A SECURITY BINDING FOR EFFICIENT AUTHENTICATION IN 3G-WLAN HETEROGENEOUS 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 one-pass EAP-AKA authentication procedure for the 3G-WLAN heterogeneous networks, which reduces significantly the authentication signaling traffic without compromising the provided level of security of the 3G-WLAN networks.

I. BACKGROUND

A. Two-Pass EAP-AKA Authentication

The security architecture of the 3G-WLAN heterogeneous networks, which is proposed in 3GPP 33.234, specifies that a WLAN user, in order to get access to the 3G packet switched services or the public internet through the 3G Public Land Mobile Network (PLMN), he must follow a two-pass EAP-AKA authentication procedure. The latter includes two discrete authentication steps, which are presented in Fig. 1 and analyzed below:

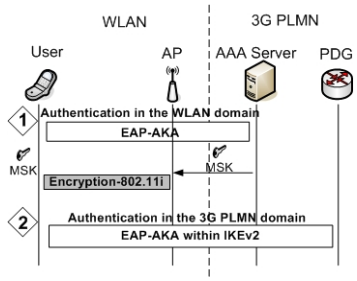

Fig. 1 Two-Pass EAP-AKA Authentication

Initial authentication. The user and the WLAN are authenticated each other using EAP-AKA. This authentication step involves the user, an Authentication, Authorization, Accounting (AAA) client that is actually a wireless Access Point (AP), and the AAA server that may obtain authentication information (i.e., 3G authentication vectors) from the Home Subscriber Server (HSS)/Authentication Centre (AuC) of the 3G PLMN, where the user is subscribed. After the execution of EAP-AKA, the user and the AAA server share the EAP-AKA *Master Key* (*MK*) key, which is used for the execution of the EAP-AKA fast re-authentication procedure. In addition, the *MK* is used to generate the EAP-AKA Master Session Key (*MSK*) between the user and the AAA server. The latter forwards to the wireless AP (see Fig. 1) the *MSK key*, which is employed in the 802.11i security framework for the generation of the WLAN session keys. After a successful EAP-AKA authentication, the user obtains a local IP address to execute the IKEv2 protocol (i.e., next authentication step).

Second authentication. As shown in Fig. 2, in the second authentication step the user and the entity called Packet Data Gateway (PDG) that allows the user to access the 3G packet switched services, execute the IKEv2 negotiation protocol, which encapsulates EAP-AKA for authenticating the user and the 3G PLMN. At the end of this phase the user obtains from the PDG a global IP address, called Remote IP address, which is used for access to the 3G packet switched services or the public Internet via the 3G PLMN. After a successful execution of IKEv2 an IPsec-based Virtual Private Network (VPN) tunnel is deployed between the user and the PDG, which is based on the Encapsulation Security Payload (ESP) protocol, to provide confidentiality and integrity to the data exchanged between them.

B. Motivation for Improving the Two-Pass EAP-AKA Authentication

The analyzed two-pass EAP-AKA authentication procedure involves a double execution of EAP-AKA. The first is carried out to register the user in the WLAN domain, while the second registers him in the 3G PLMN. Therefore, the two-pass EAP-AKA authentication procedure is not efficient, since it introduces a duplicated authentication overhead.

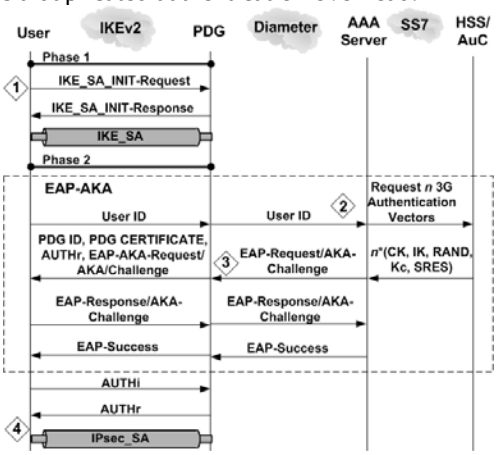

Fig. 2 EAP-AKA within IKEv2 (two-pass EAP-AKA authentication)

This overhead is related to the exchange of messages that cause delays in users' authentication and consume radio resources, as well as to the computational processing at the level of mobile devices, which may induce energy consumption issues. It has to be noted that the mobile devices usually are characterized by low computational capabilities and limited energy power.

II. ONE-PASS EAP-AKA AUTHENTICATION

A. Outline

To address the duplicated authentication overhead of the two-pass EAP-AKA authentication procedure, this paper proposes a one-pass EAP-AKA authentication for the 3G-WLAN heterogeneous networks. The proposed procedure reduces the authentication traffic, compared to the two-pass EAP-AKA authentication, without compromising the provided level of security.

Similarly to the two-pass EAP-AKA authentication, the proposed one-pass EAP-AKA authentication procedure includes two authentication steps. In the first step, the user and the WLAN are authenticated each other performing EAP-AKA. In

This work has been supported in part by the project CASCADAS (IST-027807) funded by the FET Program of the European Commission and the project NoE CONTENT (IST-384239)

addition, in this step the user and the AAA server generate and store the *MK* key, which is used in the next step. In the second step, the user is authenticated to the 3G PLMN domain by executing pure IKEv2 that omits the encapsulation of EAP-AKA. In this step the authentication of the negotiating end-points (i.e., the user and the PDG) is based on the *MK* key, which is generated in the previous step from the execution of EAP-AKA. Thus, the proposed one-pass EAP-AKA authentication combines the first and the second authentication step by making a security binding between them. This binding eliminates the requirement for duplicated execution of EAP-AKA, reducing the overall authentication overhead.

The proposed one-pass EAP-AKA authentication procedure has minimal impact on the existing 3G-WLAN network infrastructure and functionality. The only requirement is that the PDG must be capable of retrieving the *MK* key, generated in the initial EAP-AKA authentication, from the AAA server. As mentioned previously, the AAA server stores the *MK* key and maintains a list which associates the user's identities with the *MK* key. Thus, the PDG can retrieve the *MK* key from the AAA server using the Diameter protocol. It is worth noting that there is a trusted relationship between the PDG and the AAA server, since there is a pre-established IPsec tunnel between them that protects the exchange of Diameter messages. In addition, this tunnel protects the conveyance of the *MK* key during the proposed one-pass EAP-AKA authentication execution.

B. Authentication Procedure

Since the initial authentication step of the proposed one-pass EAP-AKA authentication is the same with the one of the two-pass, we do not elaborate it further. Thus, we assume the followings: i) a user has performed a successful initial authentication in the WLAN domain using EAP-AKA; ii) both the user and the AAA server have stored the *MK* key generated during EAP-AKA; and iii) the user and the wireless AP apply encryption to the data conveyed over the radio interface using the WLAN session keys.

During the second authentication step of the proposed procedure, the user and the PDG are authenticated using the IKEv2 protocol. In addition, they establish a VPN tunnel that protects the data conveyed between them. The IKEv2 is executed in two phases (i.e., phase 1 and phase 2). In phase 1 the user and the PDG establish a bidirectional IKE_SA that protects all the subsequent IKEv2 messages. To initiate this phase, the user sends to the PDG the SAi1 (message 1-Fig. 3), which denotes the set of cryptographic algorithms for the IKE_SA that he supports, the KEi that is the Diffie-Hellman value, and a Ni value that represents the nonce. The nonce is used as input to the cryptographic functions employed by IKEv2 to ensure liveliness of the keying material and protect against replay attacks. The PDG answers with a message (message 2-Fig. 3) 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 PDG share a bidirectional IKE_SA that provides confidentiality and integrity services to the following IKEv2 messages.

After the establishment of the IKE_SA, the second phase of IKEv2 authenticates the peers and establishes an IPsec_SA. To achieve this both the user and the PDG calculate a hash value (i.e, the AUTHi and the AUTHr payloads, respectively), using the *MK* key generated during the execution of EAP-AKA in the initial authentication step. Then, they send to each other the AUTHi and AUTHr payloads for verification achieving the security binding between the initial authentication step (i.e., the execution of EAP-AKA in the WLAN domain) and the second authentication step (i.e., the execution of IKEv2 in the 3G PLMN domain).

More specifically, in the second phase of IKEv2, the user sends to the PDG a message that includes his identity, the SAi2 payload that contains the chosen cryptographic suit for the IPsec_SA that the user supports, the traffic selectors (TSi and TSr) that allow the peers to identify the packet flows that require processing by IPsec, and the Configuration Payload Request (CP-Request) that is used to obtain a Remote IP address from the PDG and get access to the 3G-PLMN. The user also includes in this message the AUTHi payload, which is a Hash Message Authentication Code (HMAC) over the first IKEv2 message (i.e., message 1-Fig. 3) using the stored *MK* key.

After receiving this information, the PDG forwards to the AAA server the user identity (IDi) including a parameter, which indicates that the authentication is being performed for access to the 3G PLMN. This will facilitate the AAA server to distinguish between authentications for WLAN access or for 3G PLMN access. Based on the user's identity, the AAA server retrieves the appropriate *MK* key and sends it to the PDG via the Diameter protocol (message 4 -Fig. 3). Recall that the *MK key* is conveyed in a secure manner, since there is a pre-established IPsec tunnel between the PDG and the AAA server.

Upon receiving the *MK* key, the PDG verifies the AUTHi payload in order to authenticate the user. In the sequel, it generates the AUTHr payload by computing a HMAC over the second IKEv2 message (i.e., message 2 in Fig. 3) using the obtained *MK* key and sends it to the user. Except for the AUTHr payload, this message also includes the PDG's identity that identifies the provided 3G services, the traffic selector payloads (TSi and TSr), the SAr2 payload that contains the chosen cryptographic suit for the IPsec_SA that the PDG supports, and the assigned user's Remote IP address that is included in the Configuration Payload Reply (CP-REPLY) payload. Finally, the user verifies the AUTHr payload using the *MK* key and authenticates the PDG. At this point the authentication in the 3G PLMN is completed and an IPsec_SA is established between the user and the PDG that provides security services (see Fig. 3).

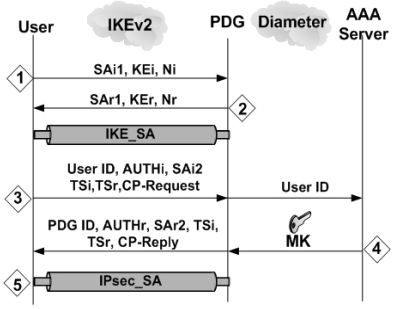

Fig. 3 IKEv2 execution (one-pass EAP-AKA authentication)

III. CONCLUSIONS

The proposed one pass EAP-AKA authentication procedure reduces significantly the authentication burden compared to the two-pass EAP-AKA without compromising the provided level of security. The proposed procedure combines the first and the second authentication step by making a security binding between them. This binding eliminates the need for duplicated execution of EAP-AKA, reducing the overall authentication overhead. The proposed one-pass EAP-AKA procedure has minimal impact on the existing 3G-WLAN network infrastructure and functionality.