Computer Communications 33 (2010) 1682–1694

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Privacy-enhanced fast re-authentication for EAP-based next generation network

F. Pereniguez [a,*], G. Kambourakis [b], R. Marin-Lopez [a], S. Gritzalis [b], A.F. Gomez [a]

[a] Department of Information and Communications Engineering (DIIC), University of Murcia, Facultad de Informatica, Campus de Espinardo S/N, Murcia, Spain
[b] Laboratory of Information and Communication Systems Security, Department of Information and Communication Systems Engineering, University of the Aegean, Samos GR-83200, Greece

ARTICLE INFO

Article history:
Available online 24 February 2010

Keywords:
EAP
Fast re-authentication
Next generation networks
Privacy
Seamless handoff

ABSTRACT

In next generation networks one of the most challenging issues is the definition of seamless and secure handoffs in order to assure service continuity. In general, researchers agree on the use of EAP as an authentication framework independent of the underlying technology. To date, efforts have focused on optimizing the authentication process itself, leaving out other relevant but sometimes important aspects like privacy. In this paper we present a solution that provides a lightweight authentication process while preserving user anonymity at the same time. The goal is to define a *multi-layered pseudonym* architecture that does not affect the fast re-authentication procedure and that allows a user to be untraceable. Taking as reference our previous work in fast re-authentication, we describe the extensions required to support identity privacy. Moreover, results collected from an implemented prototype, reveal that the proposed privacy-enhanced fast re-authentication scheme is attainable without significant cost in terms of performance in 4G foreseeable environments.

1. Introduction

During recent years, users have shown high interest in the *always connected* experience. To support the combination of mobility and access to network services anywhere and anytime, communication networks are moving towards an *all-IP* network configuration, integrated by an IP-based network core and a set of access networks based on different wireless technologies. This scenario, which represents the 4*th* generation (4G) of mobile communications, enables the convergence of different heterogeneous wireless access networks in order to combine all the advantages offered by each link layer technology per se.

For the provision of high-quality multimedia services in the 4*th* generation (4G) of mobile communications, one of the most important challenges lies in reducing the time devoted to executing the network access control when the mobile user changes the point of attachment to the network. By decreasing this time, active communications can be re-established faster and therefore the perceived quality by the end-user can be significantly improved. One important factor that is part of the network access control is the authentication process required by network operators in order to control that only legitimate users are able to employ the operator's resources. A common way of performing this process in wireless networks has been guaranteed by the deployment of the so-called *Extensible Authentication Protocol* (EAP) [1]. The success of this protocol has been motivated by three important aspects: flexibility, wireless technology independence and integration with AAA infrastructures.

However, EAP has shown some drawbacks when a mobile scenario is taken into account. Typically, an EAP authentication lasts a considerable time and involves multiple message exchanges [2]. Moreover, these authentication messages have to travel to the user's home domain (HD), which could be situated far from the point of attachment to the network. Furthermore, this process is usually performed each time the mobile user changes the point of attachment during a *handoff*. Consequently, the resulting authentication mechanism is extremely inefficient. To solve this problem, researchers agree that is necessary to define a fast re-authentication process [3] that involves a *local re-authentication server* placed near the mobile user. In particular, it has been argued [4] that a fast and secure three-party key distribution process seems to be a more appropriate model for achieving this goal.

Another challenging issue associated with heterogeneous wireless networks is the privacy of the end-user. The nature of wireless networks allows a malicious user to eavesdrop or capture messages from any active communication that takes place under its coverage area. As a consequence, among other implications, this situation enables the user's activity to be monitored [5]. For this reason, privacy is a serious concern for both emerging applications and mobile users in future wireless networks. In fact, the protec-

* Corresponding author. Address: Department of Information and Communications Engineering (DIIC), University of Murcia, Facultad de Informatica, Campus de Espinardo S/N, 30100 Murcia, Spain. Tel.: +34 868 88 78 82; fax: +34 868 88 41 51.
E-mail addresses: pereniguez@um.es (F. Pereniguez), gkamb@aegean.gr (G. Kambourakis), rafa@um.es (R. Marin-Lopez), sgritz@aegean.gr (S. Gritzalis), skarmeta@um.es (A.F. Gomez).

0140-3664/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2010.02.021

tion of user's privacy may become a sine qua non for the so-called *Next Generation Networks* (NGN), since without privacy-preserving mechanisms in place, the end-user can be easily tracked and profiled in the mid or long term. Thus, the user is left defenseless to spamming and/or other related threats that violate his private sphere.

In general, privacy is a complex concept that affects aspects such as location, identification and authentication [6]. While location privacy requires that the location of a mobile user is untraceable to unauthorized parties (including the network), identification privacy mandates users anonymity, except by authorized parties. As we can see, these types of privacy are interrelated. If the user's identity is private, then location data is useless. At the same time, both types of privacy strongly depend on the authentication process, where user permanent identity must be exchanged. If the authentication mechanism does not have an adequate level of privacy to protect identification related data, the location can be revealed to unauthorized third parties.

Given these problems, this paper presents a novel and simple multi-layered architecture for pseudo-random pseudonym generation that offers a privacy-preserving mechanism for fast re-authentication processes in EAP-based NGN. In particular, to show the benefits of our proposal, we apply our solution on our previous work [7] which proposes a secure three-party protocol named 3PFH, especially adapted for performing fast network access in EAP-based wireless networks. As we will show, our solution is even applicable when the handoff takes place between different administrative domains (e.g., different network operators), regardless of the wireless technologies deployed. Additionally, using several real scenarios, we demonstrate that the overload imposed by the privacy-enhanced solution is negligible in comparison with the non-privacy case.

The remainder of the paper is structured as follows: the next section offers the necessary background to understand the proposal. Section 3 presents the proposed *multi-layered pseudonym* architecture together with the required extensions to the 3PFH protocol to support our solution. In Section 4, we provide some implementation details and information about the deployed testbed that implements the privacy framework. In Section 5, over different scenarios, we further demonstrate that the privacy extensions require an insignificant overload and, therefore, their use does not suppose an additional latency during the re-authentication process. Section 6 shows relevant related work. Finally, Section 7 concludes the paper and provides some future directions.

2. Background

We provide here some basic concepts required to understand the context of application of our proposal. In particular, we present a brief overview of EAP and the basics of our secure three-party protocol (3PFH) so as to understand how it has been extended with our multi-layered pseudonym architecture.

2.1. EAP authentication in next generation networks

The *Extensible Authentication Protocol* (EAP) [1] proposes a framework that enables a user (called *EAP peer*) to execute an authentication protocol (*EAP method*) against an authentication server (called *EAP server*) through an *EAP authenticator* which merely forwards packets between the EAP peer and EAP server. While the EAP authenticator is typically placed in the *Network Access Server*, the EAP server can be co-located with the EAP authenticator (*standalone configuration*) or with a backend AAA server (*pass-through configuration*). In order to deliver EAP messages, an *EAP lower-layer* is used to transport the EAP packets between the EAP peer and the EAP authenticator. Additionally, when it is necessary to contact a backend AAA server, an AAA protocol (such as RADIUS [8] or Diameter [9]), is used for the same purpose between the EAP authenticator and the AAA server.

The authentication process starts when the authenticator requests the peer's identity through an *EAP Request/Identity* message. The peer answers with an *EAP Response/Identity* that contains its identity, represented using the *Network Address Identifier* (NAI) format [10]. After several exchanges of EAP Request and Response messages between the peer and EAP server, a successful EAP authentication finishes with an EAP Success message and the provision of keying material [11]: the *Master Session Key* (MSK) and the *Extended Master Session Key* (EMSK).

However, a typical EAP authentication may require several exchanges and must be executed each time the peer changes to a new authenticator. Furthermore, typical deployments require contacting the EAP server located in the peer's HD, which may be far from the EAP authenticator, especially when the peer is visiting a domain. To address all these problems, the authors have designed a novel approach based on a secure three-party protocol named 3PFH [7] and a companion transport based on a new EAP method named EAP-FRM [12]. Nevertheless, the important aspect of user privacy during authentication process was not addressed in these previous works.

2.2. The three-party protocol for fast handoff (3PFH)

The 3PFH protocol is composed by four main exchanges, as Fig. 1 depicts.

As can be observed, 3PFH is executed between three entities namely A, B and S. The protocol assumes that A and S share a symmetric key K_{AS}. This key is dynamically derived from a key hierarchy started from the EMSK exported during a full EAP authentication (or EAP re-authentication) involving A (acting as EAP peer) and S (acting as EAP server). This process is carried out in the so-called *bootstrapping phase*, which usually happens when the mobile gets network access for the first time or when the EMSK lifetime has expired. Similarly, it is also assumed that a pre-established key K_{BS} is only known by B and S.

Fig. 2 shows how 3PFH is used in conjunction with the transport EAP-FRM [12] to achieve a complete, fast network access solution. Without loss of generality, we assume that the EAP server and fast re-authentication server (named KDS in the 3PFH context) are implemented over the same AAA server. In particular, Fig. 2(a) summarizes the case where the EAP peer already shares a key K_{AS} with a local server and roams between different EAP authenticators under the same server (*intra-KDS handoff case*). Conversely,

1. A $\Rightarrow$ B: A_{id},$\{N_A, SEQ_{AS}, B_{id}\}_{K_{AS}}$
2. B $\Rightarrow$ S: B_{id},$\{N_B, A_{id}\}_{K_{BS}}$,A_{id},$\{N_A, SEQ_{AS}, B_{id}\}_{K_{AS}}$
3. S $\Rightarrow$ B: $\{A_{id}, B_{id}, N_A, N_B, N_S\}_{K_{AS}}$,$\{A_{id}, B_{id}, N_A, N_B, N_S, K_{AB}\}_{K_{BS}}$
4. B $\Rightarrow$ A: $\{A_{id}, B_{id}, N_A, N_B, N_S\}_{K_{AS}}$

where

- A, B are the entities to which a key is distributed;
- S is key distribution server (KDS) which acts as fast re-authentication server;
- X_{id} denotes the identity of entity X;
- $\{X\}_K$ refers to X encrypted with key K providing confidentiality and integrity;
- K_{XY} refers to a symmetric key shared between parties X and Y;
- N_X refers to pseudo-random number acting as nonce and provided by the entity X;
- SEQ_{XY} is a sequence number maintained by parties X and Y;

Fig. 1. Typical 3PFH execution.