ABFAB Working Group	S. Winter
Internet-Draft	RESTENA
Intended status: Standards Track	J. Salowey
Expires: April 29, 2012	Cisco
	October 27, 2011

Update to the EAP Applicability Statement
draft-winter-abfab-eapapplicability-01

Abstract

This document updates the EAP applicability statement from RFC3748 to reflect recent usage of the EAP protocol in unprecedented contexts.

Status of this Memo

Copyright Notice

Table of Contents

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 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 lists examples where EAP is being used for more than authentication and/or more than network access. This section also provides considerations and guidelines for EAP usage in these areas. Section 4 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 beyond the original applicability statement

2.1. Communication of Authorisation Information

In some cases EAP methods carry authorization information. An EAP-AKA attribute, AT_TRUST_IND [3GPP TS 24.302], has been defined in 3GPP to allow the authentication server to signal to the EAP peer if it is attached to a trusted network. If the attribute indicates the network is not trusted then the EAP peer would establish an IPsec tunnel to its home network to protect its communications. If the attribute indicates a trusted network then the EAP Peer may send its traffic without establishing an IPsec tunnel since the network is authorized to handle it.
It is also common for EAP methods to communicate information about access control decisions beyond just success and failure. For example, MSCHAPv2 signals (lack of) authorisation of an authenticated user to use a service. An MSCHAPv2 failure packet as defined in section 6 of MSCHAPv2 [RFC2759] can indicate condition 646 "Restricted Logon hours". This determination is an authorisation check which happens subsequent to the authentication step (a user needs to be positively identified to correlate his identity to a list of permitted logon hours).
This use of EAP is not covered by the EAP applicability statement since it goes beyond authentication. There are some potential issues that can arise from carrying authorization data in EAP. First, there is no generic mechanism for EAP methods to carry authorization data. In order to make use of and communicate the authorization data the EAP method will have to provide custom interfaces and capabilities. This will inhibit the ability for different EAP methods to be used in a pluggable fashion within deployments. It addition, if the authorization information is specific to a particular media, then it may interfere with the media independent property of EAP.
Extending individual EAP methods to carry authorization data for a specific deployment, technology, or media type is NOT RECOMMENDED. If the authorization data is informative such that the system operation is not significantly change if it is missing and if it is of a general nature then authorization data MAY be carried. If there is significant need for deployment specific, technology specific or media specific authorization information to be carried within EAP methods then a well defined mechanism and framework must be defined so the type of authorization data can be independent of the EAP method. This would allow the deployment of different EAP methods to support peers and servers with different credential types.

2.2. Endpoint Assessment

[Editor's note: This section needs to be updated to include some of the considerations when performing NEA in an EAP method. Some of the considerations include handling peer and server names, tight binding to particular EAP methods, and bulk data transport]

The IETF working group "Network Endpoint Assessment", nea, is chartered to define exchange information about the state of a user's equipment during network authentication. One of the channels over which to transport this information is EAP; either embedded within other EAP methods or as a stand-alone EAP method. The information exchanged is unrelated to user authentication - the information covers the state of the computing device only, independently of the user who is using it. This use of EAP is not covered by the EAP applicability statement since it goes beyond user authentication. However, there are multiple implementations of NEA information transport, some in wide deployment (e.g. recent implementations of PEAP with "Statement of Health (SoH)" support. It is thus due to extend the EAP applicability statement to include "Equipment Auditing".

2.3. Credential Management

Another enhancement to EAP is in the area of credential management. For example, EAP-MSCHAPv2 includes limited support for user account management, namely the possibility for a user to change his password, should it have expired. This is defined in section 7 of [RFC2759].
This use of EAP is not covered by the EAP applicability statement since it goes beyond authentication. In general, account management tasks within EAP SHOULD be limited to tasks directly associated with the credentials used for authentication. The renewal of a password or the maintenance of a PIN code are examples of this type of task. Tasks that are of a more general nature such as payment or service maintenance are NOT RECOMMENDED since they are likely to be very deployment specific leading to EAP methods that are not reusable in other environments. In addition these more general tasks often involve extensive user interaction and the exchange of additional data which can be dangerously close to "bulk data transport".

2.4. Different Lower Layers

The original EAP applicability statement states that EAP is applicable in cases where "IP layer connectivity may not be available". The wording in the applicability statement leaves open whether the usages of EAP that require some level of network access available are in scope or not. Examples of EAP over IP protocols include PANA protocol [RFC5191] and IKEv2. Since protocols which carry EAP over IP already exist and have been deployed, it is due to make this use case explicit and reflect it in the revised applicability statement.
There are some considerations when EAP is used over other transports. The statement needs to take into account that EAP requires ordering guarantees from its lower layers, which may not delivered by IP or some other lower layer in itself. This limits the use of EAP to transport layers which are on top of IP, and provide their own ordering guarantees. In addition, many EAP methods do not provide fragmentation so lower layers that limit the payload size may artificially constrain

the use of some EAP method. Since it is common for the authentication server to be separated from the authenticator, lower layer protocols MUST provide a mechanism for the EAP Peer and EAP authenticator to prove possession of the EAP MSK to ensure the EAP Peer and EAP authenticator are authenticated to one another. In addition lower layers should register a "EAP Lower Layer" type for channel binding purposes defined in [I-D.ietf-emu-chbind]

2.5. 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 authenticate which service it contacts. [Discussed: is authentication the right word here?]
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.
In parallel to ABFAB, there is other ongoing work on Channel Binding in the IETF (emu working group). The introduction of channel bindings into EAP mitigates the impersonation threat and makes EAP suitable for use beyond network authentication. Pending issuance of a Channel Binding RFC, it is thus due to extend the EAP applicability statement to include non-network access contexts if - and only if - this context mandates channel bindings.

3. Summary of changes

The new text for the EAP Applicability statement is stated in the next section. It is meant to replace section 1.3 of [RFC3748]. Its main changes are the widened scope (generic resource admission instead of only network authentication), the explicit mention of transporting EAP over IP, and the requirement for channel bindings if used for anything but network access.
This document also updates references to EAP-TLS and SCTP, whose original RFCs have been obsoleted by newer specifications.

4. Revised EAP applicability statement

EAP was designed for use in network access authentication, where IP layer connectivity may not be available. Under some circumstances, it may also be used for generic resource admission decisions. Use of EAP for other purposes, such as bulk data transport, is NOT RECOMMENDED.
EAP systems have evolved over time as have the capabilities and expectations of EAP methods. Modern EAP methods are expected to generate key material and perform mutual authentication. Some methods provide additional capabilities. These capabilities include the following:

- *Credential Management
- *Authorization
- *Endpoint Assessment

These usages must be carefully considered. The management of credentials directly related to the authentication method may be in scope of an EAP method. In many cases management tasks, such as registration, may be site specific, require the exchange of many messages or require extensive interaction with a user. These tasks are not well suited for inclusion an EAP method.

Some methods have evolved to carry authorization information. Since there currently is not generic authorization capability available to EAP methods, adding this capability tends to make EAP methods specific to deployments and lower layer technologies which reduces the reusability, extensibility and media independence of EAP methods. If authorization functionality is required then it should be added in a fashion that is largely independent of authentication mechanism, such as within a tunnel method.

EAP methods are currently used to carry endpoint assessment data. This has similar considerations as for authorization data. In addition the endpoint assessment process does not always provide mutual authentication so this process alone may not meet the requirements in environments where peer and server identities are required for various processes.

Systems have also evolved to use EAP in environments outside the traditional lower layer network access. In these cases it is important for the lower layer to prove possession of the EAP MSK between the EAP Peer and EAP Authenticator. In addition, at a minimum, a lower layer should define an "EAP Lower Layer" type for use in channel bindings. Usages, such as those that interface with application protocols must define channel binding information that is sufficient to validate that the application service is being correctly represented to the peer. In addition lower layers need to provide the transport support need by EAP as described below.

Since EAP does not require IP connectivity, it provides just enough support for the reliable transport of authentication protocols, and no more.

EAP is a lock-step protocol which only supports a single packet in flight. As a result, EAP cannot efficiently transport bulk data, unlike transport protocols such as TCP [RFC0793] or SCTP [RFC4960].

While EAP provides support for retransmission, it assumes ordering guarantees provided by the lower layer, so out of order reception is not supported.

Since EAP does not support fragmentation and reassembly, EAP authentication methods generating payloads larger than the minimum EAP MTU need to provide fragmentation support.

While authentication methods such as EAP-TLS [RFC5216] provide support for fragmentation and reassembly, the EAP methods defined in this document do not. As a result, if the EAP packet size exceeds the EAP MTU of the link, these methods will encounter difficulties.

EAP authentication is initiated by the server (authenticator), whereas many authentication protocols are initiated by the client (peer). As a result, it may be necessary for an authentication algorithm to add one or two additional messages (at most one roundtrip) in order to run over EAP.

Where certificate-based authentication is supported, the number of additional roundtrips may be much larger due to fragmentation of certificate chains. In general, a fragmented EAP packet will require as many round-trips to send as there are fragments. For example, a

certificate chain 14960 octets in size would require ten round-trips to send with a 1496 octet EAP MTU.
Where EAP runs over a lower layer in which significant packet loss is experienced, or where the connection between the authenticator and authentication server experiences significant packet loss, EAP methods requiring many round-trips can experience difficulties. In these situations, use of EAP methods with fewer roundtrips is advisable.

5. Security Considerations

Lots.

6. IANA Considerations

This document has no actions for IANA.

7. Acknowledgements

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

8. References

8.1. 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. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.
[RFC5191]	Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H. and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, May 2008.
[RFC5216]	Simon, D., Aboba, B. and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, March 2008.
[I-D.ietf-emu-chbind]	Hartman, S, Clancy, T and K Hoeper, "Channel Binding Support for EAP Methods", Internet-Draft draft-ietf-emu-chbind-11, October 2011.

8.2. Informational References

[RFC0793]	Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.
[RFC2759]	Zorn, G., "Microsoft PPP CHAP Extensions, Version 2", RFC 2759, January 2000.
[RFC4960]	Stewart, R., "Stream Control Transmission Protocol", RFC 4960, September 2007.

Authors' Addresses

Stefan Winter Winter Fondation RESTENA 6, rue Richard Coudenhove-Kalergi Luxembourg, 1359 LUXEMBOURG Phone: +352 424409 1 EMail: stefan.winter@restena.lu URI: http://www.restena.lu.

Joseph Salowey Salowey Cisco Systems
2901 3rd Ave Seattle, 98121 USA EMail: jsalowey@cisco.com