

ABFAB Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 1, 2013

S. Winter
RESTENA
J. Salowey
Cisco
July 31, 2012

**Update to the EAP Applicability Statement for ABFAB
draft-ietf-abfab-eapapplicability-00**

Abstract

This document updates the EAP applicability statement from [RFC3748](#) to reflect recent usage of the EAP protocol in application oriented use cases proposed in ABFAB

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 February 1, 2013.

Copyright Notice

Copyright (c) 2012 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 (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Requirements Language	3
2.	Uses of EAP for Application-Layer Access	3
3.	Revised EAP applicability statement	4
4.	Security Considerations	5
5.	IANA Considerations	5
6.	Acknowledgements	5
7.	References	5
7.1.	Normative References	5
7.2.	Informational References	5

1. Introduction

The EAP applicability statement in [[RFC3748](#)] defines the scope of the Extensible Authentication Protocol to be "for use in network access authentication, where IP layer connectivity may not be available.", and states that "Use of EAP for other purposes, such as bulk data transport, is NOT RECOMMENDED."

While some of the recommendation against usage of EAP for bulk data transport is still valid, some of the other provisions in the applicability statement have turned out to be too narrow. [Section 2](#) describes the example where EAP is used to authenticate application layer access. [Section 3](#) provides new text to update the paragraph 1.3. "Applicability" in [[RFC3748](#)].

1.1. Requirements Language

In this document, several words are used to signify the requirements of the specification. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#). [[RFC2119](#)]

2. Uses of EAP for Application-Layer Access

Ongoing work in the IETF (abfab working group) specifies the use of EAP over GSSAPI for generic application layer access. In the past, using EAP in this context has met resistance due to the lack of channel bindings [[I-D.ietf-emu-chbind](#)]. Without channel bindings, a peer does not know what service will be provided by the authenticator. In most network access use cases all access servers that are served by a particular EAP server are providing the same or very similar types of service. The peer does not need to differentiate between different access network services supported by the same EAP server.

However as additional services use EAP for authentication, the distinction of which service is being contacted becomes more important. Consider an environment with multiple printers; if a peer printed a document in the wrong location then potentially sensitive information might be printing in a location where the user associated with the peer would be unable to retrieve it. It is also likely that services might have different security properties. For example, it might be more likely that a low-value service is compromised than some high value service. If the high-value service could be impersonated by a low-value service then the security of the overall system would be limited by the security of the lower value service.

This distinction is present in any environment where peers' security depends on which service they reach. However it is particularly acute in a federated environment where multiple organizations are involved. It is very likely that these organizations will have different security policies and practices. It is very likely that the goals of these organizations will not entirely be aligned. In many situations one organization could gain value by being able to impersonate another. In this environment, authenticating the EAP server is insufficient: the peer must also validate that the contacted host is authorized to provide the requested service.

For these reasons, channel binding **MUST** be implemented by peers, EAP servers and AAA servers in environments where EAP authentication is used to access application layer services. In addition, channel binding **MUST** default to being required by peers for non-network authentication. If the EAP server is aware that authentication is for something other than a network service, it too **MUST** default to requiring channel binding. Operators need to carefully consider the security implications before relaxing these requirements. One potentially serious attack exists when channel binding is not required and EAP authentication is introduced into an existing non-network service. A device can be created that impersonates a Network Access Service to peers, but actually proxies the authentication to the service that newly accepts EAP authentications may decrease the security of this service even for users who previously used non-EAP means of authentication to the service.

It is important for the application layer to prove possession of the EAP MSK between the EAP Peer and EAP Authenticator. In addition, the application should define an channel binding attributes that are sufficient to validate that the application service is being correctly represented to the peer.

3. Revised EAP applicability statement

The following text is added to the EAP applicability statement in [[RFC3748](#)].

In cases where EAP is used for application authentication, support for EAP Channel Bindings is **REQUIRED** on the EAP Peer and EAP Server to validate that the host is authorized to provide the services requested. In addition, the application **MUST** define channel binding attributes that are sufficient to validate that the application service is being correctly represented to the peer. It is important for the protocol carrying EAP to prove possession of the EAP MSK between the EAP Peer and EAP Authenticator.

4. Security Considerations

In addition to the requirements discussed in the main sections of the document applications should take into account how server authentication is achieved. Some deployments may allow for weak server authentication that is then validated with an additional existing exchange that provides mutual authentication. In order to fully mitigate the risk of NAS impersonation when these mechanisms are used, it is RECOMMENDED that mutual channel bindings be used to bind the authentications together as described in [\[I-D.hartman-emu-mutual-crypto-bind\]](#)

5. IANA Considerations

This document has no actions for IANA.

6. Acknowledgements

Large amounts of helpful text and insightful thoughts were contributed by Sam Hartman, Painless Security.

7. References

7.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowitz, "Extensible Authentication Protocol (EAP)", [RFC 3748](#), June 2004.
- [I-D.ietf-emu-chbind] Hartman, S., Clancy, T., and K. Hoyer, "Channel Binding Support for EAP Methods", [draft-ietf-emu-chbind-16](#) (work in progress), May 2012.

7.2. Informational References

- [I-D.hartman-emu-mutual-crypto-bind] Hartman, S., Wasserman, M., and D. Zhang, "EAP Mutual Cryptographic Binding", [draft-hartman-emu-mutual-crypto-bind](#)

00 (work in progress),
March 2012.

Authors' Addresses

Stefan Winter
Fondation RESTENA
6, rue Richard Coudenhove-Kalergi
Luxembourg 1359
LUXEMBOURG

Phone: +352 424409 1
Fax: +352 422473
EMail: stefan.winter@restena.lu
URI: <http://www.restena.lu>.

Joseph Salowey
Cisco Systems
2901 3rd Ave
Seattle 98121
USA

EMail: jsalowey@cisco.com

