Editor: Barry Leiba • leiba@computer.org

Inside the Identity Management Game

Lucy Lynch • *The Internet Society*

Techniques for managing authentication and authorization are critical to the next round of Internet innovation. Cloud-based services, the social Web, and rapidly expanding mobile platforms will depend on identity management to provide a seamless user experience. Although a number of standards have been advanced, an Internet scale identity solution remains elusive.

There's an old saying in American baseball – "You can't tell the players without a program," which seems particularly relevant to the current state of online identity management. The combination of a protracted development cycle, shifts in technologies and use cases, and legal requirements for both privacy and security have all led to the creation of a vital but somewhat fractured landscape.

Early authentication schemes relied on creating site-specific user accounts with their corresponding user names and passwords. The World Wide Web and its proliferation of sites and services has resulted in a site-by-site account management pattern that's been a strain for users and service providers alike. Increasing use of the Internet as a way to share and manage protected resources has also brought an additional burden for verification and authorization. The past 10 years have seen several developments in both the authentication and authorization arenas. The primary goal has been a Web-based, scalable solution that combines the ease of single-sign-on (SSO) with authorization based on an exchange of identity-related assertions across security domains.

A number of problems must be solved before we'll see a robust, full-featured, Internet-scale identity management system in place, but progress has been made on authentication/authorization solutions for the Web. Two in particular are gaining broad acceptance. The relatively mature SAML/SOAP paradigm and SAML-based federations have traction in enterprise, educational networks, and e-government. The rapidly advancing combination of OpenID and OAuth (the Web Authorization Protocol) solutions has major advantages for connection-driven RESTful API developers and is being widely deployed. Large service providers such as Microsoft, Facebook, Google, Yahoo, and PayPal all contribute to development efforts.

Many of the major standards organizations are represented in the identity ecosystem, but a number of key specifications come from smaller efforts with open source roots. Identity management has also drawn the attention of governments, policy makers, and advocacy groups, as well as industry consortia, all of which bring their own expectations and requirements to the table. This diverse set of players has led to a proliferation of organizations, each with its own set of participants, preferred development tools, and proposed solutions.

The Identity Ecosystem

A good place to begin to get the identity management big picture is with the ITU Study Group 17 (the lead study group on identity management) and the ISO/IEC Joint Technical Committee 1/SC 27 Working Group 5 (identity management and privacy technologies). Both these groups have taken on defining frameworks for identity management and collecting and harmonizing common terms used in developing identity- and privacy-related standards. A quick review of current work programs also provides a useful catalog of open design issues as well as the large number of outside activities they're tracking. The definitions documents are both freely available and recommended

Published by the IEEE Computer Society
1089-7801/11/$26.00 © 2011 IEEE

Editor's Introduction

As we've taken to using the Web for more and more interrelated things, it's become important to identify ourselves to many different organizations – "domains" in Internet terms – and to want those identities to work, in some fashion, between domains. Perhaps we want to share information between our Facebook and Flickr accounts or would like to have one "wish list" on several shopping sites. Perhaps we just don't want to have to remember myriad sign-on identifiers. We need "identity management."

Identity management has become a significant issue on the Internet, and there are many organizations working on the problem. In this issue, Lucy Lynch of the Internet Society gives us an overview of the landscape. Next time, we'll take an in-depth look at the US Government's approach to identity management, in NIST's National Strategy for Trusted Identities in Cyberspace (NSTIC).

reading, as most new identity efforts begin with (yet another) attempt to find a common vocabulary.

OASIS, the W3C, and the IETF all provide standards that underlie current identity management designs, and we can combine these building blocks in multiple configurations. OASIS supplies SAML and the Web services (WS-*) suite of standards, as well as the Identity Metasystem Interoperability (IMI) specification used for Information Cards. The W3C's HTTP architecture, URIs, and the service-related SOAP are leveraged by federated and distributed identity solutions. The IETF provides several relevant standards, including HTTP, the Simple Authentication and Security Layer (SASL), Transport Layer Security (TLS), and Public-Key Infrastructure (PKIX) along with numerous active efforts including OAuth, Abfab (Application Bridging for Federated Access Beyond the Web), and the recently proposed Web Object Encryption and Signing (WOES) standard.

The more loosely organized open source community has also contributed some key specifications, and several new organizations have formed to house and drive these efforts. The OpenID Foundation (OIDF) is a nonprofit that hosts numerous active working groups, publishes specifications, and manages the open-code repository. Oauth.net is an even less formal effort including an active set of implementers organized around the original OAuth 1.0 specification. The Information Card Foundation (ICF) was an industry consortium established by members such as Microsoft, Equifax, Google, Novell, Oracle, and PayPal to advance the user-centric, wallet-like metaphor IMI offers. In 2011, Microsoft declared its own Information Card implementation "feature complete" and announced that it won't be shipping CardSpace 2.0. Although the ICF is still intact, most partners are currently more focused on OpenID/OAuth implementations.

Any overview of the identity ecosystem wouldn't be complete without some consideration of its implementers and adopters. There is a mailing list, a code repository, or an event to match nearly every interest. Communities range from the loosely aligned Identity Commons to the more formal European-Commission-funded Stork project. The former houses a few working groups but is best known for hosting the semiannual Internet Identity Workshop (IIW), which has focused on user-centric identity. Meetings feature a self-organizing structure that lends itself to brainstorming and advancing small specifications. A recent such specification is Simple Cloud Identity Management (SCIM), which used the spring 2011 IIW meeting to solidify interest in work on standardizing common API-based solutions already in the market. The Stork project aims at implementing an EU-wide interoperable system for recognition of eID and authentication that will enable businesses, citizens, and government employees to use their national electronic identities in any member state (see https://www.eid-stork.eu/index.php?=61).

Another recent example is the proposed National Strategy for Trusted Identities in Cyberspace (NSTIC) being driven by the US government to seek a partnership with private enterprise to manage authenticated citizen engagement with government sites. Three organizations have already stepped up to provide trust framework services that meet NIST SP 800-63 requirements for levels of assurance in some fashion: The Open Identity Exchange (OIX) will provide listing services and support the development of additional frameworks. The Kantara Initiative will serve as a special assessor and will leverage its existing certification programs to provider auditors and interoperability testing. InCommon, an Internet2 consortium of inter-federated educational institutions, will provide an interface to research and education with strong levels of assurance based on its own internal controls.

Advancing SAML Federations

After the initial SAML 1.0 standard was published, two complementary projects adapted the protocol and its associated capabilities to address their own use cases. The Liberty Alliance was formed by a consortium of major software vendors and focused on federated cases for large enterprises, including governments. Meanwhile, the Internet2-based Shibboleth project focused on higher education needs.

These early adopters of federated identity solutions were supporting

organizations and enterprises with large user bases, significant protected resources, complex authorization patterns, and data and services spread across multiple domains. As early adopter development efforts progressed, OASIS continued work on SAML 1.1 and ultimately SAML 2.0, adding features such as attribute profiles, metadata capabilities, and the use of pseudonyms. OASIS has also advanced the WS-* suite of specifications, which addresses several identity-related concerns. The Liberty Alliance work moved toward formalizing the requirements for "circles of trust," with proposed frameworks for testing interoperability and compliance with US National Institute of Standards and Technology (NIST) levels of assurance. With the publication of its Assurance Framework, the Liberty board took a decision to wind up the Alliance and contribute all Liberty assets to the Kantara Initiative. The Shibboleth project continues to develop the Shibboleth federation software and the OpenSAML libraries.

SAML federations are deeply embedded in education, government, and corporate intranets and have been customized to address the security concerns of verticals such as healthcare and banking. All this activity has produced a mature but complex set of standards that have evolved to meet primary stakeholders' needs. Sophisticated problems related to inter-federation, discovery, user privacy, data minimization, informed consent, and service provision "below the Web" are active topics for developers. Issues and solutions are driven by the federation operators, and users and service providers are sometimes seen as problems to be managed, rather than as full participants in the identity exchange.

SOAP vs. REST, XML vs. JSON

Why haven't SAML federations solved the identity management problem? While early adopters were developing standards, building tools, and extending use cases, the world around them changed.

Social applications turned the "authenticate, then authorize" model inside out as users rushed to connect. Mobile phones and other Internet-enabled devices began to efficiently use native applications. The new generation of innovators viewed the Internet from inside the Web and brought a new set of languages and tools to bear on development. While still focused on Web services, coders looked to JavaScript Object Notation (JSON) and REST to build their APIs. The features that had made SOAP attractive to SAML users were viewed as too rigid and too difficult to manage in the fast-paced Web 2.0 world.

The increasing use of Web-based APIs favored the REST model, which can bypass SOAP, SAML, and the Web Services Description Language (WSDL) in favor of a simple exchange of well-defined, consistent HTTP messages between client and server. The reuse of existing HTTP architecture features allows for immediate interoperability. On the other hand, SOAP-based exchanges enabled customized message vocabularies that weren't guaranteed to interoperate. SOAP provided for methods for back-channel exchanges that included both security- and privacy-enhancing features and permitted use with protocols other than HTTP, but came with heavy ties to XML. Although XML can also be used in the REST model, the trend has been for a more stripped-down approach. JSON, based on a subset of JavaScript, is purpose-built for data exchange and bills itself as the "fat-free alternative to XML." The social Web environment is driven by a rapid development cycle and a need to enable seamless exchanges among multiple end points to deliver a coherent experience for users. The combination of REST and JSON has enabled that process and is widely used in current start-up efforts.

OpenID for Lightweight Identity

As Web 2.0 users looked for ways to collaborate with others across multiple sites and services, the need for a simple, persistent way to identify oneself became a compelling issue. Some users wanted the ability to represent themselves with a single identifier, whether publishing a set of photos or posting comments on a friend's blog. The process of adding a new account for every site was cumbersome and often disappointing, as individuals often found their preferred user name taken and grew frustrated with managing multiple accounts and the related passwords. Security concerns also grew as users recycled passwords among sites, with little regard to the relative values of their banking-related account versus their blog accounts. Lightweight SSO became a goal. The social identifier was conceived as something unique but that wouldn't require a high degree of proofing.

The proposed solution was to let users create and assert an identity that would be widely accepted, thereby letting them use a single password and present a unified persona online. The pattern would require coordination among three parties: the end user (data subject), the service provider (relying party, or RP), and a designated identity provider (IdP). Web developers, and blog software implementors in particular, introduced several models for decentralized authentication, and then these efforts were merged into the OpenID 1.0 specification in 2005. In the OpenID scenario, a user creates an account with the IdP of his or her choice and can then use an agent — usually browser-based software — to negotiate authentication. If the IdP doesn't recognize the asserted OpenID,

or if the user refuses the request from the RP, authentication fails.

While OpenID sought to solve the SSO problem for users, the three-party authentication dance brought new issues. Two in particular are worth mentioning, both related to RP adoption. The first is the so-called "NASCAR problem" (referencing the proliferation of sponsor logos plastering race cars), which arises because users must pick an OpenID from among the many available options. Although RPs can provide a generic text-entry box for OpenID entry, this proved to be confusing, and sites quickly began displaying logo buttons of the most popular OpenID providers, such as Facebook, Google, and Yahoo. This simplified the user experience and helped drive adoption among a few IdPs. But as new providers entered the identity market, the number and placement of logos became problematic.

The second issue is particular to those RPs that aren't also IdPs. By agreeing to accept authentication from the large external IdPs, the RP loses some control over its relationship with any given user and his or her associated identifying data. Although this might be appealing to users, it doesn't provide much incentive to service providers. Meanwhile, the large providers can leverage OpenID to extend existing relationships and manage internal delegation among their own service offerings.

The OpenID 2.0 specification was published in late 2007. It added functionality, including a format for extensions to allow for attribute exchange, and also added several new identifier types, such as the OASIS-sponsored Extensible Resource Identifier (XRI) as well as a special identifier for Open ID providers (OP). The new identifiers were intended to aid in discovery. The specification also included a security considerations section that outlined some risks associated with using OpenID, along with some proposed solutions. The 2.0 release was also supported by the completion of patent-related nonassertion agreements from all key contributors to earlier OpenID specifications.

OAuth for User Authorized Delegation

With decentralized authentication well under way, attention turned to the problem of authorization in the Web 2.0 context. The original OAuth specification (from 2006) aimed to complement OpenID and let users delegate access to an API acting on the user's behalf to share a protected resource with the data requester. The metaphor often used to describe this functionality is the "valet key" you would hand to a parking lot attendant. Such a key will only let the valet drive the car within a limited range and might block access to the on-board radio or phone.

The concept is simple: users authorize limited access to resources (photos uploaded to a website) to another service provider, who then might print the photos or release them to a blog writer for reuse. The access grant is accomplished through the exchange of a shared secret between users and the first-party service, which then grants access to the third party via a token. The token need not reveal either users' identifying information or their long-lived authentication credentials, and doesn't give the third party service full access to users' first-party accounts. In OAuth terms, the third party is the *consumer* (that is, the consumer of the token).

The exchange of tokens and the desire to protect users' identity and resources brought an increased need for security and the inclusion of cryptographic requirements. The deployment scenarios also covered Web-based applications, desktop clients, and mobile applications. Early implementers found the cryptography elements difficult to manage and struggled to create a simple set of workflows that provided good user experiences in diverse environments. As an illustration of the loose organization around the work, one specification author, Eran Hammer-Lahav, leveraged his blog to detail these issues and chronicle how OAuth and related delegation mechanisms were deployed. In 2008, the OAuth document editors introduced their work to the IETF, and Oauth 1.0 has since been published as RFC 5849 (http://tools.ietf.org/html/rfc5849). The IETF then chartered a working group to look at formal standardization of the OAuth 1.1 protocol. Although a few original participants continued to work on the IETF variant of OAuth, work also continued in the deployment community with little attention being paid to the IETF effort.

By 2009, several OAuth implementations existed in the wild, and the original core specification's limitations were beginning to cause fractures in the development community. In April of 2009, a major security vulnerability based on session attacks shook the community, and a competing proposal — OAuth Wrap, introduced at the IIW meeting in November — further divided efforts. In April 2010, various authors introduced a new draft proposal for OAuth 2.0, incorporating features from OAuth Wrap. This work is advancing in the IETF, and additional drafts have been submitted to deal with security considerations and token usage. The various documents are headed for working group approval, but some outstanding issues must still be closed out.

Meanwhile, OAuth implementation and deployment continues to grow, and issues with interoperablity arise, depending on which draft is used for guidance.

OpenID Connect

The last OpenID specification (2.0) was published in 2007, is seriously

Scorecard in Identity Management Standardization

The following organizations are working on standards related to identity management:

- The OpenID Foundation (OIDF; http://openid.net/foundation/) — OpenID 1.0/2, OpenID Connect
- OAuth (community site; http://oauth.net) — OAuth 1.0/OAuth Wrap
- Internet Engineering Task Force (IETF; www.ietf.org) — OAuth/WOES/Abfab/HTTP
- World Wide Web Consortium (W3C; www.w3.org) — HTML/HTTP/SOAP
- Organization for the Advancement of Structured Information Standards (OASIS; www.oasis-open.org) — SAML/XML/WS-*/XRI
- Shibboleth Project (www.shibboleth.net) — Shibboleth/OpenSaml 1.0/2.0
- US National Strategy for Trusted Identities in Cyberspace (NSTIC; www.nist.gov/nstic)
- Open Identity Exchange (OIX; http://openidentityexchange.org)
- Kantara Initiative (http://kantarainitiative.org) — proceeded by the Liberty Alliance
- InCommon Federation (www.incommon.org/about.html)
- US National Institute of Standards and Technology (NIST; www.nist.gov)
- Identity Commons (www.idcommons.net)
- Information Card Foundation (ICF; http://informationcard.net/foundation)
- International Telecommunications Union (www.itu.int/ITU-T/studygroups/com17/index.asp) — ITU-T Study Group 17
- International Organization for Standardization (ISO; www.iso.org)

outdated, and no longer reflects either the current state of deployment or potential new use cases — some of which will require a higher level of assurance than we can obtain with just a self-asserted identifier. In addition, the use of OAuth, which wasn't considered in the 2.0 case, has become common. Whereas XRI is now moribund, the Extensible Resource Descriptor (XRD) is nearing completion and might now be preferred for discovery in some cases. OpenID also needs to work both with native applications and in mobile devices, features not explicitly addressed in the current version.

The OIDF continues to house development efforts and has moved toward a more formal structure with dedicated working groups, each with a charter and a mutually agreed-on intellectual property regime. In 2010, two of those working groups, OpenID Artifact Binding and OpenID Connect, combined their efforts to address extended use cases and account for the use of OpenID in conjunction with OAuth. Initially labeled OpenID ABC, this work is now titled OpenID Connect. In a recent announcement, OIDF executive director Don Thibeau says, in part,

> We'll continue to engage developers and potential deployers about OpenID Connect at upcoming OpenID Summits ... to better understand, critique, refine, test, and ready OpenID Connect for prime time. (See http://openid.net/2011/05/20/openids-second-act-openid-connect.)

Still very much a work in progress, OpenID Connect is intended to work with OAuth 2.0 and JSON-based token formats for encryption and signing to create a social Web identity stack, and will impose some new requirements, such as using Secure Sockets Layer (SSL) to help address ongoing security concerns. With the addition of attribute exchanges and artifact bindings, this proposed stack begins to resemble older SAML federations — built with RESTful APIs and using JSON instead of XML.

The Connect work depends on both the IETF's successful standardization of OAuth 2.0 and the outputs of the recently proposed WOES working group, also in the IETF.

The need for identity management will only continue to grow. As individuals, we now find ourselves using multiple devices to access multiple accounts and services. We're also encouraged to store protected resources in various locations across the Internet. Just managing our own personal contacts and calendars can be a challenge. When we add the desire to share some of our information with others while continuing to protect our most sensitive data, the issues become even more complex.

Identity management implementations have come a long way, but greater coordination among the current players is necessary. The dominant models each bring useful properties to the table, but convergence has been slow. As new partnerships such as the NSTIC advance, and services like mobile Internet access and cloud computing gain traction, integration will become even more important. It's time to play ball!

Lucy Lynch champions the Trust and Identity Initiatives for the Internet Society. Her interests include the development and deployment of Internet-scale trust-enabling technologies and policies. Lynch has an MS in mass communications from the University of Oregon. Contact her at lynch@isoc.org.