NETWORK WORKING GROUP
Internet-Draft
Expires: August 5, 2007

N. Williams
Sun
M. Richardson
SSW

February 2007

Extensions to IKEv1 and IKEv2 to indicate use of Better-Than-Nothing-Security
draft-richardson-btns-ikeextensions-00.txt

Status of this Memo

Copyright Notice

Abstract

This document specifies how to use the Internet Key Exchange (IKE) protocols, such as IKEv1 and IKEv2, to setup "unauthenticated" security associations (SAs) for use with the IPsec Encapsulating Security Payload (ESP) and the IPsec Authentication Header (AH). This is part of the Better-Than-Nothing-Security (BTNS) work. Two optional IKE extensions are documented here, and the format for one certificate payload type is fully specified.

Table of Contents

1. Introduction

When two nodes decide to use BTNS, they may wish to communicate this intention to the remote party.

There are no protocol reasons to require this intention to be communicated, however, it is useful for diagnostic purposes to be able to indicate this fact in the IKE negotiation.

As part of the BTNS IKE negotiation, it will be necessary for the parties to exchange authentication keying material, and one option is to use the certificate payload. The use of Raw RSA Key type (11) is clarified with some examples.

2. IKE Notify

A new notify message is defined for both IKEv1 [RFC2408] and IKEv2 [RFC4306]. The name of the new notify is BTNS_AUTHENTICATED, and the notify number is TBD1.

This notify message MAY appear in any exchange of phase 1 (IKEv1), and in any exchange of the PARENT_SA (IKEv2). It SHOULD be sent in after the phase 1 SA has become private, since there is little reason to advise a third party of what kind of authentication is being done.

This means it SHOULD be sent during the third exchange of MAIN MODE (IKEv1), in the second exchange of Aggressive Mode (IKEv1), and during the second exchange of IKEv2.

Note: Aggressive mode is SHOULD NOT be used for BTNS.

3. Exchange of public keys

A BTNS negotiation MUST include a public key for each end-point. This key will be carried in a Certificate Payload (section 3.6 of [RFC4306] and section 3.9 of [RFC2408]). There are several options as to how to carry the key.

The public KEY MUST be sent in a Certificate Type 11: Raw RSA Key. This code point is hereby defined for IKEv1 identically to IKEv2.

An implementation MAY also include the same public KEY in a Certificate Payload of type 1 (PKCS #7 wrapped X.509), and it may be self-signed or relative to some CA.

An IKEv2 implementation MAY also include the same public KEY as a Hash and URL of X.509 certificate bundle (type 13), or certificate (type 12). (In general, an implementation should not send both type 1 and types 12 or 13, as it would be redundant.)

An implementation MAY also send additional Certificate Payload types which it believes may be useful, provided that they all lead to the same RSA key. An implementation SHOULD avoid using so many Certificate Payload types that it causes the IKE messages to be fragmented.

An implementation receiving more than one Certificate Payload SHOULD use the following sources to arrive at a public key to use to authenticate the peer, in the following order:

a preconfigure RSA key contained in a local trusted store.

an in-band X.509 certificate that can be verified against a locally trusted root CA

a certificate or certificate bundle retrieved from the indicated URL, that matches the hash, and can be verified

the key contained in the raw RSA Key payload

All Certificate Payload types other than type 11 are optional, and type 11 is mandatory, so there will always be a public key available to confirm the signature on in the IKE AUTH payload.

The additional payloads are present to deal with the situations where the trust relationship may in fact be asymetrical, such as for the Asymetrical SAB (A-SAB), and for the Asymetrical IKE CBB (AI-CBB). (see [I-D.ietf-btns-prob-and-applic])

4. IANA Considerations

Please assign NOTIFY Type TBD1. from the Notify-Types in the ipsec-registry of IKEv1.

Please assign NOTIFY Type TBD1. from the IKEv2 Notify Message Types table of the ikev2-parameters registry.

5. Security Considerations

This document does not introduce any new mechanisms or modes to IKEv1 or IKEv2. It details the order in which to look for authentication data for a protocol which does not in itself require any authentication data.

6. Normative References

[I-D.ietf-btns-connection-latching]
Williams, N., "IPsec Channels: Connection Latching", draft-ietf-btns-connection-latching-00 (work in progress), February 2006.

[I-D.ietf-btns-prob-and-applic]
Touch, J., "Problem and Applicability Statement for Better Than Nothing Security (BTNS)", draft-ietf-btns-prob-and-applic-03 (work in progress), June 2006.

[I-D.ietf-kitten-gssapi-channel-bindings]
Williams, N., "Clarifications and Extensions to the GSS-API for the Use of Channel Bindings", draft-ietf-kitten-gssapi-channel-bindings-01 (work in progress), October 2005.

[I-D.ietf-nfsv4-channel-bindings]
Williams, N., "On the Use of Channel Bindings to Secure Channels", draft-ietf-nfsv4-channel-bindings-03 (work in progress), February 2005.

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

[RFC2408] Maughan, D., Schneider, M., and M. Schertler, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC2743] Linn, J., "Generic Security Service Application Program Interface Version 2, Update 1", RFC 2743, January 2000.

[RFC4251] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006.

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

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

Authors' Addresses

Nicolas Williams
Sun Microsystems
5300 Riata Trace Ct
Austin, TX 78727
US

Email: Nicolas.Williams@sun.com

Michael C. Richardson
Sandelman Software Works
470 Dawson Avenue
Ottawa, ON K1Z 5V7
CA

Email: mcr@sandelman.ottawa.on.ca
URI: http://www.sandelman.ottawa.on.ca/

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).