Application Security Using the Role-based Access Control Model

Ronke Oyemade, CISA, has more than 13 years of experience working in the consulting industry. Her areas of expertise include IT audit and security, software life cycle and development, and Sarbanes-Oxley compliance. She has worked with firms such as Ernst & Young and Deloitte. Oyemade also is an experienced training instructor, who has trained employees of *Fortune* 500 companies, such as Coca-Cola and Johnson&Johnson. She was the lead instructor at the ISACA Atlanta Chapter's Oracle Audit training session in October 2009. She can be reached at *ronkkey@yahoo.com.*

Securing an application environment involves a set of three components:

- Technology infrastructure security, which involves securing the network and host
- Operating environment security, which involves securing the database and operating system
- Application security, which involves securing the actual application. This includes user access management and role-based access control (RBAC).

This article addresses application security focusing on the RBAC model. It takes a look at some of the currently publicized security breaches and privacy violations and the risk involved and discusses how RBAC implementation minimizes such events and risks. Finally, it addresses the implementation of this model within the Oracle E-Business Suite.

With a large user base using an information system, administering user accounts can become a resource-intensive, time-consuming task and can lead to a system where segregation of duties conflicts prevail.[1] In addition, instances of security breaches and violations of privacy with regard to data kept by corporations are constantly in the news.[2] Most publicized security breaches originate from unauthorized access of information systems from external sources, but a significant percentage of breaches come from the inside and these pose a serious threat to companies because they come from trusted users.[3] For example, according to Privacy Rights Clearinghouse, a senior financial analyst at Countrywide downloaded sensitive social personal information (including Social Security numbers) of an estimated 2 million mortgage loan applicants over a period of two years. He told law enforcement that he profited anywhere from US $50,000 to US $70,000 from the sale of the Countrywide-owned data to buyers from business center stores.[4]

It only takes one mouse click to send sensitive data all over the world.

Security breaches and privacy issues can lead to a loss of reputation, customer trust and market share. In addition, corporations may be faced with the need to comply with privacy regulations such as the US Health Insurance Portability and Accountability Act (HIPAA).[5]

Corporations are constantly trying to balance these security issues, compliance requirements and the constant pressure of providing their services to their customers online. For example, in the US, an investment of US $20 billion in federal funds is planned to achieve widespread deployment of electronic medical record (EMR) systems. This is being planned to reduce long-term costs and increase the effectiveness of health care business processes and, ultimately, to improve the US health care system. EMR systems will result in capturing and disseminating medical and health-related information for patients online, resulting in individuals being empowered to make health decisions for themselves, easily choose among providers, selectively disclose medical conditions and receive optimum care during emergencies.[6] However, the security and privacy issues relating to providing patients information online include accidental or for-profit disclosure or alteration of patients' information by insiders, the specific type of data at risk (patient identification, financials and medical information), and the scale at which data can be exposed (i.e., number of patient records threatened).[7] For example, an unauthorized disclosure of medical records to the press for an individual with the HIV virus could lead to devastating effects, such as family or community ostracism, job loss and denial of medical benefits. A large security breach could lead to HIPAA violations with severe consequences or penalties.[8]

WHY IMPLEMENT AN RBAC SECURITY MODEL?

Management can minimize risk by introducing an RBAC model to administer and manage user access to the organization's information systems. Using a security platform based on an RBAC model simplifies user access administration and management, assists in maintaining a high level

of customer privacy, provides the capability to grant more appropriate access permissions, ensures data security, protects business interest, and ensures compliance with government regulations.[9] It also allows for corporations to build a "least privilege"-compliant access model with roles that meet segregation of duties requirements.

Through an RBAC model, permissions are associated with roles and users are made members of appropriate roles based on their job responsibilities and qualifications/geographical locations. Users, therefore, acquire the roles' privileges.[10]

There are many components to an RBAC model and, therefore, it can be described as multifaceted. It involves assigning users to roles, assigning permissions to roles and assigning roles to roles to define a role hierarchy. The goal of all these activities is to connect users with permissions.

Through this approach, a corporation can control and manage groups of users by defining to which information each group has access, based on the job responsibilities/ geographical locations defined for the group within the corporation. So, when a new user is added to the system, the user is assigned to the appropriate role based on his/her job title. Through that role, he/she is provided menus that provide the permissions required to access authorized data.

RBAC MODEL IN ORACLE E-BUSINESS SUITE

This section revisits the RBAC model and describes its implementation in the Oracle E-Business Suite.

Security in the Oracle E-Business Suite is in the form of a core security framework made up of three layers, built one on top of the other, as shown in **figure 1**. The first layer is the function security layer on which the second layer, data security, is built. The third layer is the RBAC layer, which is built on the two previous layers.

Access control is defined through roles, and the access given to a user is defined through the roles granted to the user. In **figure 2**, the user, Dr. Smith, is given access to the Oracle E-Business Suite through the assigned role called "Doctor."

Roles can also be included in a role inheritance hierarchy whereby a superior role inherits all the properties of the subordinate role, as well as any of that role's subordinate roles. With reference to **figure 2**, the Doctor role inherits, in addition to its access level, the access levels granted to

Figure 1—Oracle Core Security Components

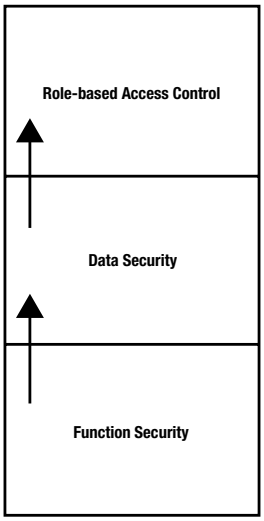
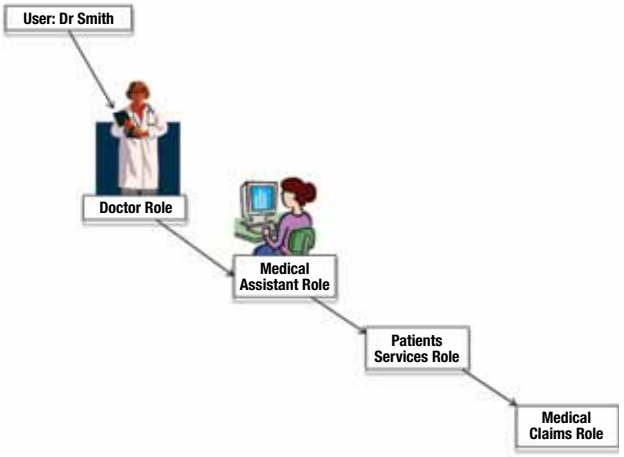


Figure 2—User Role Association



the Medical Assistant role, the Patients Services role and the Medical Claims role (which are subordinate roles to the superior Doctor role).

Creating a role is a one-time setup, whereby the role is associated with privileges that define what data can be accessed and how that data can be accessed. Privileges are in the form of responsibilities and permissions. Responsibilities and permission are defined in Oracle E-Business Suite through data and function security layers.

The function security layer restricts user access to individual menus and menu options within the system. In **figure 3**, the Clearinghouse has restricted access to Patient Medical data through the menu options assigned to the Medical Claims role. **Figure 4** shows that the menu options provided through the function security layer allow the Clearinghouse to update, view and delete rendered patient medical services records and update the Billing Code field. Even though the function security layer provides the user with access via submenus to update, view and delete rendered patient medical services records, the user will not be able to do so. This is because access to the actual data has been further restricted via the data security layer, allowing the user only to view these records.

KEYS TO IMPLEMENTING THE RBAC MODEL

Even though the RBAC model has many advantages, its implementation needs to be carefully planned to avoid the risk of increasing existing risk levels. Appropriate controls need to be implemented to fit an RBAC model to an existing enterprise resource planning (ERP) environment. During the planning stage, business and technical requirements should be identified. This should include understanding the business processes and controls as well as the jobs of the associated staff. For example, within the health care system, staff jobs that require immediate access to medical records include emergency technicians, admitting staff, doctors, nurses, and back-office personnel in billing and accounting. The level of access required for these jobs needs to be identified and appropriately analyzed.

During the design stage, the RBAC model should be designed. This should include identifying and designing roles based on the jobs or geographical locations identified in the planning stage, and then identifying and designing the permissions that are associated with these roles.[11] Care should be taken when identifying these permissions because exclusion of a permission that should have been assigned to a particular role may lead to a catastrophe. For example, in the health care field, exclusion of "viewing" permissions could lead to a surgeon unable to view critical images in the operating theater.[12] In addition, security management processes and compliance monitoring controls surrounding this model should be designed.[13]

CONCLUSION

While this article reviews RBAC implementation within the Oracle E-Business Suite, similar implementations based on the RBAC concept can be successfully developed in other technologies and application environments, including home-built applications.

Proper implementation can be achieved through effective collaboration among the data guardians (business process

Figure 3—Role Inheritance Hierarchy

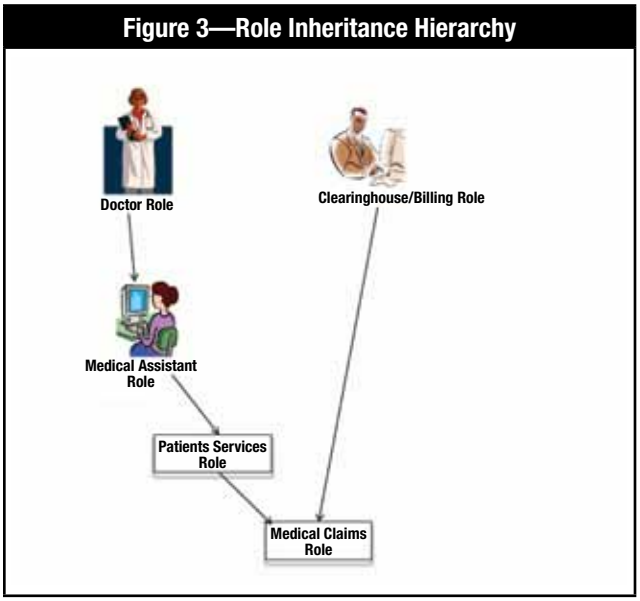
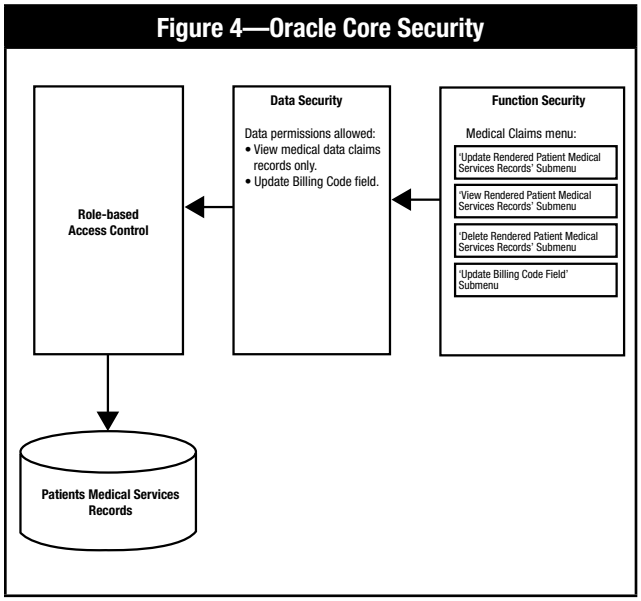


Figure 4—Oracle Core Security



owners) and the security administrator. The data guardian defines the overall approach to security and the security framework. The security framework includes defining the employees' job descriptions and tasks and identifying the roles and functions within those descriptions and the data required to be accessed to perform each task.

The security administrator implements and maintains the security setup based on the security framework provided by the data guardians. Using this framework, the security administrator creates and assigns roles to users as well as creates and assigns responsibilities and permissions to roles.

Proper RBAC model implementation provides adequate controls that will minimize the risk of continuous occurrence of security breaches and privacy violations from the inside. The RBAC model, if implemented in the health care industry, for example, will assist in improving the protection of individuals' private health records and prevent identity theft.

ENDNOTES

[1] Deloitte LLP, "Point of View: Strengthening Your Oracle User Management," 2008

[2] Covich, Jennifer; "Role-based Access," *HIPAA Watch*, Health Management Technology, July 2001, *www.healthtech.com*

[3] AppsHosting and Experian, "Managing a Secure Oracle Applications Environment," 2007

[4] McGlasson, Linda; "Identity Theft: Lender Countrywide's Insider Case—Two Years of Thievery Nets 2 Million Mortgage Applicants," *Bank Information Security*, 14 August 2008, *www.bankinfosecurity.com*

[5] Murrell, Laurie; "Role-Based Access Offers Security for e-Business," *National Underwriter*, Life & Health/Financial Services Edition, 13 August 2001

[6] Nanji, Feisal; "Security Challenges of Electronic Medical Records," *CSOonline.com*, 19 February 2009

[7] Lirov, Yuval; "Electronic Medical Billing Software, HIPAA Compliance, and Role Based Access Control," *http://EzineArticles.com/?expert=Yuval_Lirov*, 24 July 2006

[8] *Op cit*, Nanji

[9] *Op cit*, Murrell

[10] Sandhu, Ravi; Venkata Bhamidipati; "Role-Based Administration of User-Role Assignment: The URA97 Model and Its Oracle Implementation," *Journal of Computer Security*, vol. 7, 1999, p. 317-342

[11] *Op cit*, Deloitte LLP

[12] *Op cit*, Nanji

[13] *Op cit*, Deloitte LLP

The *ISACA Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *ISACA Journal* does not attest to the originality of authors' content.

www.isaca.org