Position Paper for the W3C Workshop on Transparency and Usability of Web Authentication

John Merrells, CTO, merrells@sxip.com
Dick Hardt, Founder and CEO, dick@sxip.com

Sxip Identity
Suite 206 55 Water Street
Vancouver, BC
V6B 1A1 Canada
604.678.3500

Workshop Background

"This Workshop aims to identify steps W3C can take to improve Web Security from the user-facing end of the spectrum: Practical security online often fails because users can be induced to make decisions that jeopardize their security and privacy, based on a lack of working authentication of Web sites' identities (phishing). We will look at technologies that can support Web users to better assess the trustworthiness and identity of sites with which they deal."

-- Toward a More Secure Web, http://www.w3.org/2005/Security/usability-ws/

Position Statement

The purpose of this position paper is to propose the requirements for improving the security of Web interactions. We believe that the web, and the Internet in general, requires a new identity infrastructure that places the user at the center of their identity transactions. By making users central in authentication and identity transactions, security and privacy risks are minimized thus leading to levels of trust that allow the Web to reach its full interactive potential. We call this the "user-centric view of identity management" or "Identity 2.0". This paper describes the criteria for an identity infrastructure that would provide user-based identity management.

Identity 2.0 - Design Requirements

The adoption and endurance of any identity management solution is based on the degree to which users trust the system. To gain this trust, the system must place the user at the center of their identity transactions – that is, users must own their information and have control over how that information is released and used. With current identity management systems, policy decisions (such as the location where identity data is stored and the circumstances when it is used) are opaque to the user. An Identity 2.0 solution makes policy transparent to users by using social cues that users understand and are familiar with. This leads to the following design requirements:

1. Provide a mechanism for presenting users with the information that is being requested.

   When users are informed regarding the information required by a Web entity, they know whether or not the requested information is available and can decide if they need to acquire that information in order to complete the transaction. For example, currently if a user's identity transaction is terminated because the requested information was not provided, the user is not necessarily informed of the reasons for the termination.

2. Provide a mechanism for users to identify the recipient of the identity information they release.

Online identity transactions do not have the same immediate social advantages of real-world interactions. That is, the user cannot see the entity that is using the provided information. Furthermore, the entity is not another human being but an automated service that the user cannot see. Consequently, when users are asked to release their identity information, they need a cue—such as a link, image or statement—that authenticates the identity of the party that will be receiving the information.

3. Provide a mechanism for relying parties to inform users of the reason for requesting the information and how the information will be used.

   Understanding the purpose of the transaction is a core component of trust. With this information, the user can make an informed decision about whether or not they want to release their identity information in order to engage in the transaction.

4. Provide a mechanism for users to compartmentalize their identity information according to the context of the interaction.

   Not all aspects of identity are appropriate for all kinds of transactions. Users must be able to tailor their identity into sub-sets of data, thus enabling them to present alternative sets of information in different contexts.

5. Provide a mechanism that ensures that user information is only released after the user consents to its release.

   In order to foster trust, users must be at the center of every identity transaction. Requests for identity data must be passed via the user, giving the user full visibility over the transaction and the ability to allow or deny the release of information.

6. Provide a mechanism for the user to specify what the relying party can do with the information.

   To have confidence in identity transactions, users must be informed regarding the purposes for which their information will be used. Users may be willing for their information to be used for one purpose but not another, and should therefore be notified of all the uses intended for their identity information.

7. Provide users with a mechanism for granular control over the information that they are releasing.

   Beyond authorizing the overall transaction, users should also be able to specify which pieces of identity data are released. For example, if proof of membership in an organization is requested, the only attribute that is released as part of the claim should be the information that states the user's membership credentials.

8. Provide a mechanism for separating the transaction for acquiring a claim from the transaction for presenting a claim.

   When a relying party requests a claim, the only parties involved in the transaction are the user and the party that has requested the claim. This prevents leakage of user data to the third-party that issued the claim.

9. Provide users with the ability to choose their identity storage agent.

   Users can choose where their identity data is stored. They may prefer to store their data with a trusted external agent, or within an application on their own machine. The power of choice provides users with the ability to select the storage agent that is most secure and / or convenient.

10. Provide pairwise identifiers for anonymous identity transactions.

    By providing pairwise (or "uni-directional") identifiers, the relying party cannot track a user's online activity. It also prevents multiple parties from using the identifier to correlate the user's identity information.

11. Provide identifiers for public identity transactions.

    The ability for users to establish a reputation brings an aspect of social identity to the Web, whereby participants can engage in subjective (rather than purely objective) interactions. In order for users to develop an online reputation, they should have the option to establish a common identity across different sites.

12. Provide interoperability with existing platforms and standards.

    In evolutionary technologies, users and websites have an existing infrastructure, that, while insufficient for more sophisticated usages, represents considerable investment both in terms of implementation cost and in terms of user familiarity. Identity infrastructure must be interoperable, for example by supporting the LAMP, Java and Microsoft stacks, including support for common languages such as Java, Perl, Python, PHP, Ruby and C/C++.

13. Provide a low barrier to entry.

    Although the system should provide levels of security, including cryptographic keys for sites that require it, a flexible gradient of security levels should be provided to allow entry-level sites to participate.

14. Provide a consistent user experience by ensuring that the user always sees the same agent, regardless of the context.

    The user has a choice regarding the agent they use to store their identity data, whether it is an external site or an application on their own machine. Once they have selected their agent, however, the user experience must be consistent and informative regarding the agent involved in the transaction, regardless of the platform, the level of security or the nature of the relying parties and issuers that they are interacting with.

Identity 2.0 – Implementation

A number of organizations are working on identity infrastructure solutions that seek to satisfy these requirements. Among them, Sxip Identity has developed a protocol - SXIP, the Simple eXtensibe Identity Protocol - that meets all these design requirements.

Sxip has been leading an effort within the IETF to codify a simple and secure protocol for identity information exchange and has proposed the core of the SXIP 2.0 protocol as a possible solution. The IETF mailing list for the group is called “DIX”, for Digital Identity eXchange, and discussions are currently centered around the establishment of a Working Group.

References

Kim Cameron’s Seven Laws of Identity:
http://www.identityblog.com/stories/2004/12/09/thelaws.html

The Identity Gang:
  http://www.identitygang.org/
Identity 2.0 Vision Presentation:
  http://www.identity20.com/media/WEB2_2005/
SXIP 2.0:
  http://www.sxip.org
DIX Mailing List:
  http://www.ietf.org/mail-archive/web/dix/