

IDENTITY MANAGEMENT

February 2008

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of, and may not be reproduced in whole or in part without the express permission of the Government of the HKSAR.

Disclaimer: Whilst the Government endeavours to ensure the accuracy of the information in this paper, no express or implied warranty is given by the Government as to the accuracy of the information. The Government of HKSAR accepts no liability for any error or omission arising from or related to the use of the information.

TABLE OF CONTENTS

Summary	2
I. Introduction.....	3
What is Identity Management?	3
Models and Techniques	4
II. Challenges of Identity Management.....	8
Identity Theft.....	8
Identity Management Adoption And Benefits	9
III. Conclusion.....	11

SUMMARY

Identity management in an enterprise is a combination of processes and technologies to manage and secure access to the information and resources of an organisation. Common identity management models, as well as authentication techniques and authorisation models, are discussed in this paper. As the threat of identity theft increases, both businesses and governments are strengthening identity protection using the latest technology. But relying on security technologies is not sufficient. Users and organisations adopting identity management systems need to pay close attention to the most appropriate security measures and best practices in terms of identity management systems that use password-based authentication and Single sign-on (SSO) mechanisms.

I. INTRODUCTION

WHAT IS IDENTITY MANAGEMENT?

Identity management in an enterprise is a combination of processes and technologies to manage and secure access to the information and resources of an organisation while also protecting user profiles, including customer profiles. It includes the entire process of deciding who should have access to resources, and to what resources; providing, changing and terminating such access when appropriate; managing the process and monitoring it for compliance with internal and external policies. This usually applies to situations where a person has to identify who he/she claims to be by means of a verified identity, such as a passport or identity card at border control, login credentials for e-banking, biometric identification for account access at an ATM machine, and so on.

Identity management has two principal components: management “of” the identity and management “by” the identity¹. Management of the identity is the process of issuing and using digital identities and credentials (such as usernames and passwords) for authentication. Management by the identity combines the proven identity of the user with their authorisation, in order to grant access to resources. Authentication and authorisation are discussed later in this paper.

¹ Peter Wood, “*Implementing identity management security - an ethical hacker's view*”, **Network Security**, Volume 2005, Issue 9, September 2005, Pages 12-15.

MODELS AND TECHNIQUES

Identity Management Models

Identity of an entity has its own life cycle. For example, an employee's login account for accessing the company network would be created, maintained, synchronised and deleted across multiple systems or platforms. The employee's login credentials, with proper access rights, would be granted by a process called user provisioning. This account would be maintained and updated whenever new privileges are assigned to this employee, perhaps due to internal transfer, promotion, demotion, and so on. The employee's data or passwords would be synchronised among different IT systems and platforms. Finally, his/her login credentials can be deleted across all systems due to, say termination of employment or retirement. This removal of access rights is a process called user de-provisioning.

There are three common identity management models²:

Isolated identity management

This model requires that each user possess an identifier for access to each isolated service. This system is used a lot in online services and resources, because it is relatively simple for service providers to manage, but it is rapidly becoming unmanageable for users. The exponential growth in online services has led to users being overloaded with identifiers and credentials (different logins and passwords) that they need to remember and manage. For this reason, new identity management models are being proposed and implemented.

² <http://sky.fit.qut.edu.au/~josang/papers/JP2005-AusCERT.pdf>

Federated identity management

Federated identity management simplifies the account management problem. A set of agreements and standards are defined among a group of service providers who recognise user identifiers from one another. A customer of one particular service provider could access all services provided by another service provider in the group with only a single identifier. For such standardised methods of information exchange within the group to work, implementation of a common technology standard such as OASIS (Organisation for the Advancement of Structured Information Standards) SAML (Security Assertion Markup Language)³, the open source initiative, Shibboleth⁴, and so on is required.

Centralised identity management

In this model, the same identifier and credential are used by each service provider. This could for example be implemented by having a PKI, where a Certificate Authority (CA) issues certificates to users. Each user can then use the same certificate to access different services, and all providers authenticate the client through the same certificate before granting access to their services. Another example could be the Single sign-on (SSO) model, which requires a user to login once and be authenticated automatically by all other service providers. The Kerberos Authentication Server and Microsoft .Net Passport are examples of SSO implementation. A drawback of this approach is that should one of the trusted identity providers fail (e.g. under a DoS attack), the normal services of all service providers may be affected.

Authentication and Authorisation

³ http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

Authentication techniques make use of one or more of the following factors:

1. something you know (e.g. password),
2. something you have (e.g. a smart card),
3. something you are (e.g. fingerprint)

If two of these factors are needed for successful authentication, it is termed a “two-factor authentication”. Two-factor authentication is generally believed to be more secure, and therefore many high-risk systems such as Internet banking are now implementing schemes like this.

Authorisation is a process that determines whether an entity is allowed access to a given asset or resource. Common access control models are⁵:

1. Discretionary Access Control (DAC): in this mechanism, users own the objects under their control, and the granting and revoking of access control privileges are left to the discretion of individual users.
2. Mandatory Access Control (MAC): it is a means of restricting access to objects based on the sensitivity of the information contained in the objects, along with formal authorisation of subjects to access information of such sensitivity.
3. Role-based access control (RBAC): it is an authorisation mechanism in which access decisions are based on the roles that individual users have as part of an organisation.

When assigning access rights to an entity, the principles of least privilege and separation of duties are strongly recommended. The principle of least privilege recommends that the

⁴ <http://shibboleth.internet2.edu/>

⁵ <http://csrc.nist.gov/rbac/NIST-ITL-RBAC-bulletin.html>

least amount of privileges necessary to perform one's task should be granted to an entity. The principle of segregation of duties suggests that critical functions are divided into steps among different individuals to prevent a single individual from subverting a critical process.

II. CHALLENGES OF IDENTITY MANAGEMENT

IDENTITY THEFT

The Internet now covers the whole world and a large part of the economy. One major challenge to e-Commerce on the Internet is that of authentication. On the Internet, we do not have a sure way of knowing who and what we are really connecting to. According to a survey by Gartner in 2007, the number of identity theft victims in the US has increased by more than 50 percent since 2003⁶.

Many information systems employ a username and password for authentication purposes. Early Internet banking applications have been using this authentication mechanism. Increasing identity theft incidents such as phishing have prompted institutions to use more advanced authentication mechanisms to identify their customers. The Hong Kong Monetary Authority has also recommended using stronger customer authentication in e-Banking applications⁷. The Internet banking systems of certain banks in Hong Kong now require two-factor authentication for login. Bank customers need a one-time password generated from a security token given to them by the bank, in addition to their standard username / password information.

⁶ <http://www.gartner.com/it/page.jsp?id=501912>

⁷ <http://www.info.gov.hk/hkma/eng/bank/spma/attach/TM-E-1.pdf>

IDENTITY MANAGEMENT ADOPTION AND BENEFITS

Advances in identity management technology help enhance overall identity protection. Instead of simply relying on traditional password-based technology, two-factor authentication using biometric technology has grown as the price of biometric hardware and software has dropped. Some common characteristics that can be used for biometric identification include: fingerprints, hand geometry, retina scans, iris scans, face recognition and voice analysis.

While biometric authentication has its advantages, it also has limitations and drawbacks. Biometric identification systems might not be 100% reliable. Sometimes, a legitimate user finds they need to try more than once before he / she can be authenticated. As a pre-requisite to using a biometric identification system, a customer might need to 'register' his / her biometric features in the system, and this raises concerns about personal privacy.

Identity management in the public domain also requires stronger authentication. The Hong Kong Government has been issuing smart ID cards since 23 June 2003, and this provides a means for Hong Kong residents to access to a variety of government electronic services in a safe and secure manner⁸. Another example would be the US initiative for an electronic passport, which could provide automatic identity verification and greater border protection and security⁹. Biometric information such as face recognition, fingerprints or iris scans would be stored in the electronic passport.

⁸ <http://www.smartid.gov.hk/en/index.html>

⁹ http://travel.state.gov/passport/eppt/eppt_2788.html

Benefits of Identity Management

Apart from improvements in security, a well-implemented identity management system brings at least two business benefits to an organisation: cost reduction and improved service levels.

With an enterprise-wide identity management system in place, an organisation does not need to dedicate human resources to handling user ID related issues for each individual application. As a result, fewer people are needed for ID administration activities, which could in turn reduce IT operation costs. In addition, fewer calls to the help desk regarding user ID problems would contribute to more cost savings.

A common user complaint in the enterprise environment is the slow response when dealing with user ID resets, or other ID management functions. With the help of an automatic identity management system, response times for requests relating to user IDs would be improved, resulting in an improvement to IT service levels and better user ID management activities.

III. CONCLUSION

Passwords are still the most common authentication method. To reduce the possibility of passwords being compromised using brute-force attacks, consecutive unsuccessful log-in trials should be controlled. This can be accomplished by disabling an account after a limited number of unsuccessful log-ins. Alternatively, a mechanism of increasing the time delay between each consecutive login attempt could be considered as a way of preventing password guessing activities.

In a SSO, a user essentially only needs to remember one credential, so an attacker who can compromise that credential could break in to all the systems authorised by that user. Therefore, extra security measures are required in order to protect key credentials when implementing any SSO. A strong password policy and frequent password changes should be enforced to deter password attacks. Additional authentication methods, such as biometrics or two-factor authentication, could also be considered to strengthen the authentication process. Functions requiring another level of authorisation should be implemented using re-authentication. In addition, idle logged-on sessions should be timed-out after a set period to prevent attackers from stealing idle session information.

Individual accountability should also be established to hold each employee responsible for his or her actions. Within information systems, accountability can be accomplished by identifying and authenticating users of the system with a user identity (user-ID). This user-ID should uniquely identify a single individual, such that subsequent tracing of the user's activities on the system is possible should an incident occur or if a violation of the IT security policy is detected. Shared or group user-IDs should be prohibited unless it is unavoidable due to specific business needs.