Computing, Information Systems, Development Informatics & Allied Research
ISBN 978-2257-44-7(Print) ISSN 2167-1710 (online)
Vol.1 No.1 2010

A Proposed Cryptography-Based Identity Management Scheme for Enhancing Enterprise Information Systems Security

Adebimpe, L.A
Dept of Computer Science
Emmanuel Alayande College of Education, Oyo, Nigeria
dradebimpela@yahoo.com

Longe, O.B (PhD)
Fulbright Fellow
International Centre for Information Technology & Development
Southern University System
Baton Rouge, Louisiana, USA.
longeolumide@fulbrightmail.org

Abstract.

Enterprises are faced with the challenges of managing users' identity across multiple systems and applications. User identity usually includes personal information such as names, contact information, and demographic data; legal information which is the information about legal relationship between the enterprise and the user; and login credentials to managed systems for identification and authentication such as login ID and password, PKI certificate, tokens, biometrics, and so on. As a result of these challenges, enterprises contend with problems of data inconsistency, repetition of access to multiple systems, security exposure, unreliability of data, complexity in systems usage, and difficulty in managing large data. These problems are compounded as enterprises deploy more IT infrastructures (systems and applications) and have more users (employees, customers, partners, contractors, vendors, and so on).Our research is aimed at addressing these challenges by building on existing identity management technologies through the creation of a hybrid technology using Identity Management and Cryptographic techniques. We present the research direction in this paper.

Keywords: Enterprises, Identity Management, Identity Management Technology, Cryptography

1. INTRODUCTION

Identity management is the collection of business process and technology used to manage data on IT systems and applications about users. Managed data includes user objects, identity attributes, security entitlements and authentication factors.[1] The area of identity management also covers anonymising techniques and user profile storage.[2] Identity management is a source of worry for enterprises. Modern enterprises run a complex combination of I.T infrastructure, which includes: Network operating systems; Application servers running web servers, databases and similar software; Mainframe and midrange servers; E-mail and other collaboration software; User directories publishing lists of users and other network objects; Human resources, payroll and contractor management systems; Customer relationship management (CRM) and enterprise resource planning (ERP) applications; and Electronic commerce applications.

Several kinds of users access these systems including Employees, Contractors, Partners, Vendors, and Customers. Every system and application tracks its own users, how they sign in and their privileges. Therefore, identity data such as Personal information, Legal information, and Login credentials to managed systems should be effectively managed by these systems. The diversity of these systems, each with their own security management user interface, administrators and change request processes creates complexity. This complexity impacts the IT operation, e.g. the same human user must be managed by different IT staff on different parts of the infrastructure. The complexity also impacts users, e.g. it can take a long time to make required changes and users are forced to memorize multiple login IDs, passwords and application sign-on processes. This complexity leads to high IT cost, lower user productivity and security exposures.

The remaining part of the paper is organized as follows. In the next section we review related work. This is followed by a section on research methodology. Next is the analysis of research data. We present the discussion of findings and conclude in the last section

2. RELATED WORKS

Identity management (ID management) is a broad administrative area that deals with identifying individuals in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity. [3] Identity management describes the management of individual identities, their authentication, authorization, and privileges/permissions within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks. [4] Identity management refers to the process of employing emerging technologies to manage information about the identity of users and control access to company resources. [5]

It is a term related to how humans are authenticated (identified) and authorized across computer networks. It covers issues such as how users are given an identity, the protection of that identity, and the technologies supporting that protection (e.g., network protocols, digital certificates, passwords, etc.).[4] The driver licensing system is a simple example of identity management: drivers are identified by their license numbers and user specifications (such as "can not drive after dark") are linked to the identifying number. In an IT network, identity management software is used to automate administrative tasks, such as resetting user passwords.

Enabling users to reset their own passwords can save significant money and resources, since a large percentage of help desk calls are password-related. Password synchronization (p-synch) enables a user to access resources across systems with a single password; a more advanced version called single sign on enables synchronization across applications as well as systems. In an enterprise setting, identity management is used to increase security and productivity, while decreasing cost and redundant effort. Standards such as Extensible Name Service (XNS) are being developed to enable identity management both within the enterprise and beyond. [3]
The goal of identity management is to improve productivity and security while lowering costs associated with managing users and their identities, attributes, and credentials. [5] A key component of security plans is well-managed access to services that protect online resources and user privacy while enabling ease of use. Centralizing the management of user identity and related information not only reduces the staff required to manage appropriate access and monitoring, but also allows better service through automatic granting (or revoking) of services based on institutional roles. [6] Identity management system acts as the backbone for access control and security, and if it were to be compromised then the security of the entire company would also be compromised.
Therefore, it must encrypt stored confidential information such as social security numbers and passwords. It must also encrypt confidential information during transmission between components of the identity management infrastructure, which includes the network transmissions during synchronization, replication, and authentication. [5] Respondents to 2003 EDUCAUSE survey ranked security and identity management as critical issues not only because of their strategic importance but also because of the high staff requirements in both the management and technical areas. [6] As contained in computerweekly site [7], Identity and access management (IAM) helps to make sure that IT users are who they say they are, and to ensure that authorisation policies are upheld. A growing range of tools are available, from two-factor authentication, to security tokens and biometrics. We analyse the trends to help you choose the identify and access management products that are right for your needs.
Though the technology brings convenience, it also creates a dilemma. For instance Lapses in information security are a result of inefficiencies in current identity management processes. Due to the difficulty in managing user identities, the IT staff usually does not have enough time to correctly manage identities.

For example, users can be granted too much access because it is the easy thing to do. Because the IT staff does not have time to interpret how security policies affect each user, users can be granted access rights in violation of company security policies. Because the priority of the IT staff normally lies with new and existing, terminated users can easily be ignored. Consequently, departing employees find that they can still access company resources through their old accounts, other orphaned accounts, or undocumented access points. [5].

Significant challenges exist for an identity management.[5] Taylor, Lips and Organ (as cited in Wikipedia)[4] provided a glimpse into the issues in identity management, these include privacy issues or risk related to the stealing of identity (identity theft). Christopher Staite [2] wrote a thesis on “Portable Secure Identity Management”.

This paper focused on developing an identity maintenance and distribution system, and the storage of profile data on a centrally accessible, yet distributed system. [2] Also, Jason Crampton Hoon, Wei Lim Kenneth, and G.

Paterson [8], in their paper titled "What Can Identity-Based Cryptography Offer to Web Services?", focused on applying identity-based cryptography (IBC) to web services.

The key idea is to generate and use public keys based on publicly available information which can be used to uniquely identify users. [8]. Birgit Pfitzmann and Michael Waidner [9] published a paper titled "Federated Identity-Management Protocols–Where User Authentication Protocols May Go", and this paper suggested and discussed Federated identity management as providing a simple user management in an increasingly dynamic world. The paper also discussed the functionalities of Federated identity management protocols. [9] A World Wide Web Consortium position paper, Requirements for a Global Identity Management Service, cited on unified communications site[3] maintains that establishing global identity management is crucial for the development of the Web and Web services. The W3C position paper stipulates, among other things, that such a system that must be universally portable and interoperable; that it must support unlimited identity-related attributes; that it must provide adequate mechanisms for privacy and accountability; and that it must be overseen by an independent governing authority.

3. STATEMENT OF THE PROBLEM

The major challenges faced by enterprises are managing user identities and entitlements across multiple systems and applications. These challenges are evident because enterprises run a complex collection of IT infrastructures such as Application Servers, Network Operating Systems, Mainframe and midrange servers, email software, user directories, human resources and payroll management systems, e-commerce applications, and so on. In addition, many kinds of users access these systems whose identity data must be effectively tracked and managed. Therefore problems may arise as a result of managing user identities and entitlements across these multiple systems and applications.

Such problems are high IT cost, data inconsistency, usability problem (because users access multiple systems, they may be presented with multiple login IDs, multiple passwords and multiple sign-on screens), low user productivity, redundant administration, and security exposures.

4. RESEARCH JUSTIFICATION

In order to eradicate these challenges of effectively managing of identity data across multiple systems, Enterprise Identity management technologies simplify the administration of this distributed, overlapping and sometimes contradictory data about users. In other words, as enterprises deploy an ever wider array of IT infrastructure, managing that infrastructure and in particular managing users, their identity profiles and their security privileges on those systems becomes easy with Enterprise Identity management. Thus, this research work aims to resolve the challenge of managing that infrastructure and in particular managing users, their identity profiles and their security privileges on those systems and applications by developing network directories (which are network services that manage information about users, the enterprise and IT assets such as servers and peripherals) using Lightweight Directory Access Protocol (LDAP) and Federation (which enables applications in different domains to share information about users).

In order to further enhance the security of users' identity data, such data are converted into cyphertext (through encryption) during storage and then decrypted by authenticated and authorized users during retrieval using a key. Therefore, the successful completion of this research work will elicit a hybrid identity management technology called LFC (LDAP, Federation, and Cryptography) that will provide a secure, consistent, efficient, usable, reliable, and scalable identity management framework for enterprises to eradicate the challenges of managing user identities and entitlements across multiple systems and applications, as well as ensuring trusted information sharing mechanism among enterprises.

5. RESEARCH DIRECTION

The objectives of this research project are:

1. To develop a network directory to manage information about users, the enterprise and IT assets using lightweight directory access protocol (LDAP).

2. To apply cryptography in securing identity data during storage and retrieval.
3. To develop an authentication and authorization model that will allow applications in different domains (different enterprises) to access and share identity data (information about users). In this model, an application in one enterprise will be authenticated only once and then granted access to information owned by several enterprises.

6. METHODOLOGY

In implementing the network directory, Lightweight Directory Access Protocol (LDAP), which is an identity management technology, will be used. LDAP also has an associated schema which can be used to build a data structure for the directory. Blowfish encryption algorithm will be used in encrypting and decrypting identity data. To construct authentication and authorization model, Federation will be used. Federation is an identity management technology that makes identities portable across domains so that they can be efficiently shared with and leveraged by trusted partners. It provides the mechanism whereby an enterprise can accept that external users have already been authenticated by a trusted partner and can grant them access — without having to be responsible for managing all their identity information. Within this framework, users enjoy seamless, secure access to partners' services via a single sign-on (SSO) to multiple applications. [10]

7. SCOPE

This research work focuses on integrating Lightweight Directory Access Protocol (LDAP) and Federation identity management technologies with Cryptography to create a hybrid technology that will provide a high-level security of identity data and highly effective management of users' identity data across multiple systems and applications within an enterprise, and also to ensure reliable sharing of users' information among enterprises.

8. EXPECTED RESULTS

A lot of research work has been carried out in the area of enterprise identity management by developing network directories using LDAP, as well as using Federation to automate the process of sharing identity information across traditional organizational boundaries. Many research projects had been executed in the area of Identity-based cryptography. This research work is expected to contribute to knowledge by combining LDAP, Federation, and Cryptography (LFC) such that cryptography will be applied to encrypt identity information that is sent to the network directory through LDAP, as well as linking several enterprises together for the purpose of sharing identity information through Federation, while pulling data from the network directory. Thus, LDAP and Federation will be made to operate synchronously to provide a high-level identity management framework.

REFERENCES

[1] Hitachi ID Systems, Inc. (2010) Defining Enterprise Identity Management System. Retrieved July 11, 2010 from http://www.p-synch.com/docs/defining-enterprise-identity-management.html

[2] Staite, C. (2009) Portable Secure Identity Management. Retrieved July 11, 2010 from http://www.cs.bham.ac.uk/~cxs548/papers/ RS MG3.pdf

[3] Identity Management (ID Management). (n.d.). Retrieved from http://searchunifiedcommunications.techtarget.com/definition/identity-management

[4] Identity Management. Retrieved July 11, 2010 from http://en.wikipedia.org/wiki/Identity_management.
[5] Spencer C. Lee (2003). An Introduction to Identity Management. SANS Security Essentials Certification
[6] Bruhn M., Gettes M., & West A. (2003). Identity and Access Management and Security in Higher Education. *EDUCAUSE QUARTERLY, 4*, 12-16.

[7] Identity and Access Management Products News, Help and Research. July 11, 2010 from http://www.computerweekly.com/resources/Identity-and-access-management-products.

[8] Crampton, J., Lim, H. W., and Paterson, K. G. (2007). What Can Identity-Based Cryptography Offer to Web Services?. UK: Information Security Group, Royal Holloway, University of London, Egham, Surrey. Retrieved July 11, 2010 from http://citeseerx.ist.psu.edu/viewdoc/download

[9] Pfitzmann, B. and Waidner, M (2004) Federated Identity-Management Protocols - Where User Authentication Protocols May Go. Retrieved July 11, 2010 from http://citeseerx.ist.psu.edu/viewdoc/download

[10] Sun Microsystems (2001). Identity Federation: Transcending the Boundaries of Business for Secure Collaboration. Retrieved July 11, 2010 from http://www.sun.com/software/products/identity/wp_id_federation_secure_collab.pdf