PPNTier

Additional N-Tier / Proxy / Delegation Support

Shibboleth currently implements protocols and profiles that address authentication of a user relying on a browser. From the begining of the project, however, there has been interest in SAML's relevance to n-tier use cases. When an SP receives SAML tokens, what, if anything, can it do with them in order to authenticate that user to a backend service? How would it do this? There have been several attempts to define approaches to this problem.

An initial work item for this is listed above and is under development.

Generally (but not always), the proposed solutions involve using SAML, or possibly a non-SAML protocol to allow for a request to the IdP for additional assertions that can remap identities or include new attributes, and then a way to attach the new assertions to whatever protocol the SP is using to communicate with the backend service.

- To what degree can the exchange with the IdP be generic, and/or rely on a standards-based protocol with marketplace traction?
- What kinds of back-end protocols are of interest and can be supported? Is SOAP a dead end at this point in favor of REST? Is using SAML with SOAP and WSS viable anyway, allowing for SOAP toolkit limitations?

We are seeking a detailed use case, describing the flow, the protocols that would be used, and the toolkits that would be used in the SP and in the backend service to implement this functionality. (This area has not matured to the point where the toolkits can be separated from the protocol stack implementations.)

Some possible use case outlines follow.

1. Transferring Kerberos tickets from an IdP as attributes
    - One approach that has been suggested to the delegated credentials problem is to pass forwardable or proxiable Kerberos tickets to the mid-tier SP as SAML attributes. This approach would likely only be usable within a domain; cross-domain Kerberos has yet to take hold in the marketplace.
    - A simple implementation, without any policy constraints, might be straightforward. With the 2.1 IdP, Kerberos tickets are now available within the attribute resolver when Kerberos authentication is used. However, the consensus is that a deployable implementation would require significant policy and configuration work in both the IdP and the SP.
    - We seek specific, detailed use cases that spell out the policy requirements in each component. (See KAML email list; see recent email thread; see previous discussion on the shibboleth-users email list with Russ Alberry)
2. Information Card support for active clients
    - The Information Card profiles include features designed for clients or servers with more capability than a browser.
    - The IdP's support for Information Cards would need to be more full-featured than the basic support needed for Web SSO, with more advanced WS-Security and WS-Trust features.
    - The resulting assertions would still need to be attached in an application-specific way, requiring tooling support, but Microsoft claims to have developed .NET libraries for leveraging all of this. Is that enough to motivate it?
3. OAuth
    - OAuth seems to be getting some traction, and may contain a number of interesting pieces that are relevant, either alone, or along with supporting oAuth itself.
    - Figuring out whether the IdP can play a role with an unmodified use of OAuth is important.
    - A SAML adaptation of OAuth may be worth looking at as well.
4. A highly simplified SOAP interface to the IdP to obtain assertions
    - Building something extremely bare-bones, relying on TLS or basic authentication, and a simple GET operation would be simple, and require developing some amount of policy control that would be needed for most of the more complex approaches.