Network Working Group V. Smyslov
Internet-Draft ELVIS-PLUS
Intended status: Standards Track P. Wouters
Expires: July 17, 2015 Red Hat
January 13, 2015

The NULL Authentication Method in IKEv2 Protocol
draft-ietf-ipsecme-ikev2-null-auth-02

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 un-authenticated IKE sessions for those use cases where a peer is unwilling or unable to authenticate itself. This ensures IKEv2 can be used for Opportunistic Security (also known as Opportunsitic Encryption) to defend against Pervasive Monitoring attacks without the need to sacrifice anonimity.

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 key exchanges.

In some situations mutual authentication is undesirable, superfluous or impossible. The following three examples illustratate these un-authenticated 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 measurment, 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 un-authenticated encrypted communication is prefered over cleartext communication. The peers want to use IKE to setup an un-authenticated 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 anonymous un-authenticated key exchange.

To meet these needs this document introduces the NULL authentication method, and the ID_NULL identity 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 authentiation 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]).

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

2.1. Authentication Payload

The NULL Authentication Method 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 the NULL Authentication Method, 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 KEv2 Authentication Method value for the NULL Authentication Method is 13.

2.2. Identity Payload

When a remote peer is not authenticated, any ID presented in the Identification Data field of the Identification Payload cannot be validated and MUST be ignored. A new Identification Payload ID Type is introduced to avoid the need of sending a bogus ID Type with placeholder data. Furthermore, sending a traditional ID field might unwittingly compromise the anonimity of the peer.

This specification defines a new ID Type of ID_NULL, which SHOULD only be used with the NULL Authentication Method. The Identification Data field of the Identification Payload MUST be empty.

The IKEv2 Identification Payload ID Type for ID_NULL is 13.

2.3. INITIAL_CONTACT Notification

The identity of the peer which uses the NULL Authentication Method cannot be used to distinguish between IKE SAs created by different peers. For that reason the INITIAL_CONTACT notifications MUST be ignored for IKE SAs using the NULL Authentication Method.

When a new IKE SA is established using the NULL Authentication Method, implementations MAY perform a Liveness Check on all other IKE SAs that were established using the NULL Authentication Method. To mitigate the potential impact of sending Liveness Check messages on a large number of IKE SAs, implementations are advised not to blindly perform Liveness Check on every such SA, but to take into considerations additional information, that may indicate that the particular SA is alive. This information may include the recent receipt of cryptographically protected message on the IKE SA or any of its Child SAs, or a successfull Liveness Check that was performed recently.

3. Security Considerations

If both peers use the NULL Authentication Method, the entire key exchange becomes unauthenticated. This makes the IKE session vulnerable to active Man-in-the-Middle Attacks. Un-authenticated IKE sessions MUST only attempted when authenticated IKE sessions are not possible for the remote host and the only alternative would be to send plaintext. See [RFC7435] for details.

Implementations SHOULD use the ID_NULL Identity Type with the NULL Authenticated Method. If an un-authenticated remote IKE peer presents an Identity Type different from ID_NULL, the Identification Payload data MUST NOT be used for anything except logging.

Using an ID Type other than ID_NULL with the NULL Authentication

Method compromises the client's anonimity. This should be avoided for regular operation but could be temporarilly enabled, for example to aid with troubleshooting diagnostics. Sending an unverifiable identification for any other purpose is strongly discouraged as it leads to a false sense of security,

IKE implementations without the NULL Authentication Method have always performed mutual authentication and were not designed for use with un-authenticated 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 un-authenticated 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. Implementations that add the NULL Authentication Method 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-meassures in an attempt to distinguish attacking IKE packets from legitimate IKE peers.

These defense mechanisms do not take into account IKE systems that allow un-authenticated IKE peers. An attacker using the NULL Authentication Method is a fully legitimate IKE peer that is only

distinguished from authenticated IKE peers by the Authenticaion Method

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 un-authenticated IKE peers, these implementation omissions and errors will be found and abused by attackers. For example, an un-authenticated IKE peer could send an abusive amount of Liveness probes or Delete requests.

3.3. IKE configuration selection

Combining authenticated and un-authenticated 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 un-authentcated peers). An un-authenticated IKE peer MUST NOT be able to reach resources only meant for authenticated IKE peers and MUST NOT be able to replace the IPsec SAs of an authenticated IKE peer.

If an IKE peer receives an IKE_AUTH exchange requesting a NULL Authentication Method from an IP address that matches a configured connection for an authenticated IKE session, it MUST reject the IKE_AUTH exchange by sending an AUTHENTICATION_FAILED notification.

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 circument 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 un-authenticated IKE MUST pass all decrypted traffic through the same packet filters and security mechanisms as plaintext traffic.

Traffic Selectors and narrowing allow two IKE peers to mutually agree on a traffic range for an IPsec SA. An un-authenticated 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 of the ways to achive that is to always assign internal IP addresses to un-authenticated 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 un-authenticated IKE peers to single host-to-host IPsec SAs.

3.5. Priviledged IKE operations

Some IKE features are not appropriate for un-authenticated IKE peers and should be restricted or forbidden.

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 Method
```

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.

[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.

[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