NETWORK WORKING GROUP
Internet-Draft
Intended status: Standards Track
Expires: October 23, 2008

N. Williams
Sun

April 21, 2008

End-Point Channel Bindings for IPsec Using IKEv2 and Public Keys
draft-williams-ipsec-channel-binding-01.txt

Status of this Memo

Copyright Notice

Abstract

This document specifies the end-point channel bindings for "IPsec channels" where the peers used the Internet Key Exchange protocol version 2 (IKEv2) and where they used public keys and/or certificates to authenticate each other. Specifically, we use hashes of the end-points' public keys.

Table of Contents

1. Introduction

Given the ability to construct IPsec channels [I-D.ietf-btns-connection-latching] and the ability to bind authentication at application layers to such secure channels [RFC5056] the only missing components are: a definition of IPsec channel bindings, and Application Programming Interfaces (APIs) by which applications can obtain them.

Here we specify the "end-point channel bindings" [RFC5056] for IPsec channels when peers use IKEv2 [RFC4306] and public keys and/or certificates [RFC3280]. IPsec APIs [I-D.ietf-btns-ipsec-apireq] are out of scope for this document, but some requirements for such APIs are provided here.

IPsec channels where the peers were authenticated by methods other than public key cryptography, such as EAP [RFC3748] or pre-shared keys (PSK), or where IKEv2 was not used (e.g., manual keying), are out of scope for this document. Channel bindings for such IPsec channels should be specified elsewhere, if at all (see [I-D.williams-ipsec-unique-channel-binding]).

The primary feature of IPsec end-point channel bindings as specified here is this: there is no reference to the actual contents of any key exchanges other than the public keys used therein. Algorithm negotiations, nonces, session keys, and so on are of no consequence. And no additional message exchanges of any kind are needed in order to establish the end-point channel bindings for an IPsec channel.

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. IPsec Unique Channel Bindings

The end-point channel bindings for IPsec channels established via connection latching [I-D.ietf-btns-connection-latching] between peers that use IKEv2 [RFC4306] and public keys (with or without PKIX certificates [RFC3280]) SHALL be:

```
HASH(HASH(ID1) XOR HASH(ID2))
```

Where HASH() is a cryptographic hash function selected by the application requesting the end-point channel bindings. Implementations MUST support the use of SHA-256 [RFC4634]. ID1 and ID2 are the raw public keys of each peer. If a peer uses a certificate, the value of the subjectPublicKey field (a BIT STRING) of the certificate's subjectPublicKeyInfo field is to be used verbatim. If a peer uses a Raw RSA CERT payload, then the Certificate Data portion of that CERT payload will be used verbatim. XOR is used here to avoid having to determine an order in which end-point IDs should be used.

The rationale for using hashes of public keys is: to greatly reduce the size of channel binding data that might need to be tracked in kernel-mode implementations (as we'd otherwise use the raw public key bit strings, which can be in excess of a kilobyte).

2.1. API Requirements

Because of the use of a hash function which must be selected by the application, implementations of IPsec connection latching and end-point channel bindings MUST provide a way, in the API for obtaining channel bindings, for the application to select the hash function to use.

Since hash agility here depends on the application and its ability to negotiate hash functions for this purpose, implementations MUST provide an API for listing the supported hash functions.

3. IANA Considerations

This document creates a type of channel binding, and so requires registration in the IANA channel binding registry (set out by [RFC5056]).

The registration procedure will be followed when this document enters the RFC-Editor queue. The registration will be as follows:

- Channel binding unique prefix (name): IPsec-end-point-IKEv2-pubkey-sha-256
- Channel binding type: end-point
- Channel type: IPsec
- Published specification: <TBD>
- Channel binding is secret: no
- Description: see Section 2
- Intended usage: COMMON
- Contact: this document's author/editor
- Owner/Change controller: IETF

4. Security Considerations

The security considerations of [RFC5056], [I-D.ietf-btns-connection-latching], and IPsec generally [RFC4301] apply. The security of an application using channel binding to IPsec channels depends critically on the overall security of each of these components: IPsec [RFC4301], including the Internet Key Exchange (IKEv2) protocol [RFC4306], ESP/AH [RFC4303] [RFC4302], IPsec connection latching [I-D.ietf-btns-connection-latching], and the application's authentication and channel binding mechanism (potentially too many to reference here, but a common example is likely to be the Kerberos V mechanism [RFC4121] for the Generic Security Services API (GSS-API) [RFC2743]. A compromise of any one of those components may compromise the application to varying degrees.

This document describes end-point channel bindings for some IPsec channels. End-point channel bindings do not uniquely identify a connection in time, but a pair of peers. This is sufficient to detect man-in-the-middle attacks via channel binding. There are no additional security considerations, relating to the type of this channel binding, beyond those described in [RFC5056].

Use of non-pre-shared Raw RSA public keys or certificates that cannot be validated to a given trust anchor is supported in the Better Than Nothing (BTNS) [I-D.ietf-btns-prob-and-applic] [I-D.ietf-btns-core] model. When combined with connection latching and channel binding BTNS can provide all the security that an application requires but without having to deploy an IPsec authentication infrastructure (e.g., a PKI, manual pre-sharing of raw RSA public keys and/or self-signed certificates).

The construction of IPsec end-point channel bindings described herein depends on the strength of the public key algorithms used by the IPsec peers to authenticate each other. Because we use hashes of _public_ keys this construction does not require confidentiality protection of the channel bindings.

We use a hash function in the construction of IPsec channel bindings. Correspondingly, we provide for hash agility, but we push the responsibility for hash agility to the application. Applications cannot know what hash function their peers support without negotiating a hash function. Supporting multiple hash functions requires computing the end-point channel bindings for each supported hash function, and it requires storing, in each IPsec channel, all the those end-point channel bindings. Thus minimizing the number of supported hash functions is important.

5. References

5.1. Normative References

[I-D.ietf-btns-connection-latching]
Williams, N., "IPsec Channels: Connection Latching", draft-ietf-btns-connection-latching-06 (work in progress), February 2008.

[I-D.ietf-btns-ipsec-apireq]
Richardson, M. and B. Sommerfeld, "Requirements for an IPsec API", draft-ietf-btns-ipsec-apireq-00 (work in progress), April 2006.

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

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

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

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

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

[RFC4634] Eastlake, D. and T. Hansen, "US Secure Hash Algorithms (SHA and HMAC-SHA)", RFC 4634, July 2006.

[RFC5056] Williams, N., "On the Use of Channel Bindings to Secure Channels", RFC 5056, November 2007.

5.2. Informative References

[I-D.ietf-btns-core]
Williams, N. and M. Richardson, "Better-Than-Nothing-Security: An Unauthenticated Mode of IPsec", draft-ietf-btns-core-06 (work in progress), January 2008.

[I-D.ietf-btns-prob-and-applic]

Touch, J., Black, D., and Y. Wang, "Problem and Applicability Statement for Better Than Nothing Security (BTNS)", draft-ietf-btns-prob-and-applic-06 (work in progress), October 2007.

[I-D.williams-ipsec-unique-channel-binding]
Williams, N., "Unique Channel Bindings for IPsec Using IKEv2", draft-williams-ipsec-unique-channel-binding-00 (work in progress), April 2008.

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

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC4121] Zhu, L., Jaganathan, K., and S. Hartman, "The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2", RFC 4121, July 2005.

Author's Address

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

Email: Nicolas.Williams@sun.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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