NETEXT WG
Internet-Draft
Intended status: Informational
Expires: October 24, 2011

S. Gundavelli
Cisco
M. Liebsch
NEC

April 22, 2011

PMIPv6 inter-working with WiFi access authentication
draft-liebsch-netext-pmip6-authiwk-02.txt

Abstract

Proxy Mobile IPv6, the IETF's protocol for network-based mobility management, requires a completed and successful authentication of the mobile node before it is registered at the mobility anchor. This document describes inter-working between access authentication mechanisms, such as IEEE 802.1X, and the Proxy Mobile IPv6 protocol to enable trusted WiFi access to a network-based mobility management domain. Furthermore, the use of authentication method specific identifiers for unique identification of mobile nodes during setup and maintenance of their mobility session is described, following recommendations of related standards organizations, such as 3GPP and the WiMAX Forum.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 24, 2011.

Copyright Notice

Table of Contents

1. Introduction

Proxy Mobile IPv6 (PMIPv6) [RFC5213] represents the IETF's protocol for network-based mobility management and is being deployed in various standards, such as the 3rd Generation Partnership Project (3GPP), to complement host mobility. According to the PMIPv6 standard, mobile nodes (MN) do not require a secure interface to the mobility anchor (LMA), as there is no direct signaling for mobility management between the MN and the LMA, but the Mobility Access Gateway (MAG) sets up and maintains a mobility binding on the LMA on behalf of the host by means of a Proxy Binding Update (PBU). [RFC5213] requires a successful authentication of the MN before the MAG sends a PBU to the LMA to set up a mobility binding for the MN. Furthermore, it assumes the MAG to be informed about a mobile node identifier (MN-Identifier), which unambiguously identifies the MN during the mobility session. Such MN-Identifier can be a static identifier or a temporary identifier, which may be derived from a static identifier.

This document intends to provide guidelines for PMIPv6 to inter-work with access authentication protocols which have been designed for IEEE 802-type of link technologies. Initial versions of this document focus on IEEE 802.1X and its recommendation to use the Extensible Authentication Protocol (EAP) [RFC3748]. Based on the procedure for general inter-working, more specific use cases are documented for discussion and reference. These use cases include the use of the Wireless LAN technology according to the IEEE 802.11 standard to provide trusted access to 3GPP's packet core network. So far, WLAN has been considered as untrusted access being even provided by third parties and MNs connect through WLAN to the mobile operator network through an established secure tunnel. Stepping towards WLAN trusted access avoids the overhead of an established IPsec tunnel with a packet data gateway in the operator's core network, but requires inter-working between WLAN access authentication and the operator's authentication and identification mechanisms. In the context of trusted WLAN access and network-based mobility management, WLAN security is being used to protect traffic on the wireless link whereas the trust relationship between a MAG and the LMA is used to convey traffic through the operator's core network.

The first version of this document discusses inter-working between IEEE 802.1X EAP and PMIPv6 as well as some specific use cases for trusted WLAN access in 3GPP's evolved packet core, which are based on recommended authentication schemes, such as EAP-AKA [RFC5448]. Further use cases with different EAP authentication schemes as well as inter-working between PMIPv6 and web authentication will be added to future versions of this document. Prior to describing details of PMIPv6 inter-working with various access authentication schemes in

Section 4, Section 3 describes functional objectives to enable trusted WLAN access to mobile operator networks and efficient inter-working between WiFi access authentication and operators' mobility management as well as policy and AAA infrastructure.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

This document uses the terminology of [RFC5213]. The following additional terms are used in the context of this draft:

- AAA -- Authentication, Authorization and Accounting
- EAP -- Extensible Authentication Protocol
- PCC -- Policy and Charging Control
- PMK -- Pairwise Master Key

3. Functional Objectives

Major motivation and objective to document inter-working between WiFi access authentication and PMIPv6 is to describe complete system operation, message sequences and identification schemes for network-based mobility management using PMIPv6 including IEEE 802.11-based access as proven and widely accepted radio technology and associated authentication mechanisms. Inter-action between access authentication and mobility management allows the specification of missing components in [RFC5213], mainly referring to MAG operation being triggered by successful MN authentication and MN identification.

The relevance of WiFi radio access is proven by various standards' initiative in specifying inter-working with IEEE 802.11-based technology. One example is the 3GPP's interest in supporting traffic offload to WLAN networks. Another example is the WiMax Forum's Network Architecture, which consider a WiFi-WiMAX inter-working function to enable access to the WiMAX network through WiFi radio access and to support handover between WiFi and WiMAX radio access.

The PMIPv6 standard [RFC5213] assumes a completed and successful access authentication of MNs (or their subscriber) before the MAG registers the MN at an LMA by means of a PBU. One objective of this document is to analyze relevant access authentication schemes and to document the operation of PMIPv6 in dependency of these authentication mechanisms. The EAP procedure as IEEE 802.X recommendation is being considered most relevant at this time. Web-authentication is a further popular access authentication scheme, which can be analyzed and inter-working with PMIPv6 can be specified, even though manual subscriber inter-action during access authentication conflicts with automatic and seamless operation, e.g. during dual radio handover from 3GPP access to WiFi access.

A further objective is to analyze the details of preferred authentication schemes, taking 3GPP and WiMAX Forum recommendations into account, and to document the use of common identifiers for access authentication and PMIPv6-based mobility management. Such identifier-specific inter-working must take further requirements, such as unique identification of a MN during the mobility session, into account. Some identifiers, which are generated during access authentication, are unique for an MN, but are not stable and valid beyond a certain radio access point. In such case, the MAG must use a different identifier or resolve such temporary identifier into a unique identifier which is valid beyond a single access point and MAG.

A further goal is to analyze inter-working between access

authentication schemes and PMIPv6 during handover, which may also imply a change in the radio access technology. Treatment of authentication methods, keys and identifiers and associated inter-working with PMIPv6 operation is documented.

Figure 1 depicts a high-level view of a WiFi network being integrated into a mobile operator network as trusted access. Instead of using a Security and Mobility Gateway, such as the 3GPP's Packet Data Gateway (PDG), which terminates an IPsec tunnel with the UE, the system relies on concatenated protected links between the UE and the WiFi access network, as well as between the WiFi access network and the LMA. The illustrated setup assumes a MAG function to be co-located with the WiFi Access Point or a WiFi Controller (Ctrlr). Inter-working between WiFi access authentication, PMIPv6 operation and the operator network's AAA and PCC (Policy and Charging Control) infrastructure is achieved by means of associated interfaces with the LMA. Future extensions may consider a direct policy configuration interface with the WiFi access network controller. This version of the inter-working document does not assume a direct policy control interface between the WiFi access network and the operator's PCC system. If needed, the PMIPv6 protocol interface may be proposed to convey associated information. Policy configuration in the WiFi access network is considered out of scope of this documentation.

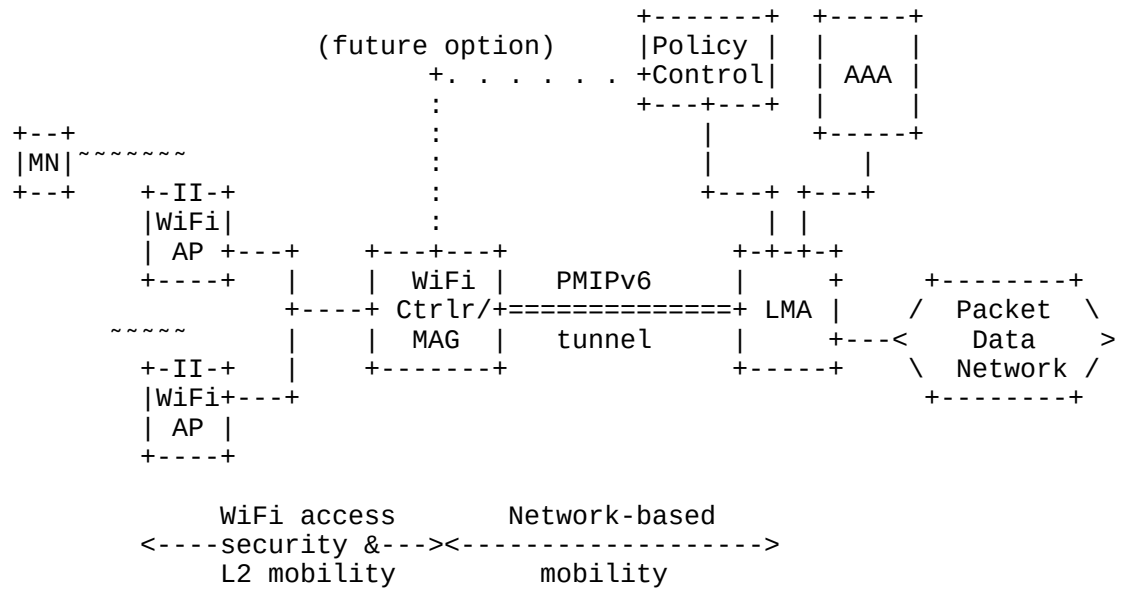

Figure 1: Integration of the WiFi radio technology to provide trusted access to mobile operator networks

4. Inter-working with IEEE 802.1X EAP

4.1. General use with authentication against a RADIUS Server

IEEE 802.1X recommends EAP for access authentication, which can make use of an Authentication Server using for example the RADIUS protocol between the Authenticator and the Authentication Server. [RFC3579] specifies RADIUS extensions to convey EAP attributes between an Authenticator and the RADIUS server. Figure 2 depicts general inter-working between PMIPv6 and IEEE 802.1X using EAP.

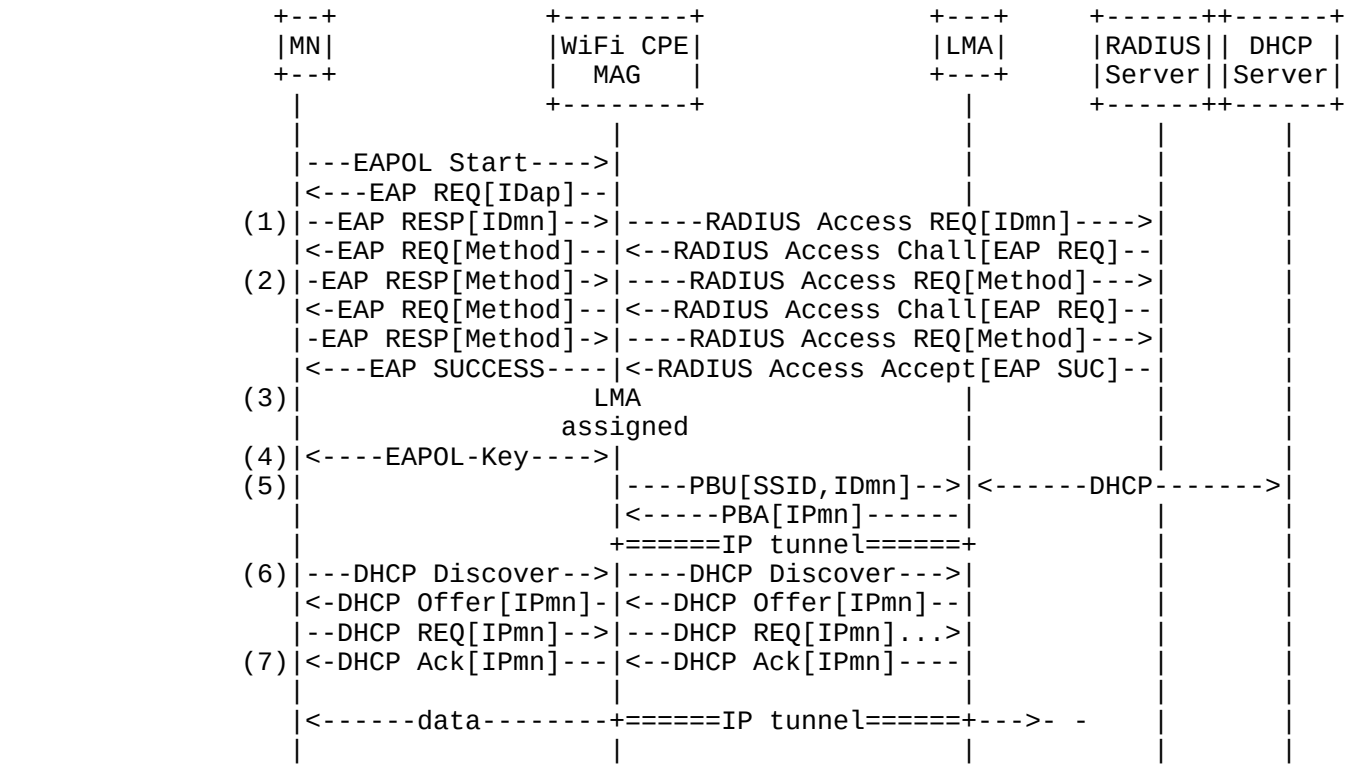

Figure 2: PMIPv6 inter-working with WPA2-802.1X access authentication against a RADIUS server

After the MN has associated with a WiFi Access Point, the EAPOL procedure starts (1). EAP attributes are mapped by the WiFi AP/Ctrlr

between EAPOL on the wireless link and RADIUS operation on the link towards the RADIUS server. The RADIUS server selects one or multiple authentication methods, which are performed with the MN in a challenge-response procedure (2). As a result of a successful EAP procedure, the RADIUS server may assign an LMA to the MN and signal the LMA identifier or the LMA IP address to the MAG function in the WiFi access network (3). The MN and the WiFi Access Point can now negotiate the Session Key to protect the wireless access (4). At that time, the MAG can take the EAP success as trigger to initiate the PBU registration of the MN with the LMA (5). The keys and identifiers being used and generated differ between the EAP and authentication method. In general, the MAG should not use the generated Session Key or security association identifier, as scope is limited to the the MN's association with the Access Point. More suitable is an identifier being negotiated during the authentication procedure with the RADIUS server, e.g. based on the Pairwise Master Key (PMK) or any identifier which derives from the PMK without including single Access Point specific information, such as the AP's MAC address. One example, which will be described in more detail in future versions of this document, is the use of the International Mobile Subscriber Identity (IMSI) to derive a NAI at the Authentication Server. This IMSI-based NAI is then used as MN-Identifier in the PBU. Such approach is being proposed in 3GPP for trusted access to the mobile operator network through non-3GPP type radio access networks [3GPP-TS23.402] [3GPP-TS33.402].

As a result of the MN's registration, the LMA performs DHCP with a DHCP server to retrieve a valid IP address for the MN (IPmn). The assigned IP address is then signaled to the MAG in the PBA. The MN learns about this IP address from the DHCP procedure (6). After successful completion of the DHCP procedure (7), the MN can use the protected wireless link to communicate with the network infrastructure.

5. Security Considerations

This document analyzes and documents inter-working between WiFi access authentication and PMIPv6 mobility management to enable trusted access to a mobile operator network which uses network-based mobility management. The document refers to standard operation of PMIPv6 [RFC5213] as well as well accepted WiFi authentication mechanisms, such as EAP using a RADIUS server as authentication server, without introducing new messages or message sequences. Solely the inter-working of access authentication and PMIPv6 is described by means of message sequence charts. Furthermore, the use of identifiers, which are built during access authentication, for MN identification in the PMIPv6-based mobility management protocol is described. Hence, the documented inter-working should not introduce any new security threats.

6. IANA Considerations

This document is based on standardized protocols for WiFi access authentication and network-based mobility management. No additional protocol messages and options are specified so far in this document.

7. Normative References

[3GPP-TS23.402]
"3GPP TS 23.402; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses (Release 10)", <http://www.3gpp.org>.

[3GPP-TS33.402]
"3GPP TS 33.402; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses (Release 9)", <http://www.3gpp.org>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5448] Arkko, J., Lehtovirta, V., and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", RFC 5448, May 2009.

Authors' Addresses

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134,
USA

Email: sgundave@cisco.com

Marco Liebsch
NEC Laboratories Europe
Kurfuersten-Anlage 36
D-69115 Heidelberg,
Germany

Email: liebsch@neclab.eu