A Multi-Layered Security Model for Learning Management System

Momeen Khan[1]
Department of Computer Science
IIC University of Technology
Phnom Penh
Cambodia

Tallat Naz[2]
Department of Information Systems and Computer Science
King Khalid University, Tohama Branch, Mahayil Asir, Saudi Arabia

Mohammad Awad Hamad Medani[3]
Department of Information Systems
King Khalid University, Tohama Branch, Mahayil Asir, Saudi Arabia

***Abstract*—A learning management system is a web-based software application that is used for the documentation, administration, tracking, reporting and delivery of training programs and educational courses. It is an efficient and effective way to give valuable information to the students in a short time. With the evolution of e-learning, the learning management system is widely adopted in the education sector as well as in corporate market. Thus, it became a valued target for attackers to focus their attacks on LMS platforms. Most of the popular learning management systems available now a day don't pay enough attention to the security mechanism and that gives opportunity to intruders to gain unauthorized access by manipulating the security gaps and breach into the system. The result is information leakage, unwanted data deletion or modification and compromised integrity of the data. The aim of this research paper is to focus on the need of security concerns and to provide a solution that can make the learning management system secure from any possible potential threats and attacks. In this paper, a complete multi-layered security model is proposed. The implementation of proposed model will provide a very secure environment for any learning management system.**

Keywords*—Multi-layered security model; designing a security model for learning management system; learning management system

I. Introduction

The application of Information Communication Technology tools in education expanded the learning methods and introduced new ways of learning. The development of Information Communication Technology includes various ways of communication [1], such as smart phones and mobiles that gives the learners the opportunity to learn anywhere and anytime. Learning management system is a platform that facilitates the learners to carry out e-learning related tasks. It is a mechanism that powers e-learning [2]. Learning management system or E-Learning is a kind of learning method that shares and distributes information and it can be used as an alternate of traditional classroom for the learners, who may not be able to attend the traditional classroom environment.

There is a noticeable increase in the number of learners that are using online learning [3] or a learning management system as compared to traditional face to face learning environment [4]. As a result, many learning institutes and organizations have adopted learning management system to increase their revenue and pedagogy. According to the statistics of the US National Center for education, almost one million students enrolled in distance learning [5], which was 35% of solely online students. From this, it is quite clear that learning management system is becoming popular in education sector and is considered as a main building block of learning and training activities. Considering its importance, there is a need to make it secured and protected against any possible attack.

Learning management systems uses the internet to share and distribute data and information. However, the internet as a backbone of any learning management system is insecure. Security is one of the significant issues in a learning management system where multiple databases are connected through the common gateway [6]. Therefore, the learning management system is subject to software and hardware attacks. These attacks may have an effect on intellectual property such as copyright and privacy. To our knowledge, little work tried to find a solution that can ensure a safer learning environment. Moreover, learning management system includes vital information and knowledge about the learners and institutes or organizations that is always considered as a critical asset.

Learning management systems have several security issues that include protection against manipulation, authentication, availability, confidentiality and data integrity. Over time, many features are usually added to the learning management system. Therefore, efforts should be made to make this sensitive information as much secured as possible. Such information should be restricted to only the authorized groups. The security threats of the learning management system have common features to E-Systems threats, therefore, managing security is also common. Managing the security of learning management systems should include content and services to ensure usable and available system [7]. For the safe and smooth operation of learning management system with a high quality, it is a challenge for institutions and organizations is to provide an immense security plan after assessing the risks and their potential impact in detail [8]. Hence, by the development of security mechanism and use of tools for security will guarantee the availability of high-quality services with a low cost.

In section 2, studies the literature review. In section 3, we discussed about the security issues in the learning management system. In section 4, we proposed a multi-layered security model for the learning management system. In section 5, we did discussion and in the last section 6, we wrote the conclusion.

II. Literature Review

In the literature review, it was found that many researchers elevated several issues concerning the security in learning management system. Some of these issues are data protection, anonymous use, privacy, and authentication. Due to the vulnerability of the networks to the hackers, an entire system can be damaged by a single virus and thus may result in the infection of other systems that are connected to the network [7]. The institutes are worried about the protection of their data. In the meanwhile, the researchers are trying to find ways to protect and secure data and learning environment.

Learning management systems are complex systems. They are open, heterogeneous and they are wide spread. There is a greater chance for them to expose to risks and threats. Therefore, security is a difficult and important challenge. It is of great concern to focus on the security of learning management system platforms and to learn about the authentication, availability, confidentiality and integrity. A high-quality learning process would be the result of a more stable and secure learning platform.

A researcher talked about user authentication as an essential issue to think in the security of learning management system [9]. His work explained that policies and strategies should be laid while changing the requirements for the software and hardware to guarantee suitable authentication of the learner. The highlighted security issues include identity theft, inadequate authentication and impersonation [10]. Various sources of security threats for a learning management system are authenticity, access control, confidentiality, integrity, availability, and non-repudiation [11] [12]. Furthermore, some of security risks or threats in learning management system includes confidentiality violation, integrity violation, denial of service, etc. and providing remedies to minimise all these risks.

From the above literature, the security issues in Learning management system can be categorised as following:

A. Authorization

Authentication checks whether the authenticated person has the right or privilege to access the contents of the system [13].

B. Identification and Authentication

Identification tries to identify legitimate users to whom access has been granted. While Authentication tries to verify that the user is the same as whom, he claims to be.

C. Availability

In Learning management system, availability is the assurance that the Learning management system's environment is accessible by authorised users, whenever it is needed. Availability can be divided into two: Denial of Service attack (DoS)–an attack that stops access to authorized users of a website, so that the site is forced to offer a reduced level of services or in some cases, ceases operation completely that results in the loss of data processing capabilities. The Learning management system users are dependent on the information on the Internet; therefore, the availability of materials and information to be accessed at any point in time and at any location is crucial [7]. Failing to fulfil this will have a huge impact on Learning management system users and providers.

D. Confidentiality

This is the protection of information in the system so that unauthorised persons cannot gain access.

E. Integrity of information

This is the protection of data from unauthorised changes (i.e. only authorised users or processes can alter contents and no changes can be made illegally). Integrity depends on access controls; therefore, it is important to positively and uniquely identify all persons who attempt access. Integrity can be compromised by hackers, masquerades, unauthorised user activity, unprotected downloaded files, LANs, and unauthorised programs (e.g., Trojan horses and viruses). Each of these threats can lead to unauthorised changes to data or programs.

III. Security Issues in Learning Management System

The security design of the learning management system is always part of discussions theoretically. However, it is important to understand the attacks in a way to correctly identify the factors that are affecting the security mechanism. It will help in the designing of the security services.

A. Authentication Attacks

The attack is to gain access to system information by using stolen passwords, keys or credentials. An attacking device pretend as a legitimate device trying to gain access to the system. These types of attacks may lead to unauthorized modification of contents and breach of confidentiality. Examples include brute force attack, dictionary attack, login spoofing attacks, key management attacks, replay attacks, Man-in-middle attacks. To counter these attacks, strong authentication method such as multi-factor authentication security system should be implemented.

B. Authorization Attack

An attack that occurs as a result of unauthorised access to specific content. Unauthorized use or elevation of access can be countered by using the principle of least privilege; strong access control lists (ACL's) or strong role-based security mechanism should be used.

C. Availability Attack

This is an attack that occurs when services of a system and contents are unavailable to legitimate users for some time. Examples of such attacks include Denial of Service, Node attacks, Line attacks, Network infrastructure attacks. A Good backup system is a way of countering these attacks, use of a scrubbing cloud DDoS mitigation technique and load sharing among several servers carrying the learning management system.

D. Confidentiality Attack

This attack tries to expose the confidential data to unauthorized users. This may be transfer of e-contents to the unauthorized persons or obtaining secret passwords. Example includes: Group session eavesdropping, Group session traffic analysis, and Group identity disclosure [14]. Strong encryption methods should to be used to counter confidentiality attack. Ex. RSA-265, Hash or above.

E. Integrity Attack

This aims to destroy or modify the contents of the system. Due to the integrity attack, the legitimate users will not get the correct contents. Examples are malicious code attacks, message injection, traffic modification**,** traffic deletion. To counter integrity attacks, digital signature, data hashing and shining can be used effectively. Authorization should be strong enough to keep unauthorized users at bay to stop them from many chances to alter the information. Protocols should be tempered resistant across communication links.

The main asset of an organization is the information that is obtained from the useful data. If the access is made easy for everybody then it will be not hard for anyone to gain access despite of the fact that that have good or bad intentions. As a result, the information is exposed to a variety of threats and vulnerabilities.

IV. Problem Statement

Implementing learning management system is not an easy task. Regardless of gaining many benefits from learning management system there are also many challenges and issues while trying to make the learning management system successful. Despite the deployment of advanced security methodologies, there are still several loopholes that must be filled. It is important to properly assess the security properties that are associated with learning management system.

V. Research Objective

Based on this assessment, a security model should be proposed that offers technological security mechanism to secure learning management system. It is of great importance to treat the security mechanism in learning management system more seriously by designing more complex security models. Therefore, a new security model based on multi-layers security mechanism is proposed.

VI. Proposed Security Model for Learning Management System

In order to ensure authentication, availability and integrity for learning management system we have developed a model with four main layers and five sub layers as shown in Fig. 1. Distribution of tasks on different layers ensures better management of security on each layer.

A. Physical Layer

In order to ensure maximum security for learning management system we will use the design as shown in Fig. 2. It will help to ensure authentication, availability and integrity. On physical layer only authorized people are given access to sensitive hardware which includes routers, proxy server, web server, database server, file server and backup server.

Users connect with router to access learning management systems. Router sends data to the firewall and a honey pot. Data travels from firewall to web server after passing through intrusion detection prevention system (IDPS) and proxy server. Database is placed on a separate server and files are placed on a separate server. While everything on the web server, database server and file server is backed up on a separate server. All these things will be discussed in more detail under other layers.

The presence of proxy server in front of the web server increases privacy and caches data. Cached data helps in faster delivery of data.

B. Network Layer

Network layer primarily deals with data coming in from internet and going out on internet. It also deals with connection of different devices for successful operation of Learning Management System.

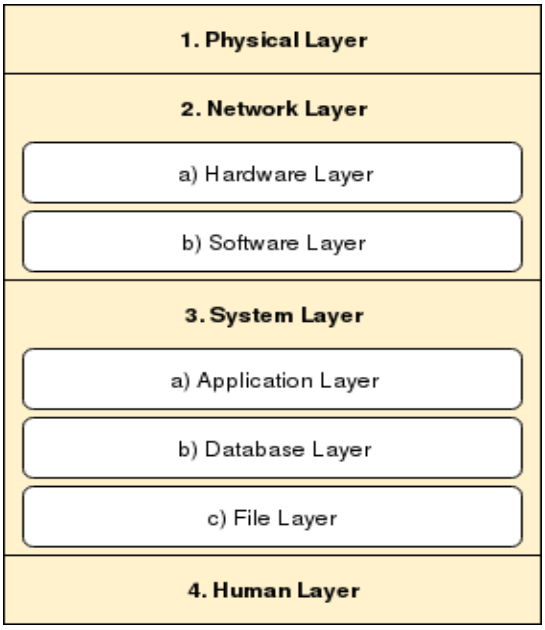

Fig. 1. Layers in LMS Security Model.

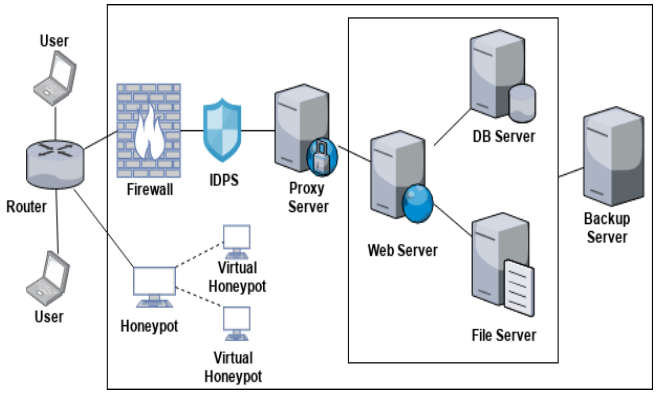

Fig. 2. Infrastructure at Physical Layer.

a) Hardware layer: On hardware layer of network layer, we have router. Routers can be helpful in the following:

- Restricting unauthorized devices from connecting to the network to ensure safety of the network.
- Cisco routers have a hardware firewall which can be used to filter traffic.
- Router can also help in restricting websites which we don't want to be opened on the network. Certain websites can contain viruses, malwares, trojans, spywares etc. These can harm devices present on our network. So, it is much better to block such websites completely.

b) Software layer: On software layer of network layer, we have the following:

- A software firewall is used to filter traffic and protect LMS from malicious traffic sent by attackers. It also logs the traffic so if needed later behavioral analysis can be performed on the logs to detect unwanted behavior.
- Intrusion prevention systems (IPS) also known as Intrusion detection prevention systems (IDPS) are used to deeply monitor the packets on the network. When any malicious activity is detected, IPS / IDPS will log and block it. It will also report this activity to alert the system administrators.

C. System Layer

On system layer we use various mechanisms to ensure security of the system, which will be discussed below:

a) Application layer: LMS is placed on the web server and following measures are taken for its security:

- Access control list (ACL) is used for authentication and it ensures that only authorized people are allowed to access the system. Whenever a user requests a resource on the LMS, it is first checked in ACL to make sure that this user is authorized to access that resource. If that user is authorized, then he / she is given access to that particular resource otherwise if that user is not authorized then access is not granted.
- Hyper Text Transfer Protocol (HTTP) is the protocol through which data is transferred between our browser and website or server to which we are connected through an insecure connection. Any attacker can get the data which is being transferred over HTTP and steal login details of legitimate users because the connection is insecure. Using Hyper Text Transfer Protocol Secure (HTTPS) encrypts the connection making it difficult for attacker to steal any information from the data being transferred over HTTPS. So, we will install SSL to ensure use of HTTPS
- All the forms in the application will use POST method instead of GET to secure login details and the data transferred.
- Prepared statements are always used while making a query to the database, it helps to protect the application against SQL injection attacks. Prepared statements help to ensure integrity because data present in the database can't be affected or changed by attacker.

Honey pot is connected with the router. Honeypots appear as vulnerable parts of the system to attackers and they mislead the attacker on concentrating all their energy on the honeypot instead of the actual system. Whenever anyone tries to connect with honeypot it gives us a clear signal that an attacker might be scanning the system and will eventually try to penetrate it. When someone scans the Honeypot, more virtual honeypots are created, and the attacker will start to scan them also. It alerts the staff to take appropriate action before any serious damage is done to the system.

Distributed Denial of Server (DDoS) Attack are well known for making the website / system unavailable for legitimate users. Honeypot can also protect against Distributed Denial of Server (DDoS) Attack and make sure that LMS is available for legitimate users.

b) Database layer: Database is deployed on the database server and following measures are taken for its security:

- Table level access control is applied. Only authorized people are allowed to read, write, update or delete anything from table.
- Sensitive information stored on database server is encrypted using hardware security module (HSM). HSM are specially designed hardware components for cryptography.
- In case of data loss, data can be retrieved from backup server to ensure data is available for legitimate users.

c) File layer: All files are stored on the file server and following measures are taken for its security:

- To ensure integrity of files a file check sum will be calculated and stored for all the files. Whenever file integrity needs to be checked, we will simply recalculate the check sum of file and then compare it with the check sum which we have already calculated and stored in the past. If checksum is same it means file is not tampered but if checksum is different, it means file is tampered and it should be deleted. After deleting such files, original files can be retrieved from the backup server.
- All directories in which files are uploaded don't have execute permissions. Only read and write permissions are given.
- Only files of the following format are allowed to be uploaded: doc, docx, ppt, pptx, xls, xlsx, pdf, png, jpeg other ones will be rejected by system. It will ensure no malicious file is uploaded on the file server.

d) Human layer

- Training for staff is vital and is of paramount importance. They need to be trained to check the URLs in address bar of browser before entering any sensitive

details in the system. They should make sure that the protocol being used in HTTPS and not HTTP.

- Staff should also be made aware of the social engineering tactics used by attackers.

VII. Discussion

The success of a learning management system needs to resolve all the challenges in the implementation, specially the security challenges. The proposed security model is designed to be a purely defense in depth model for security of LMS.

- It ensures every step is taken to stop attackers on each layer.
- It ensures authentication by application of ACL at application layer (a sub layer of system layer), encryption at database layer (a sub layer of system layer) and filtering unauthorized devices at hardware layer (a sub layer of network layer).
- It ensures availability by using proxy server, high bandwidth and backup server.
- It ensures integrity by using SSL, POST method in forms, Reputation check with checksums, prepared statements to protect against SQL injection.
- Honeypots connected to router help to detect attackers before any damage is done to the actual system.
- Honeypots can protect LMS against DoS attacks and ensure availability of LMS for respected users.

Traffic logs are maintained at a sub layer of network layer called software layer, these help in behavioral analysis of the traffic to find out any malicious traffic being sent to our network.

VIII. Conclusion

The major challenge in learning management systems today is the issue of security. In this research paper, the researchers highlighted several issues in the security of learning management system. The researchers also proposed a multi-layered model that can ensure the security mechanism of a learning management system. As per the proposed solution might seem costly in its implementation but it's return of investment (ROI) is worthwhile. The implementation of this security model shall be of great use for enterprises holding a learning management system and will make sure that both users and professors will gain trust towards a system that is well secured against tampering and manipulation of their data.

References

[1] Ally M (2007). Mobile Learning. Int. Rev. Res. Open Distance Learn. Volume 8, Number 2. ISSN: 1492-3831.

[2] Tallat Naz and Momeen Khan, "Functionality Gaps in the Design of Learning Management Systems" International Journal of Advanced Computer Science and Applications(ijacsa), 9(11), 2018. http://dx.doi.org/10.14569/IJACSA.2018.091152.

[3] Allen E, Seaman J (2014). Tracking Online Education in the United States. Babson Survey Research Group and Quahog Research Group, LLC.

[4] Pastore R, Chellman A (2009). Motivations for residential students to participate in online courses. Q. Rev. Distance Educ. 10(3):263-277.

[5] Akanegbu, Anuli (2012). 50 Striking Statistics about Distance Education in Higher Education https://edtechmagazine.com/higher/article/2012/07/50-striking-statistics-about-distance-learning-higher-education.

[6] Momeen Khan, Tallat Naz, Khalid Mahmood, (2019) "Using Blockchain to resolve Database Distribution and Security Issues in The Learning Management Systems (LMS)" International Journal of Computer Science and Network security (IJCSNS), Vol. 19 No. 11 pp. 139-150. http://paper.ijcsns.org/07_book/201911/20191120.pdf

[7] Alwi N, Fan IS (2010). E-Learning and Information Security Management. Int. J. Digit. Soc. 1(2).

[8] May M, George S (2011). Privacy concerns in e-Learning: Is using a tracking system a threat? Int. J. Inf. Educ. Technol. 1(1):1-8 [Online]. Available: http://liris.cnrs.fr/Documents/Liris5266.pdf[Accessed 25 09 2014].

[9] Levy D (2011). Lessons learned from participating in a connectivist massive online open course (MOOC). In Y. Eshet-Alkalai, A. Caspi, S. Eden, N. Geri & Y. Yair (eds.), Proceedings of the Chais conference on instructional technologies research: Learning in the technological era, (pp. 31-36). Available online at http://www.openu.ac.il/research_center/chais2011/download/f-levyd-94_eng.pdf.

[10] Chen Y, He W (2013). Security risks and protection in online learning: A survey. Int. Rev. Res. Open Distrib. Learn. 14(5).

[11] Saleh MM, Wahid FA (2015). A Review of Security Threats by the unauthorized in the E-learning. Int. J. Comput. Technol. 14(11):6240-6243.

[12] Barik N, Karforma S (2012). Risks and remedies in e-learning system. Int. J. Netw. Secur. Appl. 4(1):51-59.

[13] Assefa S, Solms V (2009). An Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS)," Proceedings of 9th WCCE, 2009.

[14] Cardenas R, Sanchez E (2005). Security challenges of Distributed E-learning systems. ISSADS, 2005.LNCS 3563 pp. 538-544.Springer Verlag Berlin Heidelberg.