Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 6, 2015

V. Smyslov
ELVIS-PLUS

September 2, 2014

The NULL Authentication Method in IKEv2 Protocol
draft-smyslov-ipsecme-ikev2-null-auth-03

Abstract

This document introduces the NULL Authentication Method for the IKEv2 Protocol. This method provides a way to omit peer authentication in the IKEv2. It may be used to preserve anonymity of or in the 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 March 6, 2015.

Copyright Notice

Table of Contents

1. Introduction

The Internet Key Exchange Protocol version 2 (IKEv2), specified in [IKEv2], 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. However the authentication methods, used by the peers, need not be the same.

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

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

- Sensor, that sleeps most of the time, but periodically wakes up, makes some measurment (e.g. temperature) and sends the results to some server. The senser must be authenticated by the server to ensure authenticity of the measurment, but the server need not be authenticated by the senser. In this case one-way authentication of the initiator 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 can use unauthenticated key exchange.

To meet these needs the document introduces the NULL Authentication Method, which is a "dummy" method, that provides no authentication. This allows peer to explicitly indicate to the other side that it is unwilling or unable to certify its 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 itself to the other side. It means that any of the peers may choose to omit its authentication by using the NULL Authentication Method. If it is not acceptable for the other peer, it MUST return AUTHENTICATION_FAILED Notification. Note, that when the Initiator uses EAP, the Responder MUST NOT use the NULL Authentication Method (in conformance with the section 2.16 of [IKEv2]).

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

2.1. Authentication Payload

Despite the fact that the NULL Authentication Method provides no authentication, the AUTH Payload must still be present in the IKE_AUTH Exchange messages and must be properly formed, as it cryptographically links the IKE_SA_INIT Exchange messages with the other messages sent over the IKE SA.

With the NULL Authentication Method the content of the AUTH Payload MUST be computed using the syntax for pre-shared secret authentication, described in Section 2.15 of [IKEv2]. The values SK_pi and SK_pr MUST be used as shared secrets for the content of the AUTH Payloads generated by Initiator and Responder respectively. Note, that this is exactly how the content of the two last AUTH Payloads is calculated for non-key generating EAP Method (see Section 2.16 of [IKEv2] for details). The value for the the NULL

Authentication Method is <TBA by IANA>.

2.2. Identity Payload

The NULL Authentication Method provides no authentication of the party using it. For that reason the Identity Payload content cannot be verified by the peer and MUST be ignored by the IKE.

This specification defines new ID Type - ID_NULL, which is intended to be used with the NULL Authentication Method to explicitely indicate anonymity of the peer. This ID Type SHOULD NOT be used with other authentication methods. The Identification Data in Identity Payload for the ID_NULL type MUST be absent and the ID Type is set to <TBA by IANA>.

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 be 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.

If endpoint receives a request to create an unauthenticated IKE SA from the IP address, which is configured on the endpoint to be authenticated, the request SHOULD be rejected.

If the peer uses the NULL Authenticated Method, then the content of its Traffic Selector Payloads must be treated with care. In particular, implementations are advised not to trust blindly that the

public IP addresses the peer put into TS Payload are really belong to it. It is RECOMMENDED for security gateways to always assign internal IP addresses to unauthenticated clients as described in Section 2.19 of [IKEv2].

4. Acknowledgments

The author would like to thank Paul Wouters, Yaron Sheffer and Tero Kivinen for their reviews and valuable comments.

5. IANA Considerations

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

<TBA>	NULL Authentication Method

It also defines new value in the "IKEv2 Identification Payload ID

Types" registry:

<TBA>	ID_NULL

6. Normative References

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

[IKEv2] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", draft-kivinen-ipsecme-ikev2-rfc5996bis-04 (work in progress), June 2014.

Author's Address

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

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