Metadata discovery for third party authorized TURN session

draft-reddy-tram-token-metadata-01

Nov 2015

IETF 94

Authors: T. Reddy, S. Nandakumar, D. Wing, B. Williams

Presenter : Brandon Williams

Problem statement

- STUN third-party authorization only allows grant or reject access to the TURN server.
- It does not restrict the server's resource utilization.
- How to provide fine grained control on the clients usage of the TURN server resources ?
  - Limiting the bandwidth usage
  - Limiting the number of allocations

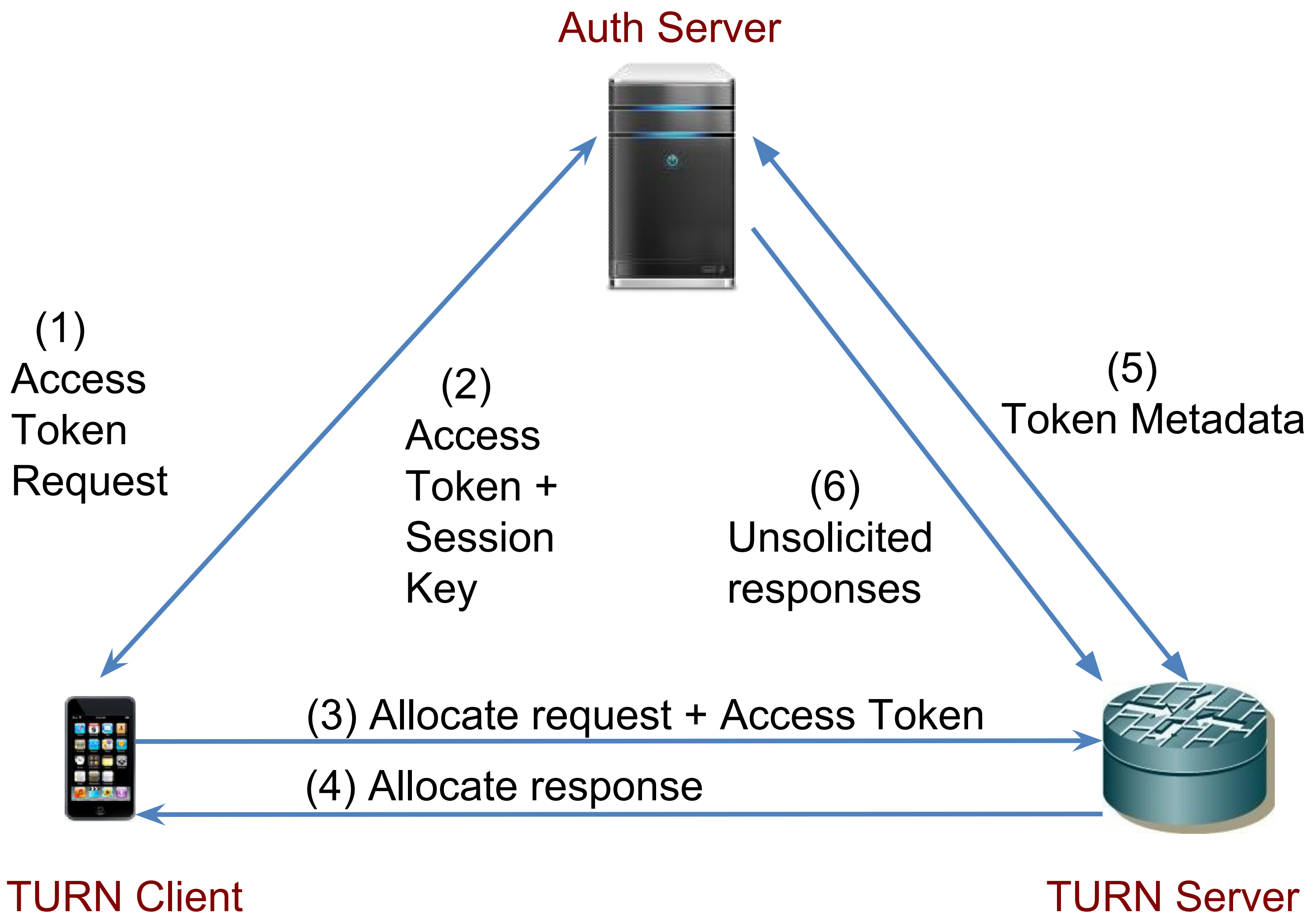
Solution Options

- Draft describes two solution options:
  - Metadata discovery using token introspection
  - In-band metadata via 3rd party auth token

Token Introspection

- TURN server queries the OAuth2.0 authorization server to determine resource restrictions for this token.
- Leverages OAuth 2.0 Token Introspection [RFC7662].

Token Introspection



Introspection Request

```
POST {scheme}://{host}:{port}/.well-known/introspection
Accept: application/json
Content-Type: application/x-www-form-urlencoded
{
    "token" : "string"
    "token_type_hint" : "string"
}
```

Introspection Response

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "active" : "boolean",
    "scope" : "string",
    "max_upstream_bandwidth" : "unsigned integer",
    "max_downstream_bandwidth" : "unsigned integer",
    "max_allocations" : "unsigned integer",
    "lifetime" :    "unsigned integer",
}
```

INTROSPECTION_ENDPOINT Attribute

- This attribute is used by the TURN client to inform the TURN server the FQDN of the Introspection Endpoint.

Notifications from Introspection Endpoint

- Unsolicited responses to TURN server
  - When the call switches from audio to video, the Introspection Endpoint notifies the increased bandwidth to the TURN server.
  - Notify to revoke the access token after the call is terminated.

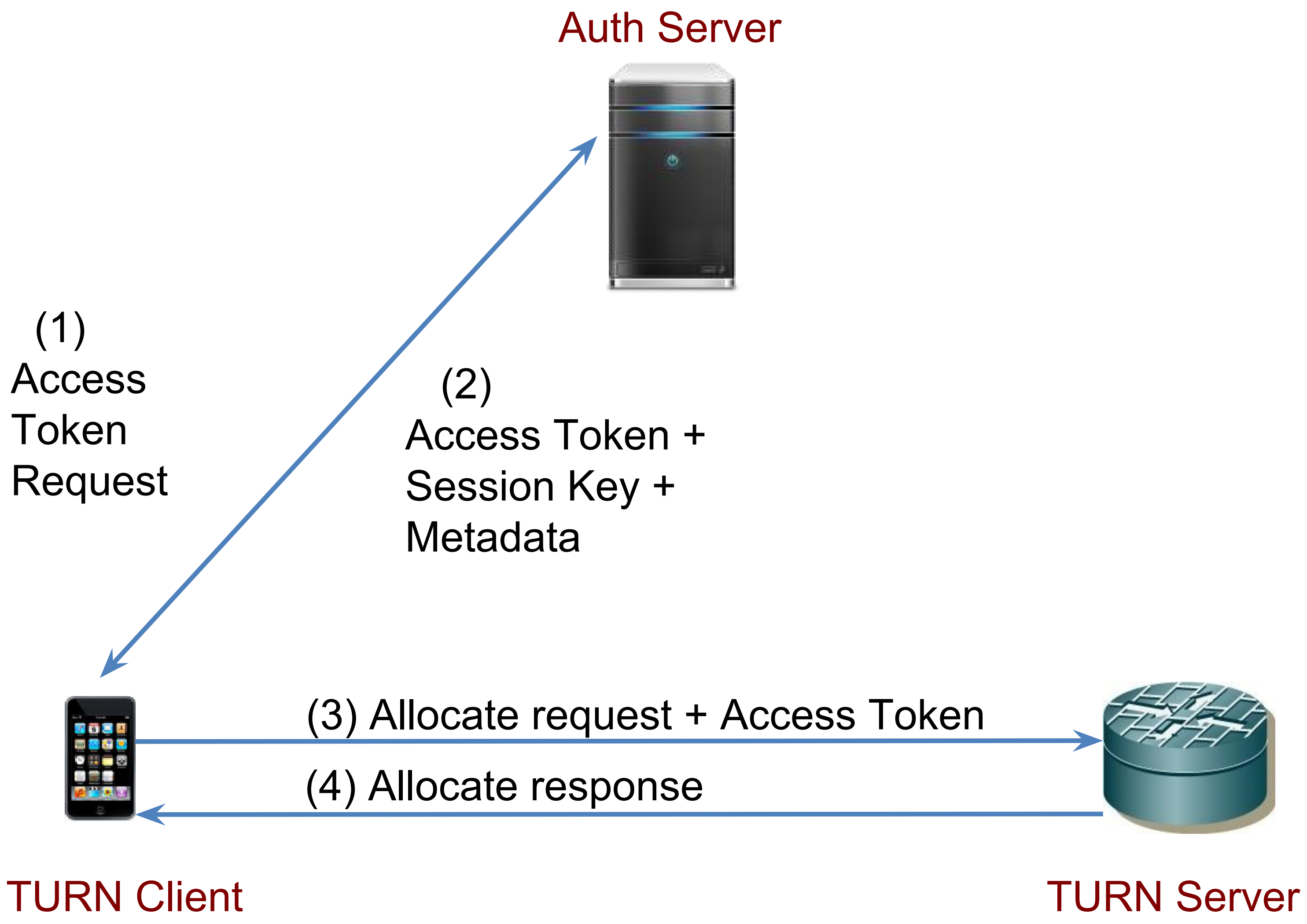
Token Instrospection: Pros and cons

- Pros
  - Maintains small token size.
  - Allows mid-stream adjustment to metadata.
- Cons
  - Requires publicly accessible auth server.
  - Session establishment delay for OOB communication.

In-Band Metadata

- Embed the metadata in the token itself.
- Append STUN TLV encoded attributes to the auth token data prior to encryption.

In-Band Metadata



Auth Server

(1) Access Token Request

(2) Access Token + Session Key + Metadata

(3) Allocate request + Access Token

(4) Allocate response

TURN Client

TURN Server

In-Band Metadata: Pros and cons

- Pros
  - Maintains existing 3rd party auth session establishment flow.
  - Private auth server keeps existing security controls.
- Cons
  - Larger TURN packet to accommodate the token.
  - Metadata communication only at session establishment.

Questions ?