Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 4, 2014

V. Smyslov
ELVIS-PLUS

March 3, 2014

The NULL Authentication Method in IKEv2 Protocol
draft-smyslov-ipsecme-ikev2-null-auth-01

Abstract

This document defines the NULL Authentication Method for the IKEv2 Protocol. This method provides a way to omit peer authentication in IKEv2 and to explicitely indicate it in the protocol run. This method may be used to preserve anonymity or in situations, where no trust relationship exists between the parties.

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 September 4, 2014.

Table of Contents

1. Introduction

The Internet Key Exchange Protocol version 2 (IKEv2), specified in [RFC5996], provides a way for two parties to perform authenticated key exchange. Mutual authentication is mandatory in the IKEv2, so that each party must be authenticated by the other, but authentication methods, used by the peers, need not be the same.

In some situations mutual authentication is undesirable or impossible. For example:

- User wants to get anonymous access to some resource. In this situation he/she should be able to authenticate server, but to leave out his/her own authentication to prevent anonymity. In this case one-way authentication is desirable.

- User wants to get some simple action from remote device. Consider garage door opener: it must authenticate user to open the door, but it is not necessary for the user to authenticate the door opener. In this case one-way authentication is sufficient.

- Two peers without any trust relationship want to get some level of security in their communications. Without trust relationship they cannot prevent active Man-in-the-Middle attacks, but it is still possible to prevent passive eavesdropping with opportunistic encryption. In this case they have to perform unauthenticated key exchange.

To meet this needs the document introduces the NULL Authentication Method, which is effectively a "dummy" method, that provides no authentication. This allows peer to explicitely indicate to the other side that he/she is unwilling or unable to certify his/her identity.

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. Using the NULL Authentication Method

In IKEv2 each peer independently selects the method to authenticate himself/herself to the other side. It means that any peer may choose to omit his/her authentication by using the NULL Authentication Method. If it is not acceptable for the peer, he/she MUST return AUTHENTICATION_FAILED Notification. Note, that when initiator uses EAP, responder MUST NOT use the NULL Authentication Method (in conformance with the section 2.16 of [RFC5996]).

The NULL Authentication Method affects how Authentication and Identity Payloads are formed in IKE_AUTH Exchange.

2.1. Authentication Payload

Even when implementation uses the NULL Authentication, the AUTH Payload must still be present in IKE_AUTH Exchange and must be properly formed, as it cryptographically links IKE_SA_INIT Messages with the other Messages sent over IKE SA.

With the NULL Authentication Method the content of AUTH Payload MUST be computed using the syntax for pre-shared secret authentication, described in Section 2.15 of [RFC5996]. The values SK_pi and SK_pr MUST be used as shared secrets for AUTH Payloads generated by Initiator and Responder respectively. Note, that this is exactly how content of the two last AUTH Payloads is calculated in case of using non-key generating EAP Method (see Section 2.16 of [RFC5996] for details). The field Auth Method MUST be set to <TBA by IANA>.

2.2. Identity Payload

The NULL Authentication Method provides no authentication of the party using it. For that reason Identity Payload content cannot be verified by the other party and MUST be ignored by IKE. As peer identity is meaningless in this case, Identification Data SHOULD be omited from ID Payload, in which case ID Type MAY be set to any value. Implementations supporting the NULL Authentication Method MUST NOT fail if they receive such "empty" ID Payload.

3. Security Considerations

IKEv2 protocol provides mutual authentication of the peers. If one peer uses the NULL Authentication Method, then this peer cannot be authenticated by the other side, and it makes authentication in IKEv2 to become one-way. If both peers use the NULL Authentication method, key exchange becomes unauthenticated, that makes it subject to the Man-in-the-Middle attack.

The identity of the peer using the NULL Authenticated Method cannot be verified by the other side and, therefore, MUST NOT be used neither for authorization purposes, nor for policy decisions. All peers who use the NULL Authenticated Method should be considered by the other party as "guests" and get the least possible privileges.

4. Acknowledgments

The author would like to thank Paul Wouters and Yaron Sheffer for their reviews and valueable comments.

5. IANA Considerations

This document defines new value in the "IKEv2 Authentication Method" registry:

<TBA> NULL Authentication Method

6. Normative References

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

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

Author's Address

Valery Smyslov
ELVIS-PLUS
PO Box 81
Moscow (Zelenograd) 124460
Russian Federation

Phone: +7 495 276 0211
Email: svan@elvis.ru