NASIG Newsletter
Vol. 33, no. 1 March 2018 eISSN 1542-3417

Columns

Standards Corner: Challenges of Identity and Authentication Management, Part One

Deberah England, Standards Committee

This is the first of a two-part review series on the topic of identity and authentication management as presented in the November 2017 NISO webinar "Engineering Access under the Hood, Part One – Challenges of Identity and Authentication Management."

The first part covers President of Informed Strategies, Judy Luther's presentation on the current state and challenges of identity and authentication management.

Todd Carpenter, NISO's Executive Director, started off the webinar with some brief observations on the highlights and challenges of identity and authentication management for libraries and providers. Carpenter noted "We, as a community, have trained them [users] not to worry about access control. They don't understand the technology that magically opens doors to subscribed content nor realistically should they have to." This creates a challenge when users are away from a campus network. Users don't understand why they can't access content. Carpenter noted, "We need to understand that identity, authentication and access controls are frequently failing the user community. It no longer makes sense with the mobility of today's users to tie access to network legacy technology."

Current State

Luther began by noting her presentation was focused on folks who are newer to the topic and thus began by covering the three core components of access – identity (Who are you?), authentication (How do we know?), authorization (What permission does that give you?). Additional personal attributes such as an ORCID ID (https://orcid.org/) could help provide more meaningful data downstream for libraries with new technologies, but they are not attainable with legacy location-based IP recognition authentication technology. If a user is on campus, they are authenticated by their institution and then authorized via IP address recognition by the content provider. If the user is off-campus, the process requires an additional layer with the use of proxy servers, which creates a more cumbersome and less smooth process.

A more current technology is Shibboleth (https://www.shibboleth.net/), an open-source single-sign-on solution, which has been adopted by some large institutions. Shibboleth allows users to authenticate through their federation based on their affiliation with their institution. Authorization continues at the content provider's end. With Shibboleth a user's privacy is safeguarded and unknown to the content provider.

Similar to Shibboleth is InCommon (https://www.incommon.org/federation/), which is a U.S.-based education and research identity federation. Participants in InCommon comprise over 600 universities and 20 government and non-profit entities along with 280 sponsored partners from the content provider world. Luther wrapped up this portion of her

talk with case studies that illustrated how InCommon has developed applications to facilitate homework delivery, enrollment verification, and a Shibboleth/EZproxy hybrid back in 2010.

Challenges Today

Since the advent of IP recognition authentication a number of challenges have altered the landscape. Users now access remotely. 67% of public university and 36% of private university students live off-campus. 28% of enrolled students are now taking at least one online course. These two statistics combined, even with overlap, creates an off-campus user population that can't easily access resources. Moreover, as of late 2016 mobile access surpassed desktop access. This creates an environment where the user workflow is outside the campus network.

Roger Schonfeld, a researcher at Ithaka S+R's Libraries and Scholarly Communication Program, conducted research that found on-campus is not the work location for most users and PCs are not the device most used. The annual Ithaka survey found that half of the respondents had problems accessing content and the majority of the time gave up and looked elsewhere, preferably for free content. The result is that content libraries paid for is not serving the user or the library well.

What is the impact of the lost use? Academic libraries spent $3 billion on content in 2015. With legacy technology, libraries know only about the users who were able to access content. What about the users who were derailed which, Luther contends, represent a much larger number of users? How would access to the derailed users' data affect acquisition decisions?

Compounding this scenario is that the library's role on campus is changing. New approaches and new metrics are needed based on how well the library operates and how well the library serves its community. Over the last decade, libraries have been increasingly requested to provide evidence of how they support the mission of the university. Current metrics fail to assist with this measure. If the library had data on the user and how they're using the content, that data could be utilized to support the library's role on campus.

According to Luther, data and metrics about when, where, and how users found content are critical for evaluation and the development of services. A potential pushback to new metrics acceptance and use comes from privacy concerns. New technology tools, especially by Shibboleth, are able to safeguard privacy and at the same time provide libraries with data metrics needed to make their case.

Privacy

Privacy is part of the fabric and culture of libraries. Library tenets underscore the library's call to protect the privacy of their patrons and the patrons' data.

Luther shared highlights of work conducted by Clifford Lynch and Sam Kome. In 2016, Lynch, Director of the Coalition for Networked Information, conducted an informal survey on authentication and authorization. Lynch found over 50% of respondents had implemented Shibboleth but were using it in areas other than content. Most content access was handled by proxy servers and IP-based authentication. Moreover, very few content providers were using Shibboleth and many seem to have no plans to implement Shibboleth. Additionally, since little data on user attributes is shared with vendors, little data was returned.

Kome, who is Director, Strategic Initiatives & Information Technology at Claremont Colleges Library looked at patron activity monitoring and privacy protection. Kome tracked users with the tools they had (patron type and ID, proxy, centralized authentication and centralized wireless) to measure building use and location of research activity. Luther noted Kome had to scrub the data to protect user privacy, which was reportedly not an easy task.

Despite libraries efforts to protect user's privacy, some users are abdicating their privacy when they choose to register directly with content providers by creating IDs

or personal profiles in order to receive recommendations, view tables of contents, or post comments.

Looking Ahead

Developments in the pipeline that may improve access include ESPReSSO (Establishing Suggested Practices Regarding Single Sign On), Shibboleth and RA21 (Resource Access for the 21st Century). According to Luther, a great deal of excellent work was done on ESPReSSO, a NISO best practice, but unfortunately, there was a lack of buy-in. Shibboleth, which has successfully garnered take-up, uses tokens to authorize access, which protects a user's privacy. Attributes can be associated with tokens without sharing the user's identity.

In the arena of streamlining users' workflow and access to content, Shibboleth offers privacy to patrons but has a cumbersome interface. Google is also working on an easy access solution but there are concerns from the community about privacy as Google is not committed to our industry nor our stakeholders. Consequently, a Google solution is a less appealing option per Luther.

Another promising project is RA21 (https://ra21.org/). RA21, a joint NISO libraries and STM initiative, was launched due to the concerns of corporate librarians. RA21's goal is to provide anytime, anywhere access, regardless of location, across key stakeholder groups – researchers, libraries, and resource providers – while at the same time addressing the important issues of network security, user privacy and usability. Currently, several RA21 pilots are underway seeking to create best practice recommendations for a smooth access process.

This concludes the report on Luther's segment of the webinar. Be sure to check out NASIG's May newsletter for a report on the second segment of the NISO webinar focusing on the OpenAthens solution, featuring Phil Leahy of OpenAthens and Ellen Rotenberg & Rick Stevenson of Clarivate Analytics. They share a provider's perspective on identity and authentication issues.