

Knowledge Management Perspective In Communication Security System

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).

1.0. 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 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 (Rus and Lindvall, 2002). 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 (Ghelase *et al.*, 2011).

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 (Nortel network, 2005). 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.

2.0 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 (Homeland Security, 2003). 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 (Homeland Security, 2003; CNSSI-4009, 2010). CSS generally includes four components: physical security, network security, communication security, and administrative security. Figure 1, was described by Caravan (2001), protection, detection and response are security indices of an organisation.

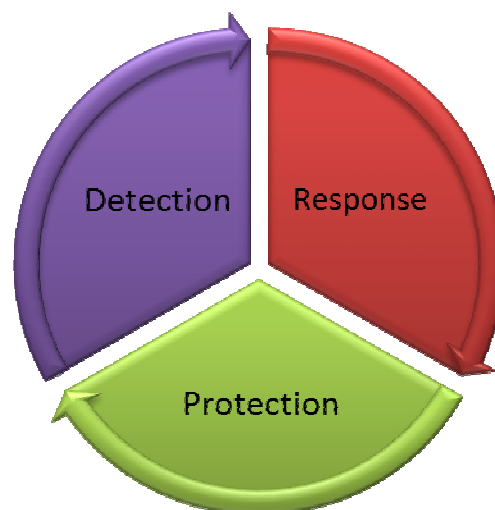


Figure 1: The Security Indices (Caravan, 2001)

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 (Smith and Marchesini, 2007). 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. Figure 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).

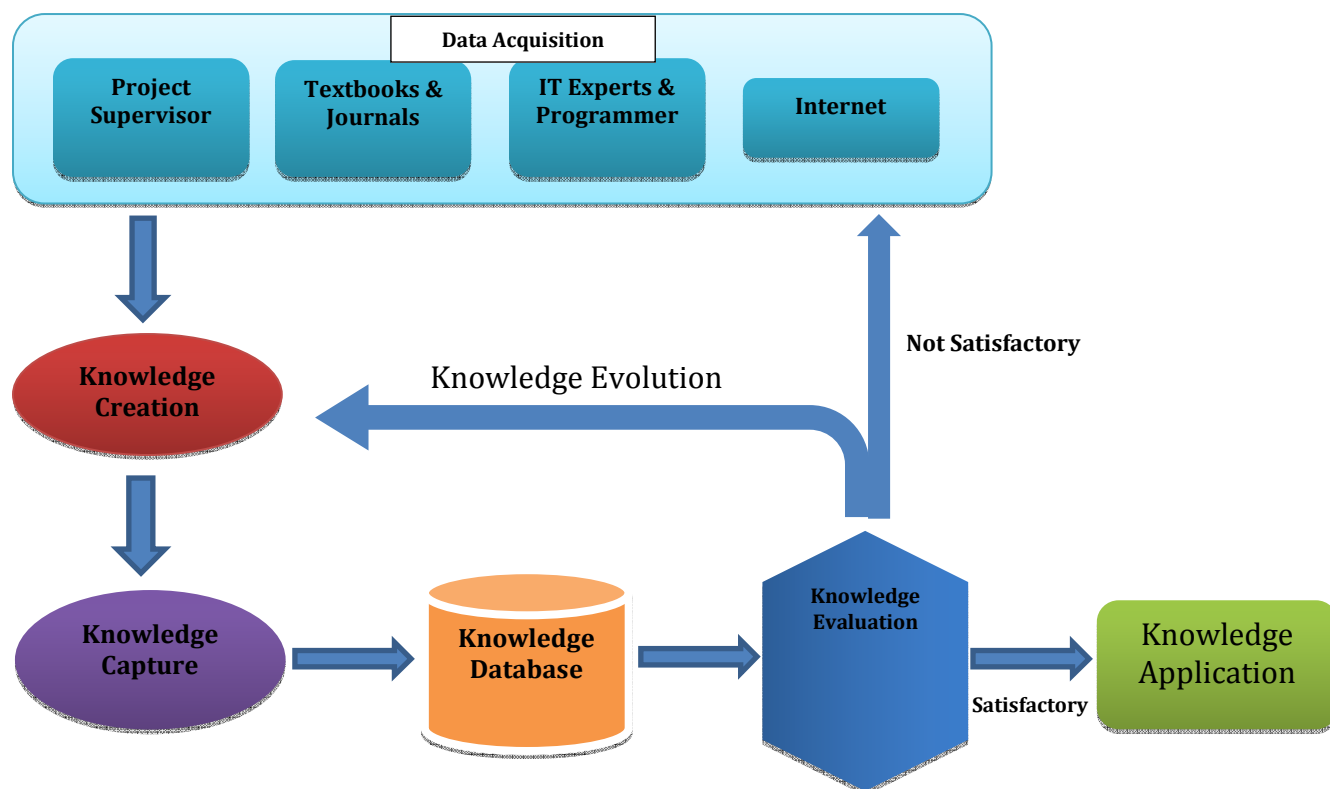


Figure 2: The Knowledge Acquisition Flow

3.0 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 (Victek and Bokowski, 2000), and MySQL—a multi-user, multi-threaded, structured query language—as query language. The performance and retrieval robustness of MySQL has been noted in Welling and Thomson (2001). 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.

Figure 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.

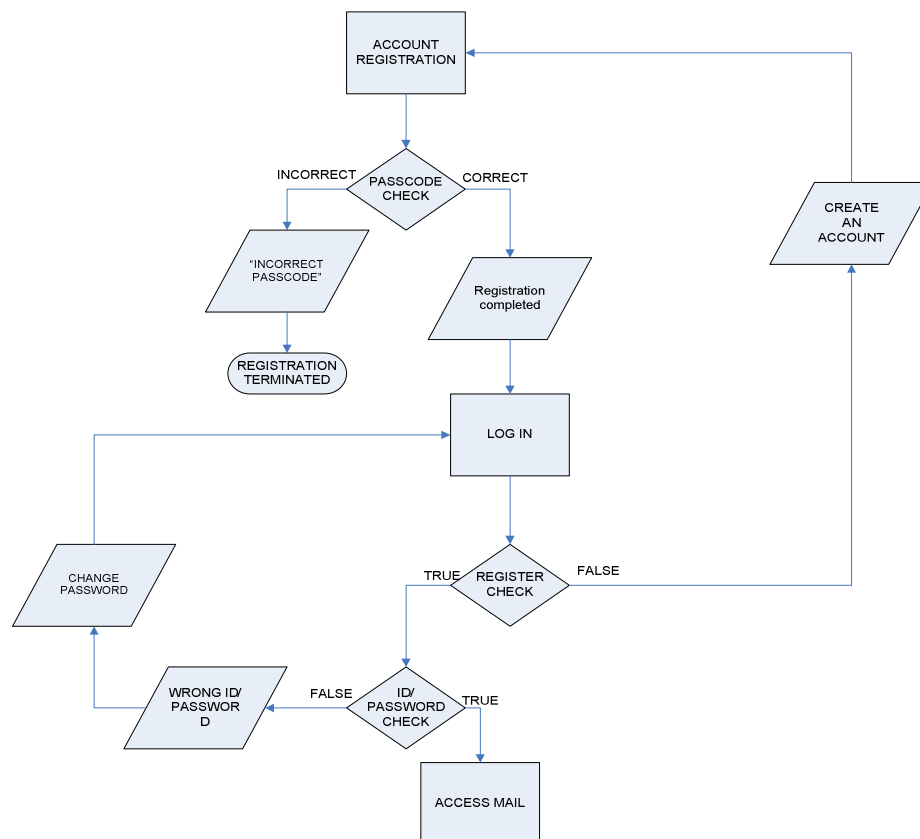


Figure 3: Flowchart of user security check procedures.

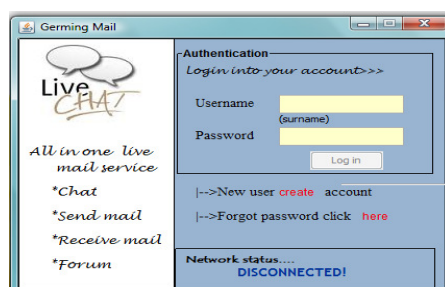
A number of API frameworks were developed which improved on existing Java programs using a layered approach to network security. A brief description of these applications is follows.

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

113 gives an overview of what can be done on the network, and when the network is
 114 connected or disconnected (shown in **Figure 4**), as well as providing a medium of
 115 performing authentication and identification on the server. For the process of
 116 authentication, a user must definitely be registered and any time such a user logs in, the
 117 server authenticates by checking the database for such a user, if found,
 118 permission/access is granted.

119



120

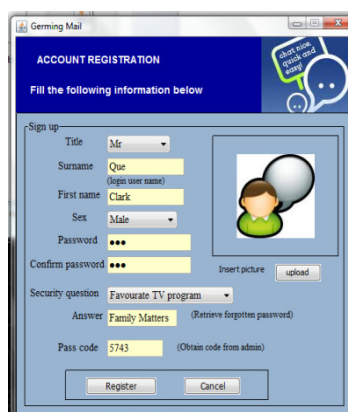
Figure 4: Login Interface

121

122

123 3.1.2 Account Registration and Mail Service Interface

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



129

Figure 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 Figure 6).

Table 1: Encrypted Message

Message Sent	Encrypted Message
How’re you doing?	JkBayFKsTcexWY6+EBiNlrmXgWuhozmi

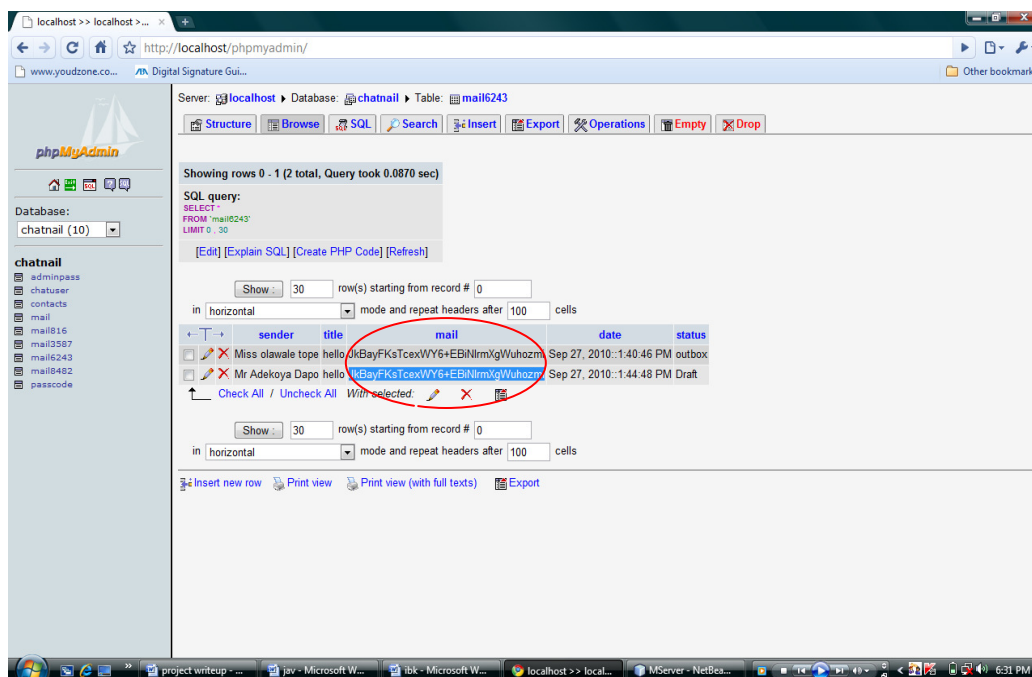


Figure 6: Encrypted mails

4.0 Knowledge Management (KM) Concept and Communication Security System

174 4.1 People

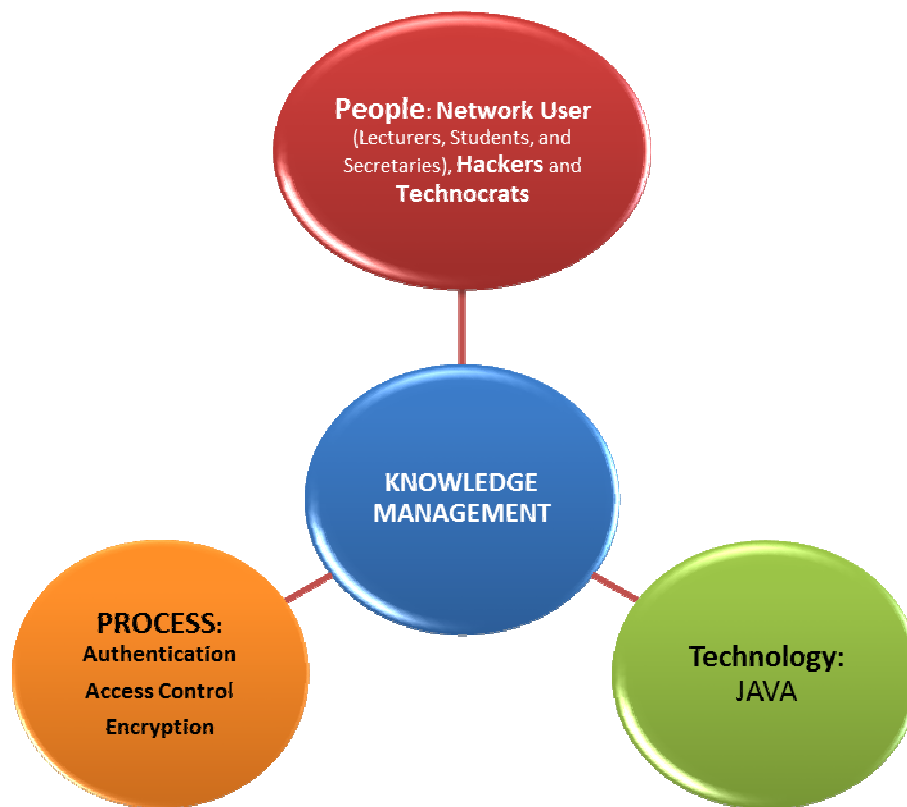
175 The 'people' component is the greater challenge of organizations or groups or any
 176 individual implementing knowledge management (Bhojaraju, 2005). Gillingham and
 177 Roberts, (2006) noted that it is the complex component to work with. In relating KM to
 178 CSS, the 'people' component can be divided into two;

179

180 (i) tacit knowledge carrier (Technocrats And Hackers) and,

181 (ii) network users, as shown in Figure 7.

182



183

184 **Figure 7: The Knowledge Management Triad**

185 The knowledge carriers are the programmers, supervisor(s) and network security
 186 expert(s). These knowledge-handlers form a major part of the 'people' component.
 187 Their views, experience, and information help to correctly understand, draft, model and
 188 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 (Bhojaraju, 2005). 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 figure 8.

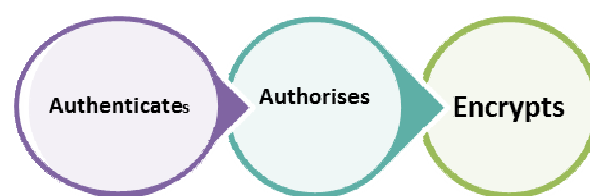


Figure 8: The 'Process' flow representation

4.3 Technology

Technology connects people with people and information (Servin and De Bruns, 2005). It provides the platform of operation of knowledge-sharing and the experience

associated with it (Bhojaraju, 2005). 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 (Cadenhead and Lemay, 2007). 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.

5.0 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 a risk management issue; as such information security is an ongoing basis since complete risk avoidance is impossible. 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.

REFERENCES

- BHOJARAJU, G. (2005) *Knowledge management: why do we need it for corporates*. Malaysian Journal of Library & Information Science, 10, 37-50.
- CADENHEAD, R and LEMAY, L. (2007). *Teach Yourself Java 6 in 21 days*, Indiana, Sams Publishing.
- CANAVAN, J.E. (2001). *The Fundamentals of Network Security*, Boston, Artech House
- USC, S. 3502. *CNSSI-4009*

- 237 GHELASE, D., DASCHIEVICI, L. and EPUREANU, A. (2011). *Knowledge management in*
238 *Mechanical Engineering*. In: Proceedings of the World Congress on Engineering.
- 239 GILLINGHAM, H. and ROBERTS, B. (2006). *Implementing knowledge management: a*
240 *practical approach*. Journal of Knowledge Management Practice, 7.
- 241 HOMELAND SECURITY, (2003) *Wireless communication security: awareness guide*, white
242 paper, www.safecomprogram.gov cited 25th May, 2015.
- 243 KLASSON, K. (1999). *Managing knowledge for advantage: content and collaboration*
244 *technologies*. The Cambridge Information Network Journal, 1, 33-41.
- 245 NORTEL NETWORK, (2005). *Application-layer security: Enabling the Next Generation of*
246 *Security*. White Paper, Nortel Network.
- 247 RUS, I. and LINDVALL, M. (2005). *Guest editors' introduction: Knowledge management in*
248 *software engineering*. IEEE software, 19, 26-38.
- 249 SERVIN, G. and DE BRUN, C. (2005). *ABC of knowledge management*. NHS National
250 Library for Health: Specialist Library.
- 251 SMITH, S. and MARCHESINI, J. (2007). *The Craft of System Security*. Pearson Education.
- 252 VICTEK, J and BOKOWSKI, B. (2000). *Confined type in Java software practical and*
253 *Experiment*. 2.
- 254 WELLING, L. and THOMSON, L. (2001). *PHP and MySQL Web Development*, Indiana,
255 Sams Publishing.