A STUDY OF IDENTITY MANAGEMENT FEATURES IN ERP SYSTEMS

Kuo Lane Chen, University of Southern Mississippi, kuo.chen@usm.edu
Huei Lee, Eastern Michigan University, huei.lee@emich.edu
Chen-chieh Shing, Radford University, cshing@radford.edu
Marn-ling Shing, Taipei Municipal University of Education, shing@tmue.edu.tw

ABSTRACT

The purpose of this paper is to discuss identity management in two specific ERP systems: SAP R/3 and Microsoft Dynamics GP. The relationship between business process management and identity management is also discussed.

Keywords: Security Management, Business Process Reporting, ERP, Identity Management

INTRODUCTION

In 2007, the retail giant TJX’s computer systems were compromised and customer data was hacked [8]. According to Wikipedia [10], “The hackers accessed a system that stores data on credit card, debit card, check, and merchandise return transactions.” Also based on Lavoie [2], “The intrusion was kept confidential as requested by law enforcement. TJX said that it is working with defense contractors General Dynamics, IBM and Deloitte to upgrade computer security.” The possible cause of the breach was a non-secure wireless network in one of the stores [6]. TJX eventually paid more than 45 millions to the credit card company to settle a lawsuit [5]. This incident explains the important of identity management to an enterprise.

What is identity management? Identity management is a “centralized policy-based management of all information required for access to enterprise systems by people, host, programs, or other resources.” [5]. Identity management can be also defined as “a broad administrative area that deals with identifying individuals in a system (such as a country, a network or an organization) and controlling the access to the resources in that system by placing restrictions on the established identities.”[10] Examples of identity management techniques include password control, authentication, and certifications. Benefits of excellent identity management are not only preventing the unauthorized intrusion but also reducing sign-on to an complex enterprise system [5].

Major corporations today have adopted the enterprise resource planning systems (ERP). These ERP systems include all the business functions such as sales, distribution, purchasing, production planning which can be used by all the branches. ERP systems enable the enterprises to standardize different subsystems and database entries. On the other hand, security control becomes particularly important. Major ERP Systems provide a component called identity management. For example, the identity management component in SAP R/3 is NetWeaver Identity Management. This paper attempts to examine the identity management in two ERP systems: 1) SAP R/3 and 2) Microsoft Dynamics GP. SAP R/3 is an ERP system for most Fortune 500 companies while Microsoft Dynamics GP is an ERP system for small and medium businesses. Because identity management is a relatively new area in the information literature, this paper is one of a few attempts to conduct an explore study and examine the identity management features in current ERP systems.

BUSINESS PROCESS MANAGEMENT AND IDENTITY MANAGEMENT

ERP systems are closely related to another term, business process management (BPM). Today, business process management is done through ERP systems. An example of business process for sales and distribution in SAP R/3 are inquiry, quotation, sales orders, picking, packing, post goods issue, shipping, billing, invoice, and payment process (See Figure 1). These processes flow through different departments in a large corporation. Sometimes, the process flow accidentally stops in the middle. For example, a customer purchased an item several months ago but he complains that he never receive the item. A trace through the ERP system may find out this item is still sitting in the warehouse because of a mistake.
A Study of Identity Management Features in ERP Systems

Volume XI, No. 1, 2010

645

On the other hand, for the security purpose, many company policies do not allow one person to completely control the whole business process. Figure 2 shows different roles and authorization should control different steps in a business process.

Different business events further make the identity management more complex. For example, an employee will go through the following process: 1) Becoming an employee to the company, 2) Changing to a new department, 3) Promoting to a new position, and 4) Leaving the company [1]. When an employer changes his job role and his department, his access right and authorization should be changed at the same time.

A recent trend is that ERP systems will move to the direction of cloud computing. However, one of the major concerns in cloud computing is security and identity management. Some businesses do not want to put financial statements online because of security concerns.

Due to the importance of identity management in ERP systems, we have the following research questions: 1) What are the major differences in identity management features between large ERP systems and small ERP systems? 2) How does the identity management work in an ERP system?

In the next two sessions, we examine SAP R/3 and Microsoft Dynamics GP. SAP R/3 is the most popular ERP systems in the US and the world. An SAP R/3 system costs from several millions to half-millions [4]. The expensive price tag prohibits many small companies to use SAP. Therefore, we also examine one of the most popular ERP systems for small companies: Microsoft Dynamics GP.

IDENTITY MANAGEMENT IN SAP R/3

The above discussion about the business process and identity management actually describes the fundamental structure in SAP R/3. SAP has a document flow function to show whether a process is finished [4]. The Figure 3 shows a screenshot on document flow for a sales order process.

Furthermore, the identity management of SAP R/3 is handled by SAP NetWeaver. SAP NetWeaver Identity Management comes from MaXware AS. NetWeaver Identity Management has four major components: 1) Data synchronization engine, 2) identity center, and 3) virtual directory server. Data synchronization engine is used for any low-level operation on the applications and repositories [7]. The identity center provides identity management, password management, and provisioning function. It uses a relational database for logging and other information. Virtual directory can be used to control identity data for different groups of users.

One of the solutions is to create a central repository containing the identity information in identity store. The information in the identity store can provide to different users: employees, partners, and customers [7].
IDENTITY MANAGEMENT IN MICROSOFT DYNAMICS GP

Microsoft has purchased more than four small ERP packages and transferred them to a series of ERP systems: Dynamics GP, Dynamics CRM, Dynamics AX, and Dynamics NAV. In this paper, we focus on Dynamics GP. Since they are Microsoft products, they use the Microsoft operating systems and databases. The access control and identity management in the Microsoft Dynamics GP can be classified into three layers:

1) Windows Authentication Systems
2) SQL Server 2005/2008
3) Dynamics GP

It is important to understand all the three layers so a user will not have problems in implementing identity management in Dynamics GP.

Layer One: Windows Authentications

Windows 2003/2008 provides two major security models: 1) Domain mode and 2) Workgroup mode. Domain mode is characterized by central control and activity directory. The identity management can be done in the activity directory in a central server called domain controller. Workgroup mode is characterized by decentralized control. Each computer handles its own security policy. In workgroup mode, each computer can set up the security through local security policy. Finally, both Windows client and server operating systems provide firewall feature and Virtual Private Network (VPN) function. A user must make sure that the firewall and VPN setting will not block the user access.

Layer Two: SQL Server 2005/2008

Dynamics GP 10.0 uses Microsoft SQL Server 2005/2008 as its database. Therefore, the second layer of identity management for Dynamics GP is SQL Server. The current version of SQL Server is 2008. Some of the security control features in SQL Server 2005/2008 are:

1. The default for the administrator account is sa (system administrator)
3. One of important jobs in implementing Microsoft Dynamics GP is that the installer has to specify SQL Server name and authentication methods.

Layer Three: Identity Management in Dynamics GP

The third layer of the identity management in the Dynamics GP is itself. Some of detailed information in Dynamics GP cannot be controlled by Windows Server Operating System and SQL Server must be defined in Dynamics GP. The identity management implementation process starts from the initial installation process of the Dynamics GP. The installer need to specify password for the following uses: 1) administrator, 2) user 1, and 3) user 2. After the installation process is finished, the system administration can add additional user anytime.

As shown in Figure 4, identity management features belongs to System Administration Function (Microsoft, 2009). More specifically, the identity management features include 1) Security Task, 3) User Class (See Figure 6), 3) Security Role, 4) Field-Level Security, and 5) Audit Tracking.

**Security Tasks**

As shown in Figure 5, examples of security tasks include in Dynamics GP: 1) Set up bank reconciliation, 2) Set up cash flow management, and 3) Fixed assets maintenance and utilities. Security tasks should be assigned to different security roles.
A Study of Identity Management Features in ERP Systems

Security Role

As shown in Figure 7, examples of security roles include purchasing manager, purchasing agent, returns management administrator, and returns management agent. Each security role has a role ID.

Audit Tracking

As shown in Figure 8, the audit tracing features in the Dynamics GP allow the system administrator to monitor a log for any users: 1) failed attempts to log in, 2) successful attempts to log in, and 3) successful attempts to log out [3]. An audit table will provide the details of record changing.

Figure 5. Security Task in Microsoft Dynamics GP

Figure 6. User Class in Microsoft Dynamics GP

Figure 7. Security Roles in Microsoft Dynamics GP

Figure 8. Activity Tracking Features in Microsoft Dynamics GP
CONCLUSIONS

This paper attempts to conduct an explore study and examine the identity management component in the ERP systems. Two ERP systems, SAP and Microsoft Dynamics GP, are examined in this paper. Both have quite complex features in identity management. It seems that there is not much difference between small and big ERP systems. Both use an activity directory for central control. However, are they easy to use? Future study will focus on whether the system administrators and users are aware of these features and whether these features are user friendliness.

REFERENCES