External Identities Workgroup Meeting at ACAMP - 2014-10-27

Approximately 50 attendees (roll was not taken).

(With thanks to Bert Bee-Lindgren for assistance in note-taking!)

1) Reviewed activities of workgroup to date.

2) Opened floor for a lively discussion of risks and concerns around the use of external IDs. Remainder of this page is a summary of comments raised in discussion.

Liability/Legal Restrictions

- Does the External IdP indemnify the university if there is a breach of the External IdP that leads to loss at an SP?
- How do you address the general lack of indemnification (assuming no)?
- Are there limitations in state laws (for public institutions) that limit the ability to leverage these services?
- Is there a concern that the identity provider could close shop or move to a model that charges us?
    - What is meant by 'identity provider' in this context? If this really just means 'authentication provider' then you simply move to a different authentication provider.
- Could a social-identity provider cancel our application keys?
    - The obvious answer is, yes. But if authN and authZ are properly separated, you just use an alternate authentication provider.
- Do we need an agreement with the social providers? By use of the External IdP's keys, you're under the "EULA" of the provider…they could just change their terms. You have to adopt their terms of service.
- Use of external IdP puts students under individual licenses rather than group licenses.
- Are there any operational restrictions imposed by the External IdP if we leverage them through personal licenses (rather than contractually in some way)?
- Is there something we (Ext ID Workgroup) can investigate around how we assess social/external identities compared to how we run our own services, and what liabilities/indemnifications we should manage?

Reliability/Applicability

- Is there a stewarding issue/requirement?
- Does the External IdP reassign IDs?
    - For Yahoo! (Known to be reassigned): Could this be addressed by periodic refreshing/revalidating of external IDs?
    - [Duplicate] Is there a concern that the identity provider could close shop or move to a model that charges us?
    - Many people lie (intentionally) about the data that's provided to External ID providers to protect their privacy.
        - Do we care about attributes (authZ) or just the credential management (authN)? Would we trust these attributes even if we thought they were well verified?
    - (Asked to the membership) Would you grant access to a student transcript based on a Google ID?
        - One answer: Not based on the google attributes, but probably based on the previously-linked identifier/credential, yes.
- Need to really think about where service begins and where it ends holistically when considering completely outsourcing the credential. eduRoam will require a local credential of some sort.
    - Counterpoint: Many campuses provide SAML integration with Google Apps but require local Google passwords for other services (IMAP, Mobile clients, etc). Campuses could "flip" this and rely on Google (or other External ID provider) for SAML authentication and then have a place to create local credentials (e.g., for eduRoam) that rely on the external ID.
- Younger generation churns through social identities more quickly than we might think
    - Counterpoint: As long as you have a robust way for them to register new external credentials, this may not be a major issue.
    - If switching credential providers means they have to reestablish access to services this behavior may change.
- What's the scoping of identifiers? E.g., FaceBook may be releasing pairwise anonymous identifiers (like ePTID). Can't use for systemwide identities, since each system will get a different ID.
    - Counterpoint: if IdP does the mapping, then only one SP is seen by external provider, so only one identifier is provided
- Are there privacy concerns for Google, etc. tracking what SPs people are accessing?
    - Counterpoint: if IdP does the mapping, then only one SP (the campus IdP) can actually do tracking.

Incident Management/General Security

- How do I demonstrate to an auditor or security people that e.g., Google does a better/sufficient job of managing authentication?
- How much trust do the SPs needs to put into the identity? External ID may not have a lot of assurance associated with the identity vetting. Can identity vetting be an add on service?
- One of the issues of accepting and external IDs instead of internal credentials is that you've accepted their reset policy.
    - Counterpoint: password reset frequently relies on email messages to an external emails. Reset process could be scored on a "strength" basis; social login could be seen as being stronger than just receiving an external email. If access to email is sufficient for resetting anyway, why not just give access based on that external credential?
- How does use of external IDs apply in remote proofing?
    - One suggestion was a point system mapping transcripts, social, etc. to point to identity. Similar to what's done in Australia. (N.b., I don't know what's done in Australia)
- There needs to be a cost/benefit review of using the External IDs based on what's being accessed.
    - Counterpoint: This (trusting the credential to be managed sufficiently for granting access to resources) is an issue even if we use local credentials.
- How would you respond to a hacked social account in a timely manner?
    - Assuming you're aware of the hack (see other issues), you'd have to unlink the external ID from the internal ID wherever the linkage is made and managed.
    - Counterpoint: this seems to favor an IdP Proxy/COManage kind of model rather than SP-based linking of IDs (Proxy has one point of linking rather than per-SP linking which has many).
- External ID will persist with not value changes (in most cases) well beyond when the person's campus affiliation changes.
    - Use of external IDs would absolutely require separation of AuthN and AuthZ.

General Observations

- There are ways to mitigate many of these issues. Touches on new entities (how the IdP is listed in metadata), federated incident response (for if there's an issue with an External ID) , etc.
- Can we leverage the length of time the credentials have existed to help validate?
- Can we use social network connections (for social providers) to help validate identities?
- Are these questions/risks the same ones that we should be asking of InCommon IdPs and communicating to SPs?
    - Many of the risks we raise here are the same ones that SPs ask about our IdPs when we release assertions to them.
- What is so different about outsourcing our identities when we already outsource our email to Google/Microsoft?
    - Email outsourcing tends to come with a contract
    - Email/documents access is much more limited than full access to someones entire identity portfolio