IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Information Systems Security: A Survey Of Access Control Measures In Universities In Kenya

Authors

(1)Dr. Charles Ochieng' Oguk: Rongo University / ogukcharles@gmail.com
2) Stephen Ochieng' Oguta: Kisii University / makoguta@gmail.com

Abstract

In many institutions, information system is essential for ensuring efficiency in operations and accountability in financial operations. Access limitations into information communication systems - ICT in organizations has been found in various studies to contribute immensely to management of information systems security. Nonetheless, studies focusing on prominence of access control components in university and their levels of implementation in universities are still insufficient. This study was conducted in universities in Kenya, with the main objective of investigating the levels of implementation of key aspects of access control. Smith's sampling formula was employed to get a sample of 91 respondents. Questionnaires were used for data collection from staff members who were mainly section heads of user departments and information systems' administrators. The data analysis produced statistical values needed to address the main objective. Results showed that while some features of access control are fairly implemented within universities in Kenya, many features are inadequately adopted. Therefore, it is recommended that universities fully implement access control measures for better security of information systems in universities. The study also recommends that information systems security policies should include key features of access control.

Keywords: access control, computer user-groups, data encryption, information systems security, user priviledge and network security.

Introduction

Shelc (2015) defines access control as the limitation of entry into an information system to only the authorized persons, in order to safeguard the confidentiality, integrity and availability of information systems. In the US, university in Texas had student information system compromised by malicious hackers using brute force attack exposing more than 55,000 names, e-mail addresses and Social Security numbers of faculty members and students. The institutions' authorities admitted that the situation could have been avoided even through ordinary and basic security precautions, like IT security metrics based on monitoring access control functionalities. In the year 2013, another university reported that two students faced charges for allegedly breaching the school's computer system security and awarded themselves and other

50 student’s better grades through recording keystrokes made by instructors as they logged into the system. The discussions above confirm that access control is so important to IT security management that its features ought to be included in the development of IT security management matrices.

Makori (2013) indicated that insiders have breached system access controls for information systems in the universities thus gaining unpermitted access. In Kenya, physical access control in a university’s computer laboratory was breached and at least two desktops went missing in the year 2013. Also, in another university in Kenya, students compromised access control of the student’s management information systems' security in the year 2011. According to Mulwa (2012), the features of access control that constitute its building blocks are: control access from external networks, web content filtration, control of access form internal networks, well configured active directory and user-group boundaries. However, other researchers' perspectives on this includes; user privileges and physical access limitations.

Statement of the Problem

While key areas of consideration for adopting access control for safeguarding information systems have been fairly highlighted, little focus has been directed on the extent to which these measures have been implemented, especially within universities in Kenya. This is the main purpose of this research study.

Objective

The objective of the study was mainly to assess the levels of implementation of various access control measures within universities in Kenya.

Literature Review

According to Shelc (2015), access control is the limitation of entry into an information system only to the authorized persons, using either physical or logical means, as a way of ensuring systems security. Access control is necessary within university's information systems security program to enhance confidentiality, integrity and availability of information resources.

Chan and Mubarak (2012) conducted an explorative study to directly investigate the levels of employee awareness on access control systems within a Higher Education Institution in South Australia. The study showed that the awareness among the employees was generally poor. There was lack of knowledge of information security concepts on physical access control in the institution, as well as very low levels of awareness on logical access control practices. It however attributed the low level employment of access control facilities to weak policies, especially on IT security. This implies that for the security benefits of the established systems' access control to be realized, there should be strong implementation of IT security policies to make access control more effective.

Human factors must be considered as playing major role in computer hardware availability and general security of all the organizational computer hardware, (Bajaj & Sion 2014). Since the human factors on information security may be deliberate or non-intentional, there are inherent human weaknesses that may lead to serious harm to the organization's information systems. In ensuring better information security, control of access by employee into information systems can be a major tool that if exploited can yield much in overcoming the inherent human weaknesses, (Evtyushkin et al., 2014). Eschelbeck and Villa (2003); Audebert and Le Saint (2002); Delimitrou and Kozyrakis (2014), & Ahlgren et al. (2012) explained that people who are involved in the systems operations constitute major factors that play significant roles in breaching information systems' security and should be controlled using suitable access control approaches. Bellare, Keelveedhi, and Ristenpart (2013) agreed with this and indicated that people are the weakest point in information security set-up, as they would try to exploit privilege escalation and access unauthorized parts of the network.

Dua, Raja, and Kakadia (2014) debated that since the characteristic behavior of the systems' users and administrators impacts information systems' security, access into the systems by users should be controlled in user-groups, web content filtration and active directory. It analyzed that well configured active directory and user-group create limiting access boundaries which could improve effectiveness of information systems' security management within universities. However, Bisong and Rahman, (2011) argued that some institutions apply user access control guidelines without involving the people from early stages of implementation, which evokes resistance and obstructs information access control technologies' implementation. Delimitrou and Kozyrakis (2014), agreed with Bisong and Rahman on resistance to implementation of access control, arguing that apart from opposition posed by the uses, access control slows down service delivery by restrictive users' access to production systems.

Colombier and Bossuet (2014) showed that employees' access control should be considered as they are often the weakest link in the protection systems of its information systems' assets, as the damages they cause are related to their levels of disgruntlement. Brickell et al. (2011) indicated that information security has been affected by users who share their access passwords contrary to the provided safe computing guidelines, hence exposing the entire information systems to vulnerability. Proper mechanisms need to be presented at every institution in order to identify the most common human factors and also the major associated attacks that threaten computer security.

Kamerman, Monteban and Mud (2000) stressed the need for access control on personal email through an organizations' network, and explained that the access to such emails prompts users to open risky mails, which opens way for spamming, spying and virus injection into the organizational computer network. The study argued that use of portable devices to transfer data from one computer to another could be a dangerous behavior as it propagates the spread of malware. Fernandes et al., (2014) supported the argument and recommended limitation of access by workers to the institutional networks to ensure better IT security management.

In a different perspective, the construct of dissatisfaction among workers at the work - place has been observed to directly relate to major information systems' security breaches in organizations. Therefore, imposing access control on system users can protect the institutions' IT systems in case of staff disgruntlement (Gibson & Van 2000). This includes the disgruntled employees, who out of anger may vandalize the physical information systems for self gratification reasons. Users' disgruntlement could be about dissatisfaction with the organization, superiors, colleagues or situation and should be a factor to be considered in the access control programs. Nevertheless, Gibson and Van further argued that the institutions' information systems could be more harmed, if the disgruntled staff is a senior IT administrator in charge of all systems password allocation and control. Moreover, Gleichauf, Teal and Wiley (2002) identified lack of access control from external networks as among the possible causes for high security risks in information systems. The identification corresponded with Gubbi et al (2013), which showed that inadequate access control from both internal and external networks is a major contributor to information systems' integrity breaches.

In Uganda, studies showed that apart from harmful practices associated with disgruntled staff members on information security, there are other practices which are associated with system administrators, and which also expose information systems to danger. Kancharla and Manapragada (2014) showed that such administrative roles which could create security vulnerability o information systems include lack of regular software patches and updates, uncontrolled access to suspicious hyperlinks, encouraged password loans and encouragement of the use of very weak and easy to guess systems access passwords are major challenges in implementing successful access control. A study by Deloitte East Africa (2011) indicates that insiders present a higher information security threat to east African businesses than outsiders, as the insiders more easily breach the internal access controls. The study showed that information-rich networks found in universities have raised increased appetite for attacks upon university information security infrastructures both from within and outside the organizations, justifying the need for strict access control systems. It argued that insiders are likely to have knowledge of critical data and their locations within the organizations' information network, password for systems access; hence they could gain easy access to unauthorized areas. Also O'Flynn and Chen (2014) concurred with Deloitte, and showed statistical correlation between systems attacks from external sources and the insider activities on information systems.

Ope (2014) studied the IT security situation in universities in Kenya and found that inadequate provision of physical access control was one of the major barriers to information security in the Kenyan public universities. This was attributed, not only to inadequate access control facilities, but also to lack of awareness among IT administrators about the required physical access control and the exact levels of the physical access control that were already installed within the universities. The conclusion made in this case was that the importance of physical security controls around IT systems is given little priority within the universities. The study further concurred with Mulwa (2012), that access control as an IT security element should be composed of: According to the features of access control that constitute its building blocks are: control access from external networks, web content filtration, control of access form internal networks, well configured active directory and user-group boundaries.

While the studies stressed the need for both logical and physical access control for secure IT infrastructure, and the need for increased awareness among IT staff members on physical and logical security access controls, the study did not involve the levels to which access control features have been implemented in the various institutions.

Research Method

This study was exploratory in nature, wherein both qualitative and quantitative approaches were employed. Qualitative approach described the results in terms of effectiveness of implementation, while quantitative approach adopted percentage and ratio values for the analyzed data.

Sampling Procedure

Multiple sampling procedures were applied including: Smith's sampling formula, stratified sampling, ten percent sampling and purposive sampling. Since the users and administrators of infromation systems in all the universities in Kenya is not distinct, Smith's formula was applied as:

Smith's sampling formula

$$n_0 = \frac{Z^2 \sigma^2}{e^2}$$

……………………………………..Smith

Where:

n_0 is the sample size,

z is the abscissa of the normal curve that cuts off an area a at the tails given by 1.64

e is the desired level of precision given by 0.05

□□ is the variance of an attribute in the population given by 0.291.

$$n_0 = \frac{1.64^2 \text{ x } 0.291^2}{0.05^2} = 91.103 \text{ respondents}$$

Therefore, a sample size of 91 respondents (since there is no fraction of human being) was used.

Stratified sampling

The universities were grouped into two main stata as public and private univesities. This was due to the need for collecting data on IT security elements and IT security measurements from the two main categories of universities in Kenya. As at the year 2018, there were 37 private universities and 33 public universities according to commision for university education, (CUE, 2015)

Simple Random Sampling

With regards to the thirteen (13) operation areaswhich are: IT leadership, systems administration, network administration, security administration, database administration, students' finance, student’s registration, examinations, human resources, internal audit, library, computer, laboratory, and student leadership; and applying ten percent on the 70 universities, (13x7=91), which is coincidentally equivalent to the Smith's sample size above. Since the universities under each strata were considered homogenous from the perspective of implementation of IT security elements, random sampling was applied.

The Purposive Sampling

Since not every staff member in the entire university work force deals with information systems, there was a need to concentrate on the employees who directly work with university information systems, as this gave reliable data. In this study, users and administrators of IT systems were considered to be richer in information needed for the study, especially, in IT security experience and data desired by the researchers, who employed purposive sampling for the various categories of employees (who interacted daily with IT systems, and were possible victims of IT security breaches) in each university, to get reliable responses. Pirzadeh (2011) highlighted operation areas in IT administration as basically areas as IT department leadership, network section, database section, IT security, system administration as the major IT operation areas for IT administration.

Research Instruments and Data analysis

Structured questionnaires were adopted in this study as the primary instrument for data collection. In addition, interview schedule was conducted to collect information from ICT leaders in the various universities. The researcher used two sets of questionnaire which were divided into two sections, with the first part designed to give a brief introduction of the purpose for data collection. The second section was seeking to collect data on the variables adopted for the study. The questionnaires used in this study contained both the closed-ended and open ended questions. The closed ended questions helped collect observations and opinions of the respondents regarding the elements of IT security. The open-ended questions would facilitate freedom of response thus gathering diverse opinion from the respondents as well. According to Graveter and Forzano (2003), questionnaires are recommended for survey because they allow researchers to collect data from a large number of respondents and also provide for an ease of investigation through accumulation of data. In this study, survey was used to collect data on the implementation levels of IT security elements and metrics from the university users and administrators of information systems. Data was analyzed using SPSS and Microsoft Excel to yield various frequency values for the study.

Results and Discussion

This study found that 92 percent of the respondents showed that there is system's controlled password expiry within the universities as shown in below. It also found that bio-metrics and access control cards are rare authentication methods used in the universities to control access into the universities' server rooms. Only 12 percent showed that they use access control cards while 41.7 percent of the respondents indicated the use of bi-metrics to access university server rooms as only 16 percent incorporate the use of access passwords in the authentication.

Access control mechanism applied

	No	Yes
System controlled password	8	92
Bio-Metrics authentication	58.3	41.7
Access Control Cards authentication	88	12
Mixed / Combinations with passwords authentication	84	16

The study further found out that most universities still rely on physical access control mechanisms like the grills and physical locks to control access into the server rooms. Table 4.7 below shows that only 28 percent of the universities use system based authentication method. 72 percent of the respondents still use physical intervention approaches to control access into the server rooms.

Nature of authentication used to access server room

Response	Percentage
System Based	28.0
Physical	72.0
Total	**100.0**

The use of portable external storage media contributes so much to malware transfer from one computer system to another, and could be a major concern for data security within universities, Ismail and Zainab (2011). This study found that use of portable devices remains un-controlled within 48.9 percent of the universities in Kenya. Access to the university server room is much restricted in the universities, as 60 percent of the respondents indicated that it is very difficult, as over 90 of the respondents showing that it is difficult. Only 47 percent of the universities operate on encrypted files and folders, while 53 percent do not. Encryption protects data files from unauthorized access.

The problem of un-managed university network is further shown in the study by the revelation that 56 percent of the universities have not effectively configured the active directories. In some universities, windows server operating systems exist, yet the security features like active directories have never been activated. Activation of this computing feature infuses access restriction in terms of various domains including network sections, computers and time restrains for access. Further, over 82 percent of the universities have well controlled user groups with members restricted to given access privileges. Besides, access to given internet sites from the university local area network is restricted in over 75 percent of the universities.

It was found that 60 percent of the universities do not effectively control access from external networks while only 32 percent are controlling the access from internal threats effectively. 60 percent of the respondents do not effectively implement web-content filtration, meaning access to any universal resource locators (URLs) is not restricted in such universities. This is a security threat as the uncontrolled access may encourage social engineering and spam injection into the university information systems.

The study found that 52 percent of the university networks are still not segmented, meaning users can still access resources freely from any part of the network, without restrictions. For universities with security appliances, 72 percent have not effectively conducted penetration testing, thus are not aware of the effectiveness of the security appliances employed. 56 percent of the universities do not have effective tools for internet bandwidth management. If the entire internet bandwidth drop in a university's local area network cannot be managed, it could be a sign of misused bandwidth resource and risky access to cortical data.

Conclusion, Recommendations and Further Research

This study found that system access control is a very important element of information technology security management. While some key aspects of access control are well implemented, many features still remain poorly implemented. This finding concurs with Shelc (2015) which defined access control as the limitation of entry into an information system to only the authorized persons, in order to safeguard the confidentiality, integrity and availability. The study recommends that access control measures should be implemented fully to ensure better security for information systems, since most of the elements of access control are poorly implemented. There is a need therefore, to study factors contributing to poor implementation of access control within the universities.

References

Audebert, Y., & Le Saint, E. (2002). *U.S. Patent Application No. 10/085,127*.
Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., & Ohlman, B. (2012). A survey of information- centric networking. *IEEE Communications Magazine*, *50*(7).

Bisong, A., & Rahman, M. (2011). An overview of the security concerns in enterprise cloud computing. *arXiv preprint arXiv:1101.5613*.
cluster management. In *ACM SIGPLAN Notices* (Vol. 49, No. 4, pp. 127-144). ACM.

Brickell, E. F., Hall, C. D., Cihula, J. F., & Uhlig, R. (2011). *U.S. Patent No. 7,908,653*. Washington, DC: U.S. Patent and Trademark Office.

Delimitrou, C., & Kozyrakis, C. (2014, February). Quasar: resource-efficient and QoS-aware

Dua, R., Raja, A. R., & Kakadia, D. (2014, March). Virtualization vs containerization to support paas. In *Cloud Engineering (IC2E), 2014 IEEE International Conference on* (pp. 610- 614). IEEE.

Colombier, B., & Bossuet, L. (2014). Survey of hardware protection of design data for integrated circuits and intellectual properties. *IET Computers & Digital Techniques*, *8*(6), 274-287.

Eschelbeck, G., & Villa, A. (2003). *U.S. Patent No. 6,611,869*. Washington, DC: U.S. Patent and Trademark Office.

Gravetter, F. J., & Forzano, L. A. B. (2003). *Research methods for the behavioral sciences*. Thomson.

Ismail, R., & Zainab, A. N. (2013). Information systems security in special and public libraries: an assessment of status. *arXiv preprint arXiv:1301.5386*.

Makori, E. (2013). Adoption of radio frequency identification technology in university libraries: A Kenyan perspective. *The Electronic Library*, *31*(2), 208-216.
Nyamongo, D. M. (2012). *Information systems security management* (Doctoral dissertation, Strathmore University).
Mang'ira, R., & Andrew, K. (2014). Towards establishment of a full-fledged disaster management department for Moi University libraries.

Mulwa, A. S. (2012). The influence of institutional and human factors on readiness to adopt E-Learning in Kenya: The case of secondary schools in Kitui district. *An unpublished PhD thesis of the University of Nairobi*.

Ndung'u, P. W., & Kyalo, J. K. (2015). An evaluation of enterprise resource planning systems implementation experiences for selected Public Universities in Kenya.

O’Flynn, C., & Chen, Z. D. (2014). Chipwhisperer: An open-source platform for hardware embedded security research. In *International Workshop on Constructive Side-Channel Analysis and Secure Design* (pp. 243-260). Springer, Cham.

Ope, J. O. (2014). An information systems security framework for Kenyan public universities (Doctoral dissertation, University of Nairobi).

Shelc, R. (2015). Authorized Access and the Challenges of Health Information Systems.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.

Tarus, J. K., Gichoya, D., & Muumbo, A. (2015). “Challenges of implementing e-learning in Kenya: A case of Kenyan public universities”. *The International Review of Research in Open and Distributed Learning*, 16(1).

Tongco, M. D. C. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Research and applications*, *5*, 147-158.

Ope, J. O. (2014). An information systems security framework for Kenyan public universities (Doctoral dissertation, University of Nairobi).

O’Flynn, C., & Chen, Z. D. (2014). Chipwhisperer: An open-source platform for hardware embedded security research. In *International Workshop on Constructive Side-Channel Analysis and Secure Design* (pp. 243-260). Springer, Cham.

Mulwa, A. S. (2012). The influence of institutional and human factors on readiness to adopt E-Learning in Kenya: The case of secondary schools in Kitui district. *An unpublished PhD thesis of the University of Nairobi*.

Ope, J. O. (2014). An information systems security framework for Kenyan public universities (Doctoral dissertation, University of Nairobi).

O’Flynn, C., & Chen, Z. D. (2014). Chipwhisperer: An open-source platform for hardware embedded security research. In *International Workshop on Constructive Side-Channel Analysis and Secure Design* (pp. 243-260). Springer, Cham.

Mulwa, A. S. (2012). The influence of institutional and human factors on readiness to adopt E-Learning in Kenya: The case of secondary schools in Kitui district. *An unpublished PhD thesis of the University of Nairobi*.

Deloitte, L. L. P. (2011). Mobile telephony and taxation in Kenya. *Nairobi: Deloitte LLP*.

Kancharla, P., & Manapragada, R. K. (2014). *U.S. Patent Application No. 14/299,739*.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645- 1660.

Gleichauf, R. E., Teal, D. M., & Wiley, K. L. (2002). *U.S. Patent No. 6,499,107*. Washington, DC: U.S. Patent and Trademark Office.

Gibson, G. A., & Van Meter, R. (2000). Network attached storage architecture. *Communications of the ACM*, *43*(11), 37-45.

Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security*, *13*(2), 113-170.

Gleichauf, R. E., Teal, D. M., & Wiley, K. L. (2002). *U.S. Patent No. 6,499,107*. Washington, DC: U.S. Patent and Trademark Office.

Gibson, G. A., & Van Meter, R. (2000). Network attached storage architecture. *Communications of the ACM*, *43*(11), 37-45.

Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security*, *13*(2), 113-170.

Kamerman, A., Monteban, L., & Mud, R. (2000). *U.S. Patent No. 6,067,291*. Washington, DC: U.S. Patent and Trademark Office.