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

Abstract

   This document specifies the NULL Authentication method and the
   ID_NULL Identification Payload ID Type for the IKEv2 Protocol. This
   allows two IKE peers to establish single-side authenticated or mutual
   unauthenticated IKE sessions for those use cases where a peer is
   unwilling or unable to authenticate or identify itself. This ensures
   IKEv2 can be used for Opportunistic Security (also known as
   Opportunistic Encryption) to defend against Pervasive Monitoring
   attacks without the need to sacrifice anonymity.

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 August 1, 2015.

Table of Contents

1. Introduction

The Internet Key Exchange Protocol version 2 (IKEv2), specified in
[RFC7296], provides a way for two parties to perform an authenticated
key exchange. While the authentication methods used by the peers can
be different, there is no method for one or both parties to remain
unauthenticated and anonymous. This document extends the
authentication methods to support unauthenticated and anonymous IKE
sessions.

In some situations mutual authentication is undesirable, superfluous
or impossible. The following three examples illustrate these
unauthenticated use cases:

o A user wants to establish an anonymous secure connection to a
   server. In this situation the user should be able to authenticate
   the server without presenting or authenticating to the server with
   their own identity. This case uses a single-sided authentication
   of the responder.

o A sensor that periodically wakes up from a suspended state wants
   to send a measurement (e.g. temperature) to a collecting server.
   The sensor must be authenticated by the server to ensure
   authenticity of the measurement, but the sensor does not need to
   authenticate the server. This case uses a single-sided
   authentication of the initiator.

o Two peers without any trust relationship wish to defend against
   widespread pervasive monitoring attacks as described in [RFC7258].
   Without a trust relationship, the peers cannot authenticate each
   other. Opportunistic Security [RFC7435] states that
   unauthenticated encrypted communication is preferred over
   cleartext communication. The peers want to use IKE to setup an
   unauthenticated encrypted connection, that gives them protection
   against pervasive monitoring attacks. An attacker that is able
   and willing to send packets can still launch an Man-in-the-Middle
   attack to obtain access to the decrypted communication. This case
   uses a fully unauthenticated key exchange.

To meet these needs this document introduces the NULL Authentication
method, and the ID_NULL ID type. This allows an IKE peer to
explicitly indicate 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. A peer may choose to refrain from
authentication by using the NULL Authentication method. If a peer
that requires authentication receives an AUTH payload containing the
NULL Authentication method type, it MUST return an
AUTHENTICATION_FAILED notification. If an initiator uses EAP, the
responder MUST NOT use the NULL Authentication Method (in conformance
with the section 2.16 of [RFC7296]).

NULL Authentication affects how the Authentication and the
Identification payloads are formed in the IKE_AUTH exchange.

2.1. Authentication Payload

NULL Authentication still requires a properly formed AUTH payload to
be present in the IKE_AUTH exchange messages, as the AUTH payload
cryptographically links the IKE_SA_INIT exchange messages with the
other messages sent over this IKE SA.

When using NULL Authentication, the content of the AUTH payload is
computed using the syntax of pre-shared secret authentication,
described in Section 2.15 of [RFC7296]. The values SK_pi and SK_pr
are used as shared secrets for the content of the AUTH payloads
generated by the initiator and the responder respectively. Note that
this is identical to how the content of the two last AUTH payloads is
generated for the non-key-generating EAP methods (see Section 2.16 of
[RFC7296] for details).

The IKEv2 Authentication Method value for NULL Authentication is 13.

2.2. Identification Payload

When a remote peer is not authenticated, any ID presented in the
Identification Data field of the ID payload cannot be validated. To
avoid the need of sending a bogus ID Type with placeholder data, this
specification defines a new ID Type, ID_NULL. The Identification
Data field of the ID payload for this ID Type MUST be empty.

If NULL Authentication is in use and an anonymity is a concern then
ID_NULL SHOULD be used in Identification payload. In some cases
there may be good reasons to use non-null identities (and ID Types
other than ID_NULL) with NULL Authentication. The identities may be
used for logging, troubleshooting or in scenarios when authentication
takes place out of band after the IKE SA is created (like in
[AUTOVPN]). In any case, when NULL Authentication is employed, the
content of Identification payload MUST NOT be used for any trust and

policy checking in IKE_AUTH exchange.

ID_NULL is primarily intended to be used with the NULL
Authentication, but it MAY also be used in other situations, when the
content of Identification payload does not matter. For example,
ID_NULL can be used when authentication is performed via raw public
keys and the identities are these keys themselves. Another example
is EAP authentication when the client identity in ID payload is not
used.

The IKEv2 Identification Payload ID Type for ID_NULL is 13.

2.3. INITIAL_CONTACT Notification

The identity of a peer using NULL Authentication cannot be used to
distinguish from IKE SAs created by other peers using the NULL
Authentication method. For that reason the INITIAL_CONTACT
notifications MUST be ignored for IKE SAs using NULL Authentication.

The standard IKE Liveness Check procedure, decribed in Section 2.4 of
[RFC7296], can be used to detect stale IKE SAs created by peers using
NULL Authentication. Inactive unauthenticated IKE SAs should be
checked periodically. Additionally, the event of creating a new
unauthenticated IKE SA can be used to trigger an out-of-order check
on existing unauthenticated IKE SAs, possibly limited to identical or
close-by IP addresses or to identical identities of the just created
IKE SA.

Implementations should weight the resource consumption of sending
Liveness Checks against the memory usage of possible orphaned IKE
SAs. Implementations may choose to handle situations with thousands
of unauthenticated IKE SAs differently from situations with very few
such SAs.

2.4. Interaction with Peer Authorization Database (PAD)

Section 4.4.3 of [RFC4301] defines the Peer Authorization Database
(PAD), which provides the link between Security Policy Database (SPD)
and the IKEv2. The PAD contains an ordered list of records, with
peers' identities along with corresponding authentication data and
Child SA authorization data. When the IKE SA is being established
the PAD is consulted to determine how the peer should be
authenticated and what Child SAs it is authorized to create.

When using NULL Authentication, the peer identity is not
authenticated and cannot be used. If ID_NULL is used with NULL
Authentication, there is no ID at all. The processing of PAD
described in Section 4.4.3.4 of [RFC4301] must be updated.

If NULL Authentication is supported and allowed, then a special entry
MUST be included in the PAD. This entry MUST contain no
authentication data. It MAY contain a set of constraints for
creating Child SAs as described in Section 4.4.3 of [RFC4301]. When
a peer uses NULL Authentication, regular matching rules for the PAD
MUST be ignored and this special entry MUST be selected regardless of
the peer identity. Likewise, if a peer uses any other authentication
method, then this special entry MUST NOT be selected regardless of
the peer identity and the regular search of the PAD described in
Section 4.4.3.4 of [RFC4301] MUST be performed.

Implementations SHOULD allow to be configured so, that when a peer
requests NULL Authentication, then regular PAD entries are searched
before selecting the special entry, to ensure that there is no entry,
containing peer's IP address. In this case implementations MUST
reject the IKE_AUTH exchange by sending an AUTHENTICATION_FAILED
notification if such an entry is found.

2.5. Traffic Selectors

Traffic Selectors and narrowing allow two IKE peers to mutually agree
on a traffic range for an IPsec SA. An unauthenticated peer must not
be allowed to use this mechanism to steal traffic that an IKE peer
intended to be for another host. This is especially problematic when
supporting anonymous IKE peers behind NAT, as such IKE peers build an
IPsec SA using their pre-NAT IP address that are different from the
source IP of their IKE packets. A rogue IKE peer could use malicious
Traffic Selectors to obtain access to traffic that the host never
intended to hand out. Implementations SHOULD restrict and isolate
all anonymous IKE peers from each other and itself and only allow it
access to itself and possibly its intended network ranges.

One method to achieve this is to always assign internal IP addresses
to unauthenticated IKE clients, as described in Section 2.19 of
[RFC7296]. Implementations may also use other techniques, such as
internal NAT and connection tracking.

Implementations MAY force unauthenticated IKE peers to single host-
to-host IPsec SAs. When using IPv6 it is not always possible, so in
this case implementations MUST be able to assign full /64 address
block to the peer as described in [RFC5739], even if it is not
authenticated.

3. Security Considerations

   If authenticated IKE sessions are possible between the peers, then
   unauthenticated IKE SHOULD NOT be used, unless implementations make
   sure to keep authenticated and unauthenticated IKE sessions separate,
   and has policy rules to specify when to use which IKE session. See
   [RFC7435] for details.

   If both peers use NULL Authentication, the entire key exchange
   becomes unauthenticated. This makes the IKE session vulnerable to
   active Man-in-the-Middle Attacks.

   Using an ID Type other than ID_NULL with the NULL Authentication
   Method may compromise the client's anonimity in case of an active
   MITM attack.

   IKE implementations without NULL Authentication have always performed
   mutual authentication and were not designed for use with
   unauthenticated IKE peers. Implementations might have made
   assumptions that are no longer valid. Furthermore, the host itself
   might have made trust assumptions or may not be aware of the network
   topology changes that resulted from IPsec SAs from unauthenticated
   IKE peers.

3.1. Audit trail and peer identification

   An established IKE session is no longer guaranteed to provide a
   verifiable (authenticated) entity known to the system or network.
   Implementers that implement NULL Authentication should audit their
   implementation for any assumptions that depend on IKE peers being
   "friendly", "trusted" or "identifiable".

3.2. Resource management and robustness

   Section 2.6 of [RFC7296] provides guidance for mitigation of "Denial
   of Service" attacks by issuing COOKIES in response to resource
   consumption of half-open IKE SAs. Furthermore, [DDOS-PROTECTION]
   offers additional counter-measures in an attempt to distinguish
   attacking IKE packets from legitimate IKE peers.

   These defense mechanisms do not take into account IKE systems that
   allow unauthenticated IKE peers. An attacker using NULL
   Authentication is a fully legitimate IKE peer that is only
   distinguished from authenticated IKE peers by having used NULL
   Authentication.

   While implementations should have been written to account for abusive
   authenticated clients, any omission or error in handling abusive

clients may have gone unnoticed because abusive clients has been a
rare or non-existent problem. When enabling unauthenticated IKE
peers, these implementation omissions and errors will be found and
abused by attackers. For example, an unauthenticated IKE peer could
send an abusive amount of Liveness probes or Delete requests.

[3.3](#). IKE configuration selection

Combining authenticated and unauthenticated IKE peers on a single
host can be dangerous, assuming the authenticated IKE peer gains more
or different access from non-authenticated peers (otherwise, why not
only allow unauthenticated peers). An unauthenticated IKE peer MUST
NOT be able to reach resources only meant for authenticated IKE peers
and MUST NOT be able to replace the Child SAs of an authenticated IKE
peer.

[3.4](#). Networking topology changes

When a host relies on packet filters or firewall software to protect
itself, establishing an IKE SA and installing an IPsec SA might
accidentally circumvent these packet filters and firewall
restrictions, as the encrypted ESP (protocol 50) or ESPinUDP (UDP
port 4500) packets do not match the packet filters defined. IKE
peers supporting unauthenticated IKE MUST pass all decrypted traffic
through the same packet filters and security mechanisms as plaintext
traffic.

4. Acknowledgments

The authors would like to thank Yaron Sheffer and Tero Kivinen for their reviews and valuable comments.

5. IANA Considerations

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

   13   NULL Authentication

This document also defines a new entry in the "IKEv2 Identification
Payload ID Types" registry:

   13   ID_NULL

6. References

6.1. Normative References

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

[RFC4301]   Kent, S. and K. Seo, "Security Architecture for the
            Internet Protocol", RFC 4301, December 2005.

[RFC5739]   Eronen, P., Laganier, J., and C. Madson, "IPv6
            Configuration in Internet Key Exchange Protocol Version 2
            (IKEv2)", RFC 5739, February 2010.

[RFC7296]   Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T.
            Kivinen, "Internet Key Exchange Protocol Version 2
            (IKEv2)", STD 79, RFC 7296, October 2014.

6.2. Informative References

[RFC7258]   Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an
            Attack", BCP 188, RFC 7258, May 2014.

[RFC7435]   Dukhovni, V., "Opportunistic Security: Some Protection
            Most of the Time", RFC 7435, December 2014.

[AUTOVPN]   Sheffer, Y. and Y. Nir, "The AutoVPN Architecture", Work
            in Progress, draft-sheffer-autovpn-00, February 2014.

[DDOS-PROTECTION]
            Nir, Y., "Protecting Internet Key Exchange (IKE)
            Implementations from Distributed Denial of Service
            Attacks", draft-ietf-ipsecme-ddos-protection-00 (work in
            progress), October 2014.

Authors' Addresses

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

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

    Paul Wouters
    Red Hat

    Email: pwouters@redhat.com