Chapter 8
Identity Management Systems: Models, Standards, and COTS Offerings

Reema Bhatt
State University of New York – Buffalo, USA

Manish Gupta
State University of New York – Buffalo, USA

Raj Sharman
State University of New York – Buffalo, USA

ABSTRACT

Identity management is the administration of an individual's access rights and privileges in the form of authentication and authorization within or across systems and organizations. An Identity Management system (IdM) helps manage an individual's credentials through the establishment, maintenance, and eventual destruction of their digital identity. Numerous products, applications, and platforms exist to address the privacy requirements of individuals and organizations. This chapter highlights the importance of IdM systems in the highly vulnerable security scenario that we live in. It defines and elaborates on the attributes and requirements of an effective identity management system. The chapter helps in establishing an understanding of frameworks that IdM systems follow while helping the reader contrast between different IdM architecture models. The latter part of this chapter elaborates on some of today's most popular IdM solutions.

1. INTRODUCTION

We live in an age where information systems dominate our world. For everything, from paying bills to ordering food or from buying apparel to managing bank accounts; we make use of the vulnerable and susceptible medium-the internet. Organizations-whether commercial or governmental, rely heavily on their intranet and internal information systems for efficient operations, management and day to day functioning. When making services available via computer networks, there is often a need to know who the users of the system are and what information they are authorized to view or access (Jøsang & Pope). Almost all websites and web services require users to present their identities

DOI: 10.4018/978-1-4666-7381-6.ch008

in order to be authenticated and granted access. Users are identified by their digital identities that comprise of usernames passwords, date of birth, search history, purchasing behavior, passphrases etc. This calls for user privacy management and related issues. Researchers argue that information exchanged online is susceptible to numerous threats which arise from two main factors. Firstly, users have no control over who views their information for e.g. a user knows that their passwords are stored in a database but they have no control over people who access the database. Secondary to this threat is the fact that the user's information is stored indefinitely which means that the identity thief can lie in the future as well (Alkhalifah & D'Ambra, 2012). According to a recent Forrester Research (Kark, 2010) identity and access management was identified as a top security issue for 2011 that needed to be considered as a critical component of corporate security strategies (Cser, 2008).

Two parts of identity management are identified by:

1. Providing users with credentials that can uniquely identify them; and
2. Using these credentials to authenticate users and grant them access and privileges based on these credentials (Jøsang & Pope). The dominance of digital identities, however, also raises concerns about protecting user privacy. Privacy is one of the most challenging issues related to identity management. Privacy related requirements impose several restrictions on identity management systems and therefore are extremely critical (Glasser & Vajihollahi). Users seldom have control over their own digital identity. Information that they provide as a part of mandatory disclosure is stored indefinitely in systems and databases that the users themselves have no control over. This has made it possible for hackers and criminals to rob people off money and information from the comfort of their own homes. Identity theft is thus increasingly becoming one of the prominent cyber-crimes; hackers that can manage to steal an individual's digital identity get access to confidential information such as credit card numbers, bank passwords, SSN etc. Identity management systems, IdM, were therefore created to address these security concerns.

The contributions of this chapter are manifold. First it provides an overview of different architectures and applications of IdM systems. It provides an insightful discourse on the components and attributes of IdM systems so as to be able to decide what kind of systems will best fit the reader's organizational needs and requirements. It will serve as an excellent primer for IT and security professionals in understanding what options are available to them, which can immensely help them in decision making. It also presents a rich discussion of the background of IdM systems and the challenges that today's organizations can face in management of IdM systems. The last section presents some of the most popular and effective commercial off the shelf IdM systems that are available for purchase. This section will benefit organizations that do not wish to build customized IdM solutions but instead purchase one from commercial software vendors; which is not only the most widely used but also considered to be the most cost effective approach. Discussions and presentations in this chapter can act as an aid for security managers and professionals in understanding the current identity management solutions and technologies while facilitating their decision making and risk management. The goal of this chapter is to provide a broad view of IdM systems and help professionals make decisions that would benefit their company.

The organization of this chapter is as follows. Section 2 throws light on why IdM systems should be used, how they help a business and how they work. Section 3 highlights the key components