Chapter 12
Identity Management Systems

Waleed Alrodhan
Imam Muhammed Ibn Saud University, Saudi Arabia

ABSTRACT

In this chapter we provide an overview of five of the most widely discussed web-based identity management systems, namely Microsoft CardSpace, the Higgins project, the Liberty Alliance project, the Shibboleth project, and OpenID. These systems are discussed throughout the chapter; we also investigate certain security limitations shared by all these systems.

Next, we discuss the practicality of identity management systems, and consider how their practicality can be enhanced by developing reliable integration and delegation schemes. We also provide overviews of the Project Concordia integration framework, and the Shibboleth and OAuth delegation frameworks, as well as reviewing the related literature.

INTRODUCTION

An identity management system enables authoritative sources to perform identity management tasks via an operational framework. Most of today's web-based identity management systems adhere to one of the practical identity management models described in the previous chapter(i.e. the isolated, Information Card-based or Federated identity management models).

DOI: 10.4018/978-1-61350-498-7.ch012

The last few years have seen the development of a number of web-based identity management systems, including AOL OpenAuth[i], Yahoo BBAuth[ii], and Flickr Authentication API[iii]. Many of these systems are isolated, and they are largely not interoperable with one another.

After an open dialogue with a number of identity management experts, in 2005 Microsoft published its Laws of Identity (Cameron, 2005). These laws reflects Microsoft's vision of the requirements that should be met by any web-based identity management system. A list of these laws,

with Microsoft's interpretation of them, is given below (note that we have changed the terminology slightly to use the term 'identity management system' instead of 'identity system').

1. **User control and consent:** The identity management system must only reveal information identifying a user with the user's consent.
2. **Minimal disclosure for a constrained use:** The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.
3. **Justifiable parties:** The identity management system must be designed so that the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.
4. **Directed identity:** The identity management system must support both 'omnidirectional' identifiers for use by public entities and 'unidirectional' identifiers for use by private entities.
5. **Pluralism of operators and technologies:** The identity management system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.
6. **Human integration:** The identity management system must define the human user to be a component of the distributed system, integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.
7. **Consistent experience across contexts:** The identity management system must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

It seems reasonable to believe that, by following the laws stated above, identity management systems can reach an acceptable level of usability, reliability, flexibility, and privacy. We also observe that a number of these laws were derived from the OECD principles for personal data protection (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980).

In this chapter we describe five identity management systems and frameworks, namely Microsoft CardSpace, Higgins, the Liberty Alliance Project, Shibboleth, and OpendID. We also discuss enhancing the practicality of identity management systems by enhancing both their interoperability (using integration schemes) and their usability and flexibility (using delegation schemes).

Microsoft CardSpace

Back in 1999, Microsoft introduced.NET Passport, a ticket-based single sign-on system. Although. NET Passport was supported by a number of well-known service providers, such as eBay and Visa, it was not widely used for SSO. The single sign-on features have since been restricted to Microsoft web sites only, and Passport now functions simply as a means of logging-in to these web sites. In 2005, Microsoft published two white papers that discuss the 'failure' of.NET Passport (Cameron, 2005, Microsoft Corporation, 2005a), and this analysis has clearly influenced Microsoft's subsequent offerings in this area, including the development of Microsoft CardSpace.

Microsoft CardSpace (henceforth abbreviated to CardSpace) is the name for a Microsoft WinFX software component that is described by Microsoft as an 'identity metasystem'; using our terminology, it is an identity management system. It is designed to comply with the seven Laws of Identity, as promulgated by Microsoft. A new version of CardSpace, CardSpace 2.0, is expected to be officially released in 2010 (a Beta version has recently been released); however, Microsoft has stated that it will be compatible with the currently deployed version of CardSpace[iv].