Security Requirements, Analysis and Policy Formulation for Educational Institutions

Peter Okpamen

Ambrose Alli University,
Ekpoma-Edo State,Nigeria

Doi:10.5901/jesr.2013.v3n5p93

Abstract

This project is a design implementation of Security requirements, analysis, and policy formulation of Educational Systems. Security of Information Systems in Educational institutions therefore concentrates on the collective efforts of all institutions to produce markedly secured Information systems to help deal with the threat or problems of Identity management within and outside the institution. Identity Management (IDM)" refers to the analysis of procedures of utilizing technologies, models/methods, standards/mechanisms in order to manage essential information in the institution's network about the identity of all users, and control access to School's resources. In this project, apart from the design implementation and analysis, emphasis was also placed on the Identity Management(IDM), which guarantees the Identity and Integrity of every registered users in the Network in order to apply appropriate access policy, deliver visibility into Network activity, and secure the local, centralized, distributed, and web/globalizes management of remote devices, while providing Authentication, Authorization, and Accounting functionality across the institution's Network devices.

Keywords: *Security Requirements, Analysis, Policy, Educational Institutions.*

1. Introduction

This project is focused on a design of a security requirements, analysis, and policy formulation of educational institutions. The essence of this design is to enable school managers to design an appropriate security Network to guarantee the security of Information Systems in their establishments. In the course of the design, the following were taken into consideration: Assets in the school, the operations of each staff and student in terms of authentication and authorization policy; role allocation policy, and threat policy. The confidentiality policy, as well as the availability of the system was also of paramount importance to the design. In the course of the design, the researcher/designer placed emphasis on the threats to the security system in particular, such as access by unauthorised persons either by way of identity theft such as obtaining someone else's password, and attempting to alter information that could create serious crisis in the institution; as well as the integrity of the designed security system. In view of this development, the design was built on the premise that Identity management is a key to the implementation design.

2. Challenges of Security Systems

The performance of any security system in any organization depends highly on the level of care put in place during the design. Security of Information Systems has therefore culminated into tough web of technology concepts and standards. And there seems to be no end in sight in terms of standard or consistency, not even a single organization. At the moment the issue appears to be beyond software and system users. The errors are only discovered only after the damage has been done to the system. “The only true security system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards-and even then there are still doubts”-(Gene Spafford 2007 : 291). ISO 27001, an information security management standard and certification program; encompasses a set of information security requirements and it helps to reassures customers, employees, and suppliers that information security is of paramount importance for the organization. The organization on its part owes it a point of duty to establish a standard security system to deal with information security threats and issues. Accordingly, ISO27001 is deeply associated to all classes of organizations, and is generally applied for certification purposes. Once the organization meets the standard of ISO 27001 requirements, the security features is often certified by an external registrar. Broadly speaking, a lot of IT managers do not have the required coherent framework and genuine methodology for achieving enterprise security. A security plan that includes technology, personnel, and policies would be a much better approach to developing an organization security strategy (Hazari, 2005). Essentially, the building of a security model requires a clear understanding of the security functional requirements of the organization, and a standard security policy strategy (FIP Standard, 2004; FIP Standard, 2006). Accordingly, the literature suggests that different levels were adopted by researchers to examine access control requirements. Foremost in their approach is the threat analysis-based approach; and it has been found to be very essential as studied intensively by researchers (Debar et al., 2006; Thomson and Von Solms, 1998; Whitman, 2004). The second approach is the evaluation-criteria based. The emergence of this approach over time gained immense popularity among researchers. And this framework has also been adopted by the US department of defence; as well as the European Union. As a result of this development, it is widely known as the common criteria (ISO/IEC, 20050). Accordingly, this school of thought have recommended that this become a basis for every security model. However, to formally evaluate any security system, an evaluation methodology with a set of security requirements is required in order to define the functionality of the security system. Adequate care for the existing technology expertise may well overwhelm an information company, irrespective of position and size. The bottom line therefore should be a regular assessment of risk in order to ensure that the goal of achieving organizational security is not a mirage.

3. Methodology

3.1 Assets in Educational System:

This section contains sample representations of personal details of staff and students, unit registered (u), examination marks (u), financial information and degree registered by the students.

Table 1: Personal detail of Students

Student-ID	First Name	Last Name	D-O-B	Gender	Address	Post Code
7096	Peter	John	20-03-88	Male	50 Shelly Road	E6 3AL
7084	Allwin	Dixit	07-03-89	Male	63 Stratford Road	4L CFR
8124	Lizzy	Harris	14-05-87	Female	75 London Road	SE6 1XX

Location	Email Address	Year of Entry	Expected Year of Graduation
London	peter@yahoo.com	2008	2012
Manchester	Allin@yahoo.com	2008	2012
London	Liz@yahoo.com	2007	2011
Liverpool	Dani@yahoo.com	2007	2011

The above table contain records of the full details of the individual student in the school. The attributes are: Name of Student, Student number, Date of Birth, Gender, Permanent home address, E-mail address, Year of entry and Expected year of graduation.

Table 2: Personal Details of Staff

Staff-ID	First Name	Last Name	D-O-B	Gender	Address	Post code
24861	Michael	Macaulay	02-07-68	Male	45 Rumford Road	R6 6HG
244789	George	Ubakaman	18-06-65	Male	65 London Road	BU7 4S
24623	Ali	Ahmed	24-08-70	Male	75 Shelley Road	E7 8AK
24794	Paul	David	29-09-60	Male	65 Dixit Road	8DK WN

Location	Email Address	Date of Employment
London	Mac@yahoo.com	2001
Glasgow	Geal@yahoo.com	2000
Edinburgh	Ali@yahoo.com	1997
Liverpool	Paul@yahoo.com	1999

Above is the record containing the details of the individual staff in the institution. The attributes are: Name of Staff, Staff number, Date of Birth, Gender, Permanent home address, Email address, and year of employment.

Table 3: Unit register table

Student Identity	Unit Registered (u)
7076	Security
	Research Method
	Multimedia system

The table above is a sample representation of the various units registered with respect to (u); where (u) represents the different units registered by each student.

Table 4: Examination Marks

Student - ID	Examination Marks	Remarks
7056	Web Tech (65B), SPM (66B), Java (77A), DBM (60B)	Passed
7077	Web Tech (62B), SPM (45D), Java (39E), DBM (57C)	Failed
8045	Web Tech (56C), SPM (57C), Java (75A), DBM (56C)	Passed
8167	Web Tech (56C), SPM (89A), Java (77A), Business (65B)	Passed
7098	Web Tech (67B), Java (86A), SPM (56C), DBM (88A)	Passed
8125	Web Tech (61B), SPM (67B), Java (67B), ISM (66B)	Passed

The table above is a sample representation of the examination marks of the students showing details of letter grades and their respective remarks; Pass/Fail.

Table 5: Financial Information

Student Identity (ID)	Fees Paid	Balance	Remarks
7096	20/09/11 (£5,500), 12/12/11 (£3,400)	£1,300	Debtor
7195	13/09/11 (£5,200), 13/01/12 (£2,000)	£1,800	Debtor

8043	12/09/11 (£5,200), 18/01/12 (£2,000)	£600	Debtor
8124	25/09/11 (£8,900),	--	Paid in full

The table above is a sample representation of financial information with respect to fees payment with dates, balance of fees payment of each student in the school; coupled with the remarks on the financial status of the students.

Table 6: Degree Registered

Student Identity (ID)	Degree Registered	Duration of Study
7027	PhD (Management)	1 Year
7076	PhD (Business Administration)	2 Year
8021	PhD (Advanced Information Management)	2 Year
8043	PhD (Business Administration)	1 Year

The above table is a representation of the degree registered for by each student.

3.2 The Operations:

The operations determine the typical permit action(s) to be carried out by the individual in question. This can be seen from the access control matrix (ACM) table displayed below:

Table 7: Access Control Matrix

Asset↔ Roles↨	Details (id)	Unit Reg. (u)	Examinations/ Records (u)	Accounts Records	Degree Registered (c)
HOD	{view}	{view}	{view}	{view}	[view, edit}
Course Director (x)	{view, edit} If x=id	{view, register} If x=u	{view}	---	{view} If x=c
Unit Leader (y)	--	{view}	{view, edit} If y=u	---	{view]
IT-Man	{view}	{view}	{view}	---	--
Student (z)	{view, Edit If z=id	{view}		[view, edit}	{view}
Finance		{view}			{view}

From the table above, the view operation only permits the user to read through the source document, while the edit operation allows the user to write or make changes in the source document as required. However, while some persons can only perform one operation, some can perform both operations depending on their roles. Below is the sample representation of the operation policy.

Table 8: Illustration of ("View and Edit") Operation

HOD	View Degree Registered (C) (AIT) Cannot make changes	Edit Degree Registered (c) Make changes

Unit Leader (y)	View (Examination Marks) for security	Edit (Examination Marks) for (Security) If y=u, where y is the unit leader of security Unit.
Student (z)	View (Personal Details)	Edit; if z=id, then (make particular changes)

Table 9: Roles

User ID	Role	Description
Mark(s)	Head of Department	Attends to daily memo, preside over DBS meeting and appoints course directors.
Macaulay	Course Director	Allocates units, compile examination scores of students, attend to matters relating to the courses, etc,
Paul	Unit Leader	Teaching, Marking, and recording of scores, organize tutorials relating to the units, etc
Val	IT Manager	Supervises IT equipments, manage the database of employees, etc.

The role of every individual in the school is clearly spelt out as shown above.

4. Potential Threats to the Security System

Essentially, threats are those dangers associated to the various Assets, with respect to operations carried out. In dealing with threats, the first thing we do is to identify the various threats. Secondly, we have to find out the vulnerabilities of the system and ways to keep the threats from occurring. Basically, threats could be intentional or unintentional. An intentional threat involves a situation where someone purposely damage asset/property or information in the system. On the other hand, unintentional threats are associated to an unauthorized or accidental modification of software. For instance, someone using the system could accidentally delete an important file, or tripped over a power cord. The potential threats are within and outside the security system. As part of effort to protect the security system against threat, it was designed to provide confidentiality to every source document in terms of privacy. However, below is of the threats the security system was designed to handle:

- An influx of virus to the disk containing students' records,
- The incident of fire outbreak,
- Falsification of examination scores/statement of results, and
- Fake admission of students

4.1 Vulnerable Spots in the Security System:

In the security design, the possible vulnerability could either come from the operating system, or from the internet connection. The security system design is being run by an operating system. The consequence of this is that, should anyone have knowledge about the operating system, then he/she could be able to access the system and possibly exploit the weakness within it. In addition, because the security system is also connected to the internet, it is also susceptible to threats in this regard. Since the services are always on the internet, it makes it easy for anyone to find you and take your information and send you a virus.

However, the threat to privacy has been taken care of by the security system because of the in-built of pass-word hashing in the design. For instance, Mark (Head of Department) may be interested in editing a unit leader's marks in an examination. Obviously this is not possible because Mark does not have access to the hash pass-word of the unit leader.

Essentially, integrity involves any unauthorized change to information stored in a system. The integrity of the system is such that it is capable of preventing any attempt by unauthorized person to change examination Marks. For instance, if Head of Department (HOD) has access to (Unit Leader) username and password, it means he can in addition to viewing (Unit Leader') examination Marks of students; can also edit the scores as required. In terms of availability of the security system, the design makes it possible for individuals to have access to its usage any time of the day.

4.2 Preventive Measures:

i. Making sure that the system is frequently checked for security patches and update of dates in order to keep the system more secure,

ii. Purchasing a firewall and anti-virus programs that will have to keep the information safe from attack when connected to the internet for a long period of time.

iii. Being aware of the threats and vulnerability is a necessity towards making security system safer and secure.

iv. Knowing ahead of time just what could compromise your security information and becoming educated in ways of preventing these will make the system more prepared for any attack.

5. Authentication:

"This is a process of identifying an individual, usually based on a user name and password. In security system, Authentication is distinct from authorization which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he/she claims to be, but says nothing about the access rights of the individual." (Webopedia, 2007). Authentication is the process of determining whether someone or something is in fact, who or what it is declared to be. It is also a method of uniquely identifying a user. In private and public computer networks (including the internet), authentication is commonly done through the user of login passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user register initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The authentication table below contains a description of the username and password of each staff and students in the school. The username is unique in the sense that no two people must have same username to avoid a login error. The password is made up of characters not more than 10 digits. The essence of the authentication is to validate the correct user. The limitation of this is that, any person that has access to another person's username and password would be validated as the authentic user.

Table 10: User Authentication

Username	Password	Hashed
Mark	Spoon	@?/:@'&8g
Ali	Sunlight	*:<.>@{/?*&m49w

The above table is used to authenticate the user for login, interact with a personal username and its associated hash password. The purpose of authentication is to validate the identity of the user to ascertain whether he/she is qualified to carry out an operation. The table below is an illustration of authentication. In particular, the password of each student and staff are hashed for protection sake. The design is such that each time a student wants to authenticate, he/she first enters his password; while the system computes the hash password and compares with entry in the password file. If the hash password is the same, then the password is accepted and the user is authenticated.

6. Authorization

“This is a process of granting or denying access to network resources. Most computer security systems are based on a two step process. The first stage is authentication, which ensures that a user is who he or she claims to be. The second stage is authorization, which allows the user access to various resources based on the user’s identity” (Webopedia, 2007). Authorization is also the process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which person is allow to view or edit, hours of access, amount of allocated storage space, etc). Assuming that someone has logged-in to a computer operating system or application, the system or application may want to identify what resources the user can be given during the session. Thus, authorization is sometimes seen as both the preliminary setting up of permission by a system administrator and the actual checking of the permission values that have been set up when a user is getting access. As soon as the individual passes through the stage of authentication, the next step is the application of any given operation. The access control matrix presents a representation of each person in the school and the asset(s) he/she can access. The mode of operation here is either a View only or View and Edit happening same time. However, note that the View Operation only enables the user to Read only, and cannot make any changes. On the other hand, View and Edit allows the user to Read and make changes on existing information.

Table 12: Role Allocation

This table is an example of role allocation of two lecturers in the school. The full table containing the roles of individuals in the school is displayed in the appendix section.

User Identity	Roles
Chang	Course Director (ISM)/Unit Leader (JAVA)
Macaulay	Course Director (AIT)/Unit Leader (Multimedia)

For example, Professor Ali, a lecturer in the faculty of Business and Economics wants to check his roles in view of his course allocation for the semester. What he simply does is to type in his user ID and password. Similarly, same goes for two students in different departments, wishing to check their respective department.

7. Confidentiality

Basically, the essence of confidentiality is to protect the system and the user from unauthorized user having access to confidential information. Otherwise, it can go a long way to undermine the efficiency of the system. To prevent this act, the hashing password was designed in the security system. Any user whose hashed password doesn’t have a match with stored password cannot be authenticated, neither can he be authorized. Furthermore, examination scores are kept confidential from the reach of unauthorized persons. Examination question papers are also kept confidential in a place called “strong room”. For example: An attempt to change examination mark of Unit Leader (y); where y = Security Unit lecturer, by a student (z) is practically impossible because student (z) does not know the hash password of Unit Leader (y).

7.1 Availability/Auditing/Integrity

Availability with respect to the security design implies that the security system must be available all the time to every person that has link with the school. Furthermore, information met for authorized persons must not find their way into the hands of unauthorized users because they may prevent others from having access to it. The system runs for 24 hours and can even be accessed through self service mode outside school hours. The Audit facility itemizes all attempted log-on and failed password/IDs. It will also detail the time and duration of every user activity. By and large, the system has been designed in such a way that, it takes into account every operation that takes place. In other words, whenever somebody log-in to make some changes, the changes are kept in the audit file. In the event that there is crisis or fraud that requires investigation, the dealings can be accessed. Below is a table describing the use of an audit facility.

Table 14: Audit Mechanism

Student ID	Personal Detail	Date	Log-in Time	Log-out Time	Action	Location	IP
7084	63 Stratford Road, London	20-02-11	19:29	20:05	View	London	185.0.86.9
7096	50 Shelley Road, London	20-03-12	16:15	16:45	View, Edit	Manchester	208.76.9.75

The above tables represent a practical demonstration of how a typical audit mechanism works in a security system. Anytime a user login into the system to perform any operation, the log file will be generated according to his/her identification. At this point the time the user login is recorded, as well as the action carried out and the location of the user at the time when he uses the system. In case of any problem involving a misuse of the system warranting the presence of law enforcement, the auditing system keeps track of identity of the user and can always reproduce all the information done by the culprit. **Integrity** as used in this research implies protecting the system against threat. Such threat may include changing of examination marks by an unauthorized user, which invariably can affect the aim of the project. For instance, for there to be integrity in the system, it must provide for the security of examination marks. The integrity of the system is guaranteed by the presence of hashed password.

8. Detection and Reaction

Detection with respect to the system implies how, and when can the system detects certain things that are not suppose to happen; and when it happens, how do we react? Furthermore, Closed Circuit Television (CCTV) cameras are also available within the premises to monitor activities within. This will help to detect fraud users, when and how the wrong was carried out. The reaction expected is to fish out the culprits through the help of the CCTV. The appropriate policy on erring persons will be applied to the letter to serve as a deterrent to others. Also, components or the full assets will be replaced if necessary. Also, the security system is designed to recover from a complete service interruption without manual intervention. The durability of the security system makes it possible for it to withstand a partial or gradual degradation that would occur in the event of failure of the physical components. Finally, the security system has the ability to withstand a complete service interruption and invoke subsequent recovery in the event of the failure of physical components.

9. Concluding Remark

The security system design for educational system no doubt took into account all the relevant assets of interest in the school that need to be controlled security-wise. In particular, the system was developed under the framework of the assets, existing and non existing threats to the system, authentication/authorization and roles of everyone in the institution. At the end of the day, the principal focus of the system was based on confidentiality, availability and integrity because any compromise could undermine the essence of the project. It is highly recommended for all Educational institutions especially in Nigeria, to have an effective and efficient Security Network in order to guarantee the security of Information Systems in the enterprise. If the above measures are readily in place then the security system can be markedly secure and the threats from within and outside the institution would be a mirage.

References

Debar, et al; (2006) Using contextual security policies for threat response, Lecture notes in computer science, 109-128.

Hazari, S (2005) Perceptions of end-users on the requirements in personal firewall software: an exploratory study, Journal of organizational and end user computing, July-September.

International Organization for Standardization {ISO/IEC} (2005 ;) Information technology-Security techniques-Information Security Management Systems Requirements. Geneva: ISA.

Whitman, M.E (2004) In defence of the realm: Understanding the threat to Information Security. International Journal of Information Management, 24: 43-57.

Internet Reference

(Webopedia, 2013) retrieved from http://www/webopedia.com/TERM/A/authentication.html

(Webopedia, 2013) retrieved from http://www.webopedia.com/TERM/A/authorization.html