Robust Header Compression
Internet-Draft
Intended status: Standards Track
Expires: February 1, 2008

C. Bormann
Universitaet Bremen TZI
July 31, 2007

A ROHC Profile for CID shutdown (ROHC-DOWN)
draft-bormann-rohc-shutdown-profile-00.txt

Status of this Memo

Copyright Notice

Abstract

This document specifies a ROHC (Robust Header Compression) profile for shutting down context IDs (CIDs). The profile, called ROHC-DOWN, enables the decompressor to free resources and the compressor to be sure no residual state from a previous use survives on a CID.

$Id: draft-bormann-rohc-shutdown-profile.xml,v 1.5 2007/07/31 15:40:11 cabo Exp $

Table of Contents

1. Introduction

Both the original ROHC standard [RFC3095] and the current work on the now separately defined framework [I-D.ietf-rohc-rfc3095bis-framework], have an issue with ambiguities in the re-use of context IDs (CIDs) induced by packet losses and reordering.

While the current mechanisms as defined in the cited specifications suffice for the detection of accidental confusion about the current use of a CID, they might be circumvented in a malicious "decompressor confusion attack" to subvert the integrity protection of channels carrying header-compressed flows.

The ROHC shutdown profile (ROHC-DOWN) provides a reliable way for a compressor to prepare a CID for reuse, without the danger of that CID reuse to be misused for a decompressor confusion attack.

As a secondary consideration, ROHC-DOWN provides a compressor the generally useful ability to indicate to the decompressor when the use of a CID has ended in order to allow it to free associated resources.

2. Profile Operation

This section gives an overview of the operation of ROHC-DOWN.

The ROHC-DOWN profile operates by not allowing any packet to be decompressed from a context in this profile; it is thus indistinguishable from an uninitialized context.

To allow the compressor to ascertain that a CID is indeed shut down, the IR packet may include a (possibly empty) nonce to be echoed in a feedback item.

2.1. Creating Contexts

A ROHC-DOWN context is created using an IR (initialization/refresh) packet, which contains a ROHC framework header followed by the ROHC-DOWN nonce:

If the x bit is set to 1, the compressor expects the decompressor to echo back the (0-or-more byte) nonce in a feedback item. If the x bit is set to 0, no such feedback is expected (the nonce can still be supplied, but has no effect).

```
        0   1   2   3   4   5   6   7
       --- --- --- --- --- --- --- ---
      :         Add-CID octet         :  if CID 1-15 and small CID
      +---+---+---+---+---+---+---+---+
      | 1   1   1   1   1   1   0 | x |  IR type octet
      +---+---+---+---+---+---+---+---+
      :                               :
      /      0-2 octets of CID        /  1 or 2 octets if large CIDs
      :                               :
      +---+---+---+---+---+---+---+---+
      |            Profile            |  1 octet
      +---+---+---+---+---+---+---+---+
      |              CRC              |  1 octet
      +---+---+---+---+---+---+---+---+
      :                               :
      /             NONCE             /  0-or-more bytes of Nonce
      :                               :
      +---+---+---+---+---+---+---+---+
```

2.2. Using Contexts

No ROHC-DOWN packet types other than IR are defined. The decompressor MUST treat non-IR packet types in a context initialized for the ROHC-DOWN profile as it would treat them in an uninitialized context.

2.3. Feedback

If a reply is requested in an IR packet by setting x to 1, the decompressor SHOULD send back the nonce byte-string in a ROHC feedback message. If the nonce is empty (zero bytes), the feedback is sent as a ROHC FEEDBACK-1 message consisting of a single zero byte. If the nonce is at least one byte, the feedback is sent as a ROHC FEEDBACK-2 message, preceded by one zero byte. The zero byte is composed of the ROHC framework Acktype of 0 (ACK, see ROHC framework) and six bits that MUST be zero. In effect, the nonce is prefixed by a zero byte in both cases. In both cases, the feedback is not to be received as a valid acknowledgement if this byte is not actually zero.

```
        0   1   2   3   4   5   6   7
      +---+---+---+---+---+---+---+---+
      | 1   1   1   1   0 |   Code    |  feedback type
      +---+---+---+---+---+---+---+---+
      :             Size              :  if Code = 0
      +---+---+---+---+---+---+---+---+
      :         Add-CID octet         :  for small CIDs and (CID != 0)
      +---+---+---+---+---+---+---+---+
      :                               :
      /  large CID (5.3.2 encoding)   /  1-2 octets if for large CIDs
      :                               :
      +---+---+---+---+---+---+---+---+
      /         FEEDBACK data         /  variable length
      +---+---+---+---+---+---+---+---+

      FEEDBACK-1:

        0   1   2   3   4   5   6   7
      +---+---+---+---+---+---+---+---+
      |               0               |  1 octet
      +---+---+---+---+---+---+---+---+

      FEEDBACK-2:

        0   1   2   3   4   5   6   7
      +---+---+---+---+---+---+---+---+
      |Acktype|           0           |
      +---+---+---+---+---+---+---+---+  at least 2 octets
      :                               :
      /             NONCE             /  0-or-more bytes of Nonce
      :                               :
      +---+---+---+---+---+---+---+---+

      Acktype:  0 = ACK
```

3. Security considerations

The security considerations of [RFC3095] apply.

The objective of this draft is mainly to mitigate a potential attack based on confusing the decompressor sufficiently that it accidentally forwards information to receivers of packets previously sent on a context. By waiting for positive acknowledgement of channel shutdown before re-using a channel, this attack can be effectively prevented.

Note that in an HCoIPsec environment, there is never a pressing need to re-use a context; a compressor that is somehow running out of CIDs can always negotiate a new SA and thus a new ROHC channel. For some applications, a new SA will be set up for each new flow in any case. Being able to re-use contexts may, however, simplify running more long-term SAs as ROHC channels.

Apart from the uses described above, the ROHC-DOWN profile can also be used as a way to probe the channel at various packet sizes and to send traffic obfuscating the packet size signature. For the first use, sending a ROHC-DOWN IR packet on an unused CID with x==1 acts as a kind of ping mechanism. A compressor can use this mechanism to regularly probe a channel, investigating whether it is subject to malicious packet dropping at particular (larger) packet sizes. For the second use, sending a ROHC-DOWN IR packet in an unused CID with x==0 acts as a no-operation, allowing to randomly add packets of otherwise possibly telltale sizes to the channel.

4. IANA Considerations

The ROHC profile identifier 0x0099 [# Editor's Note: To be replaced before publication #] has been reserved by the IANA for the profile defined in this document.

[# Editor's Note: rest of this section to be removed before publication: #]

Two ROHC profile identifiers must be reserved by the IANA for the new profile defined in this document. A suggested registration in the "RObust Header Compression (ROHC) Profile Identifiers" name space would then be:

Profile	Usage	Reference
0x0099	ROHC DOWN	[RFC XXXX (this)]

Author's note: This suggestion must be updated before sending to IANA.

5. Contributors

The author would like to thank Pasi Eronen, who emphasized the importance of the decompressor confusion attack in his comments to HCoIPsec, and Jonah Pezeshki, who narrowed down the problem sufficiently for the author to find this solution.

6. Acknowledgements

This document was prompted by the work on HCoIPsec by Emre Ertekin, Chris Christou, and others.

7. References

7.1. Normative References

[I-D.ietf-rohc-rfc3095bis-framework]
Jonsson, L., "The RObust Header Compression (ROHC) Framework", draft-ietf-rohc-rfc3095bis-framework-04 (work in progress), November 2006.

7.2. Informative References

[RFC3095] Bormann, C., Burmeister, C., Degermark, M., Fukushima, H., Hannu, H., Jonsson, L-E., 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.

Author's Address

Carsten Bormann
Universitaet Bremen TZI
Postfach 330440
Bremen D-28334
Germany

Phone: +49 421 218 7024
Fax: +49 421 218 7000
Email: cabo@tzi.org

Full Copyright Statement

Intellectual Property

Acknowledgment

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