UMA telecon 2013-01-10
UMA telecon 2013-01-10

Date and Time

- **Focus** meeting on Thursday, 3 Jan 2013, at 9am PT (time chart) – technical, educational
  - Skype: +9905100000481
    - Special GoToMeeting link for Gluu OXAuth demo portion: https://www2.gotomeeting.com/join/757116370 – we'll keep the regular WG audio line

Agenda

- **Action item** review
- Security considerations/threat model review and planning
- Plan terminology changeover in other UMA publications
  - Binding Obligations
  - Circle graphic
  - Use cases and case studies
  - Other
- At x:45: Demo of Gluu’s OX UMA support (see link above)
- AOB

Minutes

Security considerations/threat model review and planning

Links: latest [OAuth threat model spec](#), Domenico’s and Eve’s comments

For a bearer-style token, without audience restrictions or proof of possession, there’s definitely a problem – with OAuth as well as UMA. What are the differences between the two? Audience restriction is kind of a lightweight "binding obligations" attempt, though it's highly vague and non-interoperable in OAuth at present. There's a discussion going on around audience vs. scope in Justin's token introspection spec now. Is the audience meant for the entity that asked for the token?

If protected resources don't require any client authentication, UMA is subject to the same threat as OAuth. Neustar's work on Ultraviolet uses of OAuth, and they have chosen to authenticate the client (not common practice in OAuth, though when done, it's often done with HTTP Basic over SSL) and to put in audience restrictions. The JWT assertion profile makes possible a signed JWT as a client authentication mechanism as well. OpenID Connect is working on making a JWT signed with a private key available as a solution. The UMA client could also sign the RPT, though this doesn't mitigate a replay attack. The client authentication to the resource server could be as simple as an API key, which is a simple shared secret.

What are the actual threats? A malicious client could easily help others impersonate them for many of these methods. A clueless client that doesn't sufficiently protect the token is a different threat. Lightweight client authentication helps a little with token leakage (though the cost may not be worth the benefit). Are there legitimate use cases for deliberately shared tokens in "chaining" styles of A2A collaboration a la Facebook being comfortable with HikingTrails.com sharing the token for deeper mashup scenarios?

If we want the client "registration" to the RS to be dynamic and OAuth-based, we could literally use the dynamic client registration profile. We have a portion of the "get a token" flow that does involve the client and RS first getting to know each other, during which they could exchange whatever association handle or authenticator they want. Mutual TLS matching the subject in the certificate may be simplest, if PKI (or rather, "pre-configured asymmetric key") is already assumed in the environment. In OpenID Connect, there are already certain parameters reserved for certificate consumption.

We suspect that identifying it generically as a threat is sufficient, along with pointing out policy-level mitigations in Binding Obligations and the cornucopia of technical solutions that deployers may want to avail themselves of; we could recommend that they document the profile.

Plan terminology changeover in other UMA publications

Links: original [circle graphic](#) (attached to old UMA Explained page), Binding Obligations, case studies

- Binding Obligations
- Circle graphic
- Use cases and case studies
- Other

One new proposal is this:
One challenge with the logarithmic spiral diagram is that the RO works through a client as well, and it’s not shown. We definitely need to spell out the names of everything! “RP” is particularly problematic. Let’s explore real-world trials of both the circle and the spiral.

AI: Domenico: Create a beautiful logarithmic spiral diagram for us to review more closely.

Gluu OX demo

This is all open-sourced under the MIT license. They held off on some desired UMA work so that they can integrate their SAML and OpenID Connect implementations more closely, but in another week they’ll be able to turn to a more comprehensive demo that involves the RS and C vs. the AS.

The role he’s demonstrating is the organizational IT administrator. They’re putting the UMA functionality under OAuth 2.0. They already support dynamic client registration for OIDC. You can create metadata about the client, such as whether it’s a native app, what scopes (a la SAML attribute release policies) it’s allowed to have, and authorized groups who can get access to the website. Gluu’s main goal for supporting UMA is to enable API authorization: You’re an institution that wants to restrict access to an API of yours. For a host (RS), you can define scope descriptions, and resource sets (with URLs that have asterisks as path regexes) that bind to the scope URLs. Most of the use cases for WAM systems is “this user can get to this URL”; UMA gives you scopes you can work with in addition. This is useful for controlling access to APIs. It’s not a fine-grained authorization engine like XACML, but it solves a big number of use cases for organizations when you need to go beyond coarse-grained "whole URL" access. E.g., in SiteMinder, you can get as far as the URL with regexes and HTTP methods and group or role membership. The UMA way of handling scopes goes beyond that grain with scopes, and also adds clients to the access requester mix. In SAML, clients identify themselves with SAML metadata. In OpenID Connect, you can potentially use dynamic client registration. They’ve had some expressions of interest, but don’t have the first customer yet.

AI: Eve: Write up a draft Enterprise API Authorization case study for Mike/Will review.

The "new Venn of access control for the API economy" seems to be coming alive. Each of the API management platform vendors seems very proprietary around API authorization, partly due to OAuth hasn’t solved this yet. This is where UMA can really help. WS-Security:OAuth::SAML:OpenID Connect::XACML::UMA

All of Canada may go 100% EduRoam. Do we have the opportunity to share these new solutions with them? RADIUS authentication into wifi is still the coin of the realm. Any higher-level standard is usually out of the question. The SIP SAML work, which uses the artifact pattern, potentially shows the way, i.e. binding authn/authz that were originally for the web to non-web or pre-web transports.

Attendees

- Alam
- Keith
- Eve
- George
- Sal
- Domenico
- Mike
- Lukasz
- Peter
- Maciej

Next Meetings

- Focus meeting on Thursday, 17 Jan 2013, at 9am PT (time chart) –