3-Party Approach for Fast Handover in EAP-Based Wireless Networks

Rafa Marin, Pedro J. Fernandez, and Antonio F. Gomez

Dept. de Ingeniería de la Información y las Comunicaciones,
New Faculty of Computer Science , Campus de Espinardo, Murcia, Spain
{rafa,pedroj.fernandez,skarmeta}@dif.um.es

Abstract. In this paper we present a solution for reducing the time spent on providing network access in mobile networks which involve an authentication process based on the *Extensible Authentication Protocol*. The goal is to provide fast handover and smooth transition by reducing the impact of authentication processes when mobile user changes of authenticator. We propose and describe an architecture based on a secure 3-party key distribution protocol which reduces the number of roundtrips during authentication phase, and verify its secure properties with a formal tool.

Keywords: Fast handover, security, key distribution, authentication.

1 Introduction

During these recent years, wireless networks have become widely prevalent. Due to their high proliferation, the deployment of wireless access networks is becoming a reality. At the same time, the wireless access providers are showing increasing interest in controlling the network access through authentication and authorization processes, in order to guarantee that only authenticated wireless nodes are allowed to communicate with external hosts in both directions. Traditionally, this problem has been solved through the deployment of *Authentication*, *Authorization* and *Accounting* (AAA) infrastructures [1]. However, the authentication and network control access are time-consuming processes which can last several hundreds of milliseconds with the corresponding high delays and packet loss which affect negatively the quality of the on-going communications. In this way, there is an increasing demand for studying a solution which achieves the goal of reducing the impact of authentication and network access control in mobile users.

Typically, authentication in wireless networks is based on the *Extensible Authentication Protocol* (EAP) [2], which provides a flexible way to perform authentication through the so-called *EAP authentication methods*. However, the EAP method execution is also a time-consuming process [3]. In fact, it involves several round trips between two parties: the EAP peer (the mobile node) and the EAP server (usually an AAA server), which indeed may be placed far from the EAP peer.

R. Meersman and Z. Tari et al. (Eds.): OTM 2007, Part II, LNCS 4804, pp. 1734–1751, 2007.

In order to reduce the latency introduced by the EAP authentication during handover, the *Internet Engineer Task Force* (IETF) has designated the *HandOver KEYing Working Group* (HOKEY WG) to provide a solution which allows to solve this problem. The basic idea consists on securely distributing specific keys between the mobile node (the EAP peer) and the access device from a trusted server, without running lengthy full EAP authentications. The distributed key material will eventually serve for the establishment of security associations between the mobile node and the access device. Thus, this key distribution process involves three parties: the EAP peer, the access device and the server. However, EAP follows a two-party model [4] since it involves the EAP peer and the EAP server. This is valid for mutual authentication but turns out inappropriate for key distribution between three parties [5]. Even so, following this traditional EAP two-party model for key distribution, the IETF, through the HOKEY WG, is trying to standardize the protocol ERP [6]. This alternative provides a fast re-authentication process between the EAP peer and the EAP server in a single round trip at the cost of heavy modifications on the existing EAP deployments. However, as explained, this solution has inherited the EAP model for key distribution, that is, a two-party model which is incomplete in order to a wider problem such as the key distribution between the three parties involved during mobile handover.

Another parallel alternative called EAP-HR [7] has been proposed and it also reduces the number of round trips as ERP does. Although it modifies the EAP stack as well, its design impacts EAP in less degree. Interestingly, EAP-HR has in mind a three party model but it fails to design the secure 3-party protocol allowing a replay attack (e.g. message 3 does not include any nonce or timestamp to prevent this attack). On the other hand, in parallel to ERP, the HOKEY WG is trying to standardize a framework [8] for key distribution based on a 3-party protocol between different entities involved during handover [1]. This framework does not focus in the handover process itself since this task is delegated to the ERP proposal. However, again the 3-party key distribution protocol (which has been inherited from EAP-HR proposal) fails to provide a secure 3-party key distribution protocol.

Taking into account this problematic, this paper presents a solution and an architecture for handover keying based on a three party (*3-party*) key distribution model. The approach improves and complements the security features in the existing handover keying alternatives and provides a proper framework for secure key distribution in mobility scenarios. In the authors' opinion, the main contributions of this paper are: the definition of a 3-party key distribution based architecture; a secure 3-party protocol which reduces the number of round trips required for providing a secure key distribution in wireless networks; and a demonstration how our proposal achieves secure properties, by means of a model checker as a proper formal tool.

The remainder of the paper is organized as follows: in section 2 we analyze EAP and the associated fast handover problematic. Section 3 describes the

[1] Note that this Internet-Draft appeared just before the submission of our paper.