Chapter 7
Towards a Trust Management Enabled Identity Metasystem

Weiliang Zhao
Macquarie University, Australia

Jian Yang
Macquarie University, Australia

ABSTRACT

Existing identity metasystems provide enabling tools to manage, select, and control of digital identities but they have not provided the support of trust management that should cover how trust requirements associated with digital identities are modeled, how runtime conditions for trust are evaluated, and how the results of trust evaluation are consumed by systems/applications. In this paper, the authors propose an approach toward a trust management enabled identity metasystem that covers the analysis of trust requirements and the development of trust management system in a consistent manner. The proposed trust management architecture extends the existing identity metasystems by introducing computing components for carrying out typical trust management tasks associated with digital identities. The computing components in proposed architecture provide intelligent services for these tasks. The proposed high level architecture targets the automation of the development of the trust management layer for digital identities.

1. INTRODUCTION

More and more economic and social activities are carried out on the Internet. The Internet was originally built without a way to know who and what users are connecting to. Digital identities are widely employed for providing enable solutions to address the above "unknown" issue in different information systems and applications on the Internet. Service-oriented computing has become a well adopted technology and it has reshaped a vast number of business models and processes. Digital identities have been widely employed as crucial components for weaving a world of cooperating Web services where application components are assembled to support dynamic business processes

DOI: 10.4018/978-1-4666-1577-9.ch007

that span multiple enterprizes, organizations, and computing platforms.

In the "The laws of identity" (Cameron, 2005), a digital identity is defined as a set of claims made by one digital subject about itself or another digital subject. The digital subject is a person or thing represented or existing in the digital realm which is being described or dealt with and a claim is an assertion of the truth of something. There are different management tasks for the processes of representing, recognizing, and usage controlling of digital identities. The identity management in the digital world normally relates to the behavior of corresponding entities of digital subjects in their real world activities (Claub & Kohntopp, 2001). Digital identities normally convey sensitive information of their subjects. The employment of digital identities will normally bring in many critical security and privacy issues such as identity phishing, pharming, and privacy protection for sensitive information embedded in digital identities. The disclosure of digital identities must be under the control based on the satisfaction of related trust requirements (Josang, Fabre, Hay, Dalziel, & Pope, 2005). The existing identity systems including CardSpace (Bertocci, Serack, & Baker, 2007), Sxip (Sxip, 2009), Higgins (Eclipse-Foundation, 2009), and OpenID (OpenID-Foundation, 2009) have provided different functions for users to manage, select, and control digital identities. However, these identity systems have not provided further support for the modeling of trust requirements associated with digital identities, evaluation of runtime status for trust, and a range of mechanisms of trust consumption related with digital identities. The privacy and security are still a hindrance for digital identities to support wide range of e-commerce, governmental and social activities.

When digital identities are used on the Internet, their usages normally cross business boundaries and security domains. Identity 2.0 (stemming from Web 2.0) brings in a digital revolution of identity verification on the Internet. It employs user-centric technologies such as Information Cards (Bhargavan, Fournet, Gordon, & Swamy, 2008) and OpenID (OpenID-Foundation, 2009) for providing a simple and open method to employ digital identities in supporting transactions as corresponding physical identities in the physical world. These information cards and OpenID are the employed digital identities. There are two categories of identity management. The first category includes those domain-centric approaches such as the Liberty Alliance (The Liberty Alliance Project, 2009) which are actually based on federation protocols. These approaches have the limitation for supporting grander structures beyond federated domains on Internet. The second category includes user-centric approaches such as Microsoft's CardSpace (Bertocci et al., 2007), Sxip (Sxip, 2009), and Higgins (Eclipse-Foundation, 2009). These approaches leverage Internet and Web protocols with different ways for storing identity attributes and using digital identities for securing associated transaction and/or interactions. The approaches in the second category have the issue of interoperability. The currently existing identity management approaches in both categories only target providing facilities to enable users to have convenience and control over their digital identities by defining how to generate, select, and verify them. The further trust management concerns about how to define trust mechanisms, evaluate runtime status, manage various ways of trust consumption are not included in these approaches. The trust management for digital identities is always related with a range of trust relationships which can be specified based on users, relying parties, required digital identities, and context specific requirements. It is highly desirable to have a formal model of trust relationship that can be used as a solid foundation for the analysis and modeling of trust requirements and the development of sub system of trust management for digital identities to be used on the Internet. The specification/modeling of trust relationships and the development of trust management systems should be considered in a consistent manner.