Risks Presented by Single Sign-On Architectures

Gary Ellison, Jeff Hodges, and Susan Landau
October 18, 2002

For the man on the street, the businesswoman in her office, the shopper or investor at home, identity on the Internet is a straightforward idea with a complex solution. Using Amazon, there is one sign-on and password; using United Airlines, another; connecting to L.L. Bean, yet another, and with Fidelity Investments, a fourth. Within the enterprise, each service --- on-line corporate travel, 401(k) account management, employee benefits --- may require its own sign-on and password. The same holds for business-to-business interactions. The result is cumbersome, the user experience offputting. The first challenge of Web services is a simple and secure identity mechanism, the second, and equally important, concern is privacy protection.

Single sign-on and federated network identity (a system for binding multiple accounts for a given user) are key to solving this. A federated system allows businesses to manage their own resources including customer data. Federated network identity enables consumers to retain some control over which companies have access to their information.

The mission of the Liberty Alliance Project is establishing open standards for federated network identity through open technical specifications. The intent is to enable a networked world in which individuals and businesses can more easily conduct transactions while protecting the privacy and security of vital identity information.

The Liberty Alliance version 1.0 specifications were collaboratively developed by over forty companies. The specifications describe protocols, protocol bindings and schemas by which a single sign-on over standard Internet protocols can be implemented and deployed.

Developing a single-sign-on architecture for federated network identity system in the 2002 Internet environment when the only common Web security tool is SSL (Secure Socket Layer) is technically challenging. Doing so without controlling the most important tool for user interaction --- the browser --- makes it even more so.

The Liberty protocols are a set of specifications rather than a deployed service. The distinction between specification and service is important. A specification is essentially a design blueprint; a deployed service is an implementation of the design. The difference between design and implementation is also very important. Here we give a high-level overview of the security and privacy constraints under which the Liberty version 1.0 protocols were developed. Implementers and deployers should read the overview and normative documents ‘‘Liberty Architecture Overview’’ [1], ‘‘Liberty Bindings and Profiles Specification’’ [2], ‘‘Liberty Protocols and Schemas Specification’’ [5], ‘‘Liberty Authentication Context Specification’’ [3] and ‘‘Liberty Version 1.0 Errata’’ [4] for implementation issues and details.

Perhaps the most constrictive requirement for the version 1.0 specifications was the targeted deployment environment. These protocols must leverage the existing installed base of web browsers without requiring the installation of specialized software. Additionally, Liberty protocols must utilize existing Internet protocols.

The intent of the Liberty version 1.0 protocols is to make single sign-on to multiple sites substantially as secure as giving a name and password at each site. We list the Internet issues that make this a challenging problem and that require care by any Liberty version 1.0 implementor or deployer.

- Weak passwords in a single sign-on environment can pose a significant risk. The compromise of a users password could result in unauthorized access to protected resources and information. Liberty specifications do not specify use of any particular authentication technology. The Liberty specifications offer a flexible facility to describe the context of an authentication event. Thus, authentication services are free to deploy stronger forms of authentication that diminish the threat weak passwords present.

- The currently-installed browser base includes many browsers that only have weak 40-bit cryptography enabled. This poses a significant threat to single sign-on environments that require confidentiality to securely engage in authentication or other protocol exchanges. To combat this risk Liberty specifications suggest the use of cipher suites with minimally have effective key sizes of 112-bits.

- The Domain Name System (DNS) [6] provides the critical function of resolving host names to Internet addresses. However DNS is not a secure protocol. A common solution implemented to inhibit this risk is to utilize SSL server authentication. The Liberty specification recommends this.

- In the past single sign-on architectures have not dealt with privacy threats presented by network participants. That is in many single sign-on environments the identity of the user is shared by all parties. There is a threat of collusion among network participants which may not be desired by the user. The Liberty Alliance is quite concerned about protecting privacy and security of identity information, and in order to achieve this, the Liberty specifications have been designed to obscure the identity of the user so that each network participant is presented a unique pseudonym for the user. This confounds the ability of network participants to collude with each other in order to garner identity information the user did not authorize to be disclosed.

The risks and threats described in this paper are common to most Internet-based applications. Some of the risk pose an even greater risk in a single sign-on environment since a breach in one system could be leveraged to attack other reliant systems. We described the basic mechanisms specified in the Liberty protocols that work to mitigate these threats. We know of no specific vulnerabilities in the version 1.0 specifications. Implementers are encouraged to adhere to the guidance given in the Liberty specifications and should certainly be well aware of the perils of their deployment environment.

References

1. Hodges, J., ‘‘Liberty Architecture Overview version 1.0,’’ July 2002, http://www.projectliberty.org/specs/liberty-architecture-overview-v1.0.pdf

2. Rouault, J., ‘‘Liberty Bindings and Profiles Specification version 1.0,’’ July 2002, http://www.projectliberty.org/specs/liberty-architecture-bindings-and-profiles-v1.0.pdf

3. Madsen, P., ‘‘Liberty Authentication Context Specification version 1.0,’’ July 2002,

http://www.projectliberty.org/specs/liberty-architecture-authentication-context-v1.0.pdf

4. Hodges, J., ‘‘Liberty Version 1.0 Errata,’’ October 2002, http://www.projectliberty.org/specs/draft-liberty-version-1-errata-00.pdf

5. Beatty, J., ‘‘Liberty Protocols and Schemas Specification version 1.0,’’ July 2002, http://www.projectliberty.org/specs/liberty-architecture-protocols-schemas-v1.0.pdf

6. P.V. Mockapetris, ‘‘Domain names - implementation and specification,’’ RFC 1035, November 1987, http://www.isi.edu/in-notes/rfc1035.txt