Chapter XXVI
Emerging Frameworks in User-Focused Identity Management

Manish Gupta
State University of New York, USA

Raj Sharman
State University of New York, USA

ABSTRACT

A paradigm shift is occurring in identity management philosophy. User-focused identity management is one the emerging and most promising paradigms. One of the fundamental principles of the user-focused identity management frameworks is that the users control their identity formations, revelations, and interactions. This means that users must be given the choice of which identities to use at which services; they have choice to decide what identity information will be disclosed to services and how those services will use their identity information. User-focused identity management frameworks are posed to make users' online interactions easier and safer. In this chapter, we survey 11 of the most common user-focused identity management frameworks that are emerging, and their associated technologies. First, the chapter discusses issues and challenges with domain-centric identity management paradigm and presents unique value propositions of user-focused frameworks. Secondly, this chapter provides a comprehensive and cohesive coverage of common user-focused identity management frameworks. Users, technologists, businesses; and systems and security managers will gain a comprehensive understanding of the concepts, frameworks and associated technologies relating to user-focused identity management.

1. INTRODUCTION

Digital identities come in all shapes and sizes. Usually people use different digital identities in different contexts depending on association of different information with each identity. For example, an identity that we use with a online retailer will allow access to personal information such as credit card information, shipping information, purchasing history and personalized recommendations, the one used with social networking sites such as orkut.com does not. There are different methods and protocols to create new identities depending on context and user preferences. Insecure identity management has led to severe consequences. Recent research (Javelin, 2007) shows that the number of US is 8.4 million in 2007 and total one-year fraud amount is $49.3 billion in 2007.

Identity is a collection of unique characteristics of an entity which are either inherent or are assigned by another entity (Pfitzmann and Waidner, 2004). A digital identity comprises electronic records that represent network principals, including people, machines, and services (Windley, 2005; March, 2003). To be able to create, maintain and use digital identities the deployment of a digital identity management system is required. The term "identity management" (Casassa, 2003) is currently associated with technologies and solutions, mainly deployed within enterprises, to deal with the storage, processing, disclosure and disposal of users' identities, their profiles and related sensitive information. This infrastructure uses identities in the process of authentication and maps identifiers to the information needed for identification and authorization (Buell and Sandhu, 2003; Pfitzmann and Waidner, 2004). Identity Management covers the spectrum of tools and processes that are used to represent and administer digital identities and manage access for those identities (Allan et al., 2008). The three main business drivers for identity management solutions are security efficiency (lower costs and improved service), security effectiveness (including regulatory compliance) and business agility and performance (including workforce effectiveness and customer convenience) (Allan et al., 2008).

Identity Management is a means to reduce such risks, representing a vital part of a company's security and auditing infrastructure ((Buell and Sandhu, 2003). The secure and efficient administration of numerous personal attributes that make up digital identities is one of the key requirements in open and closed networks. Especially in respect to confidentiality and integrity, the users themselves, rather than popular external threads like viruses, phishing, or pharming attacks represent the main risk (Stanton et al, 2005). As a result of incorrect account management and inadequately enforced security policies users accumulate a number of excessive rights within the organizations' IT systems over time, violating the principle of the least privilege (Ferraiolo et al., 2003). Moreover, people have a hectic life and cannot spend their time administering their digital identities (El Maliki and Seigneur, 2007). Identity Management in open networks like the Internet has received tremendous attention throughout the last years with researchers. Although considered important, Identity Management in closed networks, however, has not gained comparable significance within the research community.

In this paper, we survey eleven of the most common user-focused identity management frameworks that have evolved and their associated technologies. Contributions of the paper are two-fold. First, the paper discusses issues and challenges with domain-centric identity management paradigm and presents unique value propositions of user-focused frameworks. Secondly, the paper provides a very comprehensive and cohesive coverage of most common user-focused identity management frameworks. Users, technologists, companies and systems and security managers will gain a comprehensive understanding of the concepts, frameworks and associated technologies