draft-ietf-abfab-aaa-saml

Josh Howlett

IETF 90

Remaining issues (recap from IETF 89)

- SAML naming of AAA entities
  - The focus of this presentation
- Alejandro previously noted that RFC2865 requires either a password or state attribute in a RADIUS Access-Request message
  - Assertion request/query profile will be updated to require RADIUS State attribute
- Document still feels a bit terse
  - Further review would be much appreciated

Background: SAML naming of entities

- Syntactically, SAML entities are named using a URI (“Entity Identifier”) of not more than 1024 characters in length; there are no semantics
- The URI value is typically used by SAML entities to find the protocol endpoints & public keys of their correspondent entities in local configuration (“SAML federation metadata”), and so communicate
- This configuration effectively enumerates all of the SAML entities that a SAML entity knows, somewhat like hosts.txt

Background: why name AAA entities in SAML?

- AAA actors also have local configuration that describes their AAA correspondents (e.g., a NAS's RADIUS server)
- Unlike SAML federation metadata, this local configuration usually only describes a very small part of the AAA system, because of the use of AAA fabrics that use intermediaries (such proxies or Trust Routers)
- This fabric enables AAA correspondents to trust each other (to some value of trust), even if it is not enumerated in the local configuration
- However naming the entities involved in SAML exchanges between AAA correspondents improves their ability to enforce policy at the SAML layer
- It is therefore desirable to name aaa-saml endpoints in the absence of SAML federation metadata

Proposal: SAML naming of ABFAB RP

- RFC7056 already describes how RADIUS attributes can be named using a URI
  - urn:ietf:params:gss:radius-attribute <numeric RADIUS name>
- RFC7055 already assigns RADIUS attributes naming an ABFAB acceptor
  - GSS-Acceptor-Service-Name (164), GSS-Acceptor-Host-Name (165), GSS-Acceptor-Service-Specifics (166), GSS-Acceptor-Realm-Name (167)
  - e.g.,“urn:ietf:params:gss:radius-attribute 164”
- Put these together:
  - Append the value of the RFC7056 RADIUS attribute URIs with the RADIUS attribute values, space delimited:
    - e.g., “urn:ietf:params:gss:radius-attribute 164 nfs”
  - Concatenate these extended values, space delimited:
    - e.g., “urn:ietf:params:gss:radius-attribute 164 nfs urn:ietf:params:gss:radius-attribute 165 fileserver urn:ietf:params:gss:radius-attribute 167 example.com”
  - This identifies an entity that is an NFS server called “fileserver.example.com”
- Prepend this string with a string that explicitly denotes this entity as an ABFAB entity:
  - e.g., “urn:ietf:params:gss:abfab-acceptor urn:ietf:params:gss:radius-attribute 164 nfs urn:ietf:params:gss:radius-attribute 165 fileserver urn:ietf:params:gss:radius-attribute 167 example.com”

Proposal: SAML naming of ABFAB IdP

- Assumption: the realm of the user's NAI uniquely names the IdP
  - e.g., user@example.com has an IdP called "example.com"
- These is no RADIUS attribute for realm, so can't use RFC7056 approach immediately
- Options:
  - Specify a new URN to name the NAI realm:
    - e.g., "urn:ietf:params:gss:abfab-idp example.com"
  - Define a new (extended?) RADIUS attribute and use RFC7056 approach and generalise the prepended URN to mean a SAML entity ID

Summary

- Pick an approach and define needed URN/RADIUS attribute(s)
- AAA entities, or their intermediate AAA fabrics, must apply policy constraints controlling the names that other AAA entities can claim
- The implementation of these constraints is necessarily specific to the AAA protocol and/or AAA fabric in question, and so out-of-scope of aaa-saml