

Access Control

Authors:

A. Minaburo <anaminaburo@gmail.com>

Laurent Toutain <Laurent.Toutain@imt-atlantique.fr>

Ivan Martinez <ivan.Martinez_bolivar@nokia-bell-labs.com>

SCHC Access Control

- Updates from -00
 - Added Terminology Section
 - **TODO:** Uniform terms from 8724 and draft archi
 - Changed SCHC Management Architecture
 - Added Threat Model
 - Added TV/MO/CDA Combinations

Terminology

- Set of Rules (SoR), Context, Rule database, Rule set ?
- Instance, session ?
- Rule Manager (RM) ?

SCHC Management Architecture

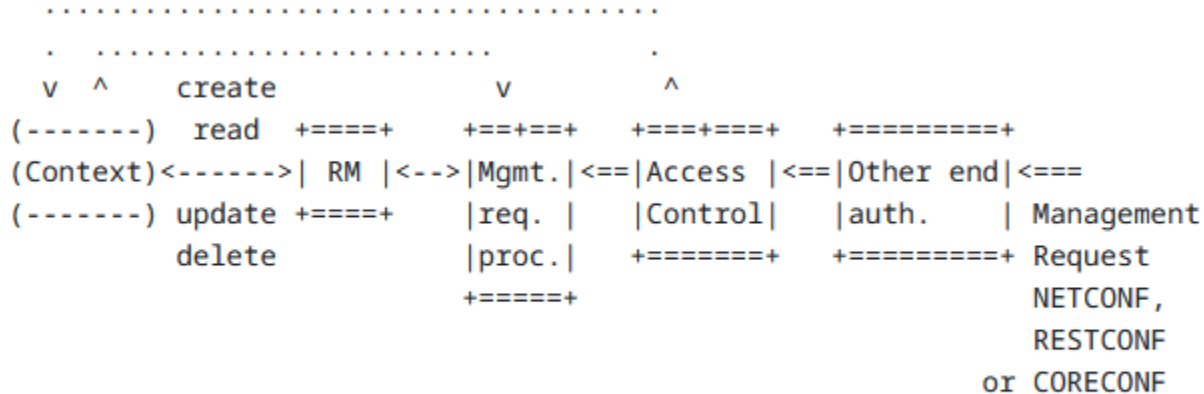


Figure 1: Overview of management architecture.

Threat Model

1. There is a RM in charge of applying changes to the **rules database (context)** when a management request arrives at a SCHC end-point.
2. Changes can only be effectively applied when it is sure that all end-points of an instance have made the change.
3. The selection of a rule to be applied in an accurate endpoint when a packet arrives is made by selecting the rule offering the **best- performance**
4. The attack scenarios considered are limited to the rule management layer and only involve that **a single endpoint in a given instance has been compromised**.
5. Therefore, the compromised endpoint is able to effectively **deliver management requests using NETCONF, RESTCONF, or CORECONF to the other endpoint**.

TV/MO/CDA Combinations

TV / MO	CDA						
	not-sent	value	mapping	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	x	absurd	ok	x	absurd	absurd	absurd
-mapping	x	x	absurd	x	absurd	absurd	absurd
not set / Match	x	x	absurd	x	absurd	absurd	absurd
-mapping	x	x	absurd	x	absurd	absurd	absurd

Allowed behavior

Might be an attack vector

Figure 2: SCHC TV, MO, CDA valid combinations

Attack Scenarios

- **Scenario 1 – Compromised device:**

Compromised Device A Device RM, under the control of an attacker, **sends some management messages to modify the SCHC rules in the core** in order to direct the traffic to another application.

The impact of this attack is different depending on the original rule:

1. Rules containing exclusively the pair **MO -- CDA : (ignore -- not- sent)** or rules such as **no-compress** or **no-fragmentation**:
 - No risk of information lost
 - There is a risk of a DoS-type attack as it can flood empty packets that pass at the core level.

Attack Scenarios

- **Scenario 1 – Compromised device:**

2. Management messages aiming at changing rules where the length of the residue changes:

- * There can be a risk of desynchronizing rules between the core and the compromised device.
- * The attack is limited to a single end-point (the device) since it does not have the right to change core-level rules.

Attack Scenarios

- **Scenario 2 – Compromised core:**

A Core RM, under the control of an attacker, **sends some management messages to modify the SCHC rules in the device** in order to delete the device's data. In such a scenario, the attacker will try to inject destructive rules.

The main characteristic of these rules is that **the combination of MA -- CA reduces the size of the residue**, which has, in turn, made it more attractive since it increases the rate of compression.

The impact of this attack could be: *** Lost of devices' information if nothing is done to preempt a compromised core to change such a rule.**