Internet Engineering Task Force (IETF)
Request for Comments: 6867
Category: Experimental
ISSN: 2070-1721

Y. Nir
Check Point
Q. Wu
Huawei

January 2013

An Internet Key Exchange Protocol Version 2 (IKEv2) Extension to Support EAP Re-authentication Protocol (ERP)

Abstract

This document updates the Internet Key Exchange Protocol version 2 (IKEv2) described in RFC 5996. This extension allows an IKE Security Association (SA) to be created and authenticated using the Extensible Authentication Protocol (EAP) Re-authentication Protocol extension, as described in RFC 6696.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6867.

1. Introduction

IKEv2, as specified in [RFC5996], allows (Section 2.16) authentication of the initiator using an EAP method. Using EAP significantly increases the count of round trips required to establish the IPsec SA and also may require user interaction. This makes it inconvenient to allow a single remote access client to create multiple IPsec tunnels with multiple IPsec gateways that belong to the same domain.

The EAP Re-authentication Protocol (ERP), as described in [RFC6696], allows an EAP peer to authenticate to multiple authenticators while performing the full EAP method only once. Subsequent authentications require fewer round trips and no user interaction.

Bringing these two technologies together allows a remote access IPsec client to create multiple tunnels with different gateways that belong to a single domain as well as using the keys from other contexts of using EAP, such as network access within the same domain, to transparently connect to VPN gateways within this domain.

Additionally, it allows for faster set up of new tunnels when previous tunnels have been torn down due to things like network outage, device suspension, or a temporary move out of range. This is similar to the session resumption mechanism described in [RFC5723]. One exception being that instead of a ticket stored by the client, the re-authentication Master Session Key (rMSK) (see Section 4.6 of [RFC6696]) is used as the session key stored on both the client and the Authentication, Authorization, and Accounting (AAA) server.

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 [RFC2119].

2. Usage Scenarios

This work is motivated by the following scenarios:

- Multiple tunnels for a single remote access VPN client. Suppose a company has offices in New York City, Paris, and Shanghai. For historical reasons, the email server is located in the Paris office, most of the servers hosting the company's intranet are located in Shanghai, and the finance department servers are in New York City. An employee using a remote access VPN may need to connect to servers from all three locations. While it is possible to connect to a single gateway, and have that gateway route the requests to the other gateways (perhaps through site to site VPN), this is not efficient; it is more desirable to have the client initiate three different tunnels. It is, however, not desirable to have the user type in a password three times.

- Roaming. In these days of mobile phones and tablets, users often move from the wireless LAN in their office, where access may be granted through 802.1x, to a cellular network, where a VPN is necessary, and back again. Both the VPN server and the 802.1x access point are authenticators that connect to the same AAA servers. So it makes sense to make the transition smooth, without requiring user interaction. The device still needs to detect whether it is within the protected network, in which case it should not use VPN. However, this process is beyond the scope of this document. [SECBEAC] is a now-abandoned attempt at this.

- Resumption. If a device gets disconnected from an IKE peer, ERP can be used to reconnect to the same gateway without user intervention.

3. Protocol Outline

Supporting EAP Re-authentication Extension (ERX) requires an EAP payload in the first IKE_AUTH request. This is a deviation from the rules in [RFC5996], so support needs to be indicated through a Notify payload in the IKE_SA_INIT response. This Notify serves the same purpose as the EAP-Initiate/Re-auth-Start message of ERX, as specified in Section 5.3.1 of [RFC6696]. The "Domain Name" field contains the content of the Domain-Name TLV as specified in Section 5.3.1.1 of the same document.

A supporting initiator that has unexpired keys for this domain will send the EAP-Initiate/Re-auth message in an EAP payload in the first IKE_AUTH request.

The responder sends the EAP payload content to a backend AAA server. If that server has a valid rMSK for that session, it sends those along with an EAP-Finish/Re-auth message. The responder then forwards the EAP-Finish/Re-auth message to the initiator in an EAP payload within the first IKE_AUTH response.

The initiator then sends an additional IKE_AUTH request that includes the AUTH payload, which has been calculated using the rMSK in the role of the MSK as described in Sections 2.15 and 2.16 of [RFC5996]. The responder replies similarly, and the IKE_AUTH exchange is finished.

If the backend AAA server does not have valid keys for the Re-auth-Start message, it sends back a normal EAP request, and no rMSK key. EAP flow continues as in [RFC5996].

The following figure is adapted from Appendixes C.1 and C.3 of [RFC5996], with most of the optional payloads removed. Note that the EAP-Initiate/Re-auth message is added.

```
IKE_SA_INIT Exchange:
| init request          --> SA, KE, Ni,
|
| init response       <-- SA, KE, Nr,
|                         N[ERX_SUPPORTED]

IKE_AUTH Exchanges:
| first request       --> EAP(EAP-Initiate/Re-auth),
|                         IDi,
|                         SA, TSi, TSr
|
| first response      <-- IDr, [CERT+], AUTH,
|                         EAP(EAP-Finish/Re-auth)
|
| last request        --> AUTH
|
| last response       <-- AUTH,
|                         SA, TSi, TSr
```

The IDi payload MUST have ID Type ID_RFC822_ADDR, and the data field MUST contain the same value as the KeyName-NAI TLV in the EAP-Initiate/Re-auth message. See Section 3.2 for details.

3.1. Clarification about EAP Codes

Section 3.16 of [RFC5996] enumerates the EAP codes in EAP messages that are carried in EAP payloads. The enumeration goes only to 4. It is not clear whether or not that list is supposed to be exhaustive.

To clarify, an implementation conforming to this specification MUST accept and transmit EAP messages with at least the codes for Initiate and Finish (5 and 6) from Section 5.3 of [RFC6696], in addition to the four codes enumerated in [RFC5996]. This document is intentionally silent about other EAP codes that are not enumerated in those documents.

3.2. Username in the Protocol

The authors, as well as participants of the HOKEY and IPsecME working groups, believe that all use cases for this extension to IKE have a single backend AAA server doing both the authentication and the re-authentication. The reasoning behind this is that IKE runs over the Internet and would naturally connect to the user's home network.

This section addresses instances where this is not the case.

Section 5.3.2 of [RFC6696] describes the EAP-Initiate/Re-auth packet, which, in the case of IKEv2, is carried in the first IKE_AUTH request. This packet contains the KeyName-NAI TLV. This TLV contains the username used in authentication. It is relayed to the AAA server in the AccessRequest message and is returned from the AAA server in the AccessAccept message.

The username part of the Network Access Identifier (NAI) within the TLV is the EMSKName [RFC5295] encoded in hexadecimal digits. The domain part is the domain name of the home domain of the user. The username part is ephemeral in the sense that a new one is generated for each full authentication. This ephemeral value is not a good basis for making policy decisions, and it is also a poor source of user identification for the purposes of logging.

Instead, it is up to the implementation in the IPsec gateway to make policy decisions based on other factors. The following list is by no means exhaustive:

- In some cases, the home domain name may be enough to make policy decisions. If all users with a particular home domain get the same authorization, then policy does not depend on the real username. Meaningful logs can still be issued by correlating VPN gateway IKE events with AAA servers access records.

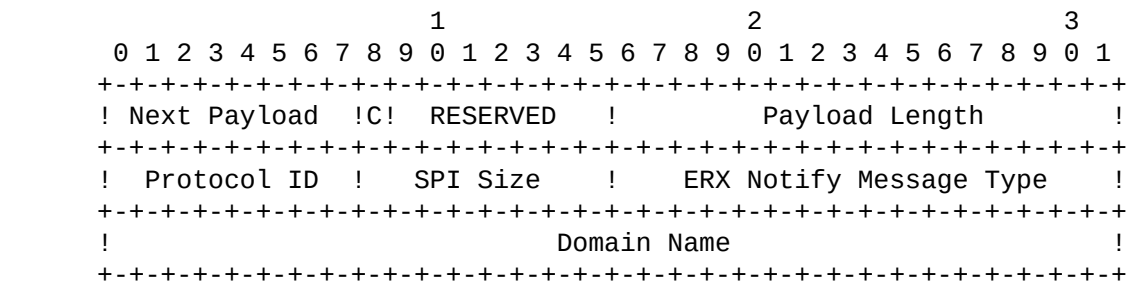
- Sometimes users receive different authorizations based on groups to which they belong. The AAA server can communicate such information to the VPN gateway, for example, using the CLASS attribute [RFC2865] in RADIUS and Diameter [RFC6733]. Logging again depends on correlation with AAA servers.

- AAA servers may support extensions that allow them to communicate with their clients (in our case -- the VPN gateway) to push user information. For example, a certain product integrates a RADIUS server with the Lightweight Directory Access Protocol (LDAP) [RFC4511], so a client could query the server using LDAP and receive the real record for this user. Others may provide this data through vendor-specific extensions to RADIUS or Diameter.

In any case, authorization is a major issue in deployments, if the backend AAA server supporting the re-authentication is different from the AAA server that had supported the original authentication. It is up to the re-authenticating AAA server to provide the necessary information for authorization. A conforming implementation of this protocol MAY reject initiators for which it is unable to make policy decisions because of these reasons.

4. ERX_SUPPORTED Notification

The Notify payload is as described in [RFC5996]:



- Protocol ID (1 octet) - MUST be zero, as this message is related to an IKE SA.

- Security Parameter Index (SPI) Size (1 octet) - MUST be zero, in conformance with Section 3.10 of [RFC5996].

- ERX Notify Message Type (2 octets) - MUST be 16427, the value assigned for ERX.

- Domain Name (variable) - contains the domain name or realm, as these terms are used in [RFC6696] and encoded as ASCII, as specified in [RFC4282].

5. Operational Considerations

This specification changes the behavior of IKE peers, both initiators and responders. The behavior of backend AAA servers is not changed by this specification, but they are required to support [RFC6696]. The same goes for the EAP client, if it's not integrated into the IKE initiator (for example, if the EAP client is an operating system component).

This specification is silent about key storage and key lifetimes on either the EAP client or the EAP server. These issues are covered in Sections 3, 4, and 5 of [RFC6696]. The key lifetime may be communicated from the AAA server to the EAP client via the Lifetime attribute in the EAP-Finish/Re-auth message. If the server does not have a valid key, while the client does have one, regular EAP is used (see Section 3). This should not happen if lifetimes are communicated. In such a case, the IKEv2 initiator / EAP client MAY alert the user and MAY log the event. Note that this does not necessarily indicate an attack. It could simply be a loss of state on the AAA server.

6. Security Considerations

The protocol extension described in this document extends the authentication from one EAP context, which may or may not be part of IKEv2, to an IKEv2 context. Successful completion of the protocol proves to the authenticator, which in our case is a VPN gateway, that the supplicant or VPN client has authenticated in some other EAP context.

The protocol supplies the authenticator with the domain name with which the supplicant has authenticated, but does not supply it with a specific identity. Instead, the gateway receives an EMSKName, which is an ephemeral ID. With this variant of the IKEv2 protocol, the initiator never sends its real identity on the wire while the server does. This is different from the usual IKEv2 practice of the initiator revealing its identity first.

If the domain name is sufficient to make access control decisions, this is enough. If not, then the gateway needs to find out either the real name or authorization information for that particular user. This may be done using the AAA protocol or by some other federation protocol, which is out of scope for this specification.

7. IANA Considerations

IANA has assigned a notify message type of 16427 from the "IKEv2 Notify Message Types - Status Types" registry with the name "ERX_SUPPORTED".

8. Acknowledgements

The authors would like to thank Yaron Sheffer for comments and suggested text that have contributed to this document.

Thanks also to Juergen Schoenwaelder for his OPS-DIR review comments.

9. References

9.1. Normative References

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

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[RFC5295] Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)", RFC 5295, August 2008.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[RFC6696] Cao, Z., He, B., Shi, Y., Wu, Q., and G. Zorn, "EAP Extensions for the EAP Re-authentication Protocol (ERP)", RFC 6696, July 2012.

9.2. Informative References

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC4511] Sermersheim, J., "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, June 2006.

[RFC5723] Sheffer, Y. and H. Tschofenig, "Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption", RFC 5723, January 2010.

[RFC6733] Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol", RFC 6733, October 2012.

[SECBEAC] Sheffer, Y. and Y. Nir, "Secure Beacon: Securely Detecting a Trusted Network", Work in Progress, June 2009.

Authors' Addresses

Yoav Nir
Check Point Software Technologies Ltd.
5 Hasolelim st.
Tel Aviv 67897
Israel

EMail: ynir@checkpoint.com

Qin Wu
Huawei Technologies Co., Ltd.
101 Software Avenue, Yuhua District
Nanjing, JiangSu 210012
China

EMail: sunseawq@huawei.com