Chapter 48
A Technology and Process Analysis for Contemporary Identity Management Frameworks

Alex Ng
University of Ballarat, Australia

Paul Watters
Massey University, New Zealand

Shiping Chen
CSIRO Computational Informatics, Australia

ABSTRACT

The digital profile of a person has become one of the tradable digital commodities over the Internet. Identity management has gained increasing attention from both enterprises and government organisations, in terms of security, privacy, and trust. A considerable number of theories and techniques have been developed to deal with identity management issues using biometric multimodal approaches. In this chapter, the authors review, assess, and consolidate the research and development activities of contemporary biometric and non-biometric identity management in 21 privately and publicly funded organisations. Furthermore, they develop a taxonomy to characterise and classify these identity management frameworks into two categories: processes and technologies. The authors then study these frameworks by systematically reviewing the whole lifecycle of an identity management framework, including actors, roles, security, privacy, trust, interoperability, and federation. The goal is to provide readers with a comprehensive picture of the state of the art of the existing identity management frameworks that utilise biometric and non-biometric technologies with the aim to highlight the contemporary issues and progress in this area of identity management.

DOI: 10.4018/978-1-5225-7113-1.ch048

INTRODUCTION

Identity and Access Management (IAM) is the key to the secure access of an organisation's assets. We have seen traditional IAM takes a technology-driven approach to protecting against security threats and vulnerabilities. Nowadays, identity is increasingly mobile, cross-domain and transactional. However, we have witnessed IAM has evolved from a disparate manner. On one end, we saw many mission critical applications (such as defense or physical access control systems) that relies on the biometrics industry companies to shoulder the burden of promoting adoption of biometric IAM systems which shows a disproportionate focus on technology issues. Existing biometric IAM solutions and researches are confined to a limited number of pre-selected combinations of biometric modalities such as, face recognition, voice recognition, and/or hand geometry comparisons (Veeramachaneni, Osadciw, & Varshney, 2005) with add-on technologies such as Match-On-Card (Bringer, Chabanne, Kevenaar, & Kindarji, 2009). Governments in some countries have also taken charge in imposing strategic solutions to combat the situation. In Australia, for example, there is a dedicated section of the Attorney General's Department that deals with identity security, having developed a national Document Verification System (DVS) for government-issued credentials across national and state agencies (Attorney General's Department, 2007).

On the other hand, we saw numerous financial applications which have multi-trillion monetary significant rely purely on digital security proof (such as user-id/password or chip-and-pin payment method). More importantly, we saw multiple vendors supplying multiple end point products often provide solutions with user data being stored and managed in multiple locations within an organisation, and in users having multiple user ID's and passwords creating islands of data and redundant software/hardware investments, and most importantly, hindering business growth due to low level of manageability of the business assets and processes (Beaver & Shaw, 2011). Meeting the increase in demands for a unified identity management system, major software and hardware vendors have also flocked the market with a multitude of solutions such as Oracle Identity Management, Microsoft Identity Integration Server, IBM Tivoli Identity Manager, Novell Identity Manager, Hitachi ID Management Suite, Intercede MyID etc. These commercial identity management systems provide application and platform specific identity and access control functionality, by aggregating identity-related information from multiple data-sources. The primary goal of these enterprise identity management systems is to provide organisations with a unified view of a user's/resources identity in a heterogeneous enterprise IT environment through the use of middleware, and provide practical outcomes for users, such as Single Sign On (SSO) authentication. Furthermore, cloud computing has revolutionised the way that organisations use computers to run applications and access services, which raises new challenges for identity management. Thus, Citrix OpenCloud Access is an example which provides SSO, provisioning, and access workflow management for a variety of cloud-based applications.

IAM has become a critical issue in enterprises and public government agencies, as reflected in a survey conducted by Gartner in 2010 that ranked identity management as the first of the top five priorities for security in enterprises (Messmer, 2010). However, at the same time, we have seen a low adoption rate of IAM systems in enterprises, with only 3 in 10 IT professionals reporting that their companies have IAM solutions (Deeds, 2011). Viewing the problem from a broader sense, biometric identity management has great impact on many aspects of our daily life, including:

- Public and individual safety (such as, identity theft and fraud, cybercrime, computer crime, organised criminal groups, document fraud and sexual predator detection);