Information Systems Security, 16:152–163, 2007
Copyright © Taylor & Francis Group, LLC
ISSN: 1065-898X print/1934-869X online
DOI: 10.1080/10658980701401959

Security for Enterprise Resource Planning Systems

Wei She and
Bhavani Thuraisingham
University of Texas at Dallas,
Richardson, TX, USA

ABSTRACT Enterprise Resource Planning (ERP) is the technology that provides the unified business function to the organization by integrating the core processes. ERP now is experiencing the transformation that will make it highly integrated, more intelligent, more collaborative, web-enabled, and even wireless. The ERP system is becoming the system with high vulnerability and high confidentiality in which the security is critical for it to operate. Many ERP vendors have already integrated their security solution, which may work well internally; while in an open environment, we need new technical approaches to secure an ERP system. This paper introduces ERP technology from its evolution through architecture to its products. The security solution in ERP as well as directions for secure ERP systems is presented.

KEYWORDS authorization, Enterprise Resource Planning, exchange infrastructure, policies, RBAC, Web services

INTRODUCTION

Enterprise Resource Planning, a business integration approach, has been widely deployed in various kinds of organizations since it was first defined by the Gartner Group in 1990 as the next generation of Manufacturing Business System and Manufacturing Resource Planning software. Today, ERP is considered to be "the price of entry for running a business" (Kumar and van Hillegersberg, 2000).

An ERP system is an integrated, configurable, and tailorable information system which plans and manages all the resources and their use in the enterprise, and streamlines and incorporates the business processes within and across the functional or technical boundaries in the organization. With ERP, an enterprise can automate its fundamental business applications, reduce the complexity and the cost of the collaboration, force the enterprise itself to take part in the Business Process Reengineering (BPR) to optimize its operations, and finally result in a successful business.

The objective of this paper is to give an overview of the state of the art in ERP technology and the security issues for an ERP system. In particular,

Address correspondence to the authors at wxs061000@utdallas.edu or bhavani.thuraisingham@utdallas.edu

we discuss the evolution of ERP, its key components, the status of vendor products, and what has been done with respect to security. Our research as well as plans for secure ERP systems will also be discussed.

The organization of this paper is as follows. The history and evolution of ERP systems will be given in the next section. ERP technologies and framework including the communication platform such as EDI, ALE, and Exchange Infrastructure are presented in the "ERP Technology" section. This section also includes a discussion of the ERP architecture, some aspects of SAP, and the emerging web services for ERP. Major ERP vendors and their products are discussed in the "Vendors and Products" section. Security issues for ERP systems are discussed in the following section, "Security in ERP." In particular, the overview of the ERP security using a layered approach, as well as the RBAC model for ERP is discussed. We will compare these security features with the authorization function in SAP R/3 system and the Baan security solution. Some of our researches in ERP as well as trends are discussed.

HISTORY OF ERP SYSTEMS AND APPLICATIONS

The history of ERP traces back to the 1960s, when most organizations were developing the centralized computing systems using Inventory Control Packages (IC) in order to automatically manage a company's inventories. These legacy systems are mostly based on programming languages such as COBOL and FORTRAN. In the 1970s, Material Requirements Planning (MRP) systems were developed to manage the requirements and plan production. Later, Manufacturing Resources Planning (MRP II) system emerged in the 1980s, aiming to optimize the manufacturing process. The concept of ERP was introduced in the early 1990s as an enterprise-wide and across-functional integration of the core organizational business processes, including manufacturing, distribution, accounting, financial, human resource management, project management, inventory management, service and maintenance, and so on. From the point of views of some researchers, the ERP technology after 2000 is considered as "Extended ERP" (Rashid, Hossain, and Patrick, 2002) because e-business solutions such as Customer Relationship Management (CRM) and Supply Chain Management (SCM) are included into the core modules of original ERP systems.

ERP has a wide range of applications in both industrial and non-industrial areas such as aerospace and defense, banking, consumer products, construction, healthcare, education and research, insurance, raw and processed materials, logistics, transportation, wholesale, public sectors, telecommunication, and so on. In the early years after ERP emerged, deploying and maintaining an ERP system was expensive and took a relatively long time to recover costs. Since then, the implementation and maintenance cost of ERP system was greatly reduced due to the retrofit of technical infrastructure. Nowadays, many light-weight ERP applications are developed for small and medium companies.

Various commercial products, including SAP, Oracle, and Baan, are now available in the marketplace. Furthermore, Web services and service-oriented architectures are the major underlying technologies for emerging ERP systems.

ERP TECHNOLOGY

Overview

ERP systems have evolved extensively over the years. Initially, such systems were used for simple functions such as accounting and human resources planning. With the advent of Web technologies, companies such as Oracle, SAP, and Baan began developing a suite of applications for ERP systems. The emerging technologies such as Web service and eXtensible Markup Language (XML) have had a major impact on ERP systems.

In this section, we discuss the various components of ERP systems. We start with a discussion of its architecture and various business components in the next section including financial management, human resource management, production lifecycle management, customer relationship management, and manufacturing management. In the "EDI, XML, and Information Exchange" section, we discuss exchange infrastructure, the cornerstone of ERP systems. In this section, we also discuss the two technologies for exchanging electronic documents among different entities: EDI and XML. Finally, emerging Web services and their relationship to ERP systems are discussed in the final section, "Web Services."

ERP Architecture

There are many disadvantages to MRP II and MRP technologies. In an enterprise, some systems may be developed by the enterprise itself, while others may be developed by different vendors using different databases, languages, and technologies. Systems differ from each other, which makes it difficult to upgrade the organization's businesses, strategy, and information technologies effectively. With the communication infrastructure and ERP functionalities encapsulated in components, an ERP system can easily meet these requirements. A typical ERP system should at least have the following features:

- Componentized—different business functionalities are designed as different components.
- Integrated—components are integrated and seamless data flow between components allows them to collaborate as a one function.
- Flexible—system is expandable and compatible with the old systems, the change to the business processes and strategies are easy to fulfill (Glass, 1998).
- Tailorable—system should be easily configured according to the enterprise's needs.
- Real-time—the components work in real time, online, and batch processing modes should be available.
- Profitable—system must have the potential to reduce the cost or increase profit, since these are a company's basic requirements and motivations.
- Secured—security schema has to be enforced to protect various enterprise resources regardless whether it is appropriate or sufficient.

The business logic in ERP system employs client/server architecture to create a distributed computing environment. Generally, the three-tier architecture will be used, which contains three layers of logic:

1. Presentation Layer (Front): A unified Graphical User Interface (GUI) or browser that collects input, generates requests, and returns the results back to the user.
2. Application Layer (Middle): Application programs that collect the requests from the Presentation layer and process the requests based on the business rules, functions, or logics.
3. Database Layer (Back): DBMS that manages the operational and business data throughout the whole enterprise and the user access to this information. This layer may also include the operating system and the related hardware (Sprott, 2000), since they are necessary for the system but transparent to users.

As the basis of the ERP system, an information exchange platform such as SAP NetWeaver will always be deployed before implementing ERP software. After consolidating the business logic and the technical platform, we will have the ERP system architecture as showed in Figure 1.

The components that different ERP vendors provide may vary, as they will always have some inclines due to the historical problems, yet the core functionalities are nearly the same. These functionalities include (Bakry and Bakry, 2005; Shehab et al., 2004):

- Financial Management, which may includes the functionalities such as collection and payment management, payables and receivables management, assets and properties management, cash management, loans, financial consolidation, general ledger, treasury management, and planning and budgeting.
- Human Resource Management, which may have the functionalities such as payroll management, self-service, learning management, benefits, recruitment, tutor, timer and labor management, and compensation management.

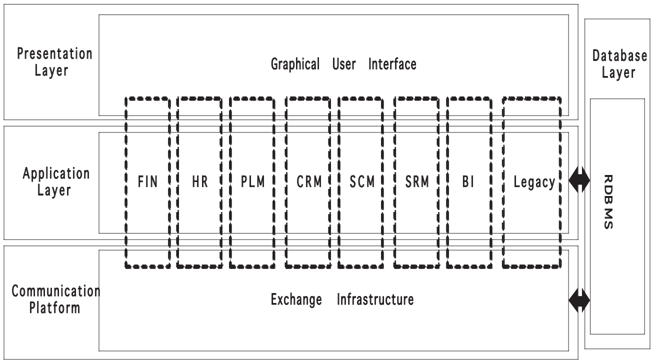

FIGURE 1 The Architecture of Enterprise Resource Planning

- Manufacturing Management, which will provide the functions such as discrete manufacturing, process manufacturing, flow manufacturing, manufacturing scheduling, and shop floor management.
- Sales, Distribution, and Logistics Management, which includes the functions as order capture, services, sales, sales incentive management, pricing, logistics, bulk stock management, inventory management, warehouse management, requirements management, and strategic account planning.
- Customer Relationship Management (CRM), which maintains the relationships between the organization and its customers and includes functionalities such as collecting, storing, and analyzing customer information.
- Product Lifecycle Management, which manages the entire lifecycle of a product from conception and design to manufacture, service, and disposal.
- Supplier Relationship Management (SRM), similar to CRM which deals with customers, SRM manages the supplier relationships by collecting, storing, and analyzing supplier information.
- Business Intelligence, whose concept has a wide range covering all the processes performing analysis and/or evaluation which either work at the strategy level, tactical level, or operational level by providing instruction for optimizing business performance. Demand management can be classified into this category.
- Supply Chain Management (SCM), which is another concept having some overlap with above components. An SCM can include the business processes such as CRM, SRM, manufacturing management, demand management, and production planning. The key point is that these business processes have to be connected across organizations in order for a business success of supply chain. These processes are inter-organizational, thus may be either included in or excluded from the scope of ERP. With the definition of extended ERP, we no longer consider ERP as internal within an organization.

The scope of the term “ERP” is a bit confusing when comparing it to the term “e-commerce.” Generally speaking, ERP is more concerned with the internal functionalities in an organization; on the other hand, e-commerce or e-business focuses on the business across companies. While under current global business strategy, companies are no longer competing with each other as individuals, coordination enables several companies to compete as a whole. SCM literature discusses much in this area, and people are considering a supply chain as the competition unit. With coordination, we cannot always assume that some components are working internally and some others are working externally. Thus, the boundary between ERP and e-commerce is blurred in many cases; and it is inappropriate and unnecessary to discuss the technical issues from the narrow concept of ERP (internal).

EDI, XML, and Information Exchange

Electronic Data Interchange (EDI), also called “paperless exchange” (Nagpal, de Bruyn and Lyfareff, 1999), is the technology that allows enterprises to exchange business information between separate computer systems, using a standard structured format (ANSI ASC X.12 in the late 1970s and EDIFACT in the 1980s) over a communication network. EDI technologies such as SAP’s exchange infrastructure (White Paper, SAP Exchange Infrastructure 2.0, 2002; White Paper, SAP R/3 Enterprise, 2002; White Paper, SAP Exchange Infrastructure 2.0 Technical Infrastructure, 2002) have been in place for many years as the footstone of all ERP technologies. Although those systems implementing EDI exchanging documents have become legacy systems today, the major contribution from EDI technology, the business semantics, is preserved by combining EDI and XML.

XML (W3C, 2006) is a flexible text format standard developed by the World Wide Web Consortium (W3C). It is a simplification of Standard Generalized Markup Language (SGML) for originally large-scale electronic publishing and later as the standard for exchanging various data over the Web. The major advantage of XML over other description languages (e.g., HTML) is its ability to represent the data format using Document Type Declaration (DTD) schema or XML schema (W3C, XML Schema Part 0, 2004; W3C, XML Schema Part 1, 2004; W3C, XML Schema Part 2, 2004). This is the reason XML is applied in many ERP applications developed in recent years. XML-based document exchange removes the obstacle faced by most small and medium organizations—high implementation and maintenance costs of exchanging infrastructure

(Iacovou, Benbasat, and Dexter, 1995). Frameworks such as xCBL (Common Business Library) and languages such as ebXML (OASIS, 2001; OASIS, 2006) were designed in recent years to support enterprise-wide applications by combining the business semantics of EDI technology and the flexible and innovative data model of XML. Furthermore, a new trend among organization management is towards knowledge-based management, which means that resources lying within an ERP system are now viewed as knowledge instead of information or data. This trend starts by distinguishing among three concepts: data, information, and knowledge. Data are simply raw numbers or facts, information is processed data, and knowledge is information processed in the mind of a person. Thus, knowledge may have more various representations that must be supported by the description languages. This is another reason exchanging infrastructure now becomes XML-based.

Web Services

Thuraisingham (2006) stated that we are now in the third wave of ERP systems. The first wave related to manufacturing applications; the second was specialized applications such as supply chain management; and the third was based on Web services.

The use of Web services eases integration and also reduces costs. Clients want to access information without having to go through ERP software. Therefore, with the use of Web services and the composition of Web services, clients as well as outsourcing vendors can access many of the ERP applications seamlessly. These applications include checking bank accounts, placing orders, and other services. Reduction in cost comes from the fact that clients can communicate with legacy ERP software through Web services and do not have to deal with the complexities of the software. Also ERP vendors are introducing the Web scenarios broker hub that will act as a broker between Web services and the ERP software. SAP offers this hub through mySAP and Oracle via its e-business suite.

VENDORS AND PRODUCTS

In this section, we provide an overview of the major ERP systems vendors. SAP is one of the most prominent vendors of ERP. Other vendors include PeopleSoft and Baan. However, PeopleSoft has been purchased by Oracle, and Oracle is emerging as a major ERP systems vendor. Furthermore, Oracle provides the server technologies that ERP applications could utilize, while SAP and Baan rely on various vendor products for server technologies. We will provide an overall discussion about the products provided by SAP, Baan and Oracle. Note that Baan has been purchased by SSA. Microsoft is also becoming a major player in ERP software.

SAP (Systems, Applications, and Products in Data Processing) was formed in 1972 by five former IBM employees in Germany. SAP focuses on the development of application software for real-time business processing, beginning with its first accounting software developed in 1973. Its first ERP product, SAP R/2, was developed in the late 1970s using a centralized database and dialog control system. In the 1990s, SAP R/3, which uses the three-tier architecture of database, application, and user interface, was unleashed on the market. R/3 was a breakthrough, making SAP the largest vendor in the ERP market by 1999. By 2005, there were around 100,000 installations worldwide, more than 1500 partners, over 25 industry-specific business solutions, and more than 30,000 customers in over 100 countries. SAP now owns 26% of CRM market share, 29% of ERP market share, and 19% of SCM market share by total software revenue. SAP NetWeaver unifies the integration technologies into a single platform, which lays the groundwork for the integration all systems SAP runs or non-SAP software. It is the basis of SAP ERP applications, partner solutions, and custom-built applications. SAP R/3 is the third generation set of highly integrated software that performs the core business functions within a company; while mySAP, which also includes R/3 component as an important building block, is intended to empower the collaboration between organizations. mySAP is a Web-based e-business suite.

Oracle, which was founded in the 1970s in the USA, is most famous for its well-known relational database Oracle and is the second-largest software company in the world. In 1987, Oracle offered its first ERP software—Oracle General Ledger. In the following years, Oracle developed other ERP software such as self-service applications, strategic procurement solution, financial consolidation engine, and flow manufacturing product. Oracle's ERP system is now known as Oracle E-business Suite, which has more than 50 different modules covering the following areas: finance, accounting, human resources, manufacturing, supply chain management, project, and front office. Oracle also has many other well-known products in other fields such as database, data warehousing, and workflow. After the acquisition of PeopleSoft and JD Edwards in 2004, Oracle gained approximately 22% of the ERP market share. PeopleSoft Enterprise is the business application suite that offers Web services integration with multivendor and homegrown applications; it is admittedly considered easier to configure and more flexible than its competitors. JD Edwards EnterpriseOne and JD Edwards World are both the business applications from J.D. Edwards Company, which has extensive experience supplying software for the IBM iSeries platform. JD Edwards World provides the Web-enabled applications for the management of plants, inventories, equipments, finances, and people.

Sage, founded in England in 1981, entered the ERP market and gained a solid market share using the strategy of acquiring small ERP vendors such as Tetra and Interact Commerce Inc. By 2005, Sage had revenue of $1.4 billion in the ERP market and claimed 6% market share as the third-largest ERP vendor. Sage Line 500 v6 is newest version of the Sage Line 500 product family, which is the Web-based integrated ERP solution covering core functionalities in a company. Sage 1000 is new, single business management software designed to offer the operations within mid-size organizations.

Microsoft, founded in 1975, is the biggest software company in the world with its famous Windows series products. Microsoft Business Solution Group (MBS) is the department that focuses on providing ERP solutions, such as Microsoft Dynamics (formerly Microsoft Business Solutions), which is the integrated business management solution that includes financials, customer relationship management, and supply chain management. By 2004, MBS had revenue of around $800 million, giving it a 4% ERP market share.

Others. In addition to the major vendors, there are several other ERP vendors that are emerging. In 2004, the biggest ERP vendors—SAP, Oracle, Sage, Microsoft, and SSA—accounted for around 70% of ERP market share by revenue. The other 30% was shared by other ERP vendors such as Geac, Intentia, Infor Global Solutions, and Lawson.

SECURITY IN ERP

Overview

Security is critical for ERP systems, as they are used in numerous industries including defense, intelligence, medical, and financial. First, we need to develop a security policy and a model for ERP systems. Many of the current systems focus on confidentiality aspects of security. In this section, we discuss the developments as well as current trends in security for ERP systems.

In the "Approaches to Security" section, we discuss what needs to be secured. In section "Current Solutions," we discuss current developments, including security, for SAP. In the "Next-Generation Models" section, we discuss some of the next-generation security models. In the concluding section "Directions on ERP Security," we provide an overview of trends, including a discussion of security policies and Web services security.

Approaches to Security

Security problems exist in every facet of an ERP system. These facets can be classified into three categories: network layer, presentation layer, and application layer, which includes business processes, internal interfaces, and database.

When a customer/partner communicates with an ERP system, or the business components located in different places interact with each other, the security problems in these cases are classified into the network security domain. ERP experts will not deal with these cases directly, instead this function will be provided by purchasing from other vendors who are experts at network security.

The presentation layer refers to the graphical user interface, browsers, and PCs. Since the transmission of GUI packets is impossible to restrict, ERP experts cannot secure the system by limiting user access to GUI. The better way to provide security may be to place a CITRIX server between the user and the ERP system.

The security in application layer invests large efforts of the ERP experts to offer an effective way to secure the business data and processes. The technicians will also choose to activate/deactivate the security functions provided by the database vendor according to the overall security solution. Van de Riet, Janssen, and Gruijter (1998) summarized some of the security aspects in an ERP system:

- Security policy and administrator: ERP experts have to provide such a way that explicit and well-defined security policies can be easily defined and maintained. The security policies will offer the rules for the access of subject to object, and these are the constraints put on the administrators when they are granting/denying permissions to the users.
- User authentication: to verify whether the user is the same person as he claims.
- Separation of duties: tasks must be classified such that certain tasks can only be performed by certain users or roles.
- Authorization: to verify whether the user has access to the relevant resources. Depending on the authorization rules, the user is granted access.
- Time restriction: the access is permissible only during certain time.
- Log and trace: the logging and tracing of relevant events has to be done with preventing the log files from breach.
- Database security.

Essentially we need end-to-end security for ERP systems. The next three sections discuss some of the current trends and directions for secure ERP.

Current Solutions

Role-Based Access Control

Many of the current systems are based on Role-Based Access Control (RBAC), although they may have different settings of either enhancements (Kern et al., 2002) or simplifications. This model (Figure 2) defines roles and grants certain access rights. According to Sandhu et al. (1996), an RBAC model consists of the following components:

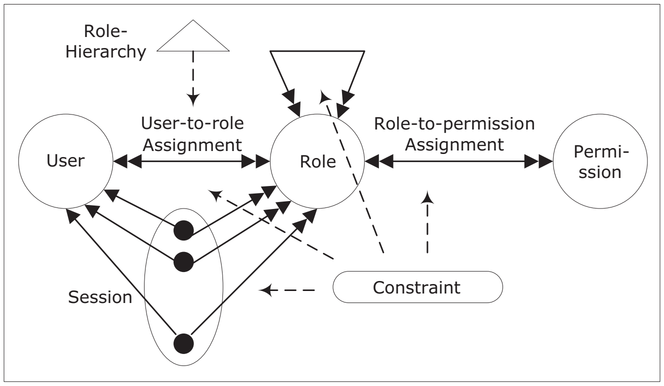

FIGURE 2 **The Model of Role-based Access Control [6]**

- Permissions: Permission is the access to one or more objects in the system. The permission has different meanings in different environment. If in a database system, the permission refers to the rights such as select, update, delete, or insert a record. If an accounting application, it may be the rights such as account creation/deletion, credit/debit, and transfer (Sandhu et al., 1996).
- Roles: A role is a named job function within the organization. A role may be hierarchical. For example, an engineer role is also an employee role.
- Users: A user is a person who may be assigned one or more roles.
- Constraints: In the system where there is only one single administrator, the constraints may be meaningless. If the administration is decentralized, meaning there are several administrators, the constraints will be used by the senior administrator to restrict the junior administrator's right to grant/deny the permissions.

Authorization in SAP R/3

Some of the concepts involved in the authorization in SAP R/3 system are listed below (White Paper, Authorization Made Easy, 2000; Goodman, 2004; Schaad, 2006):

- Authorization object, which represents the authorization concept and consists of some authorization fields.
- Authorization, which is an instance of one authorization object and defines the permitted value range of each authorization field of the authorization object.

- Authorization profile, which contains some authorizations which are assigned to the user by the administrator.
- Authorization check, which is used to protect the transactions or data you choose and is embedded in the program logic. When the authorization check is performed, the authorization profile will be used to compare the required values to run the specific transaction.
- User master record, which enables the users to log on to the R/3 system and grant limited access to the transactions and data.
- Profile generator is the component which helps the administrators create, generate, and assign authorization profiles using activity groups and user.

A profile generator may have the following components:

- Activity group is a collection of activities such as tasks, reports and transactions. An activity group usually represents a job in the enterprise. An activity group can have many users assigned to it, and a user can also be assigned to many activity groups. An activity group can be assigned to the following types of users: user ID, job, and position. Job represents the general classification of duties. Position represents a person's detailed individual assignment within an enterprise. The difference between job and position is that job is just the title which does not imply what projects you will do in the company, while position does so.
- Composite activity group is the collection of several activity groups.
- User assignment is the task that assigns one or more users/roles/positions to one or more activity groups or composite activity groups.

Another important concept in the authorization in R/3 is authorization administration, which means whether the creation, generation, or assignment of authorization is centralized or decentralized (one or more administrators).

Through these concepts, we may learn that the mechanism of R/3 authorization is actually an instance of Role-Based Access Control Model, except that it contains some elements specifically used in R/3 environment. Figure 3 provides a visual understanding of the model of authorization in R/3 system.

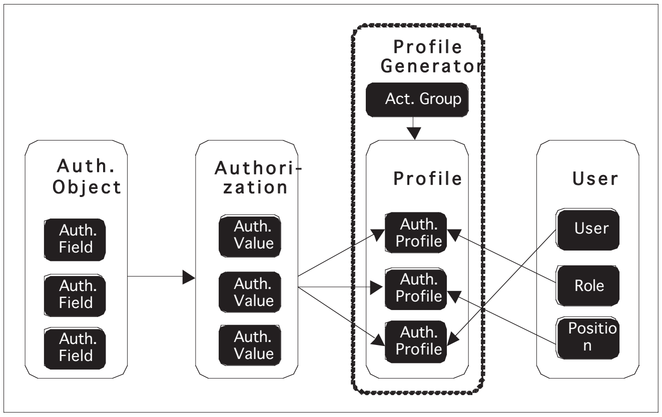

FIGURE 3 The Model of Authorization in r/3

Furthermore, Logging and Tracing is also a required component to secure the application layer of ERP system, although it is not the key function.

Baan Security using DEM

In Baan (bought by SSA) security architecture (Valente, 1999), we can easily determine if the solution is based on the RBAC model. Baan security solution uses a tool called Dynamic Enterprise Modeler (DEM) to assist the security configuration of Baan. DEM is used to model business processes or functions of an organization and define the roles. Within the architecture of Baan's security solution, there are four concepts: User Employee, Role, and Process.

- User: Baan user is the profile including all of an employee's personal information.
- Employee: The person who works in the organization.
- Role: Defined to indicate the position and the assignments of the employee. All employees must be assigned to a role, and roles will be assigned to the business processes.
- Process: Once a process is modeled in Baan ERP, roles will be attached to that process.

Next-Generation Models

Extended RBAC

Most contemporary ERP software adopts traditional access control methods such as RBAC as its primary measure to secure the system. What these methods care is whether some subject is allowed to perform the requested rights on the object. In some cases, the subject has to meet mandatory requirements before exercising the rights. A good example is that the researchers have to fill up his/her personal information before he can have the rights to read or download white papers. This mandatory requirement is Obligation (Park and Sandhu, 2004). Another important requirement for accessing the resources is the environmental or system requirement called Condition (Park and Sandhu, 2004), such as accessing time, date, and location. Since these functional predicates are not included in the idea of traditional access control methods, a straightforward enhancement of RBAC today is to introduce obligation and condition predicates. So we have so-called Extended-RBAC.

In this ERBAC model, an extra decision manager is added since obligation and condition predicates will be taken into account. In the decision process, condition requirements will be checked first; if all the environmental conditions are met, the checking procedure for the obligations will be triggered; and, at last, the decision process will check whether the user is intended to access the information. Srinivasan and Thuraisingham are examining the extended RBAC model for ERP (Srinivasan and Thuraisingham, 2006).

UCON

In recent years, a new model, Usage Control Model (UCON), was proposed in order to set up a framework for the future security techniques in ERP. UCON not only integrates three functional predicates (authorization, obligation, and condition) but also brings in the concept of time. This feature allows a security component in ERP system to be far more dynamic (Park and Sandhu, 2004).

The UCON model consists of the following core components:

- Subject and subject attributes: An entity with associated attributes which holds or exercises some certain rights on objects.
- Object and object attributes: An entity with associated attributes which one or several subjects hold or exercise rights on.
- Rights: Privileges that a subject can or cannot access an object.
- Authorization: Functional predicate determining whether a subject is allowed to perform some right on an object.
- Obligation: Functional predicate verifying whether the mandatory requirements have been fulfilled before a subject performs some right on an object.
- Condition: Functional predicate that checks whether the current environmental or system status allows a subject to perform some right on an object.

The UCON model is a large model family in which different combinations can exist for the three predicates. If we regard the UCON models with only one of these predicates used as the leaf nodes, we can build a tree rooted at $UCON_{ABC}$ model. We denote these models as $UCON_A$, $UCON_B$, and $UCON_C$. These models can be broken into several submodels based on whether time is taken into consideration. For example, $UCON_A$ will be divided into $UCON_{preA}$ and $UCON_{onA}$. Furthermore, these submodels can be divided into more detailed models depending on when and whether the update of mutable attributes will occur. We are currently investigating the applicability of UCON features for ERP security.

DIRECTIONS ON ERP SECURITY

Trends

Looking into the history of ERP technology, it is easy to find that the transformation from mainframe structure into client/server architecture is its biggest step. With this architecture, it became possible to develop a large system which integrates lots of functionalities. Now, ERP becomes the core of the operation and business in a company. ERP will not always remain the same as the requirement of automation of business evolves. The future ERP system may have the following features:

- Heterogeneous: Heterogeneous/heterogeneity means that the components from different vendors coexist and cooperate in an ERP system. It has two prerequisites: componentization and integration. It is true that some of the leading ERP vendors are going to or have already done something regarding these two aspects. Stronger communication platforms are provided to support heterogeneous applications, and applications are developed in the form of components.

- Collaborative (Jayaweera, Johannesson and Wohed, 2001): This could be in the realm of e-business. We can classify the business processes within an enterprise into two types: enterprise-centric process and collaborative process. Processes such as accounting and payroll processing are enterprise-centric; others such as supply chain management are almost completely collaborative. There are some intervenient processes, yet they are designed and developed in an enterprise-centric way. In the future, more processes will be redesigned in a collaborative way. This feature also implies the ERP system will be more open and more Internet-based.
- Intelligent: ERP system in the future will include more components that do the analysis, investigation, or even advice on the strategic transform. This feature implies that more confidential information will flow within or out of an ERP system.
- Knowledge-based: Firms are moving towards knowledge-based operation; thus, the ERP system that supports the daily business also has to trend towards knowledge-based management, communication, and operation.
- Wireless: Access to the ERP system from a mobile device.

Currently, there are two methods to secure an ERP system: access control and logging. Many companies will fail in their ERP security efforts because the security control design and implementation are costly and time-consuming. The stringent security control makes the operation become more complex, so employees will not be glad to see that. Within a large enterprise, there will be many activities regarding the change of an employee's authorization level, such as promotion, reassignment, or termination. This will make the user-based access control very hard to implement, and the administrator will always feel exhausted dealing with these issues. More detailed logging system will bring high cost and low performance to the system, since it will have to trace every event and log everything in detail. Therefore, users will not be glad. As the ERP becomes more Web-based, the security issue within an open system becomes critical.

Usually, better security solutions will bring higher cost and lower performance to a system. This contradiction always exists in any type of system. ERP is the system used to lower the cost and increase the profit of an enterprise; hence, management will consider the performance of the system first and foremost. For example, assuming solution A and B, solution A provides better security control than B. It is not definite that A will perform better than B in the real case. The key factor is whether A will bring much more cost to the system than B. The psychological factor of the users should also be considered. The solution should be amended based on its cost and impact to the performance of the system; otherwise, it may not be acceptable for the enterprises.

Policies

Much of the focus on ERP security has been on confidentiality (Thuraisingham, 2005). However, we need to include other types of policies. These include the following:

- Need-to-know policies: These are policies where access is granted based on whether a user needs to know. These policies are enforced in military environments.
- Need-to-share policies: There is now a migration from need-to-know to need-to-share policies in many organizations, including the military. Financial and healthcare operations also have to share data to carry out their operations. We discuss need-to-share policies in our paper on Assured Information Sharing (Thuraisingham, 2006).
- Trust policies: These policies ensure that data are shared only between individual organizations that are trusted.
- Integrity policies: These policies ensure that data are modified by authorized individuals. Furthermore, data quality and provenance policies that determine where the data have traveled and the accuracy of the data may also be included under the integrity policies.

Essentially an ERP system has to enforce the various policies. However, not all of these policies are needed for all applications. Therefore, one needs to examine the application, determine the policies that are relevant, and develop ways to enforce them.

Secure Content and Knowledge Sharing

The exchanging infrastructure sets up the cornerstone for an ERP system; effective coordination becomes a stringent requirement that needs to be fulfilled in today's ERP system. Therefore, securing the exchanged document is the cornerstone for ERP security; appropriate schema integrating encryption and digital signature technologies into XML framework is necessary to achieve this goal. Furthermore, appropriate security architecture or model has to be designed so as to support sharing the knowledge in an open and multi-organizational environment. Much work has been done in this area, such as trust management and the UCON model, although these security frameworks have not yet been applied in most commercial ERP products. As we mentioned earlier, the cost and return must be evaluated before implementing such technologies.

Web Services Security

As we mentioned in the "ERP Technology" section, Web services and service-oriented architectures are key technologies for ERP systems. Therefore, securing Web services and service-oriented architectures are needed.

Various efforts have been reported on securing Web services (Bertino et al., 2004). Furthermore, standards such as OASIS have developed security specifications including SAML (Security Assertion Markup Language) and XACML (XML Access Control Markup Language) (OASIS Security Specifications, 2003). In addition, securing XML documents as well as securing semantic Web technologies have received attention (Bertino et al., 2004; Thuraisingham, 2005). Program such as the Department of Defense Global Information Grid have focused on security for service-oriented architectures GIG/IA National Security Agency Presentation, 2005). However, little work has been reported on adapting the various technologies for securing ERP. This will be the major challenge.

CONCLUSION

Enterprise Resource Planning is the technology that drives the reformation in the realm of economy and impacts people's life style indirectly. ERP system now is going towards a system with more coordination/collaboration, higher heterogeneity and integrity, more intelligent, operating on the level of knowledge, and even wireless-enabled. The security issue within ERP has been there for a long time, but most of the solutions are based on the assumption that an ERP system is a closed environment. Given current trends, where the ERP is more likely to be an open system, these solutions are insufficient to provide the security. Although there are many researchers working in this area and some solutions are provided to better suite the open environment, yet the security mechanism for ERP system has not yet been brought to the open environment for discussion. Furthermore, these existing security solutions are based on the features of the current ERP system; since ERP reveals more and more new features that may be supported in the future, the security mechanism has to be retrofitted and new security issues have to be identified. The research should focus on the following areas:

- Policy, model and design of the security architecture.
- Securing the exchanged documents.
- Securing the management and sharing of knowledge .
- Securing web services and service oriented architecture.
- User authentication and authorization methods in open environment.
- Securing data transfer in wired and wireless communications, especially security issues on low power devices.
- Examining the security of the interfaces between different components (e.g., operating system, database system, and logging mechanism) and ensuring that no security loopholes are introduced due to component interactions.

REFERENCES

Bakry, A. H. and Bakry, S. H. (2005). "Enterprise resource planning - a review and a STOPE view," *International Journal of Network Management* 15. pp. 363-370.

Bertino, E. (2004). "Security for Web Services," Proceedings IEEE Web Services Conferences.

Bertino, E., Carminati, B., Ferrari, E., Thuraisingham, B., and Gupta, A. (2004). "Selective and Authentic Third-Party Distribution of XML Documents," IEEE Transactions on Knowledge and Data Engineering, 16(10): 1263–1278.

GIG/IA. (2005). "National Security Agency Presentation." http://www.nsa.gov/ia/industry/gigir.cfm?MenuID=10.3.2.2.

Glass, R. L. (1998). "Enterprise Resource Planning - Breakthrough or Term Problem," *The Database for Advances in Information Systems,* 29:2.

Goodman, E. (2004). "Security Evaluation and Management for the SAP R/3 Environment," GSEC Certification Practical.

Iacovou, L., Benbasat, I., and Dexter, A. S. (1995). "Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology," *MIS Quarterly,* 19: 4, pp. 465-485.

Jayaweera, P., Johannesson, P., and Wohed, P. (2001). "Collaborative Process Patterns for e-Business," *Siggroup Bulletin,* 22:2.

Kern, A., Kuhlmann, M., Schaad, A., and Moffett, J. (2002). "Observations on the Role Life-Cycle in the Context of Enterprise Security Management," *SACMAT'02,* June 3-4.

Kumar, K. and van Hillegersberg, J. (2000). "ERP Experiences and Evolution." *Communications of the ACM,* Vol. 43. No. 4.

Nagpal, A., de Bruyn, G. M., and Lyfareff, R. (1999). *ALE, EDI & IDoc Technologies for SAP* pp. 6-20, 376-384. Prima Publishing.

OASIS "Security Specifications." http://www.oasis-open.org/specs/index.php.

OASIS. (2001). "ebXML Technical Architecture Specification v1.0.4." http://www.ebxml.org/specs/ebTA.pdf.

OASIS. (2006). "The Framework for eBusiness." http://www.ebxml.org/.

Park, J. and Sandhu, R. (2004). "The UCONABC Usage Control Model," *ACM Transactions on Information and System Security,* 7: 1.

Rashid, M., Hossain, L., and Patrick, J. D. (2002). "The Evolution of ERP Systems: A Historical Perspective." http://jobfunctions.bnet.com.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. (1996). "Role-Based Access Control Models," *IEEE Comput.,* 29: 2.

Schaad, A. (2006). "Panel: Security in Enterprise Resource Planning Systems and Service-Oriented Architectures," *SACMAT'06,* June 7-9.

Shehab, E. M., Sharp, M. W., Supramaniam, L., and Spedding, T. A. (2004). "Enterprise resource planning - an integrative review," *Business Process Management Journal,* 10:4, pp. 359-386.

Sprott, D. (2000). "Componentizing the Enterprise Application Packages," *Communications of the ACM,* 43:4.

Srinivasan, I. and Thuraisingham, B. (2006). "Extended RBAC for ERP Systems," Technical Report, University of Texas at Dallas, November.

Thuraisingham, B. (2005). "Security Standards for the Semantic Web," *Computer Standards and Interfaces Journal,* 27(3): 257–268.

Thuraisingham, B. (2005). Database and Applications Security, *Integrating Information Security and Data Management,* pp. 2-19. Auerbach Publications.

Thuraisingham, B. (2006). "Assured Information Sharing," UTD Technical Report.

Valente, G. (1999). "Baan Application Security," ISACA Spring Conference.

van de Riet, R., Janssen, W., and de Gruijter, P. (1998). "Security Moving from Database Systems to ERP Systems." *Database and Expert Systems Applications, Proceedings,* pp. 273-280, August.

W3C. (2006). "Extensible Markup Language (XML) 1.0 (Fourth Edition)." http://www.w3.org/TR/2006/REC-xml-20060816/

W3C. (2004). "XML Schema Part 0: Primer Second Edition." http://www.w3.org/TR/xmlschema-0/.

W3C. (2004). "XML Schema Part 1: Structures Second Edition." http://www.w3.org/TR/xmlschema-1/.

W3C. (2004). "XML Schema Part 2: Datatypes Second Edition." http://www.w3.org/TR/xmlschema-2/.

White Paper. (2002). SAP Exchange Infrastructure 2.0, SAP AG and Sun Microsystems.

White Paper. (2000). "Authorizations Made Easy User Role Templates and Generating Authorization Profiles." Release 4.6A/B. SAP AG.

White Paper. (2002). "SAP R/3 Enterprise (version 1.0)". SAP AG.

White Paper. (2002). "SAP Exchange Infrastructure 2.0 *Technical Infrastructure*." SAP AG.