A Novel Security Integration for Vulnerability Avoidance in Enterprise Cloud Applications (CloudERP)

K.C. Okafor, C.M. Nwafor, & C.C. Udeze
Electronics Development Institute (ELDI-NASENI)
Awka, Nigeria

arissyncline@yahoo.com, mcchuksonline@yahoo.co.uk, udezechidiebele@yahoo.com

F.N. Ugwoke
Computer science Micheal Opara University
Umuahia, Nigeria

ndidi.ugwoke@gmail.com

ABSTRACT

Studies have shown that some existing enterprise applications including business ERPs, Social Networks, etc implement a single layer security scheme which can easily be hacked. Also, these applications suffer from multiple security vulnerabilities, including SQL Injection Attacks (SQLIA), Social engineering, spoofing, etc. For most mission critical enterprises, their organizational critical assets can be dumped in ERPs, which needs to be protected very adequately. This paper then develops a Cloud based Enterprise Resource Planning System (CloudERP) while re-engineering a second (Layer-2) security appliance called Advanced Encryption Validation Key (AEVK) which is an authentication scheme based on Advanced MD5 Encryption (A-MD5) algorithm. The proposed approach is expected to replace the overall process architecture and security integrations in existing ERP vendor systems owing to its computational as well as security features. Our methodology involved the use of Netbeans 7.0.1, JAVA Server Page and MySQL tools in this work.

Keywords: ERPs, Social networks, Vulnerabilities, Social Engineering, Assets, Encryption, Enterprise

1. INTRODUCTION

Enterprise Resource Planning (ERP), according to the APICS dictionary, is defined as a “Framework for organizing, defining and standardizing the business processes necessary to effectively plan and control an organization” ERP software provides the tools to manage business information throughout the enterprise. There are several ways to characterize the different types of ERP software. A case can be made according to the organizational capacity or size. Some organizational ERPs are designed to serve using the common Tier 1 (large company), Tier 2 (mid-sized company) and Tier 3 (small company) designations. ERP software can also be categorized by deployment strategy viz: on-premise or hosted Software-as-a Service (SaaS). Note, however, that many on-premise ERP systems are also offered through a SaaS licensing option. These categories may also be applied to identify types of Customer Relationship Manager (CRM) software and types of accounting software [1].

Also, are various other ways of designating different types of ERP systems. Some ERP systems are designed to serve specific industry vertical markets, such as the ERP for industrial equipment manufacturers, ERP for the healthcare industry, ERP for pharmaceutical companies, ERP for Banking industry, ERP for Oil and gas, ERP product for plastics companies, ERP for circuit board manufacturers, etc. With all the existing ERP solutions as well as other enterprise web applications, security vulnerability has kept on challenging the effectiveness of these solutions. In addressing the security vulnerability challenge, this paper recommends that enterprises should make their ERP vendor choice based on expertise and commitment of the vendor in a given industry.
Beside ERP hacking, SQL IA problem in web applications had continued to draw the attention of researchers and practitioners [2]. As a consequence, many solutions proposed in the literature address only some of the issues related to SQL injection. To address this problem, will present an extensive review of the different types of SQL injection attacks known to date, while developing a design framework for CloudERP that will address both the security vulnerabilities and the process architecture. This paper is organised as follows: Section II Presents the various types of ERPs, Section III presents the Related works, Section IV discussed on the methodology, Section V detailed the Implementation Approach, Section VI presents discussion and results while outline future recommendations and future directions.

2. ERPS TYPES AND FUNCTIONALITIES

Some identified types of ERP in includes: SAP R/3-, SAP B1(Business one), LN (Baan), Microsoft Dynamics NAV(Microsoft Navision)Microsoft Dynamics AX (Axapta) 2009, JD Edwards, Oracle Financials, PeopleSoft [3]. With the communication infrastructure and ERP functionalities encapsulated in components, an ERP system can must meet these requirements below as cited in [4] viz:
- 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 should be easy.
- 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, hence AEVKs. Also, the components that different ERP vendors provide may vary, but the core functionalities are nearly the same. These functionalities include [5], [6]:
  - Human Resource Management, which may have the functionalities such as payroll management, self-service, learning management, benefits, recruitment, tutor, timer and labour management, and compensation management.
  - 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 the above components. An SCM can include the business processes such as CRM, SRM, manufacturing management, demand management, and production planning.

3. RELATED WORKS

The work in [2] presented a classification of SQL injection attacks and countermeasures. In their work, an extensive review of the different types of SQL injection attacks known to date was carried out. For each type of attack, the work provides descriptions and examples of how attacks of that type could be performed. The work also, presented and analyzes existing detection and prevention techniques against SQL injection attacks. The author in [4] stated that most current ERP systems are based on Role-Based Access Control (RBAC), although they may have different settings of either enhancement [7]. According to [8], an RBAC model consists of the following components: permissions, roles, users, and constraints.
The work in [9] summarized some of the security aspects in an ERP system, they include: Security policy and administration, User authentication, Authorization, Time restriction, Log and trace, Database security. This work observes that one security administration is not ideal for a secured and sensitive business process. Only one administrator should be mandated to administer security on ERP modules for various users. Also, when more than one user is administering the security policy, conflicts resolution could be very difficult. A representative samples of works on ERP systems and security was studied in [10], [11], and [12].

In all the reviews, ERP security remains a problem yet to be fully addressed. Studies on OpenERPs, SAP, Oracle, etc all show a one layer security interface. Vulnerability is indispensable in such systems. Figure 1, 2, 3 and 4 shows layer-1 security concepts.

Figure 1: OpenERP layer-1 interface

Figure 2: OpenERP Submodule
This work argues that a one layer authentication is insufficient to protect critical data asset of an organization particularly in this era of online web vulnerabilities. In this paper, the process architecture is divided into Presentation Layer (client interface), the Application Layer (business logic), and Database Layer (server backend). The proposed CloudERP system employs client/server architecture to create a distributed computing environment while implementing the security layers. We now describe the three-tier architecture as outlined below:

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, background processes and the related hardwares. The password dictionary file, control files and background processes are found in this layer also.

After consolidating the business logic and the technical platform, we will have the ERP system architecture as showed in figure 5. As the basis of the CloudERP system, an information exchange platform which interacts with the background processes and GUI is shown in figure 5.
4. METHODOLOGY

This work first carried out an investigative research with most enterprise organizations viz-a-viz ERPs and then adopted software development life cycle methodology (SDLC) to realize figure 5. Firstly, studies were conducted on numerous ERP systems as well as other enterprise solutions. The phases and activities common to all life cycle systems development methodologies are as follows:
- Preliminary investigation
- Problem analysis
- Requirements analysis
- Decision analysis
- Design and coding with Netbeans/JSP/MySQL
- Implementation and testing. We now detailed the system operation next.

4.1 Operational Description

The system model of CloudERP shown in figure 6 comprises of two security layers. The first is for the user login AVEK and the second is for the AEVK security of the respective ERP Modules. There are 6 subsystems implemented in CloudERP as depicted in figure 6. The subsystem of CloudERP HR includes recruitment, payroll, performance, HR intelligence, vacancies and trainings. The subsystem of CloudERP manufacturing includes products, raw materials, finished products, manufacturing schedule, and dispatch. The subsystem of CloudERP Sales includes sales order, cashbook, billing, etc. The subsystem of CloudERP marketing includes inventory, customers, distributors, marketing research, products and prices, advertising, and orders. From the lock diagram of figure 6, the users supply their login details vis-a-vis AVEK layer-1 authentication. The grid control or the logic instance then connects the user process to the server process having meet all the layer security requirements. As shown in figure 6, this work used an advanced encryption algorithm to encrypt user login details from the server process (AVEK). Firstly, the user process is initialized before the validation by AVEK from the server process at the backend. After the validation, to
access any module of the CloudERP will require another authentication by AVEK. All the AVEK passkeys are securely stored in the server.

Security vulnerabilities including SQLIA were addressed during the implementation phase. Figure 7 shows the instance connection to the server.

Figure 6: CloudERP Model
4.2 System Implementation

(i) System Model

This paper formulates optimal security model for CloudERP as viz:

$$\text{Max } f(s) = \sum_{i=1}^{n} (Hr + Sa + Mf + Lg + Aud + Mk)$$

Subject to Sec Encrypt Keys $\leq 300$ keys Randomly

Where $f(s) =$ Security function, $Hr =$ Human Resource Subsystem, $Sa =$ Sales Subsystem, $Mf =$ manufacturing Subsystem, $Lg =$ logistics Subsystem, $Aud =$ audit Subsystem, $Mk =$ Marketing Subsystem.

The random keys spans from 0 to a maximum of 300 alpha numeric characters for AEVK.

(ii) CloudERP Administration Tools

In the CloudERP design, the system administration tools include: The Java Virtual Machine, Php My Admin, XAMP Control Panel, database...
connection Bridge. Next, we now discuss the development Platform for CloudERP.

(iii) JAVA NetBeans Platform

For compilation and Running of Java Codes, netbeans IDE was used as shown in figure 9. The NetBeans IDE is written in Java and can run anywhere a Java virtual machine (JVM) is installed, including Windows, Mac OS, Linux, and Solaris. A Java development kit (JDK) was used for Java development functionality. The NetBeans platform allows applications to be developed from a set of modular software components called modules. Again, the NetBeans IDE being an open-source integrated development environment, supports the development of all Java application types (Java SE including JavaFX, Java ME, web, EJB and mobile applications). The CloudMesh is written with JAVA programming language in NetBeans 7.0 and as such can run on any system.

Also, the NetBeans Platform is a reusable framework for simplifying the development of Java Swing desktop applications. The NetBeans IDE bundle for Java SE contains essential tools to start developing NetBeans plugins and NetBeans Platform based applications; no additional SDK is required in this case. The platform offers reusable services common to cloud computing applications, allowing developers to focus on the logic specific to their application. However, among the features of the platform are:

- User interface management (e.g. menus and toolbars)
- User settings management
- Storage management (saving and loading any kind of data)
- Window management
- Wizard framework (supports step-by-step dialogs)
- NetBeans Visual Library
- Integrated Development Tools

- An Ant-based project system, Maven support, refactoring, and version control (supporting CVS, Subversion, Mercurial and Clear case).

5. RESULTS AND ANALYSIS

In this work, we setup the NetBeans platform while enabling three major interfaces viz:

1. The library which comprises of my SQL connector, JDK 1.6, and Apache Tomcat 7.0.14.0.
2. Configuration files which comprises of manifest, Context. XML, Web.XML
3. The CloudERP system of figure 6 using the Netbeans platform yielded figure.

Figure 9 shows the snapshot of Apache Tomcat Power up for CloudMesh ERP. It shows the snapshot of Cloudmesh ERP coding pages. In this work beside the use of static code checkers, NewQuery Development Paradigms as outlined in [2] was adopt. Here, the use of encapsulation on database queries to provide a safe and reliable way to access CloudERP databases is reliable for the AEVK.

This technique offers an effective way to avoid the SQLIA problem by changing the query-building process from an unregulated one that uses string concatenation to a systematic one that uses a type-checked API. Within their API, they are able to systematically apply coding best practices such as input filtering and rigorous type checking of user input. By changing the development paradigm in which SQL queries are created, this technique eliminates the coding practices that make most SQLIAs possible.

Although effective, this technique has the drawback that they require developers to learn and use a new programming paradigm or query-development process iteratively. Furthermore, because our focus is on using new development process, This does not provide any type of protection or improved security for existing legacy enterprise web application ERP systems.
Figure 9: Netbeans Platform with JSP and Apache Tomcat server.

Figure 10 shows the snapshots of XAMP MySQL database for CloudMesh database structure for the server. In this case, the XAMP Control panel which provides our database is configured to work with the grid panel using SQL connector in the development environment.

Figure 10: XAMP MySQL database for CloudERP database structure.
6. CONCLUSIONS

In this paper, we have presented a novel security re-engineering for vulnerability avoidance in enterprise cloud applications (CloudERP) using AVEK. A survey on Open ERP, Oracle and other enterprise web applications was carried out. A key vulnerability issue - SQLIA was identified in most enterprise applications making for high insecurity. Starting with CloudERP system model, two security layers were introduced while preventing SQLIA vulnerabilities using NewQuery Development Paradigms. We then evaluated the considered techniques in terms of its ability to detect and/or prevent such attacks.

Besides, we detailed the development platform using Netbeans IDE. Our evaluation showed that modern web applications can be protected against security vulnerabilities as well as increasing the security layers in an ERP. We observed that many ERPs have problems of handling attacks that take advantage of poorly-coded stored procedures and cannot handle attacks that disguise themselves using alternate encodings.

We also found a general distinction in prevention abilities based on the difference between prevention-focused and general detection and prevention techniques. The proposed CloudERP is demonstrated to have better security framework compared with existing ERPs including one layer security applications. Future work will focus on evaluating the techniques of cloud integration and effectiveness in production environments. Empirical evaluations would allow for comparing the performance of the different ERPs when they are subjected to real-world attacks and legitimate inputs for validations.

REFERENCES


Author’s Brief

Engr. Okafor Kennedy Chinedu is a Systems Architect and R&D Consultant. He works with Electronic Development Institute, Awka, under National Agency for Science and Engineering Infrastructure, Nigeria, as a Senior R&D Engineer. He had his B.Eng in Electrical Electronics Engineering, (ESUT), and M.Eng. in Digital Electronics and Computer Engineering, (UNN) while currently pursuing his PhD in Electronics Engineering. He is a member of NSE, IEEE, NCS, and IAENG. He has various vendor certifications including Cisco Certified Network Associate, A+, etc. He presents technical papers in major conferences in the African Sub-region. His areas of interest include Network Design & Cloud Management, Middleware Technologies, VLSI, Enterprise-Wide Systems, Database Technologies, Application Development, Security, WSN Technologies, and Project Management. He can be reached through E-mail: arissyncline@yahoo.com

Nwafor Chukwubuikem Michael is an Electronic Engineer. He works with Electronic Development Institute, Awka under National Agency for Science and Engineering Infrastructure, Nigeria as an R&D Engineer. He had his B.Eng in Electrical/Electronics and computer Engineering, (UNIZIK), while pursing his M.Eng in Computer and Control Engineering, (UNIZIK). He has 10 publications in reputable international Journals. His areas of interest include Electronic Design & software development, security, and Project Management. He can be reached via E-mail: mcchuksonline@yahoo.co.uk

Engr. Dr (Mrs.) Ugwoke, Fidelia Ndidi received her B.Eng in Computer Science and Engineering (CSE) from Enugu State University of Science and technology (ESUT), She holds MLS in Library and Information Science from Ebonyi State University, Abakaliki Ebonyi State (EBSU), and also holds a Ph.D in Computer Science from Ebonyi State University, Abakaliki Ebonyi State. Currently, she is a Lecturer I staff in Computer Science Department, Michael Okpara University of Agriculture, Umudike Abia State, Nigeria. She belongs to a number of professional bodies including NSE, NCS and CPN.Emailaddress: ndidi.ugwoke@gmail.com, +23480371 74398, +2348116700273.

Engr. Udeze Chidiebele .C. received his B.Eng, M.Sc and PhD in Electronics and Computer Engineering from Nnamdi Azikwe University, Awka, Nigeria. He holds his PhD in computer and control systems engineering. He is a Senior R & D Engineer with Electronics development Institute Awka, Nigeria. He works with Electronic Development Institute, Awka under National Agency for Science and Engineering Infrastructure, Nigeria as an R&D Engineer. He is a member of Nigerian Society of Engineers and has his COREN registration. His current research interest is on DataCenter networks, Cloud Computing and Applications, WSN Technologies, and Control Systems Engineering. Email: udezechidiebele@yahoo.com