ACE Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 7, 2020

M. Tiloca
L. Seitz
RISE AB
F. Palombini
Ericsson AB
S. Echeverria
G. Lewis
CMU SEI

November 04, 2019

Notification of Revoked Access Tokens in the Authentication and Authorization for Constrained Environments (ACE) Framework
draft-tiloca-ace-revoked-token-notification-00

Abstract

This document specifies a method of the Authentication and Authorization for Constrained Environments (ACE) framework, which allows an Authorization Server to notify Clients and Resource Servers (i.e., registered devices) about revoked Access Tokens. The method relies on resource observation for the Constrained Application Protocol (CoAP), with Clients and Resource Servers observing a dedicated, device-specific Token Revocation List on the Authorization Server. Resulting unsolicited notifications of revoked Access Tokens complement alternative approaches such as token introspection, while not requiring additional endpoints on Clients and Resource Servers.

Table of Contents

1. Introduction

Authentication and Authorization for Constrained Environments (ACE) [I-D.ietf-ace-oauth-authz] is a framework that enforces access control on IoT devices acting as Resource Servers. In order to use ACE, both Clients and Resource Servers have to register with an Authorization Server (AS) and become a registered device. Once registered, a Client can send a request to the AS for an Access Token for a Resource Server (RS). For a Client to access the RS, the Client must present the issued Access Token at the RS, which then validates and stores it.

Even though Access Tokens have expiration times, there are circumstances by which an Access Token may need to be revoked before its expiration time, such as: (1) a registered device has been compromised, or is suspected of being compromised; (2) a registered device is decommissioned; (3) there has been a change of access policies for a registered device; and (4) there has been a change in the ACE profile for a registered device.

This document specifies a method for allowing registered devices to access and observe a Token Revocation List (TRL) resource on the AS, in order to get an updated list of revoked, but yet not expired, Access Tokens. In particular, registered devices rely on resource observation for the Constrained Application Protocol (CoAP) [RFC7641]. The benefits of this method are that it complements introspection, and does not require any additional endpoints on the registered devices.

1.1. Terminology

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.

Readers are expected to be familiar with the terms and concepts described in the ACE framework for authentication and authorization [I-D.ietf-ace-oauth-authz], as well as with terms and concepts related to CBOR Web Tokens (CWTs) [RFC8392]. The terminology for entities in the considered architecture is defined in OAuth 2.0 [RFC6749]. In particular, this includes Client (C), Resource Server (RS), and Authorization Server (AS).

Readers are also expected to be familiar with the terms and concepts related to CBOR [RFC7049] and COSE [RFC8152], the CoAP protocol [RFC7252], CoAP Observe [RFC7641], and the use of hash functions to name objects as defined in [RFC6920].

Note that, unless otherwise indicated, the term "endpoint" is used here following its OAuth definition, aimed at denoting resources such as /token and /introspect at the AS, and /authz-info at the RS. This document does not use the CoAP definition of "endpoint", which is "An entity participating in the CoAP protocol".

This specification also refers to the following terminology.

- Registered device: a device registered at the AS, as Client or RS.

- Token name: name of an Access Token, in binary format encoding. The Token Name has no relation to other possibly used token identifiers, such as the "cti" (CWT ID) claim of CBOR Web Tokens (CWTs) [RFC8392].

- Token Revocation List (TRL): a collection of Token names, in which the corresponding Access Tokens have been revoked but are not expired yet.

- TRL resource: a resource on the AS, with a TRL as its representation.

- TRL endpoint: an endpoint at the AS associated to a TRL resource.

2. Protocol Overview

This protocol defines how a CoAP-based AS informs Clients and Resource Servers, i.e. registered devices, about revoked tokens. How the relationship between the registered device and the AS is established is out of scope for this work.

At a high level, the steps of this protocol are as follows:

- When a device is registered at the AS, the AS generates a new TRL resource associated to that device. At any point in time, the TRL resource represents a list of all revoked Access Tokens referring to that registered device that are yet not expired. If the registered device is a Client, the associated TRL resource represents the revoked non-expired Access Tokens issued by the AS to that Client. If the registered device is a Resource Server, the associated TRL resource represents the revoked non-expired Access Tokens issued by the AS and to be consumed by that Resource Server. The TRL resource is communicated to the device in the course of the registration process.

- After the device registration is concluded, the device sends an observation request to that TRL resource as described in [RFC7641], i.e. a GET request with an Observe option set to 0 (register). Upon receiving the request, the AS adds the device to the list of observers of that TRL resource.

- When an Access Token is revoked, the AS adds the corresponding token name to the representation of the TRL resource. Also, when a revoked Access Token eventually expires, the AS removes the corresponding token name from the representation of the TRL resource. In either case, after updating the representation of the TRL resource, the AS sends the updated corresponding list of token names to the registered device as an Observe Notification, as described in [RFC7641].

3. Upon Device Registration

When a device is registered at an AS, the AS creates a TRL resource under the resource path "/trl". It is RECOMMENDED for the AS to use the device identifier for this resource's name, e.g. "coap://example.as.org/trl/rs1807".

The initial content of this resource SHALL be an empty CBOR array. The AS SHALL implement measures to prevent access to this resource by devices other than the registered device.

After the registration procedure is finished, the registered device performs a GET request to that resource, including the CoAP Observe option set to 0 (register), in order to register an observation of the TRL resource at the AS, as per Section 3.1 of [RFC7641]. The AS SHALL respond with the initial value of the TRL resource, i.e. an empty CBOR array, using the CoAP response code 2.05 (Content) and the CoAP Observe option with value 1.

From that point on, the device can send GET requests to the TRL resource at any time, in order to query the current list of revoked Access Tokens related to the device. Unsolicited notifications are provided through the CoAP observation mechanism, as described in Section 4.

4. Notification of Revoked Tokens

When a non-expired Access Token is revoked, the AS checks to which Client the Access Token was issued to, and which audience the Access Token addresses. Note that the audience could resolve to a list of Resource Servers. The AS then updates the TRL resources of these registered devices, to include an identifier of the Access Token, namely the corresponding token name.

Token names are generated as follows. The AS takes the binary representation of the Access Token and generates a hash value as per Section 6 of [RFC6920]. The resulting binary format name is used as the token name.

The specifically used hash-function MUST be collision-resistant on byte-strings, and MUST be selected from the "Named Information Hash Algorithm" Registry defined in Section 9.4 of [RFC6920].

The AS then sends Observe notifications to all the registered devices affected by the revocation of that Access Token, as per Section 4.2 of [RFC7641].

When a revoked Access Token expires, the AS removes the corresponding token name from the TRLs related to the affected registered devices. This will also trigger an Observe notification to those registered devices, as per Section 4.2 of [RFC7641].

5. Example

Figure 1 shows an example interaction between a Resource Server RS1 and an Authorization Server AS. The details of the registration process are omitted, but it is assumed that RS1 sends an unspecified payload to the AS, and then the AS replies with a 2.01 (Created) response. The response contains a CBOR map, which includes a "trl" parameter, specifying the path of the just created TRL resource.

The function 'h(x)' refers to the hash function used to compute the token names according to [RFC6920] (see Section 4). In addition, 'bstr.t1' and 'bstr.t2' denote the byte-string representations of the token names for the Access Tokens t1 and t2, respectively.

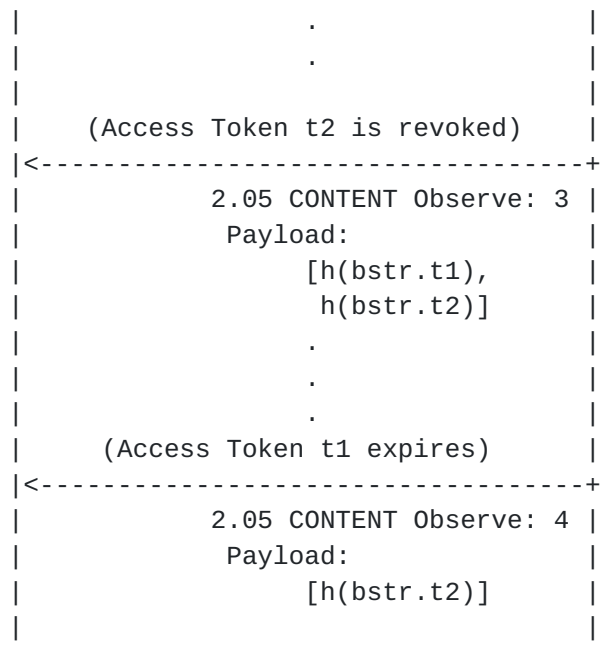

Figure 1: Example of the communication between a RS and AS

6. Security Considerations

Security considerations are inherited from the ACE framework for Authentication and Authorization [I-D.ietf-ace-oauth-authz], from [RFC8392] as to the usage of CWTs, from [RFC7641] as to the usage of CoAP Observe, and from [RFC6920] with regards to resource naming through hashes.

The AS SHOULD ensure that only registered devices associated with a TRL resource can access that specific TRL. The AS can have an access control list or similar to prevent registered devices from getting TRLs associated to other registered devices.

If a registered device has many non-expired tokens associated to it that are revoked, the TRL could grow to a size bigger than what the registered device is prepared to handle. This could be exploited by attackers to negatively affect the behaviour of a registered device. Short expiration times could help reduce the size of a TRL, but an AS SHOULD take measures to limit this size.

7. IANA Considerations

This document has no actions for IANA.

8. Normative References

[I-D.ietf-ace-oauth-authz]
Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)", draft-ietf-ace-oauth-authz-25 (work in progress), October 2019.

[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>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/info/rfc6749>.

[RFC6920] Farrell, S., Kutscher, D., Dannewitz, C., Ohlman, B., Keranen, A., and P. Hallam-Baker, "Naming Things with Hashes", RFC 6920, DOI 10.17487/RFC6920, April 2013, <https://www.rfc-editor.org/info/rfc6920>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[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>.

[RFC7641] Hartke, K., "Observing Resources in the Constrained Application Protocol (CoAP)", RFC 7641, DOI 10.17487/RFC7641, September 2015, <https://www.rfc-editor.org/info/rfc7641>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[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>.

[RFC8392] Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392, May 2018, <https://www.rfc-editor.org/info/rfc8392>.

Acknowledgments

The authors sincerely thank Jim Schaad for his comments and feedback.

The work on this document has been partly supported by VINNOVA and the Celtic-Next project CRITISEC.

Authors' Addresses

Marco Tiloca
RISE AB
Isafjordsgatan 22
Kista SE-16440 Stockholm
Sweden

Email: marco.tiloca@ri.se

Ludwig Seitz
RISE AB
Scheelevagen 17
Lund SE-22370 Lund
Sweden

Email: ludwig.seitz@ri.se

Francesca Palombini
Ericsson AB
Torshamnsgatan 23
Kista SE-16440 Stockholm
Sweden

Email: francesca.palombini@ericsson.com

Sebastian Echeverria
CMU SEI
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
United States of America

Email: secheverria@sei.cmu.edu

Grace Lewis
CMU SEI
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
United States of America

Email: glewis@sei.cmu.edu