A Consolidated Process Model for Identity Management

Alex Ng, University of Ballarat, Australia
Paul Watters, University of Ballarat, Australia
Shiping Chen, CSIRO ICT Centre, Australia

ABSTRACT

Recently, 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 within and between organisations. In this paper, the authors reviewed, assessed, and consolidated the research and development activities of identity management in 14 privately and publicly funded organisations. Furthermore, the authors developed a taxonomy to characterise and classify these identity management frameworks into two categories: processes and technologies. The authors then studied these frameworks by systematically reviewing the whole lifecycle of an identity management framework, including actors, roles, security, privacy, trust, interoperability, and federation. This paper aims to provide the reader with the state of art of existing identity management frameworks and a good understanding of the research issues and progress in this area.

Keywords: Identity Management Framework, Interoperability, Privacy, Process Model, Taxonomy

1. INTRODUCTION

Identity theft is a crime which involves stealing money or gaining a benefit by pretending to be someone else. While the Internet has improved communications and the ease of doing business, an inevitable side-effect is that criminals now have more opportunities than before to obtain personal details about a large community of unknowing victims. By stealing a person’s identity, a fraudster may access the victim’s bank account, obtain credit cards or loans in the victim’s name, and potentially ruin the victim’s credit rating. Recently, we have witnessed the uprise number of cases in identity fraud around the globe. The figures obtained from the Australian Bureau of Statistics’ first survey of personal fraud (Pink, 2008) indicate that around 3.1% (499,500) of the Australian population aged 15 years and over were victims of at least one incident of identity fraud within the 12 months prior to the survey. Furthermore, 2.4% (383,300) were the victims of bank or credit card identity fraud, and 0.8% (124,000) were victims of identity theft. A similar situation has occurred in the US - identity theft was the most common type of consumer fraud between 2000 to 2008, comprising an average 37% of...
the total number of fraud incidents each year. Alarmingly, the trend shows that the number of identity theft incidents has increased more than 10 fold from 31,140 in 2000 to 313,982 in 2008 (Finklea, 2010). Loss of personal data in the government and private sector is rampant (see Watters, 2009, for a UK survey).

At the same time, we have seen a low adoption rate of identity management systems in enterprises, with only 3 in 10 IT professionals reporting that their companies have identity access management solutions (Deeds, 2011). Conversely, identity management 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).

The key assertion in our paper is that identity management frameworks – while dealing with internal issues relating to the management of data types representing abstractions of identity – must be applicable for all types of identity theft. This would make identity management more appealing to businesses for adoption, even accounting for the complexity in their implementation. One of the key benefits of identity management can be realised when issues that arise from the mis-management of identity are prevented.

There are numerous offerings and solutions proposed from a range of communities (including industry and standards bodies). 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). 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, identity management could also be extended to the domain of telecommunications, as shown in the Cisco Trust and Identity Management Solution (CTIMS). CTISM authenticates entities, and determines access privileges based on policy, control network access policy to trusted network devices, and monitors network activities. On the other hand, 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.

Viewing the problem from a broader sense, identity management has great impact on many aspects of our daily life, including:

- Public Safety (such as, identity theft, cybercrime, computer crime, organized criminal groups, document fraud and sexual predator detection),
- National Security (such as cyber security and cyber defence, human trafficking and illegal immigration, terrorist tracking and financing),
- The finance industry (such as mortgage fraud and other financial crimes, data breaches, e-commerce fraud, insider threats and health care fraud), and
- Individual Protection (such as identity theft and fraud).
The Use of a GDSS Tool in Regional Economic Planning: A Case Study
www.igi-global.com/article/use-gdss-tool-regional-economic/50937?camid=4v1a

Organizational Culture and Employees' Computer Self-Efficacy: An Empirical Study
www.igi-global.com/article/organizational-culture-employees-computer-self/1247?camid=4v1a

Network Implementation Project in the State Sector in Scotland: The Influence of Social and Organizational Factors
www.igi-global.com/chapter/network-implementation-project-state-sector/44629?camid=4v1a