SIP Authorization Framework Use Cases

Rifaat Shekh-Yusef, Jon Peterson

IETF 91, SIPCore WG
Honolulu, Hawaii, USA
November 13, 2014

Overview

- Authorization Framework components:
  - Authentication:
    - The process of verifying the identity of a user trying to get access to some network services.
  - Authorization:
    - The process of controlling a user access to network services and the level of service provided to the user.

Authentication

- Does SIP need an identity provider feature?
  - And if so, do we need more than one?
- No shortage of approaches
  - RFC4474/STIR already has something
    - Authority provides a crypto token
    - Relying parties trust authority, authority vouches for user
  - RFC4484, draft-ietf-sip-saml (d. 2011)
    - SAML focused on attribute-based authorization
  - OpenID/OAuth has been proposed
  - Something like RTCWeb's IdP?

Authorization

- Does SIP need an authorization feature?
  - And if so, do we need more than one?
- Possible approaches
  - RFC4484, draft-ietf-sip-saml (d. 2011)
    - SAML focused on attribute-based authorization
  - OpenID/OAuth

Adhoc Audio & Video Conference

- A Conference Server provides adhoc audio and video services.
- The server controls who gets access to the service, and the level of service provided to the user:
  - Audio vs video
  - Limit on number of participants:
    - per audio conference
    - per video conference

Adhoc Conference Possible Solutions

- With a User Directory
  - The server has a User Directory with the details of services associated with the user.

- Without a User Directory
  - The server does not have a User Directory, and the services associated with the user must be specified in the request sent to the server.

Corporate-wide SSO

- An enterprise is interested in providing its users with an SSO capability to the corporate various services.
- The enterprise has an authorization server for controlling the user access to their network and would like to extend that existing authorization server to control the user access to the various services and level of service provided by their SIP network.
- The user is expected to provide his corporate credentials to login to the corporate network and get different types of services, regardless of the protocol used to provide the service, and without the need to create different accounts for these different types of services.

User-to-User Authentication

- Two users with no association between them, want to be able to call each other.
- Each user should be able to make a call to the other user and should be able to authenticate the identity of the other user.

WebRTC-based Access to IMS

- The system allows a WebRTC client to authenticate the user, and then allows that user access to the services provided by the IMS system.

Backup Slides

Mobile Client Access to SIP

- An Application Server that provides Mobile Clients with access to SIP services.
- The Mobile Client uses a proprietary protocol to communicate with the Application Server that registers and gets service from the SIP network on behalf of the user that is using the Mobile Client.

SIP SSO

- An enterprise is interested in providing its users with an SSO capability to the corporate various SIP services.
- The enterprise wants to control the services provided to their SIP users and the level of service provided to the user by their SIP application servers without the need to create different accounts for these services.
- The enterprise wants to utilize an existing authentication mechanism provided by SIP, but would like to be able to control who gets access to what service and when.
- The user is expected to use his SIP credentials to login to the SIP network and get access to the basic services, and to get access to the services provided by the various SIP application servers without being challenged to provide credentials for each type of service.

Edge Authorization

- An enterprise is interested in authenticating and authorizing a remote user trying to get access to services provided by the corporate SIP network.
- The enterprise would like to authenticate and authorize the remote user at the edge of the network using a SIP network element that does not have direct access to the SIP user account, e.g. SBC.
- The enterprise is also interested in providing the user with an SSO capability to the corporate various SIP services.
- The user is expected to use his SIP credentials to login to the SIP network and get access to the basic services, and to get access to the services provided by the various SIP application servers without being challenged to provide credentials for each type of service.

Internet-Wide SSO

- A user wants to subscribe to sip services the same way he subscribes to web services - using his identity from one of the popular internet-wide authentication services. (E.g., Google+, Facebook, Disqus.)
- After that, all that is needed to gain access to those services is to log his device in to the chosen authentication service.

Core features

- Header (or body) to carry a token
  - May be an artifact, or a URI: dereferenced to acquire the token
  - Also possible to carry the token in-band (header or body)
  - RFC4474: Identity header carries a crypto token
- Pointer to the identity provider
  - RFC4474: Identity-Info header, containing a URI
    - Locates the credentials needed to verify the token
    - Possible axis of extensibility
- Capability negotiation
  - Reject requests without tokens
  - Reject requests because the token is broken
  - RFC4474 defined error codes along these lines
    - 428 “Use Identity”, 438 “Invalid Identity Header”, etc