British Journal of Mathematics & Computer Science
13(5): 1-9, 2016, Article no.BJMCS.23217
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Knowledge Management Perspective in Communication Security System

W. O. Apena[1*], I. A. Adebanjo[1], Y. O. Olasoji[1], K. F. Akingbade[1], S. A. Oyetunji[1] and M. O. Kolawole[2]

[1]Department of Electrical and Electronic Engineering, The Federal University of Technology, PMB 704, Akure, Nigeria.
[2]Jolade Strategic Environmental and Engineering Consults, Melbourne, Australia.

Authors' contributions

This work was carried out as a team work in the research group of Communications and Applied Research. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/BJMCS/2016/23217
Editor(s):
(1) Victor Carvalho, Polytechnic Institute of Cávado and Ave, Portuguese Catholic University and Lusiada University, Portugal.
Reviewers:
(1) Kexin Zhao, University of Florida, USA.
(2) Anand Nayyar, KCL Institute of Management and Technology, India.
Complete Peer review History: http://sciencedomain.org/review-history/12833

Short Research Article

Received: 20th November 2015
Accepted: 15th December 2015
Published: 29th December 2015

Abstract

Security is an essential element in maintaining any network. This paper demonstrates the development and implementation of a communication security system that uses a layered approach to network security in the conceptual view of knowledge management, thus preserving the integrity of communication links and contents. Communication security system (CSS) is viewed and analysed as a Knowledge Management (KM) concept that process trends of information, authenticates, authorises users and encrypts any data sent across the network.

Keywords: Encryption; authentication; security and knowledge management (KM).

1 Introduction

Security is an essential element in maintaining any network and in minimizing risks. Understanding of risks involved and maintenance of network's integrity requires functional definition and initial knowledge. The term knowledge management (KM) is widely used as evolution of knowledge which describes the process of

**Corresponding author: E-mail: woapena@futa.edu.ng, adetutu.adebanjo@gmail.com;*

translating and managing information to obtain the desired output. The KM concept surfaced in the 1980s as a result of the need to obtain knowledge from disjointed information [1]. KM has grown and more applied in technical world to forecast and optimized engineering outputs, particularly in communication security evolution. In this globally competitive environment, KM provides platform for economic integration within available technologies [2].

Application of Knowledge management in communication security (CS) in a network(s) of computers can improve and also enhance knowledge sharing including knowledge discovery. Security has always been a topmost organisational challenge. Many organizations have been vulnerable to various attacks on networks such as banks transactions and messages. An alarming trend is the use of sophisticated application layer attacks, which are attractive to a potential attacker, due to the information sought for which ultimately resides within the application itself [3]. KM approach was applied to develop a communication security system for the Federal University of Technology, Akure, Nigeria. The approach involves the analysis of data obtained from stakeholders (students, academic and non-academic staff) as people involved by a technological-based process to authorise and authenticate network users.

2 Communication Security System (CSS)

Communication Security System (CSS) is the process of developing and executing specific plans, policies, and procedures to secure emergency response communications systems from possible risks and malicious actions [4]. Evaluating and implementing security plans, policies, and procedures is needed to alleviate risk to these critical communications systems. These security risks involve deliberate or undeliberate actions taken against a system that could result in the alteration, leak, or damage of sensitive or private information. These actions can degrade or fully disable system operations [4,5]. CSS generally includes four components: physical security, network security, communication security, and administrative security. Fig. 1, was described by [6], protection, detection and response are security indices of an organisation.

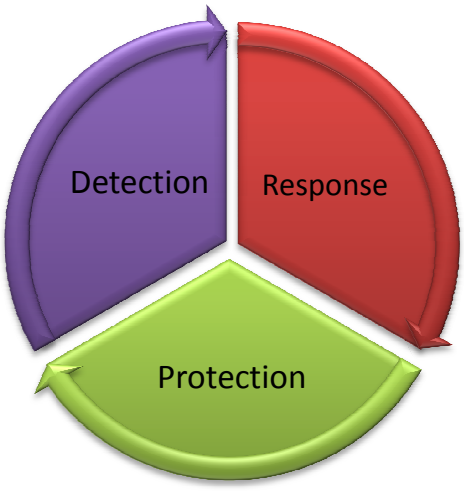

Fig. 1. The security indices [6]

The design, operation and maintenance of emergency response in communication systems could address gaps of each of these components. Firewalls, antivirus software, and intrusion detection programs also play important roles in maintaining network security [7]. In a university environment where data are continually and electronically transmitted and received, thereby, it is essential increase security efforts to promote data integrity in communication system.

2.1 Problem identification: Knowledge creation

To harness and transfer knowledge among different component parts of an organization such as a university faculty (school), a secure intranet (communication network) could be designed ensuring real time knowledge management. To minimize risks due to security violation, the intranet should be equipped to authenticate and authorise any user within the faculty/school on the network and, where interconnectivity exists between faculties/schools, similar access authentication and authorisation protocol would be required. The authentication and authorisation process would ensure that if there were an attack that compromises or bypasses one security layer it would be detected and blocked by another. This means that identification can be queried at every entry into the network.

2.1.1 Knowledge acquisition

Project implementation entails evolutional factors such as data, information and knowledge to maximise the efficiency. Fig. 2 illustrates a model knowledge acquisition flow (use and reuse). If knowledge obtained is inadequate or not satisfactory, the flow goes back to the primary source of information. Information and data is checked again until satisfaction is reached (i.e. transformation of information to application building).

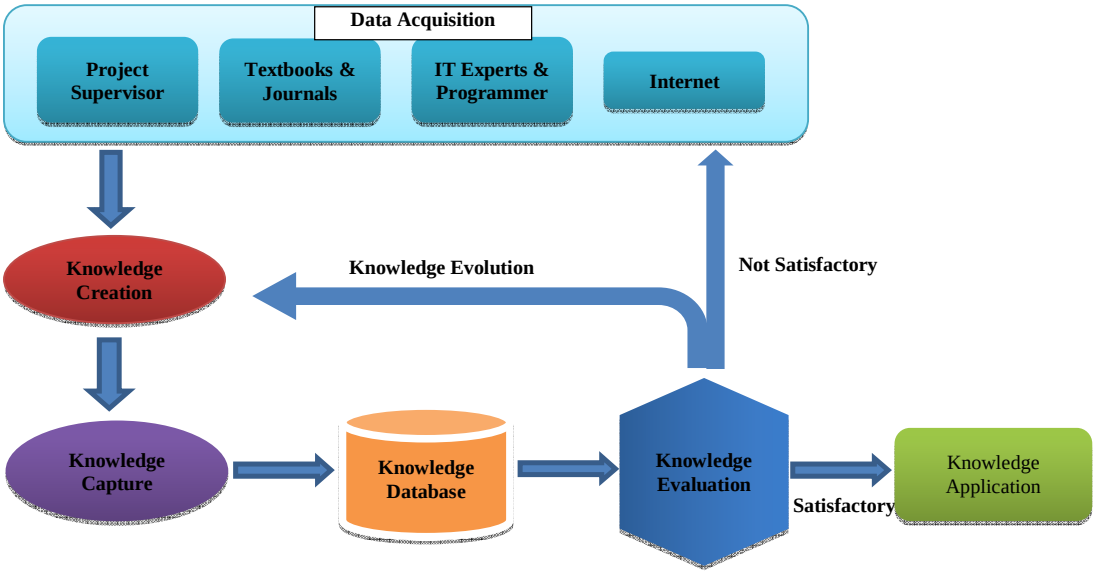

Fig. 2. The knowledge acquisition flow

3 Network Development and Security Evaluation

3.1 Network development: Making sense from knowledge management (KM)

Readily available knowledge tools such as java and MySQL were used for the university communication security project. At the initial phase of communication security system (CSS**)** development, a number of full-featured, general-purpose programming languages such as C# and VB.NET, capable of handling robust applications were experimented on. The programming language chosen was Java—a full-featured, general purpose programming language that is capable of developing robust applications [8], and MySQL—a multi-user, multi-threaded, structured query language—as query language. The performance and retrieval robustness of MySQL has been noted in [9]. The CSS development was implemented in modules allowing for enhancements, easy debugging, background checking of identity and snooping in real-time mode and friendly message graphical interface.

Fig. 3 shows the system flowchart, which analyses the pattern of security execution. The objective is developing a highly reusable and open Application Programming Interface (API) framework that emphasizes abstract interfaces, which are amenable to supporting existing standards as well as leaving room for future improvements.

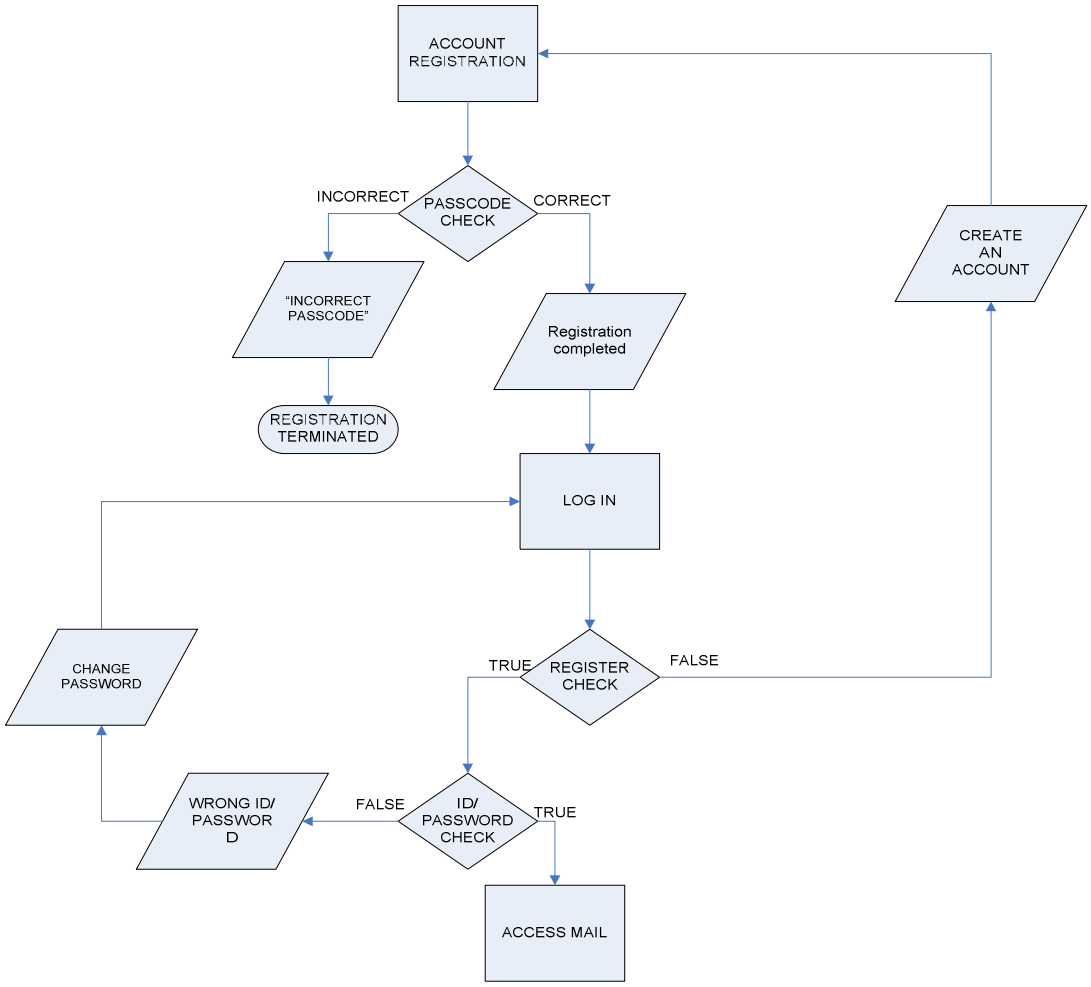

Fig. 3. Flowchart of user security check procedures

A number of API frameworks were developed which improved on existing Java programs using a layered approach to network security. A brief description of these applications is follows.

3.1.1 Mail application

The Mail application was developed to be the point of interaction with the Mail server; there are options made available for the user to create account and log in. The interface gives an overview of what can be done on the network, and when the network is connected or disconnected (shown in Fig. 4), as well as providing a medium of performing authentication and identification on the server. For the process of authentication, a user must definitely be registered and any time such a user logs in, the server authenticates by checking the database for such a user, if found, permission/access is granted.

Fig. 4. Login interface

3.1.2 Account registration and mail service interface

The Account registration application interface has text boxes and labels for entering information required (shown in Fig. 5). Before access is granted a user, passcode is granted by the administrator, which is recognized by the system. However, the system disables any concurrent usage, that is, if a used passcode was entered, the system will give a message and disallow any further activity.

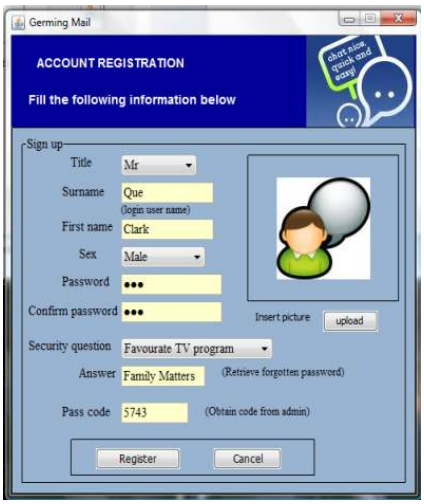

Fig. 5. Account registration interface

The ***Mail Service Interface*** provides the menu-bar services: e.g. inbox, outbox, draft, deleted, and summary envelopes, file, and Help service. This interface acts as the mail engine interfacing with outside world. There are no provisions for attachment of files in the application.

3.1.3 Mail server

Coding of the developed application was done using the NetBeans IDE. The Netbeans IDE houses the source, libraries and test packages. These packages house the necessary codes that execute any command entered on the interfaces. The source package contains elements of Java packages such as mail.model, mserver, picture (including all the .gif and .jpg files), server.controller, and other public declaring classes. The Libraries have the drivers used for running the Server application. The system database uses the MySQL driver to interact with the application codes.

3.1.4 MySQL setup

The setup of the Database was done using the Google chrome browser. The apache2triad application runs as a web application. The database was created and named "chatmail". Tables were also created in this database. Five major tables were created. Others are added as a user registers. The tables are; adminpass, chatusers, contacts, mail, and passcode. As users register, the database creates a table using the user's passcode.

3.2 Security evaluation

3.2.1 Authentication and concurrency test

Once a user has been granted access, a unique passcode is assigned, which is encrypted. If another user attempts to use the same access signature, it is viewed as an attack and access will be rejected. The current user will be notified with an envelope appearing on the screen warning of an intrusion.

3.2.2 Data encryption and decryption

Any mail sent is encrypted by letters chosen randomly: for instance, if the message "How're you doing?" was sent, an encrypted form was generated as noted in Table 1. If any user should send the same message, the encrypted form will be different. To check for encrypted mails, the MySQL page was opened on a browser page. The mails sent are viewed on the server as encrypted (indicated by the red circle in Fig. 6).

Table 1. Encrypted message

Message sent	Encrypted message
How're you doing?	JkBayFKsTcexWY6+EBiNlrmXgWuhozmi

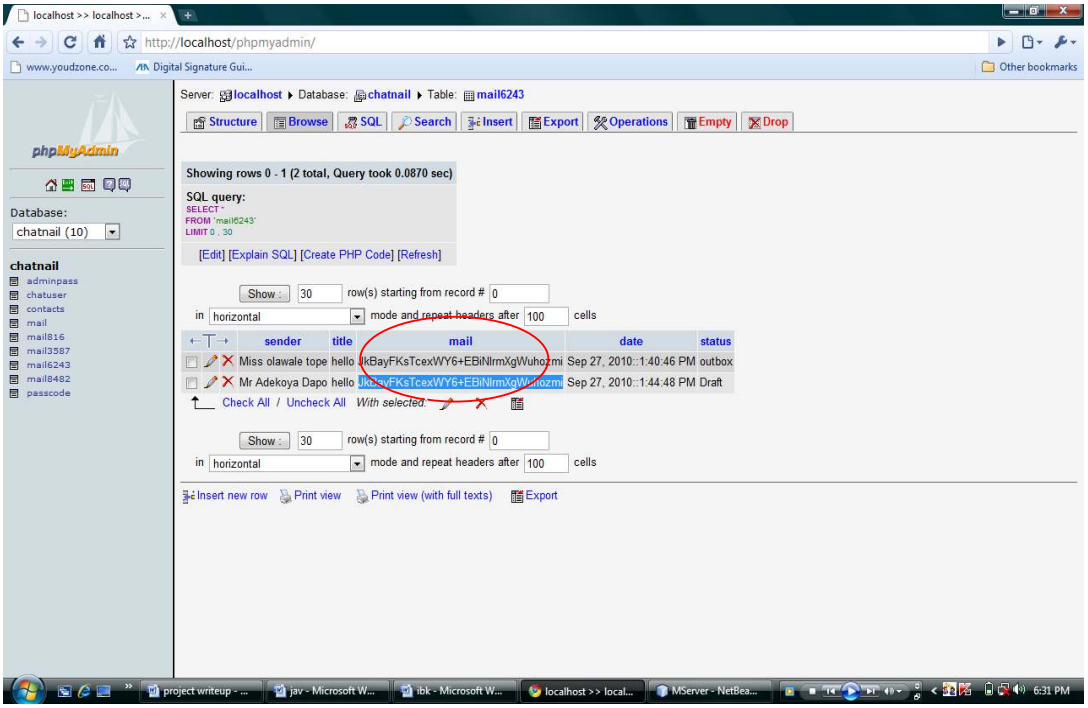

Fig. 6. Encrypted mails

4 Knowledge Management (KM) Concept and Communication Security System

4.1 People

The 'people' component is the greater challenge of organizations or groups or any individual implementing knowledge management [10]. [11] noted that it is the complex component to work with. In relating KM to CSS, the 'people' component can be divided into two;

(i) Tacit knowledge carrier (Technocrats And Hackers) and,
(ii) Network users, as shown in Fig. 7.

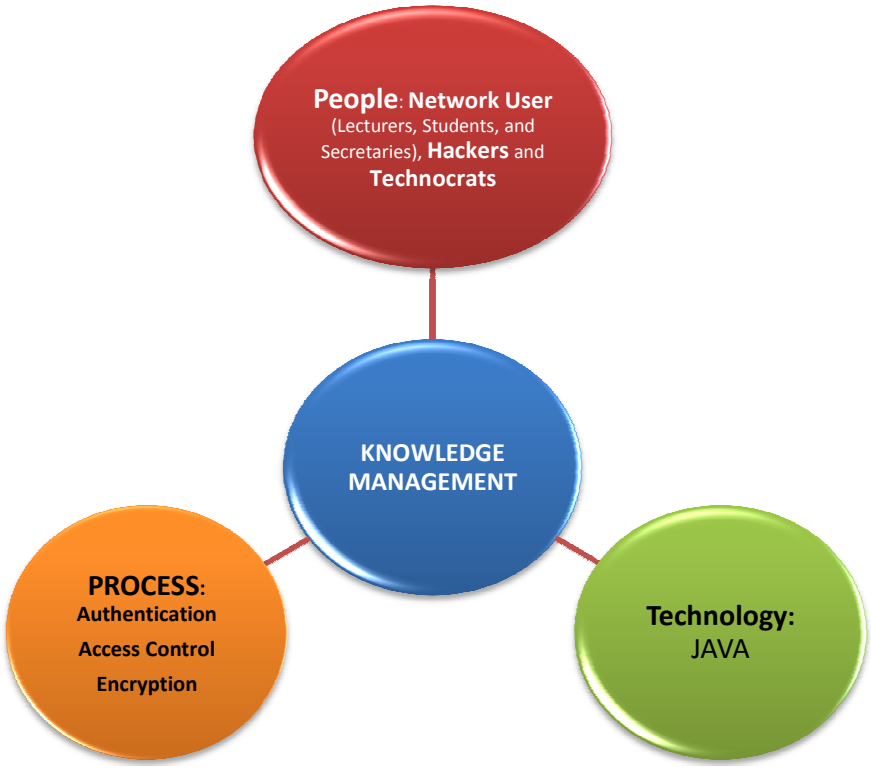

Fig. 7. The knowledge management triad

The knowledge carriers are the programmers, supervisor(s) and network security expert(s). These knowledge-handlers form a major part of the 'people' component. Their views, experience, and information help to correctly understand, draft, model and finally, develop the communication security system. They divulge helpful knowledge from experience, thereby creating the community of practice. At each stage of the project, an assessment of the project towards the resolution of the problem statement is done. The second players in the 'people' component are the Network users and Hackers. Hackers are intruders, and unwanted users. The Network users are lecturers, secretaries and students. They are the ones that want a secure platform of access and security of conversation within the network. Hackers gain access through several methods, to mention a few: Denial of Service, Trojan Horse, Trap door, man-in-the-middle, Snooping, etc. The network was built to lock out this player in the 'people' component and grant controlled and maximum access to the network user.

4.2 Knowledge process

Process includes standards for knowledge sharing, creation, testing of knowledge shared or recreated, refinement and application of knowledge, methods of documenting best-practices, storing and re-use of applied knowledge [11]. The 'process' component is the authentication, access control, and Encryption. Only authorized users have access and can send messages on the network. The server has a database that stores the basic login information of all users, permitting entry as shown in Fig. 8.

Fig. 8. The 'Process' flow representation

4.3 Technology

Technology connects people with people and information [12]. It provides the platform of operation of knowledge-sharing and the experience associated with it [10]. Though crucial, it only aids knowledge transfer and it can be applied appropriately to an organization's people and process. The 'Technology' component, in this case, is Java. Java is an open-source, object-oriented, platform-independent, and secured programming language [13]. One major advantage of Java is its *Platform neutrality*. Java programs are compiled into a format called *bytecode* that is run by any operating system (OS) software or device with a Java interpreter.

5 Conclusion

Communication network security is achievable with the use of layered approaches. Basic tests revealed that the system database undergoes a thorough check to authenticate a user and give access to available resources on the server. The authentication process ensures that if there is an attack that compromises or bypasses one security layer it is detected and blocked by another. This project implements information security as risk management issue; as such information security is an on-going basis since complete risk avoidance is impossible. The project can further be enhanced with biometrics such as fingerprints, iris and facial identification system in other to provide a proficient and robust security system. Communication Security System is a Knowledge Management tool; it obtains information of users, attaches a unique identification to each user. This identification is stored and can be queried at every entry into the network.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Rus I, Lindvall M. Guest editors' introduction: Knowledge management in software engineering. IEEE Soft. 2005;19:26-38.

[2] Ghelase D, Daschievici L, Epureanu A. Knowledge management in mechanical engineering. Proc Wor Cong on Eng; 2011.

[3] Nortel Network. Application-layer security: Enabling the next generation of security. White Paper, Nortel Network; 2005.

[4] Homeland Security. Wireless communication security: Awareness guide; 2003.
Available: www.safecomprogram.gov (Assessed 25 May 2015).

[5] Committee on National Security Systems. National Information Assurance (IA) Glossary. 2010;CNSSI-4009.

[6] Caravan JE. The fundamentals of network security. Boston: Artech House; 2001.

[7] Smith S, Marchesini J. The craft of system security. Boston: Pearson Education; 2007.

[8] Victek J, Bokowski B. Confined type in Java software practical and Experiment. 2000;2.

[9] Welling L, Thomson L. PHP and MySQL web development. Indiana; 2001. Sams Publishing.

[10] Bhojaraju G. Knowledge management: Why do we need if for corporates. Malaysian Journal of Library & Information Science. 2005;10:37-50.

[11] Gillingham H, Roberts B. Implementing knowledge management: A practical approach. J Knowl Manag Pract. 2006;7.

[12] Servin G, De Brun C. ABC of knowledge management. NHS Nat Lib Health; 2005.

[13] Cadenhead R, Lemay L. Teach Yourself Java 6 in 21 days. Indiana: Sams Publishing; 2007.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://sciencedomain.org/review-history/12833