Network Working Group
Internet-Draft
Expires: December 3, 2007

E. Ertekin
M. Casey
J. Pezeshki
C. Christou
Booz Allen Hamilton

June 1, 2007

IPsec Extensions to Support Robust Header Compression over IPsec (RoHCoIPsec)
draft-ertekin-rohc-ipsec-extensions-hcoipsec-01

Status of this Memo

Copyright Notice

Abstract

Integrating RoHC with IPsec (RoHCoIPsec) offers the combined benefits of IP security services and efficient bandwidth utilization. Before this can be realized, however, several extensions to the Security Policy Database (SPD), the Security Association Database (SAD), and the IPsec process are required. This document describes the IPsec

extensions required to support RoHCoIPsec.

Table of Contents

1. Introduction

Using IPsec ([IPSEC]) protection offers various security services for IP traffic. However, for tunnel-mode security associations, these benefits come at the cost of additional packet headers, which increase packet overhead. As described in [ROHCOIPSEC], Robust Header Compression (RoHC [ROHC]) can be used with IPsec to reduce the overhead associated with IPsec-protected packets.

IPsec-protected traffic is carried between peers by Security Associations (SAs), whose parameters are negotiated on a case-by-case basis. The Security Policy Database (SPD) specifies the services that are to be offered to IP datagrams, and the parameters associated with SAs that have been established are stored in the Security Association Database (SAD). To fully integrate RoHC and IPsec, various extensions to the SPD and SAD that incorporate RoHC-relevant parameters are required.

In addition, two extensions to the IPsec processing methodology are required. First, a mechanism for identifying RoHC packets must be defined. Second, the order of the inbound and outbound processing must be enumerated when nesting IP Compression (IPComp [IPCOMP]), RoHC, and IPsec processing.

2. Extensions to IPsec Databases

The following subsections specify extensions to the SPD and the SAD to support RoHCoIPsec.

2.1. Security Policy Database (SPD)

In general, the SPD is responsible for specifying the security services that are offered to IP datagrams. Entries in the SPD specify how to derive the corresponding values for SAD entries. To support RoHC, the SPD must be extended to include per-channel RoHC parameters. Together, the existing IPsec SPD parameters and the RoHC parameters will dictate packet disposition for traffic that is to be compressed, and subsequently protected by IPsec.

The fields contained within each SPD entry are defined in [IPSEC], Section 4.4.1.2. To support RoHC, several processing info fields must be added to the SPD; these fields contain information regarding the RoHC profiles and channel parameters supported by the local RoHC instance. The per-channel configuration parameters required for RoHC in the SPD are as follows (note that this information must only be included in the SPD if the processing info field is set to PROTECT, and if the IPsec mode is set to tunnel mode):

MAX_CID: The highest context ID number to be used by the compressor. MAX_CID must be at least 0 and at most 16383 (The value 0 implies having one context). The suggested value for MAX_CID is 15.

PROFILES: This indicates the RoHC profiles supported by the decompressor. The list of possible values this field may assume is defined in the [ROHCPROF] registry.

MRRU: The size of the largest reconstructed unit that the decompressor is expected to reassemble from segments. In general, is not anticipated that a RoHC over IPsec instance will use RoHC segmentation features. Consequently, the suggested value for MRRU is 0.

MAX_HEADER: The largest header size (in octets) that can be compressed. Note that the four RoHC profiles defined in RFC 3095 do not provide for a MAX_HEADER parameter. The parameter MAX_HEADER is therefore without consequence in these profiles. Other profiles (e.g., ones based on RFC 2507) can make use of the parameter by explicitly referencing it.

Note: The RoHC LARGE_CIDS channel parameter is set implicitly, based on the value of MAX_CID. Furthermore, the RoHC FEEDBACK_FOR channel parameter is set implicitly to the RoHC channel associated with the SA in the reverse direction. Because both of these RoHC channel parameters are set implicitly, they are not stored in the SPD or SAD.

2.2. Security Association Database (SAD)

Each entry within the SAD defines the parameters associated with each established SA. Unless if the "populate from packet" (PFP) flag is asserted for a particular field, SAD entries are determined by the corresponding SPD entries during the creation of the SA.

The data items contained within the SAD are defined in [IPSEC], Section 4.4.2.1. To support RoHC, this list of data items is augmented to include a "RoHC Data Item" field that defines the RoHC parameters. These parameters (i.e., MAX_CID, PROFILES, MRRU, and MAX_HEADER) are enumerated above in Section 2.1. The RoHC parameters used for a given SA may be initialized manually (i.e., administratively configured for manual SAs), or initialized via a key exchange protocol (e.g. IKEv2 [IKEV2]) that has been extended to support the negotiation of RoHC parameters [IKEV2EXT].

3. Extensions to IPsec Processing

3.1. Addition to the IANA Protocol Numbers Registry

In order to demultiplex header-compressed from uncompressed traffic on a RoHC-enabled SA, a "RoHC" value must be reserved in the IANA Protocol Numbers registry. If an outbound packet has a compressed header, the Next Header field of the security protocol header (e.g., AH [AH], ESP [ESP]) must be set to the "RoHC" protocol identifer. If the packet header has not been compressed, the Next Header field remains unaltered. Conversely, for an inbound packet, the value of the security protocol Next Header field is checked to determine if the packet maintains a RoHC header.

3.2. Nested IPComp and RoHCoIPsec Processing

IPComp ([IPCOMP]) is another mechanism that can be implemented to reduce the size of an IP datagram. If IPComp and RoHCoIPsec are implemented in a nested fashion, the order of the outbound and inbound processing steps must be carefully enumerated.

For outbound packets that are to be processed by IPcomp and RoHC:

- IPComp is applied, and the packet is sent to RoHC module
- The appropriate RoHC compression profile (e.g., RoHC IP-only) is applied to the packet
- The security protocol is applied to the packet

Conversely, for inbound packets that are to be both RoHC- and IPcomp-decompressed:

- A packet received on a RoHC-enabled SA is IPsec-processed
- Subsequently, the packet is sent to the RoHC module for header decompression
- The datagram is decompressed based on the appropriate IPComp algorithm

4. Security Considerations

A malfunctioning RoHC compressor (i.e., the compressor located at the ingress of the IPsec tunnel) has the ability to send packets to the decompressor (i.e., the decompressor located at the egress of the IPsec tunnel) that do not match the original packets emitted from the end-hosts. Such a scenario will result in a decreased efficiency between compressor and decompressor. Furthermore, this may result in Denial of Service, as the decompression of a significant number of invalid packets may drain the resources of an IPsec device.

5. IANA Considerations

IANA is requested to allocate one value within the "Protocol Numbers" registry [PROTOCOL] for "RoHC". This value will be used to indicate that the next level protocol header is a RoHC header.

6. Acknowledgments

The authors would like to thank Mr. Sean O'Keeffe, Mr. James Kohler, Ms. Linda Noone of the Department of Defense, and Mr. A. Rich Espy of OPnet for their contributions and support for developing this document. In addition, the authors would like to thank Mr. Rohan Jasani for his valuable assistance.

7. References

7.1. Normative References

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

[ROHCOIPSEC] Ertekin, E. and C. Christou, "Integration of Header Compression over IPsec Security Associations", work in progress , February 2007.

[ROHC] Bormann, C., Burmeister, C., Degermark, M., Fukushima, H., Hannu, H., Jonsson, L., Hakenberg, R., Koren, T., Le, K., Liu, Z., Martensson, A., Miyazaki, A., Svanbro, K., Wiebke, T., Yoshimura, T., and H. Zheng, "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", RFC 3095, July 2001.

[IPCOMP] Shacham, A., Monsour, R., Pereira, and Thomas, "IP Payload Compression Protocol (IPComp)", RFC 3173, September 2001.

[IKEV2] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[IKEV2EXT] Pezeshki, J., Ertekin, E., and C. Christou, "Extensions to IKEv2 to Support Robust Header Compression over IPsec (RoHCoIPsec)", work in progress , February 2007.

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

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

7.2. Informative References

[ROHCPROF]
"RObust Header Compression (ROHC) Profile Identifiers", www.iana.org/assignments/rohc-pro-ids , October 2005.

[PROTOCOL]
IANA, ""Assigned Internet Protocol Numbers", IANA registry at: http://www.iana.org/assignments/protocol-numbers".

Authors' Addresses

Emre Ertekin
Booz Allen Hamilton
13200 Woodland Park Dr.
Herndon, VA 20171
US

Email: ertekin_emre@bah.com

Michele Casey
Booz Allen Hamilton
13200 Woodland Park Dr.
Herndon, VA 20171
US

Email: casey_michele@bah.com

Jonah Pezeshki
Booz Allen Hamilton
13200 Woodland Park Dr.
Herndon, VA 20171
US

Email: pezeshki_jonah@bah.com

Chris Christou
Booz Allen Hamilton
13200 Woodland Park Dr.
Herndon, VA 20171
US

Email: christou_chris@bah.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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