS (or an EAP-FAILURE in case of a failure) is sent from the Radius server to the VPN enabled NAS, which ends the EAP-SIM dialogue. Together with the EAP-SUCCESS packet, the MSK key is sent to the VPN enabled NAS via the Radius protocol, as shown in figure 1 (step 5).

After finishing the EAP-SIM negotiation, the final step (step 6) of the proposed security scheme creates an IPsec_SA. In this step, both the VPN enabled NAS and the mobile user generate an AUTH payload calculated as:

$$\begin{aligned} AUTH = prf(&prf(MSK\ of\ EAP-SIM, "key\ pad \\ &for\ IKEv2"), <message\ octets>) \end{aligned} \qquad (2)$$

where the "Key Pad for IKEv2" is a set of 17 ASCII characters. Both the VPN enabled NAS and the user send each other the AUTH payload for mutual authentication. The VPN enabled NAS together with the AUTH payload sends also its traffic selector payloads TSi and TSr, and the SAr2 payload, which contains the cryptographic suit for IPsec_SA. It must be noted that an SA is a one way relationship between a sender and a receiver, and in cases where a peer relationship is needed, for two way secure exchange, then, two SAs are required. After the establishment of IPsec_SA, the keying material (KEYMAT) of this SA is generated as follows:

$$KEYMAT = prf(SK\_d, Ni \mid Nr) \qquad (3)$$

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 used to generate the keys that the IPsec protocol uses for its security purposes.

C. IPsec-based VPN Deployment

After the completion of the authentication procedure of the proposed security scheme, a pair of IPsec_SAs has been established between the mobile user and the VPN enabled

[1] | means string concatenation

NAS. This pair sets up a bidirectional VPN tunnel between them that allows secure data exchange over the air interface. At the same time, the mobile user has been subscribed to the GSM/GPRS network for charging and billing purposes with the EAP-SIM protocol. The VPN tunnel runs on top of the wireless link and extends from the user's computer to the VPN enabled NAS behind the AP, as shown in figure 2.

The deployed VPN tunnel is based on IPsec, which is one of the strongest security frameworks available in networking. The IPsec protocol is configured in tunnel mode, since the proposed security scheme aims at protecting both the payload and the IP header of the transmitted packets over the air interface. Furthermore, the deployment of the Encapsulation Security Payload (ESP) [8] protocol is considered more advantageous in this architecture, given that ESP can provide confidentiality and integrity protection as well.

A vital issue of deploying VPN in a WLAN environment is mobility. When a mobile user moves from one AP to another, its IP address changes under the control of the VPN enabled NAS, and thus the IPsec SAs must be re-established using IKEv2. However, creating new SAs implies a repetition of expensive calculations and IKEv2 messages exchange. To avoid this overhead, a mechanism for updating the IP addresses of existing SAs is needed. Such a mechanism is provided by the Mobility and Multihoming IKE (MOBIKE) [5],[6] protocol, which enables a mobile user with an established VPN to move from one access network to another, without re-establishing the SAs. The MOBIKE protocol runs on the top of IKEv2. For application on the proposed security scheme, the mobile user and the VPN enabled NAS have to incorporate the MOBIKE functionality and execute it when the mobile user moves.

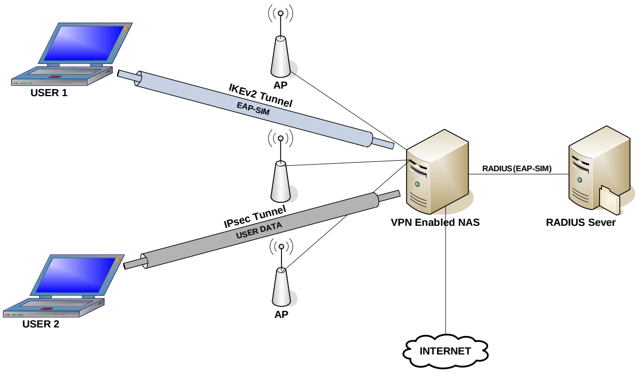


Figure 2 The IPsec-based VPN deployment

IV. Security Analysis

The proposed scheme enhances the authentication procedure of EAP-SIM, improves its security services and extends the usability of VPNs to WLANs. In the following, a qualitative evaluation of this scheme is presented, focusing on the particular advantages as well as the potential drawbacks and considerations of such security services in a WLAN environment.

A. Advantages

The main advantage of the proposed security scheme is that it enhances the authentication procedure of the EAP-SIM protocol by employing the authentication mechanism of IKEv2. Thus, the identified security weaknesses of the EAP-SIM authentication procedure and the accompanied vulnerabilities described before are eliminated. Instead, the strong authentication procedure of IKEv2 is employed. More analytically, the mobile user and the AAA server are authenticated to each other by using protected exchanges of the EAP-SIM protocol, whereas the VPN enabled NAS is authenticated to the mobile user by using its certificate. In addition, the VPN enabled NAS maintains a list that holds all the previously used RANDs. Thus, there is no way now for an adversary to mount a replay attack by stealing a GSM authentication triplet and impersonating an AAA server. In summary, all the entities that participate in the proposed scheme are authenticated, mutually, and at the same time, the possibility of performing replay attacks against the EAP-SIM authentication procedure is eliminated.

Encapsulating EAP-SIM messages in IKEv2 provides identity confidentiality services, since the IMSI is encrypted and integrity protected within the IKEv2 protocol. All vital information for network security and operation transmitted by the EAP-SIM Notification packets (EAP-Request/Notification and EAP-Response/Notification) are also confidentially protected. Furthermore, because of the fact that the EAP-Success and EAP-Failure messages are exchanged in a protected form, no denial of service attacks can be mounted by spoofing these packets.

Except for improving of the level of security supported, the employment of IKEv2 protects against various attacks on the wireless link. Since the IKEv2 does not support a username password mechanism, it is not vulnerable to dictionary or social engineering attacks, assuming that the key used for digital signature is not derived from a low entropy source. Furthermore, the mobile user and the VPN enabled NAS may refresh the keying material by initiating a new IPsec_SA exchange, when they wish to or when it is necessary. Specifically, they can exchange new Diffie-Hellman values, in order to exploit the advantages of "Perfect Forward Security" (PFS). PFS has a specific advantage when a connection is closed, since each endpoint forgets not only the keys used by the connection, but also any data that could be used to re-compute those keys. Additionally, the IKEv2 method offers an optional mechanism for DoS protection, which uses cookies and keeps the responder stateless when it receives the first IKEv2 message. However, when the DoS protection is activated, an additional round trip of message exchange is performed.

Another advantage of the proposed security scheme is related to the fact that the IKEv2 has the capability of making an explicit cryptographic binding in order to avoid man in the middle attacks (step 6 in figure 1). Reference [3] presents that when a legacy client authentication protocol, like EAP-SIM, runs inside a secure tunnel, it forms a protocol that is vulnerable to man in the middle attacks. This security hole is due to the fact that the legitimate user and the VPN enabled NAS have no way to verify that their peer in the authentication procedure, is the entity at the other end of the outer tunnel. An effective solution of this problem is to perform cryptographic binding [3], which is an authentication step to verify that the entities possessing the master session keys are indeed the legitimate user and server. That's why the mobile user and the VPN enabled NAS generate the AUTH payloads from the MSK of EAP-SIM and the prf of the IKEv2 (see equation (2)), and, then, they send to each other the AUTH payload in order to achieve the binding between the inner protocol (EAP-SIM) and the outer protocol (IKEv2) for verification purposes.

Finally, after the creation of the IPsec_SA between the mobile user and the VPN enabled NAS, an IPsec based VPN tunnel has been established between them that protects data sent over the air. IPsec provides security at the network layer and facilitates the authentication of the communicating entities. Compared to other security mechanisms, IPsec offers many architectural advantages and remarkable flexibility. The details of network security are usually hidden from applications, which therefore automatically and transparently take advantage of whatever network-layer security services their environment provides. A reasonable question is that whether IPsec can be applied over wireless links, which are characterized by limited resources. Reference [12] examines the processing and the communication overheads of IPsec, evaluates the feasibility of deploying it on handheld devices and wireless networks, and gives a positive answer to the previous question.

B. *Drawbacks*

The main drawback of the proposed security scheme is related to the fact that the existing network infrastructure that supports EAP-SIM authentication should be enhanced. Specifically, the mobile devices and the traditional NAS should be enhanced with the appropriate software that supports IKEv2 and IPsec. The enhanced NAS (i.e., VPN enabled NAS) should also maintain a list (i.e., ACL) to separate the temporary IP addresses from the privileged addresses. Moreover, the proposed scheme requires the deployment of PKI that facilitates the authentication of the VPN enabled NAS to mobile users.

Regarding network performance, the encapsulation of EAP-SIM messages 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 scheme supports.

Finally, the deployment of an IPsec-based VPN between a mobile terminal and the VPN enabled NAS influences the data transmission over the radio interface. However, as thoroughly presented in reference [12], the IPsec based VPN does not significantly increase the time required for transmission over the radio interface, and does not considerably reduce its throughput.

V. Conclusions

This paper has presented an enhanced EAP-SIM authentication scheme for securing WLAN. The proposed scheme enhances the authentication procedure of EAP-SIM, improves its security services, and extends the usability of VPNs to WLANs. More specifically, the authentication procedure of EAP-SIM is considerably enhanced by employing the authentication mechanism of IKEv2. Thus, the identified security weaknesses of the EAP-SIM authentication procedure and the accompanied vulnerabilities are eliminated. Encapsulating EAP-SIM messages in IKEv2 messages, all the vital information carried by EAP-SIM is protected preventing from spoofing and social engineering attacks. In addition, the proposed scheme has the capability of making an explicit cryptographic binding that counteracts against man-in-the-middle attacks. After the completion of the enhanced authentication procedure, an IPsec-based VPN tunnel is established between the negotiating end-points (i.e., the mobile user and the NAS). This tunnel ensures confidentiality, authentication and integrity of the data exchanged in the WLAN environment.

References

[1] C.Kaufman, “Internet key exchange (IKEv2) protocol” Internet draft, draft-ietf-ipsec-ikev2-17.txt, Sep 2004.

[2] H. Haverinen, “EAP-SIM Authentication,” Internet draft, draft-haverinen-pppext-eap-sim-16, Dec 2004

[3] N. Asokan, V. Niemi and K. Nyberg, “Man in the Middle in Tunneled Authentication Protocols”, 11th International Workshop, Cambridge, UK, published in Springer-Verlag LNCS series, April 2003.

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

[5] T. Kivinen, H, Tschofenig, “Design of the Mobike Protocol”, draft-ietf-mobike-design-05.txt, Nov 2005.

[6] P. Eronen, “IKEv2 Mobility and Multihoming Protocol (MOBIKE)”, draft-ietf-mobike-protocol-06.txt, Nov 2005.

[7] D. Harkins and D. Carrel. “The Internet key exchange (IKE)”, RFC 2409, Nov 1998.

[8] S. Kent R. Atkinson, “IP Encapsulating Security Payload (ESP)”, RFC 2406, Nov 1998.

[9] H. Krawczyk, M. Bellare, R. Canetti, “HMAC: Keyed-Hashing for Message Authentication”, RFC 2104, Feb 1997.

[10] C.de Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence, “Generic AAA Architrecture”, RFC 2903, Aug 2000.

[11] S. Kent R. Atkinson, “Security Architecture for Internet Protocol”, RFC 2401, Nov 1998.

[12] 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, [In Press 2006].