American Chemical Society Customer Advisory Panel (CAP)
IT Security Panel Report - September 2011

Members: James King (NIH), Norah Xiao (USC), Sue Jones (Dow Chemical), Jonathan Morgan (ACS), Sara Rouhi (ACS)

The ACS CAP IT Security panel was charged with exploring the issues and best practices related to authentication and access to publisher content. To explore this issue, the panel performed a literature search, conducted customer focus groups, and interviewed other publishers in the field. Though the findings were presented at the June ACS CAP meeting, conclusions and recommendations were not drawn at that time.

The findings suggest that there is an increased movement away from traditional IP-based authentication to publisher content in two ways: proxy servers and mobile devices. Many libraries and organizations are now clustering their computers behind proxy servers, making it more difficult for publishers to track and block abusive download patterns. In addition, mobile devices are not on a campus IP network and therefore require some other form of authentication like VPN. Though mobile usage and adoption is currently small in the aggregate, dramatic growth trends point to a significant shift in usage within the next several years.

As the industry diversifies away from IP-based authentication, it is clear that the traditional username/ password approach is not sustainable in today's Web environment. Delegated authentication or identity assertion frameworks, built upon the SAML (http://en.wikipedia.org/wiki/SAML_2.0) security/ identity assertion standard, appear to meet today's challenge. NISO has released a draft of their academic-focused approach to this problem (https://communities.acs.org/docs/DOC-5883) and we believe that the principles can be applied in government and corporate settings as well. The APA is also leading a related effort called the OIX Publish Trust Framework (www.PublishTrust.org) in partnership with OpenID (http://openid.net/). Both of these approaches can leverage the InCommon Federation (http://www.incommonfederation.org/) for identity management so we feel that this area is maturing enough to warrant further examination.

Based upon this research and industry trends, the ITSec panel recommends the following:

- Ensure that each of the journal Web sites are mobile-friendly.
- Internally study and explore non-IP authentication support, focusing on SAML-based methods like the ones mentioned above.
- Provide the option of maintaining online access to subscribed content for customers who had to cancel some or all content. Industry practices suggest that a small archive maintenance fee may be acceptable to offset costs of this option.
- To provide better customer support, attach a server log snippet to blockage notifications.
- To reduce legitimate searches being blocked by the abuse filters, allow pre-approved customers to have API access to the journal metadata and full text. This will help overcome limitations of the online search system and provide a "side door" access to content will allow ACS to better control and track that usage without affecting the broader platform.