Chapter 8
Identity and Access Management Architectures with a Focus on User Initiative

Takao Kojima
Institute of Information Security, Japan

Yukio Itakura
Institute of Information Security, Japan

ABSTRACT

Herein we propose the concept of “Identity and Access Management Architectures” comprising a policy-oriented management system that enables the utilization of user identity-related data. This policy-oriented management system encourages users to take the initiative in providing their own identity-related data and encourages awareness of the usage of such data by entities. This Architecture is designed to allow users to initiate “user policies” for identity-related data protection (user intention providing user data), just as entities have policies describing their intention to consume the data.

We have developed a “Privacy Policy Matching Engine” as a component of the Identity and Access Management Architectures. This engine enables the matching of a user’s intention to provide his/her identity-related data with an entity’s own privacy policy. Also, it automatically analyzes the policies with a focus on the types and handling method for identity-related data.

INTRODUCTION

With the recent explosion in the use of the Internet, many users now enjoy browsing corporate websites or online shopping in daily life. The majority of users, however, are unaware of the unfettered use of identity-related data that they provide to business entities. Despite business entities openly declaring their privacy policies, in most cases, users fail to understand of these privacy policies or just ignore them.

In this chapter, we propose the use of a new user support tool, “Privacy Policy Matching Engine”.

DOI: 10.4018/978-1-61350-498-7.ch008
The aim of this engine is to encourage users to take the initiative in selecting business entities that users feel comfortable with. By, simply matching users’ own policies with entities’ privacy policies. This ‘engine’ provides the user policy support feature and automatic collection and analysis feature. These two features give users “increased awareness” and “free choice of entities whom to connect with.”

We describe the concept of the Privacy Policy Matching Engine and how it works as a component of the Identity and Access Management Architectures and examine the prototype for implementation.

BACKGROUND

Security and privacy issues in identity-related data management play an essential role in cloud computing. In particular, it is very important to define the right means for managing such data based on policies in order to comply with privacy-related standards and regulations. As a consequence, the identity management market—or identity and access management (IAM) market—is forecasted to grow from nearly $2.6 billion in 2006 to more than $12.3 billion in 2014 (including revenues from both products and implementation services) (Forrester, 2007). The cloud computing market which stood at $36 billion in 2008 is expected to reach $160.2 billion by 2015. Market growth is fuelled by the ease of information access made possible by the cloud (WinterGreen Research, Inc, 2009). The area of identity management has been addressed as part of the Seoul Declaration of the Future of the Internet Economy (2008/06) (OECD, 2008) and US President’s Cyberspace Policy review (Whitehouse, 2009).

However, despite the fact that legal systems regarding privacy protection and personal information distribution, such as the OECD’s Eight Principles (OECD, 1980), have been progressing on a global scale and the fact that most entities openly declare their privacy policies, the majority of users tend to just click the “I Agree” button without understanding the underlying details. Even though such policies are posted on websites where users can easily access them, the details are often too difficult for general users to comprehend and many contain technical jargon.

Therefore, we have developed the “Privacy Policy Matching Engine” as a component of the Identity and Access Management Architectures. The Privacy Policy Matching Engine enables users to provide their data as intended according to one’s own policies.

MAIN FOCUS OF THE CHAPTER

Issues, Controversies, Problems

The majority of users tend to just click the “I agree” button when accessing entities’ websites, with little or no regard to their own privacy protection.

Users’ Unawareness for Identity-Related Data

Users can have “consciously provided information” and “unconsciously provided information.” Although the information is recognized as being effective in some fields, such as behavior targeting advertisement (Hayashi, K., 2007; Oda, K., N. Takahiro, S. Suda, & T. Yukawa., 2007), users have extremely low awareness when it comes to explicitly managing their intentions to provide their information, and what’s more, there is no tool to assist users in managing their intentions properly.

Usability of Privacy Policies

Entities’ privacy policies are posted on websites where users can easily access them, however, these policies are often too difficult for general users to comprehend and many contain technical jargon.