Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 21, 2014

C. Bormann
Universitaet Bremen TZI

January 17, 2014

An Authorization Information Format (AIF) for ACE
draft-bormann-core-ace-aif-00

Abstract

Constrained Devices as they are used in the "Internet of Things" need security. One important element of this security is that devices in the Internet of Things need to be able to decide which operations requested of them should be considered authorized, need to ascertain that the authorization to request the operation does apply to the actual requester, and need to ascertain that other devices they place requests on are the ones they intended.

On the ACE mailing list, an activity to create specifications for such authenticated authorization for constrained devices is contemplated.

One potential work item is an Authorization Information Format (AIF).

This document provides a strawman for such a format that is intended to enable further discussion of the objectives for its development.

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 http://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 July 21, 2014.

Copyright Notice

Table of Contents

1. Introduction

(See Abstract.)

1.1. Terminology

This memo uses terms from [I-D.ietf-core-coap] and [RFC4949].

The term "byte", abbreviated by "B", is used in its now customary sense as a synonym for "octet".

2. Information Model

Authorizations are generally expressed through some data structures that are cryptographically secured (or transmitted in a secure way). This section discusses the information model underlying the payload of that data (as opposed to the cryptographic armor around it).

For the purposes of this strawman, the underlying access control model will be that of an access matrix, which gives a set of permissions for each possible combination of a subject and on object.

For the objects, we simply use the URI of a resource on a CoAP server. More specifically, the parts of the URI that identify the server ("authority" in [RFC3986]) are considered to be the realm of the authentication mechanism (which are handled in the cryptographic armor); we therefore focus on the "path-absolute" and "query" parts of the URI (URI "local-part" in this specification, as expressed by the Uri-Path and Uri-Query options in CoAP). Similarly, we do not concern the AIF format with the subject for which the AIF object is issued, focusing the AIF object on a single row in the access matrix (such a row traditionally is also called a capability list).

At the information model level, this leaves a set of pairs of local URIs and related permissions. We simplify the model for the permissions to simply giving the subset of the CoAP methods permitted. This model is summarized in Table 1 (what is a row in an access matrix is now just a set of pairs, so it looks like a pair of columns):

local-part	Permission Set
/s/light	GET
/a/led	PUT, GET
/dtls	POST

Table 1: An authorization instance in the AIF Information Model

In this example an authenticated subject is authorized to access three resources on the server to which this authorization information applies. Different operations are allowed on the individual objects, e. g. read access (CoAP method GET) to /s/light, or create access (CoAP method POST) on /dtls.

2.1. Limitations

This simple information model only allows granting permissions for static URIs. It is probably necessary to extend the model towards URI templates [RFC6570], however, that requires some considerations of the ease and unambiguity of matching a given URI against a set of templates in an AIF object.

This simple information model also doesn't allow conditionalizing access (e.g., "opening a door is allowed if that isn't exhibiting the state 'locked'").

Finally, the model does not provide any dynamic functions such as enabling special access for a set of resources that are specific to a subject, e.g. those that the subject created itself by previous operations (PUT, POST) or that were specifically created for the subject by others.

3. Data Model

For representing the AIF object discussion in Section 2, the permission set is reduced to a single number by the following steps:

- The entries in the table that specify the same local-part are merged into a single entry that specifies the union of the permission sets
- The methods in the permission sets are converted into their CoAP method numbers
- The set of numbers is converted into a single number by taking each number to the power of two and computing the inclusive OR of the binary representations of all the numbers.

This strawman data model could be interchanged in the JSON [RFC4627] representation given in Figure 1 (more extensible/more compact representations are possible).

```
[["/s/light", 1], ["/a/led", 5], ["/dtls", 2]]
```

Figure 1: An authorization instance encoded in JSON (46 bytes)

A straightforward representation of the same information in CBOR [RFC7049] is given in Figure 2; again, several optimizations/ improvements are possible.

```
83                      # array(3)
   82                   # array(2)
      68                # text(8)
         2f732f6c69676874 # "/s/light"
      01                # unsigned(1)
   82                   # array(2)
      66                # text(6)
         2f612f6c6564   # "/a/led"
      05                # unsigned(5)
   82                   # array(2)
```

```
65                  # text(5)
   2f64746c73       # "/dtls"
02                  # unsigned(2)
```

Figure 2: An authorization instance encoded in CBOR (29 bytes)

4. IANA Considerations

This document makes no requirements on IANA. (This section to be removed by RFC editor.)

5. Security Considerations

(TBD. Some issues are already discussed in the security considerations of [I-D.ietf-core-coap] and in [I-D.garcia-core-security].)

6. Acknowledgements

TBD

7. References

7.1. Normative References

[I-D.ietf-core-coap] Shelby, Z., Hartke, K., and C. Bormann, "Constrained Application Protocol (CoAP)", draft-ietf-core-coap-18 (work in progress), June 2013.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

7.2. Informative References

[I-D.garcia-core-security] Garcia-Morchon, O., Kumar, S., Keoh, S., Hummen, R., and R. Struik, "Security Considerations in the IP-based Internet of Things", draft-garcia-core-security-06 (work in progress), September 2013.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC4627] Crockford, D., "The application/json Media Type for JavaScript Object Notation (JSON)", RFC 4627, July 2006.

[RFC6570] Gregorio, J., Fielding, R., Hadley, M., Nottingham, M., and D. Orchard, "URI Template", RFC 6570, March 2012.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, October 2013.

Author's Address

Carsten Bormann
Universitaet Bremen TZI
Postfach 330440
Bremen D-28359
Germany

Phone: +49-421-218-63921
Email: cabo@tzi.org