Workgroup: SCHC Working Group
Internet-Draft:
draft-toutain-schc-access-control-03
Published: 22 October 2023
Intended Status: Standards Track
Expires: 24 April 2024
Authors: A. Minaburo L. Toutain
Consultant Institut MINES TELECOM; IMT Atlantique
I. Martinez
Nokia Bell Labs

SCHC Rule Access Control

Abstract

The framework for SCHC defines an abstract view of the rules, formalized through a YANG Data Model. In its original description, rules are static and shared by two endpoints. This document defines defines augmentation to the existing Data Model in order to restrict the changes in the rule and, therefore, the impact of possible attacks.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 24 April 2024.

Table of Contents

1. Introduction
2. Conventions and Definitions
3. Terminology
4. SCHC TV/MO/CDA possible combinations
5. YANG Access Control
6. YANG Data Model
   6.1. leaf ac-modify-set-of-rules
   6.2. leaf ac-modify-compression-rule
   6.3. leaf ac-modify-field
      6.3.1. CoAP base header Access Control.
      6.3.2. CoAP Options Access Control.
7. Normative References
Appendix A. YANG Data Model
Appendix B. Security Considerations
Appendix C. IANA Considerations
Authors' Addresses

1. Introduction

SCHC is a compression and fragmentation mechanism defined in [RFC8724] while [RFC9363] provides a YANG Data Model for formal representation of SCHC Rules used either for compression/ decompression (C/D) or fragmentation/reassembly (F/R). The inappropriate changes to SCHC Rules leads to some possible attacks. The goal of this document is to define a augmentation to the existing Data Model in order to restrict the changes in the rules and, therefore, the impact of possible attacks.

2. Conventions and Definitions

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Terminology

It is expected that the reader will be familiar with the terms and concepts associated with the SCHC framework [RFC8724], [I-D.ietf-schc-architecture], and managmente request processing [I-D.ietf-core-comi], NETCONF[RFC6241], RESTCONF [RFC8040].

ToDo * Access Control. * Management request processing: The NETCONF, RESTCONF or CORECONF request is processed and passed to the end-point Rule Manager. * Rule Manager (RM). * Context. SCHC Rules

4. SCHC TV/MO/CDA possible combinations

SCHC compression behavior uses the TV, MO, and CDA to generate the correct residue. But not all the combinations of this fields descriptors are possible, and then an attack can be detected or avoided. Figure 1 shows all the combinations and those that are enabled. SCHC defines two TV values: set and not set. SCHC MO can be Equal, Ignore, MSB, or Match-mapping. And SCHC CDA can be not-sent, value-sent, mapping-sent, LSB, compute-*, DevIID, or AppIID.

TV / MO	CDA						
	not-sent	value -sent	mapping -sent	LSB	compute-*	DevIID	AppIID
set / Equal	ok	absurd	x	x	absurd	absurd	absurd
not set /Equal	x	x	x	x	absurd	absurd	absurd
set / Ignore	ok (D)	absurd	x	x	ok	ok	ok
not set/Ignore	x	ok	x	x	ok	ok	ok
set / MSB	absurd	absurd	x	ok	absurd	absurd	absurd
not set / MSB	absurd	absurd	x	ok	absurd	absurd	absurd
set / Match -mapping	x	absurd	ok	x	absurd	absurd	absurd
not set/ Match -mapping	x	x	absurd	x	absurd	absurd	absurd

Figure 1: SCHC TV, MO, CDA valid combinations

5. YANG Access Control

YANG language allows to specify read-only or read write nodes. NACM [RFC8341] extends this by allowing users or groups of users to perform specific actions.

This granularity does not fit this rule model. For instance, the goal is not to allow all the field-id leaves to be modified. The objective is to allow a specific rule entry to be changed and, therefore, some of the leaves to be modified. For instance, an entry with FID containing Uri-path may have its target value modified, as in the same rule, the entry regarding the application prefix should not be changed.

The SCHC access control augments the YANG module defined in [RFC9363] to allow a remote entity to manipulate the rules. Several levels are defined.

- in the set of rules, it authorizes or not a new rule to be added.
- in a compression rule, it allows adding or removing field descriptions.
- in a compression rule, it allows modifying some elements of the rule, such as the TV, MO, or/and CDA, and associated values.
- in a fragmentation rule, it allows modifying some parameters.

6. YANG Data Model

The YANG DM proposed in Appendix A extends the SCHC YANG Data Model introduced in [RFC9363]. It adds read-only leaves containing access rights. If these leaves are not present, the information cannot be modified.

6.1. leaf ac-modify-set-of-rules

This leaf controls modifications applied to a set of rules. They are specified with the rule-access-right enumeration:

- no-change (0): rules cannot be modified in the Set of Rules. This is the equivalent of having no access control elements in the set of rules.
- modify-existing-element (1): an existing rule may be modified.
- add-remove-element (2): a rule can be added or deleted from the Set of Rules, or an existing rule can be modified.

6.2. leaf ac-modify-compression-rule

This leaf allows to modify a compression element. To be active, leaf ac-modify-set-of-rules **MUST** be set to modify-existing-element or

add-remove-element. This leaf uses the same enumeration as add-remove-element:

*no-change (0): The rule cannot be modified.

*modify-existing-element (1): an existing Field Description may be modified.

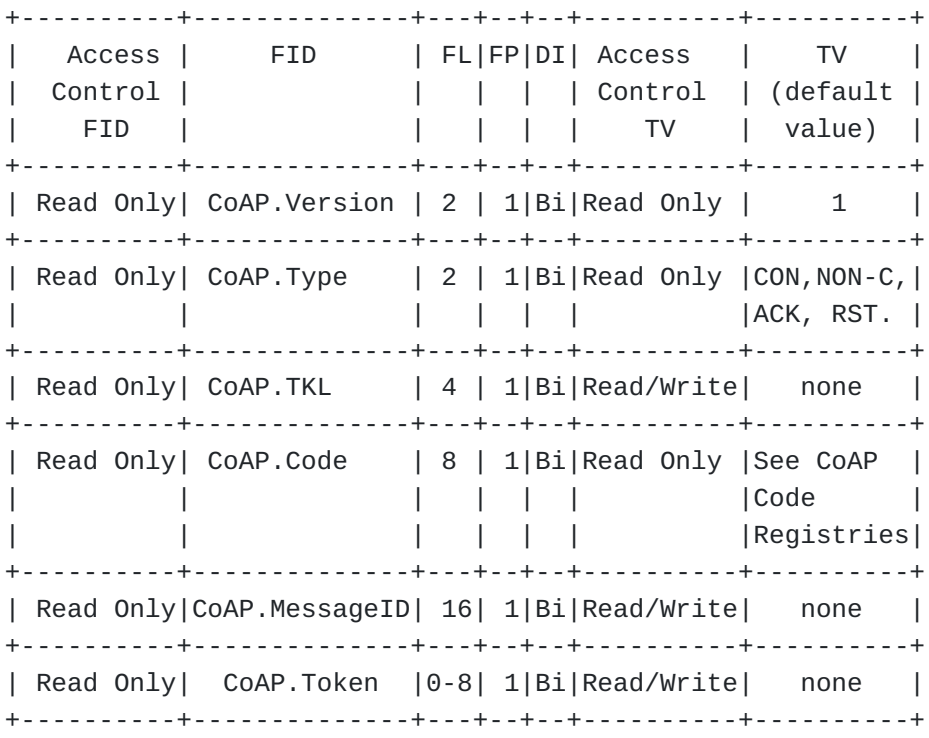
*add-remove-element (2): a Field Description can be added or deleted from the Rule or an existing rule can be modified.

6.3. leaf ac-modify-field

This leaf allows to modify a Field Description in a compression rule. To be active, leaves ac-modify-set-of-rules and ac-modify-compression-rule **MUST** be set to modify-existing-element or add-remove-element and ac-modify-compression-rule and leaf

6.3.1. CoAP base header Access Control.

CoAP protocol uses a request/reply model with compact messages. The format of these messages starts with a fixed format of 4-byte length, followed by a variable Token format with a length between 0 and 8 bytes. While applying SCHC header compression [RFC8824], the based header is only readable and **MUST** not be modified. Figure 2 shows the access-control for the FID and TV in a Rules.



Access Control FID	FID	FL	FP	DI	Access Control TV	TV (default value)
Read Only	CoAP.Version	2	1	Bi	Read Only	1
Read Only	CoAP.Type	2	1	Bi	Read Only	CON,NON-C,ACK, RST.
Read Only	CoAP.TKL	4	1	Bi	Read/Write	none
Read Only	CoAP.Code	8	1	Bi	Read Only	See CoAP Code Registries
Read Only	CoAP.MessageID	16	1	Bi	Read/Write	none
Read Only	CoAP.Token	0-8	1	Bi	Read/Write	none

Figure 2: Access Control for the CoAP Header

6.3.2. CoAP Options Access Control.

The CoAP options are used by both request and responses messages. Some of them are defined as repeatable which implies that it **MAY** be included one or more times in a message. In this case, a SCHC Rule **MAY** be able to modify the FID and the TV in order to include the repetition. The only FID's that have access to be modifiable are those that have been defined as repeatable. The Figure 3 give the control access for all the CoAP Options defined in [RFC7252]; [RFC8613]; [RFC8768]; [RFC9177]; [RFC7959]; and [RFC9175].

Access Control FID	CoAP Opt. Num.	FID	FL	FP	DI	Access Control TV	TV (default value)
Read/ Write	1	CoAP.Option. If-Match	0-8	var	Bi	Read/ Write	none
Read Only	3	CoAP.Option. Uri-Host	1-255	var	Bi	Read/ Write	Sect. 5 RFC7252
Read/ Write	4	CoAP.Option. ETag	1-8	var	Bi	Read/ Write	none
Read Only	5	CoAP.Option. If-None-Match	0	1	Bi	Read Only	empty
Read Only	6	CoAP.Option. Observe	0-3	var	Bi	Read Only	none
Read Only	7	CoAP.Option. Uri-Port	0-2	var	Bi	Read Only	Sect. 5 RFC7252
Read/ Write	8	CoAP.Option. Location-Path	0-255	var	Bi	Read/ Write	none
Read Only	9	CoAP.Option. OSCORE	0-255	var	Bi	Read Only	none
Read/ Write	11	CoAP.Option. Uri-Path	0-255	var	Bi	Read/ Write	none
Read Only	12	CoAP.Option. Content-Format	0-2	var	Bi	Read Only	none
Read Only	14	CoAP.Option. Max-Age	0-4	var	Bi	Read Only	60
Read/ Write	15	CoAP.Option. Uri-Query	0-255	var	Bi	Read/ Write	none
Read Only	16	CoAP.Option. Hop-Limit	1	1	Bi	Read Only	16
Read Only	17	CoAP.Option. Accept	0-2	var	Bi	Read Only	none
Read	19	CoAP.Option.				Read	none

Only		Q-Block1	0-3	var	Bi	Only	
Read/ Write	20	CoAP.Option. Location-Query	0-255	var	Bi	Read/ Write	none
Read Only	23	CoAP.Option. Block2	0-3	var	Bi	Read Only	none
Read Only	27	CoAP.Option. Block1	0-3	var	Bi	Read Only	none
Read Only	28	CoAP.Option. Size2	0-4	var	Bi	Read Only	none
Read/ Write	31	CoAP.Option. Q-Block2	0-3	var	Bi	Read/ Write	none
Read Only	35	CoAP.Option. Proxy-Uri	1-1034	var	Bi	Read Only	none
Read Only	39	CoAP.Option. Proxy-Scheme	1-255	var	Bi	Read Only	none
Read Only	60	CoAP.Option. Size1	0-4	var	Bi	Read Only	none
Read Only	252	CoAP.Option. Echo	1-40	var	Bi	Read Only	none
Read Only	258	CoAP.Option. No-Response	0-1	1	Up	Read Only	0
Read Only	292	CoAP.Option. Request-Tag	0-8	var	Bi	Read Only	none

Figure 3: CoAP Options access-control

7. Normative References

[I-D.ietf-core-comi] Veillette, M., Van der Stok, P., Pelov, A., Bierman, A., and C. Bormann, "CoAP Management Interface (CORECONF)", Work in Progress, Internet-Draft, draft-

ietf-core-comi-16, 4 September 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-core-comi-16>.

[I-D.ietf-schc-architecture] Pelov, A., Thubert, P., and A. Minaburo, "Static Context Header Compression (SCHC) Architecture", Work in Progress, Internet-Draft, draft-ietf-schc-architecture-01, 6 October 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-schc-architecture-01>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[RFC7959] Bormann, C. and Z. Shelby, Ed., "Block-Wise Transfers in the Constrained Application Protocol (CoAP)", RFC 7959, DOI 10.17487/RFC7959, August 2016, <https://www.rfc-editor.org/info/rfc7959>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018, <https://www.rfc-editor.org/info/rfc8341>.

[RFC8613] Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", RFC 8613, DOI 10.17487/RFC8613, July 2019, <https://www.rfc-editor.org/info/rfc8613>.

[RFC8724] Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and JC. Zuniga, "SCHC: Generic Framework for Static Context

Header Compression and Fragmentation", RFC 8724, DOI 10.17487/RFC8724, April 2020, <https://www.rfc-editor.org/info/rfc8724>.

[RFC8768] Boucadair, M., Reddy.K, T., and J. Shallow, "Constrained Application Protocol (CoAP) Hop-Limit Option", RFC 8768, DOI 10.17487/RFC8768, March 2020, <https://www.rfc-editor.org/info/rfc8768>.

[RFC8824] Minaburo, A., Toutain, L., and R. Andreasen, "Static Context Header Compression (SCHC) for the Constrained Application Protocol (CoAP)", RFC 8824, DOI 10.17487/RFC8824, June 2021, <https://www.rfc-editor.org/info/rfc8824>.

[RFC9175] Amsüss, C., Preuß Mattsson, J., and G. Selander, "Constrained Application Protocol (CoAP): Echo, Request-Tag, and Token Processing", RFC 9175, DOI 10.17487/RFC9175, February 2022, <https://www.rfc-editor.org/info/rfc9175>.

[RFC9177] Boucadair, M. and J. Shallow, "Constrained Application Protocol (CoAP) Block-Wise Transfer Options Supporting Robust Transmission", RFC 9177, DOI 10.17487/RFC9177, March 2022, <https://www.rfc-editor.org/info/rfc9177>.

[RFC9363] Minaburo, A. and L. Toutain, "A YANG Data Model for Static Context Header Compression (SCHC)", RFC 9363, DOI 10.17487/RFC9363, March 2023, <https://www.rfc-editor.org/info/rfc9363>.

Appendix A. YANG Data Model

```
<CODE BEGINS> file "ietf-schc-access-control@2023-02-14.yang"

module ietf-schc-access-control {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-schc-access-control";
  prefix schc-ac;

  import ietf-schc {
      prefix schc;
  }

  organization
    "IETF IPv6 over Low Power Wide-Area Networks (lpwan) working group";
  contact
    "WG Web:   <https://datatracker.ietf.org/wg/lpwan/about/>
     WG List:  <mailto:lp-wan@ietf.org>
     Editor:   Juan-Carlos Zuniga
       <mailto:juancarlos.zuniga@sigfox.com>";
  description
     "
     Copyright (c) 2021 IETF Trust and the persons identified as
     authors of the code.  All rights reserved.

     Redistribution and use in source and binary forms, with or
     without modification, is permitted pursuant to, and subject to
     the license terms contained in, the Simplified BSD License set
     forth in Section 4.c of the IETF Trust's Legal Provisions
     Relating to IETF Documents
     (https://trustee.ietf.org/license-info).

     This version of this YANG module is part of RFC XXXX
     (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself
     for full legal notices.

     The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL
     NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'NOT RECOMMENDED',
     'MAY', and 'OPTIONAL' in this document are to be interpreted as
     described in BCP 14 (RFC 2119) (RFC 8174) when, and only when,
     they appear in all capitals, as shown here.

     ******************************************************************

     This module extends the ietf-schc module to include the compound-ac
     behavior for Ack On Error as defined in RFC YYYY.
     It introduces a new leaf for Ack on Error defining the format of th
     SCHC Ack and add the possibility to send several bitmaps in a singl
     answer.";

  revision 2023-02-14 {
    description
```

```
    "Initial version for RFC YYYY ";
  reference
    "RFC YYYY: Compound Ack";
}

typedef rule-access-right {
  type enumeration {
    enum no-changes {
      value 0;
      description
        "No change are allowed.";
    }
    enum modify-existing-element {
      value 1;
      description
        "can modify content inside an element.";
    }
    enum add-remove-element {
      value 2;
      description
        "Allows to add or remove or modify an element.";
    }
  }
}

typedef field-access-right {
  type enumeration {
    enum no-change {
      value 0;
      description
        "Reserved slot number.";
    }
    enum change-tv {
      value 1;
      description
        "Reserved slot number.";
    }
    enum change-mo-cda-tv {
      value 2;
      description
        "Reserved slot number.";
    }
  }

}

augment "/schc:schc/schc:rule" {
  leaf ac-modify-set-of-rules {
        config false;
```

```
          type rule-access-right;
        }
  }

  augment "/schc:schc/schc:rule/schc:nature/schc:compression" {
    leaf ac-modify-compression-rule {
          config false;
          type rule-access-right;
        }
  }

  augment "/schc:schc/schc:rule/schc:nature/schc:compression/schc:entry"
    leaf ac-modify-field {
          config false;
          type field-access-right;
        }
  }

  augment "/schc:schc/schc:rule/schc:nature/schc:fragmentation" {
    leaf ac-modify-timers {
          config false;
          type boolean;
        }
  }


}

<CODE ENDS>
```

Appendix B. Security Considerations

TBD

Appendix C. IANA Considerations

TBD

Authors' Addresses

Ana Minaburo
Consultant
Rue de Rennes
35510 Cesson-Sevigne Cedex
France

Email: anaminaburo@gmail.com

Laurent Toutain
Institut MINES TELECOM; IMT Atlantique

2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

Email: Laurent.Toutain@imt-atlantique.fr

Ivan Martinez
Nokia Bell Labs
12 Rue Jean Bart
91300 Massy
France

Email: ivan.martinez_bolivar@nokia-bell-labs.com