draft-ietf-abfab-aaa-saml

Josh Howlett & Sam Hartman

ABFAB

IETF 87, Berlin

Issues

1. Use of the new RADIUS extended attribute form
2. Encapsulation of unsolicited SAML responses in the ABFAB Authentication Profile
3. NAI for ABFAB Assertion Query/Response Profile
4. Discussion of naming
5. Application of policy
6. Veracity of message
7. Metadata considerations

Use of the new extended RADIUS attribute form

- Let’s not consume scarce namespace
- TODO

Encapsulation of unsolicited SAML responses in the Authentication Profile

- SAML messages are typically encapsulated within <Request> & <Response> framing
- In ABFAB the <Request> is implicit in the underlying binding (i.e., the RADIUS Access-Request), and the IdP may choose to return an “unsolicited” <Response>.
- This is likely to be very common for the ABFAB Authentication Profile.
- For simplicity we propose that **unsolicited, unencrypted assertions** MUST be returned without <Response> encapsulation, within a new RADIUS attribute (“SAML-Assertion”)

NAI for ABFAB Assertion Query/ Request Profile

- ABFAB Authentication Profile uses the NAI (user@realm) for routing the Access-Request from the RP towards the IdP
  - bob@example.com
  - anonymous@example.com (identity in inner method)
  - @example.com (identity in inner method)
- ABFAB Assertion Query/Request Profile also needs an NAI for routing. We propose that "@realm" MUST be used, with RADIUS Service-Type of "Authorize-Only" and the RADIUS State attribute from a previous authentication; and SHOULD use it.
- By including a non-null <Subject> element the RP asserts that the previously authenticated AAA identity is the same.

Discussion of naming

- Use of security domain names
  - The security domains of the SAML issuer and RADIUS server are congruent, irrespective of their names (i.e., the SAML entityID and RADIUS realm values)
- Use of user names
  - The authenticated RADIUS user and SAML assertion's <Subject> are equivalent, regardless of their respective values. The assertion describes the authenticated RADIUS user.
  - The RP should not include a <Subject> in the authentication request.
  - The IdP claims that the <Subject> of an assertion is the same as the authenticated RADIUS user.

Application of policy

- Use of AAA names
  - SAML consumers SHOULD apply policy based on the RADIUS server's realm.
  - SAML issuers SHOULD apply policy based on the NAS identity
- Use of SAML names
  - SAML issuers MAY apply policy based on the requester's entityID after validating that the request comes from the NAS
    - NAS identity in digitally signed request is sufficient
    - NAS identity in trusted metadata is sufficient
    - Digitally signed request alone not sufficient
  - SAML consumers MAY apply policy based on the issuer's entityID after validating that the response comes from the RADIUS server
    - RADIUS realm in digitally signed response is sufficient
    - RADIUS realm in in trusted metadata is sufficient
    - Digitally signed response alone not sufficient

Other issues

- Veracity of message
  - The RADIUS server vouches for its SAML messages.
  - The RP's level of trust in these SAML messages should be consistent with the trust it places in the RADIUS infrastructure.
- Metadata considerations
  - Implementations must support not using SAML metadata