Volume 2 No. 6, June 2012 ISSN 2223-4985

International Journal of Information and Communication Technology Research

http://www.esjournals.org

Security Management Policy of LMS in AOU Bahrain Branch

Sarmad Mohammad, Abdulrahman Akhund Awadhi, Ahmad Kananah , Minimol Anil Job
Arab Open University, IT Department
Kingdom of Bahrain

ABSTRACT

Arab Open University AOU have been accommodated a security means for implementing data integrity and protection policies for students and staff involved with the e-learning. This research constructs a framework that can be used to evaluate the security requirements of the Learning Management System (LMS), the framework has four metrics; Availability, Confidentiality, Integrity and Authentication (ACIA) as key role in the security management of LMS associated with the e-learning. The capabilities of a number of existing privacy enhancing technologies, including methods for network privacy, policy-based privacy/security management, and trust systems, are reviewed. It presents the basic principles behind privacy practices and legislation. It investigates the more popular e-learning standards to determine their provisions and limitations for privacy and security. Security requirements for e-learning systems are explored with respect to online questionnaire, it covers the security aspects of the LMS website (http://www.arabcampus.org) and Students Information System (SIS), and some security questions have been answered and evaluated as an index to measure security of LMS & SIS systems.

Keywords*:* *e-learning security, web site quality, security management and monitoring*

1. METHODOLOGY

In a client/server environment, security policies and mechanisms have been designed to support the LMS & SIS security requirements for communication networks that can be grouped together under the following four metrics [1],[2]:

- **Availability**: a network service can be unavailable because of heavy traffic conditions or hardware/software failures, but a service can also be disrupted because of malicious attacks that attempt to deny service.

- **Confidentiality**: a user may wish to keep the content of a message secret from all but the intended recipient. It may also be important that a user keeps their identity secret from eavesdroppers, so the confidentiality main objective is to keep LMS information from being disclosed to anyone not authorized to access it.

- **Integrity** : measures are taken to protect data from transmission errors, but users may also wish to be protected from a message being changed deliberately for malicious reasons, also defines what rights and services the end user is allowed once server access is granted.

- **Authentication**: a user may want to be sure that a received message was sent by the user whom they purport to be and not by someone masquerading as another._ Authentication involves validating the end users' identity prior to permit them server access.

The security Methodology implements important questions [3] that have been answered by students which will give the main index about the security of LMS & SIS, given below:

- What components are most critical but vulnerable?
- What information is confidential and needs to be protected?
- How will confidentiality be ensured?
- Will the confidential information be encrypted?
- Who is authorized to access or modify information?
- What authentication system should be used?
- What intrusion detection systems should be installed?
- Who has authority and responsibility for installing and configuring system?
- What incident handling measures should be in place?
- What plans need to be in place to ensure continuity or minimum disruption?

The developed whole methodology focused on improvement of availability, performance, consistency, and reliability of E-learning system [4]. It is expected that the overall outcomes of fulfillment the questionnaire given in Table (1) point out the strengths and weakness of e-learning system security in AOU.

The suggested methodology takes into account the most serious threats to LMS & SIS are listed as follow:

- Deliberate software attacks (viruses, worms, macros, denial of service)
- Technical software failures and errors (bugs, coding problems, unknown loopholes)
- Acts of human error or failure (accidents, employee mistakes)
- Deliberate acts of espionage or trespass (unauthorized access and/or data collection)
- Deliberate acts of sabotage or vandalism (destruction of information or system)
- Technical hardware failures or errors (equipment failure)
- Deliberate acts of theft (illegal confiscation of equipment or information)
- Compromises to intellectual property (piracy, copyright, infringement)
- Quality of Service deviations from service providers (power and WAN service issues)
- Technological obsolescence (antiquated or out-dated technologies)
- Deliberate acts of information extortion (blackmail for information disclosure).

The proposed AICA methodology covers all the LMS & SIS security issues mentioned above on the elimination or mitigation of the threat associated risk, regarding the specific implementation of e-learning nature. The goal of this work is not to provide an exhaustive list of all possible attacks for e-learning systems [5],[6]; it rather tries to provide a conceptual framework by which developers of e-learning systems can decrease the number of overlooked security vulnerabilities at the design stage. The presented AICA model focus on questionnaire given in Table (1).

Table (1) Questionnaire for ACIA Security Analysis of E-learning System in AOU Bahrain Branch

	Question	**4.Always**	**3.Frequently**	**2.Sometimes**	***1.Rarely***	***ACIA Security Analysis components***
A1	How often you try to access the LMS to view your course material and you find the page is down (out-of-service)?					**AVAILABILITY**
A2	In the registration period, how often did you try to access the registration website and found it down (out-of-service)?					
A3	Do you understand the threats in the e-learning (e.g. virus attacks) ?					
A4	Do you think that the measures have been taken to protect the LMS from invalid information are good enough (e.g. access is denied after a minimum number of try)?					
A5	Do you have enough help functions and support available in LMS?					
A6	Are the LMS interruptions and disturbances handled properly?					
C7	Have you ever found your e-mail hacked and sending information to someone else?					**CONFIDENTIALITY**
C8	Have you found that someone tried to guess your logging to enter your page and falsify your data?					
C9	Do you think that course information and grades uploaded on LMS are secure and trusted?					
C10	Do you think the SIS e-payment is secure?					
C11	Do you think that the firewall is strong enough to keep the hackers out of the university network?					
C12	Do you receive your assessment grades individually?					
I13	Have you found that your personal information has leaked and fallen into					**NTEGRIT**

	someone else's hands?					
I14	Do you face the problem that someone whom didn't pay the course fees but can access the LMS?					
I15	Did you face the problem that other student can access and see your TMA answers?					
I16	Do you believe that other students are hacking your account and playing with your TMA/MTA grades?					
I17	Do you believe that other students are hacking the course page and playing with the TMA or course material?					
I18	Do you have tools installed in LMS against plagiarism?					
A19	Have you experienced unauthorized file sharing in your LMS?					AUTHENTICATION
A20	Do you receive an automated e-mail reply or verification from LMS after submitting TMA?					
A21	Do you change your LMS password for security reasons?					
A22	Does AOU-Bahrain branch use an automated system to detect and respond to intruders and hackers?					
A23	Do you trust the university online payment system using electronic cards (e.g. Visa / master card)?					
A24	Does the LMS verify the password length?					

Table -1 is based on actual feedback from students about the security of (SIS & LMS) using online voting system (for courses M150B, MT262, T324, M359 and T490). Figure-1 shows all components of availability metric (A1-A6) while Figure 5 shows the strengths in overall availability where index measured is 2.6 which is nearest to frequently available. Figure-2 shows all components of confidentiality metric (C7-C12), while Figure 5 shows the strengths in overall confidentiality where index measured is 3.0 which is system frequently confidential, Figure-3 shows all components of Integrity metric (I13-I18) , while Figure 5 shows the strengths in overall Integrity index measured is 3.12, where respondents agreed that Integrity more than frequently protected , the outcomes shown in Figure-4 & 5 measure the overall security metrics of e-learning system by being able to trace each metric, where the strengths index in overall Authentication measured is 2.7 which is nearest to frequently validating the end users. The overall of respondents stated positively about (SIS & ACES) security requirements related to ACIA.

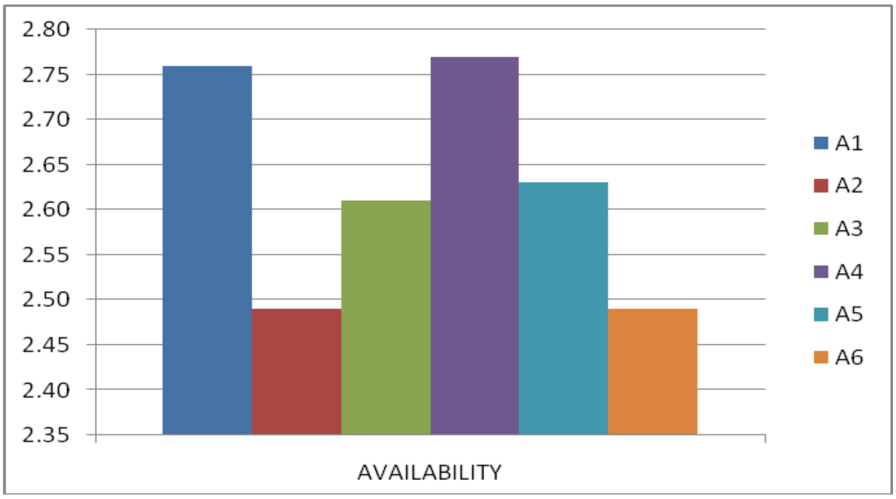

Figure 1: Availability Metrics of LMS (A1-A6)

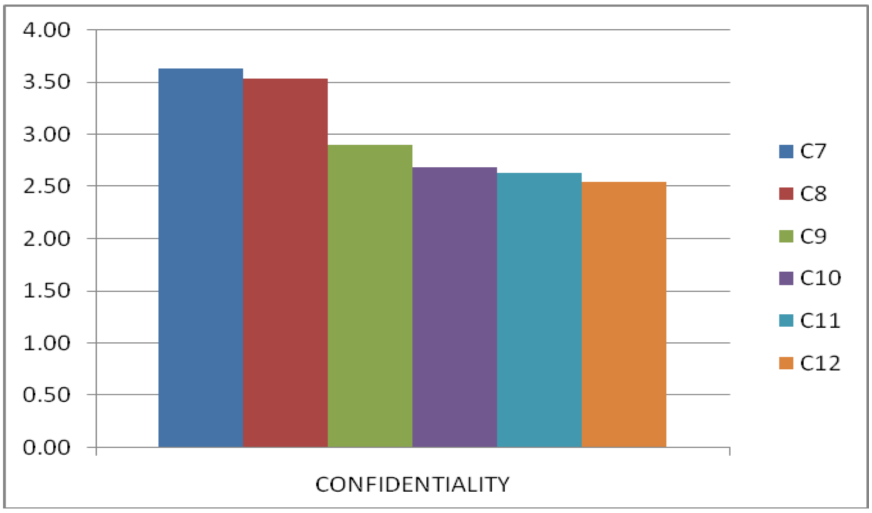

Figure 2: Confidentiality Metrics of LMS (C7-C12)

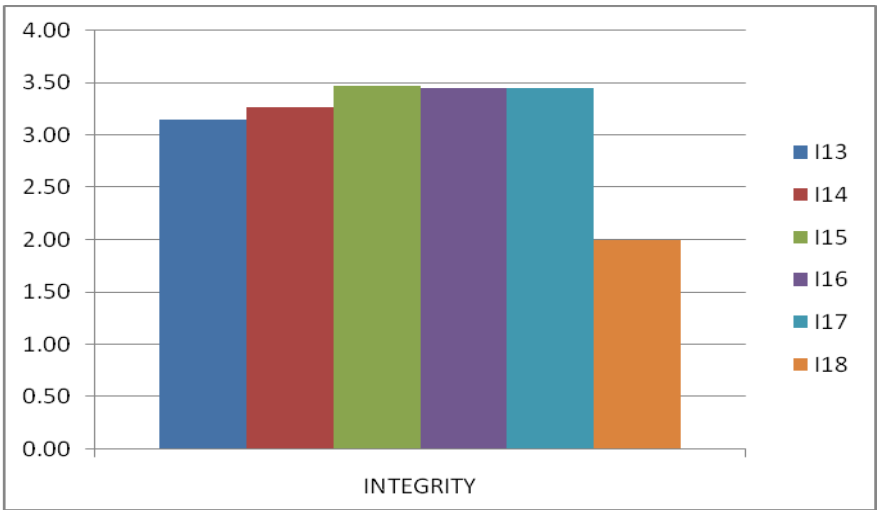

Figure 3: Integrity Components of LMS (I13-I18)

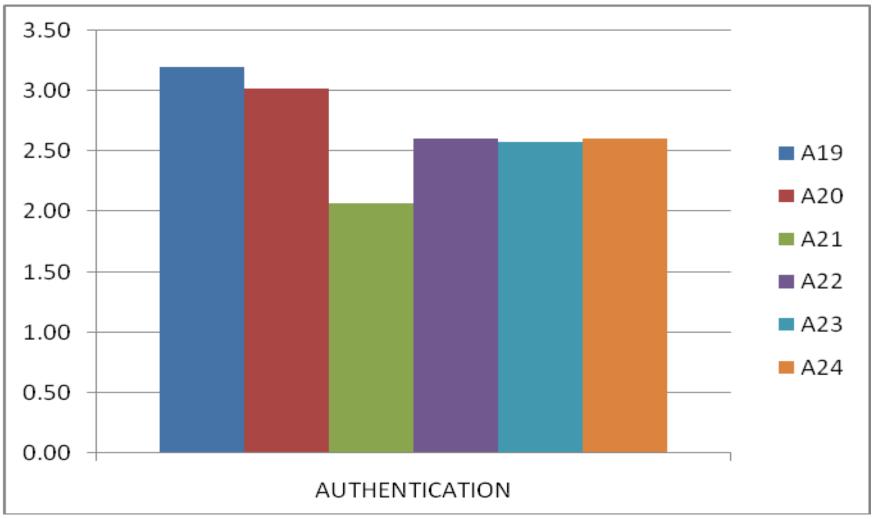

Figure 4: Authentication Components of LMS (A19-A24)

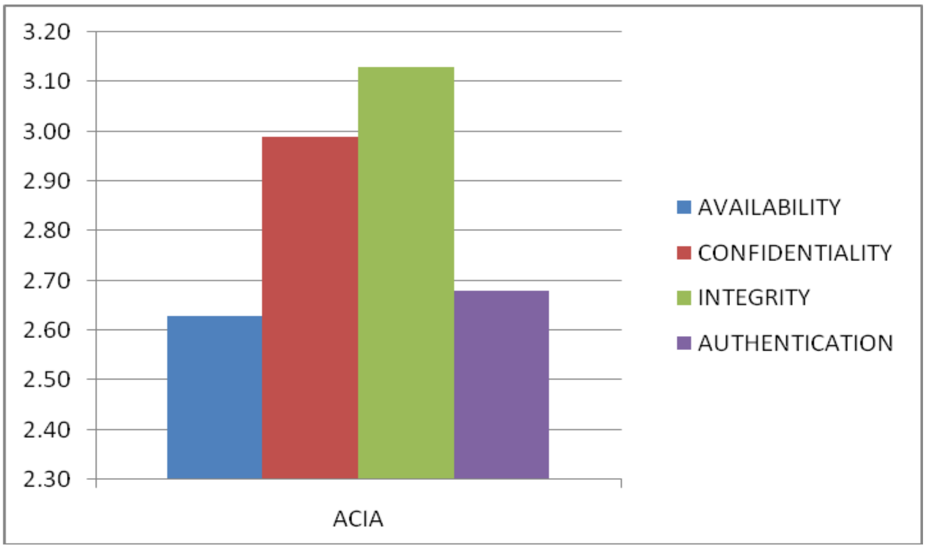

Figure 5: Overall Security Components Availability, Confidentiality , Integrity and Authentication (ACIA)

2. LMS INFRASTRUCTURE OF AOU RELATED TO SECURITY REQUIREMENTS

Connecting application and Infrastructure Figure 1 shows the Network Infrastructure block diagram, so measures have been taken to update the campus network security. This will include: attacks affect the availability and quality of system resources and an application needs awareness of these effects to cope with and survive them. A number of existing privacy enhancing technologies, including methods for network privacy, policy-based privacy/security management, and trust systems, are reviewed including also fire well & other Network components. However, the gap between application and infrastructure restricts application awareness of these changes. A middleware which bridges this gap between application and infrastructure to produce adaptive responses that is unpredictable to the attacker. Because network attacks usually target specific. Applications or exploit infrastructure vulnerabilities, a requirement for security measures is to position the adaptation control and coordination among the different mechanisms whose capabilities are used in the adaptive response in the middleware that mediates between the application and the infrastructure. This research exploits the services of various mechanisms including replication management, access control, and packet filtering to formulate the response to such symptoms [7],[8]. One of the benefits of focusing on symptoms is that many kinds of attacks produce similar symptoms, so that the capacity to cope with a finite number of symptoms results in the ability to mitigate the effects of many attacks. AOU adopt a strict e-learning system authentication measures given as follow:

- Password Strength Measure
- Password Usage Measure
- Password Initialization and Reset Measure
- No user may willfully attempt to contravene the security measure implemented on the university's IT facilities for whatever purpose.
- Username and passwords may only be used by the individuals to whom they are allocated
- User must take all strict steps given by LMS team support to protect their PCs and passwords.
- User must inform the relevant LMS team support as soon as possible if they suspect that someone else has been using their username.

Our future work developments to improve privacy and security technologies for e-learning LMS & SIS will focus are on the following areas in order to improve the average overall measured value of ACIA index, given by 2.86 (Figure-5) which is almost frequently secure system:

- Network Privacy: technologies such as efficient Routing to protect from traffic analysis attacks;
- Location Privacy: technologies to ensure location privacy for e-learners;
- Policy-based approach for privacy and security management: how to apply this approach to e-learning to satisfy the Privacy Principles; policy specification and negotiation mechanisms;
- Trust Mechanisms: how to apply this policy to e-learning to satisfy the Privacy Principles.

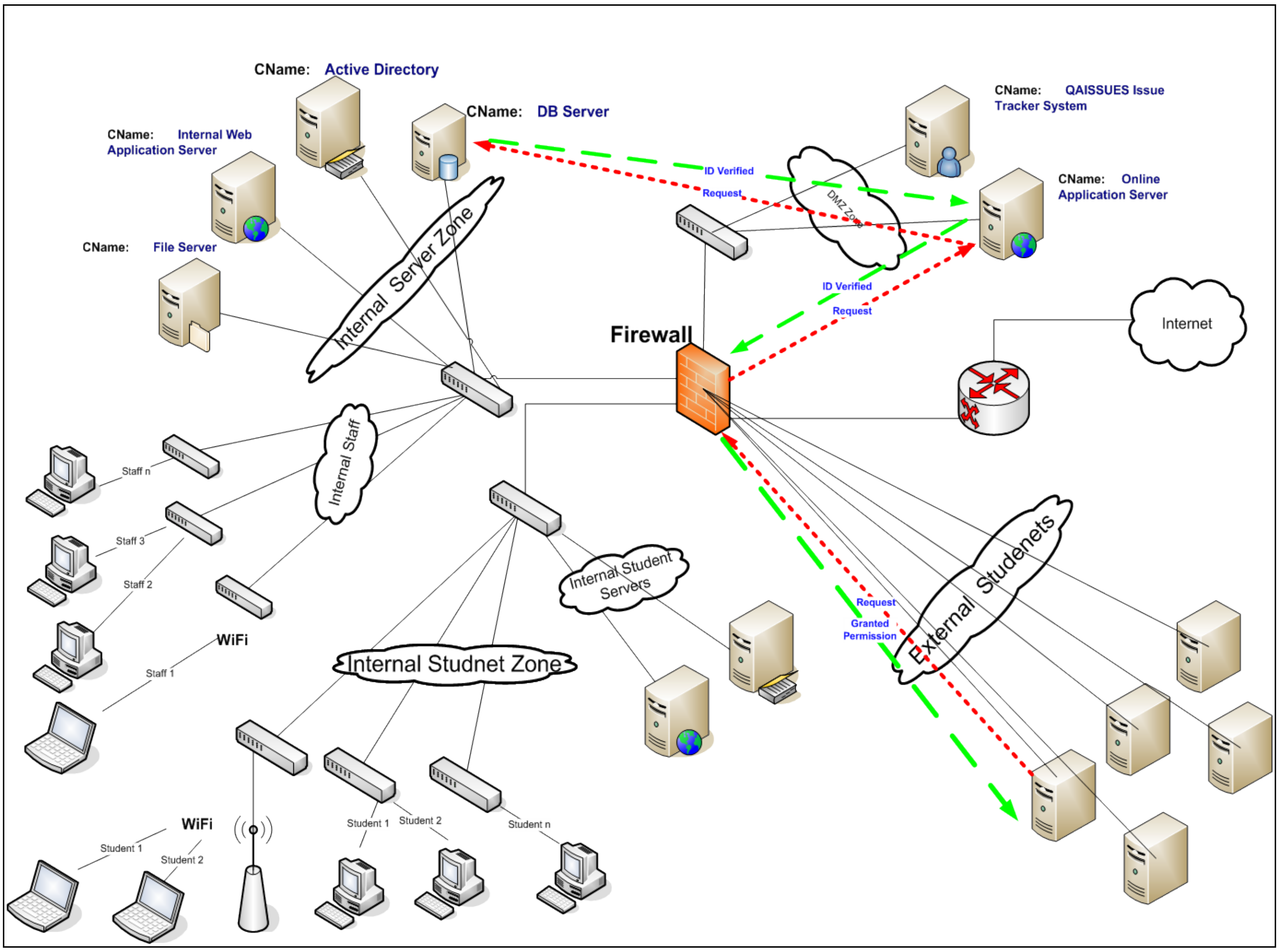

Figure 1: LMS Infrastructure under Study Related to Security Policy Requirements

3. CONCLUSIONS

The overall of respondents stated positively about (SIS & ACES) security requirements related to ACIA, the average overall measured index is 2.86 (Figure-5) which is almost frequently secure system. The suggested security policy for LMS & SIS has the following characteristics:

- The e-learning system security management is clear and concise
- Building networking closets with improved security, power, and environmental systems.
- The system has built in incentives to motivate compliance with ACIA requirements
- Security issues are verifiable and enforceable.
- System has a good control for legitimate use: access, authentication, and authorization
- There is regular backup of all critical data.
- There is a disaster recovery and business continuity plan

REFERENCES

[1] Eibl, C.J.: Privacy and Confidentiality in E-Learning Systems. In: M. Perry; H. Sasaki;M. Ehmann; G. Ortiz; O. Dini (eds.), Fourth International Conference on Internet andWeb Applications and Services (ICIW 2009), IEEE Computer Society Press, 2009,ISBN 978-0-7695-3613-2.

[2] Furnell, S. M. and Karweni, T. (2001), 'Security issues in Online Distance Learning', VINE: The Journal of Information and Knowledge Management Systems, vol. 31, no. 2.

[3] Judge, P. and M. Ammar, "Security Issues and Solutions in Multicast Content Distribution: A Survey," IEEE Network, January/February 2003.

[4] Kajava, J.: Security in e-Learning: the Whys and Wherefores. In: European Intensive Programme on Information and Communication Technologies Security (IPICS'2003), 4th Winter School, 2003.

[5] Myagmar, S., A. J. Lee, W. Yurcik, “Threat Modeling as a Basis for Security Requirements,” In Symposium on Requirements Engineering for Information Security (SREIS), 2005.

[6] Saxena, R. (2004), ‘Security and online content management: balancing access and security’,Breaking boundaries: integration and interoperability, 12th Biennial VALA Conference and Exhibition Victorian Association for Library Automation.

[7] Yang, C., Lin, F. O. and Lin, H. (2002), ‘Policy based Privacy and Security Management for Collaborative E-education Systems’, Proceedings of the 5th IASTED International Multi-Conference Computers and Advanced Technology in Education (CATE 2002), pp.501–505.

[8] Yong, J. (2007), ‘Digital Identity Design and PrivacySwiderski ,F. and W. Snyder, Threat Modeling (Microsoft Professional). Microsoft Press, 2004.