The EAP-WAI Authentication Protocol
draft-richard-emu-wai-00

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 6, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.
Abstract

The Extensible Authentication Protocol (EAP), defined in RFC 3748, provides support for multiple authentication methods. The WLAN Authentication and Privacy Infrastructure (WAPI) provides the protection to the WLAN link-level security, and support the mutual authentication between the Authentication Supplicant Entity (ASUE) and the Authenticator Entity (AE). This document defines EAP-WAI, which enable the WAPI infrastructure to reuse the AAA architecture.

Table of Contents

1. Introduction .................................................. 3
   1.1. Conventions Used in This Document .......................... 3
   1.2. Terminology ............................................... 3
   1.3. WAPI Overview ............................................. 5
   1.4. Benefits of Reusing AAA Architecture ....................... 8
   1.5. Design Idea ............................................... 8
2. Protocol Overview ............................................... 9
   2.1. Base EAP-WAI Conversation ................................. 9
   2.2. Fragmentation ............................................. 11
3. Detailed Description of the EAP-WAI Protocol .................. 12
   3.1. EAP-WAI Request Packet .................................. 12
   3.2. EAP-WAI Response Packet ................................. 13
4. IANA Considerations ........................................... 14
5. Security Considerations ....................................... 14
   5.1. Packet Modification Attacks ............................... 14
6. Acknowledgements ............................................. 15
7. References ..................................................... 15
   7.1. Normative References .................................... 15
   7.2. Informative References ................................. 16
1. Introduction

The Extensible Authentication Protocol (EAP), described in [RFC3748], provides a standard mechanism for support of multiple authentication methods. Through the use of EAP, support for a number of authentication schemes may be added, including smart cards, Kerberos, Public Key, One Time Passwords, and others. EAP has been defined for use with a variety of lower layers, including the Point-to-Point Protocol (PPP) [RFC1661], Layer 2 tunneling protocols such as the Point-to-Point Tunneling Protocol (PPTP) [RFC2637] or Layer 2 Tunneling Protocol (L2TP) [RFC2661], IEEE 802 wired networks [IEEE.802-1x.2004], and wireless technologies such as IEEE 802.11 [IEEE.802-11.1999].

The WLAN Authentication and Privacy Infrastructure (WAPI) [Draft-Amendment-ISO-DIS-8802-11-Amd-7] is brought forward by the China Broadband Wireless IP Standard Group, and was invited by the ISO/IEC/JTC1/SC6 to submit it as an international proposal in June, 2009. The WAPI infrastructure is to protect the WLAN link-level security, and is independent to AAA and EAP protocol [RFC3748].

This document defines EAP-WLAN Authentication Infrastructure (EAP-WAI), which uses the EAP packet to encapsulate the WAPI protocol and makes the WAPI reuse the AAA architecture, and it would reduce the deployment and operating costs of the WAPI application.

1.1. Conventions Used in This Document

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 RFC 2119 [RFC2119].

1.2. Terminology

This document uses terminology from the WAPI protocol specification [Draft-Amendment-ISO-DIS-8802-11-Amd-7], IEEE 802.11 standard [IEEE.802-11.1999] and Extensible Authentication Protocol [RFC3748].

In the IEEE 802.11 standard [IEEE.802-11.1999], it defines:

Station (STA): Any device that contains an IEEE 802.11-conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM).

Access Point (AP): Any entity that has station (STA) functionality and provides access to the distribution services, via the wireless medium (WM) for associated STAs.
In the WAPI protocol specification [Draft-Amendment-ISO-DIS-8802-11-Amd-7], it defines:

WLAN Network Authentication and Privacy Infrastructure (WAPI): A security scheme that is stated to provide identity authentication and data confidentiality for WLAN. WAPI comprises WAI (WLAN Authentication Infrastructure) and WPI (WLAN Privacy Infrastructure).

Authentication Supplicant Entity (ASUE): An entity that requires identity authentication through ASU. It resides in any STA.

Authenticator Entity (AE): An entity that provides authentication action for the authentication supplicant before the supplicant accesses to the network. It resides in any AP.

Authentication Service Entity (ASE): An entity that provides mutual identity authentication for the AE and the ASUE. It resides in any ASU.

Authentication Service Unit (ASU): An important part of WAI authentication framework that is based on public-key cryptography. It manages the certificates and authenticates the identities of users etc.

In the Extensible Authentication Protocol [RFC3748], it defines:

Peer: The end of the link that responds to the authenticator. In [IEEE.802-1X.2004], this end is known as the Supplicant.

Supplicant: The end of the link that responds to the authenticator in [IEEE.802-1X.2004]. In this document, this end of the link is called the peer.

Authenticator: The end of the link initiating EAP authentication. The term authenticator is used in [IEEE.802-1X.2004], and has the same meaning in this document.

AAA: Authentication, Authorization, and Accounting. AAA protocols with EAP support include RADIUS [RFC3579] and Diameter [RFC4072].

Backend Authentication Server: A backend authentication server is an entity that provides an authentication service to an authenticator. When used, this server typically executes EAP methods for the authenticator. This terminology is also used in [IEEE.802-1X.2004].
1.3. WAPI Overview

According to the [Draft-Amendment-ISO-DIS-8802-11-Amd-7], the WAPI infrastructure includes the entities of ASUE, AE and ASE. The figure 1 illustrates the relationships among three entities, and the exchange of information among them.

```
+---+ 802.11 frames  +---+ 802.3 frames  +---+
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>WAI Over 802.11</td>
<td>---</td>
<td>WAI Over UDP</td>
<td>---</td>
</tr>
<tr>
<td>---</td>
<td>-----------------</td>
<td>---</td>
<td>---------------</td>
<td>---</td>
</tr>
</tbody>
</table>
+---+                 +---+               +---+
```

Figure 1: WAPI Infrastructure

The WAI protocol is a core part of WAPI, and the authentication packets between ASUE and AE are transported by the WAI protocol with Ether Type 0x88B4, and those packets between AE and ASE are transported by the UDP socket with port number 3810.

For WAPI, a main advantage over IEEE 802.11i [IEEE.802-11I.2004] is the mutual authentication between ASUE and AE. When the authentication is successful, the ASUE can securely access to the AE; otherwise, both the ASUE and AE refuse to connect with each other.

The public-key certificate, is an important part of the construction of WAPI system. The identity of ASUE and AE can be uniquely identified by the certificate, and Public-key certificate is the digital identification of ASUE and AE. Two kinds of public-key certificate format, X.509 v3 and GBW, are supported by the WAPI.

The WAPI protocol process mainly involves three phases, and Figure 2 illustrates the process in details.

1)IEEE 802.11 Protocol Phase

In the beacon, authentication and association frames, they carry the WAPI security parameters. The process negotiates the parameters used by next phase.

2)Certificate Authentication Phase

After the ASUE associated with the AE, the AE triggers the
authentication by Authentication Activation frame. The ASUE sends its certificate and so on to the AE. The AE sends its and ASUE’s certificate to the ASE by Certificate Authentication Request. After verifying the legality of both ASUE and AE’s certificate, ASE sends the result to the AE by Certificate Authentication Response, then the AE sends Access Authentication Response to the ASUE.

3) Key Negotiation Phase

It includes the unicast key negotiation and multicast key announcement. As the phase is not involved by the EAP-WAI process, this document does not give more introduction.
Figure 2: WAPI Protocol Process
1.4. Benefits of Reusing AAA Architecture

In the Section 1.3, it explains that ASE will verify ASUE and AE’s certificates in the Certificate Authentication Phase. It is evident that the ASE plays an important role in the WAPI deployment. To enable WAPI, the operators have to cost the additional money to deploy and maintain the ASE.

Considering AAA (e.g., Radius) is widely deployed and very extensible, if the WAPI infrastructure could reuse AAA, it would bring the following benefits to the operators:

- Independent software vendor (ISV) could easily make the current AAA backend authentication server support the ASE function;

- As the deployment of the additional ASE server could be not required, it would reduce the costs of the WAPI infrastructure’s deployment and maintenance;

- The WAPI offers the link-level security to the ASUE, e.g., the authentication and confidentiality. Besides them, ASUE needs the authorization and accounting service. The AAA already support such functions well, and the WAPI could easily reuse such services if it could reuse AAA architecture;

- The IEEE 802.11i authentication is already based on the AAA, if the WAPI could reuse the AAA, it could make the authentication of 802.11i and WAPI in the same architecture, and simplify the maintenance of WLAN network.

1.5. Design Idea

AAA, e.g., Radius, is a very extensible protocol and able to support multiple authentication methods by EAP extension. In the AAA architecture, when backend authentication server is deployed, supplicant is the peer to the server, and authenticator mainly pass-through the EAP method packet exchanged between the server and the peer. The role of AE defined by the WAPI protocol specification is different to the authenticator in the EAP protocol: The AE would get the ASUE’s certificate from the Access Authentication Request, then send its and ASUE’s certificate to the ASE. In other word, the AE reconstructs the frame it received from the ASUE.

In order to reuse the AAA architecture and avoid the influence to the ASUE, the EAP packet exchanged SHOULD be between the AE and the AAA backend authentication server. As the server’s peer is ASUE, the AE SHOULD mimic itself as a peer (ASUE). By this way, from the AAA server perspective, EAP-WAI is similar to the other authentication
methods such as EAP-TLS [RFC5216].

Figure 3 illustrates how WAPI is deployed by reusing the AAA architecture. The ASE is replaced by AAA backend authentication server, and WAI is over EAP instead of the UDP protocol specified by the WAPI protocol. It SHOULD be noticed there are no any changes for the frames exchanged between the ASUE and AE, and it is not related to the EAP extension.

+----------+----------+----------+
<table>
<thead>
<tr>
<th>802.11 frames</th>
<th>802.3 frames</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAI Over 802.11</td>
<td>WAI Over EAP</td>
</tr>
<tr>
<td>ASUE</td>
<td>AE</td>
</tr>
<tr>
<td>AAA Backend Authentication Server</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3: WAPI Deployed by Reusing AAA Architecture

Base on the above idea, the EAP-WAI SHOULD support the following functions:

- SHOULD encapsulate the Certificate Authentication Request and Response defined by the [Draft-Amendment-ISO-DIS-8802-11-Amd-7];

- As AE SHOULD mimic a peer (ASUE), there is no need to let AE send the EAP-Request/Identity to ASUE any more. AE SHOULD directly send the EAP-Response/Identity to the AAA Backend Authentication Server;

- AE SHOULD handle EAP packets such as EAP-Success, EAP-Failure.

Since the unicast key negotiation and multicast key announcement are handled by the ASUE and AE, and ASE does not take part in the process, the EAP-WAI is not required to consider the topics such as Key Hierarchy.

2. Protocol Overview

2.1. Base EAP-WAI Conversation

Once having received Access Authentication Request packet from ASUE, and if the AE is configured to use EAP-WAI, the AE MUST send EAP-Response/Identity packet to AAA backend authentication server. The identity MAY be the subject [RFC3280] of ASUE’s certificate. As noted in Section 1.5, there is no need to let AE send the EAP-
Request/Identity to ASUE

After having received the Identity, the AAA backend authentication server MUST respond with an EAP-WAI packet, which is an EAP-Request packet with EAP-Type=EAP-WAI, no data. The EAP-WAI conversation will then begin.

Firstly, AE sends EAP-WAI/Certificate Authentication Request packet to the AAA backend authentication server, which is an EAP-Response packet with EAP-Type=EAP-WAI, and with Certificate Authentication Request.

After verifying the certificates of AE and ASUE in Certificate Authentication Request packet, The AAA backend authentication server then responds with an EAP-Request packet with EAP-Type=EAP-WAI. The data field of this packet will encapsulate Certificate Authentication Response.

While EAP-WAI/Certificate Authentication Response packet is sent to AE successfully, and has received the acknowledgement from AE, the AAA backend authentication server SHOULD then respond authentication result. As long as either ASUE or AE’s certificate is invalid, the verified result is failure, and the AAA backend authentication server will respond with EAP-Failure. Otherwise, the server will respond with EAP-Success.

Before sending EAP-Request/EAP-WAI packet with Certificate Authentication Response, the AAA backend authentication server SHOULD NOT respond EAP-Success or EAP-Failure. If the EAP authentication result is inconsistent with the result in Certificate Authentication Response packet, the AE SHOULD log this inconsistent event.

In the case where the EAP-WAI authentication is successful, the conversation will appear as follows:
A single WAI packet may be up to 65535 octets in length, thus be larger than the MTU size or the maximum Remote Authentication Dial-In User Service (RADIUS) packet size of 4096 octets. So the fragmentation function SHOULD be considered. Since the WAI protocol has supported fragmentation, EAP-WAI could reuse it.

However, in WAPI protocol specification, the sender will send all fragments without waiting acknowledgement to each fragment. While one fragment is lost, the whole WAI protocol packet SHOULD be retransmitted. When EAP-WAI method is used, the EAP’s retransmission mechanism will take effect instead of the WAPI’s. EAP is a simple ACK-NAK protocol, only the fragments that are lost or damaged in transit will be retransmitted.

In the case where the EAP-WAI authentication is successful, and fragmentation is required, the conversation will appear as follows:

AE
--------------
EAP-Response/
Identity (MyID) ->

AAA Backend Authentication Server
--------------
<- EAP-Request/
EAP-Type=EAP-WAI

EAP-Response/
EAP-Type=EAP-WAI
(Certificate Authentication Request) ->

<- EAP-Request/
EAP-Type=EAP-WAI
(Certificate Authentication Response)

EAP-Response/
EAP-Type=EAP-WAI ->

<- EAP-Success
3. Detailed Description of the EAP-WAI Protocol

3.1. EAP-WAI Request Packet

A summary of the EAP-WAI Request packet format is shown below. The fields are transmitted from left to right.
Code

1

Identifier

The Identifier field is one octet and aids in matching responses with requests. The Identifier field MUST be changed on each Request packet.

Length

The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length, Type, and Data fields. Octets outside the range of the Length field SHOULD be treated as Data Link Layer padding and MUST be ignored on reception.

Type

RFC Editor - please replace xxx with the value allocated by IANA for type of EAP-WAI

xxx -- EAP-WAI

WAI data

The WAI data consists of the encapsulated WAI packet.

3.2. EAP-WAI Response Packet

A summary of the EAP-WAI Response packet format is shown below. The fields are transmitted from left to right.
Code

2

Identifier

The Identifier field is one octet and aids in matching responses with requests. The Identifier field MUST be changed on each Request packet.

Length

The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length, Type, and Data fields. Octets outside the range of the Length field SHOULd be treated as Data Link Layer padding and MUST be ignored on reception.

Type

RFC Editor - please replace xxx with the value allocated by IANA for type of EAP-WAI

xxx -- EAP-WAI

WAI data

The WAI data consists of the encapsulated WAI packet.

4. IANA Considerations

Require IANA to assign a EAP type for EAP-WAI.

5. Security Considerations

5.1. Packet Modification Attacks

The Certificate Authentication Request in EAP-Response/EAP-WAI packet has no integrity protection. As a result, the data can be modified
by an attacker. But the modification will only result in a denial-of-service attack.

Since there is signature of ASE in the Certificate Authentication Response in EAP-Request/EAP-WAI packet, modification of the data will be examined by AE or ASUE verifying signature.

EAP-WAI method doesn’t provide integrity protection of EAP header fields (Code, Identifier, Length) or the Type. In most cases, modification of the Code or Identifier or Type fields will only result in a denial-of-service attack. However, an attacker can add additional data to an EAP-WAI packet so as to cause it to be longer than implied by the Length field. EAP peers, authenticators, or servers that do not check for this could be vulnerable to a buffer overrun.

6. Acknowledgements

The authors wish to thank Fei Fang, Ju Wang, Yu Liu, Yujin Zhao, Haitao Zhang, Zhifei Zhang, Yongfu Chai, Guanghui Chen, Hua Wen.

7. References

7.1. Normative References


7.2. Informative References


[IEEE.802-1X.2004] "IEEE Standard for Local and metropolitan area networks Port-Based Network Access Control",
IEEE Standard 802.1x, 2004, 

Authors’ Addresses

Yang Shi (editor)  
Hangzhou H3C Tech. Co., Ltd  
H3C Beijing R&D Center, Digital Technology Plaza,  
NO.9 Shangdi 9th Street, Haidian District,  
Beijing  
China (100085)  
Phone: +86 010 82775276  
EMail: young@h3c.com

Li Li (editor)  
Shanghai Research Institute of China Telecom Co. Ltd  
No.1835, South Pudong Road  
China (200122)  
Phone: +86 021 28970196  
EMail: lily@sttri.com.cn

Zibin Cai (editor)  
Hangzhou H3C Tech. Co., Ltd  
H3C Beijing R&D Center, Digital Technology Plaza,  
NO.9 Shangdi 9th Street, Haidian District,  
Beijing  
China (100085)  
Phone: +86 010 82774283  
EMail: zibinc@h3c.com