International Journal of Scientific and Technical Advancements
IJSTA
ISSN: 2454-1532

e-Learning Security Concerns and Measures

Namita Singh
Department of Computer Science & IT, Central University of Jammu, India
Email address: venthra@yahoo.com

***Abstract*—**The increasing use of e-learning systems has been documented by numerous studies and shows continuing growth; little attention has been given to the issue of security of e-learning systems both in research and education. Many e-learning institutions are rushing into adopting ICT without carefully planning and understanding any related security concerns. e-Learning is a new method of learning which ultimately depends on the internet in its execution. This paper therefore focuses and elaborates security concerns in e-learning and protection measures to secure the organizations who access and manage data via internet by over hundreds of networks. Moreover, this paper also discusses impact of lack of proper IT policies and procedures in e-learning systems.

***Keywords*—** ICT; e-learning; IT policies; security attacks.

I. INTRODUCTION

The present education system cannot afford to ignore the presence of e-learning. And of late, it can be seen as a modern pillar in sphere of education. It has become an important tool for teaching and is more perfect when it comes to classroom teaching in many cases [1]. The concept of anytime, anywhere learning promotes life-long learning and accordingly eliminates the problems associated with distance. The flexibilities which e-learning offer to the students is the main motivating factor in choosing online courses [2].

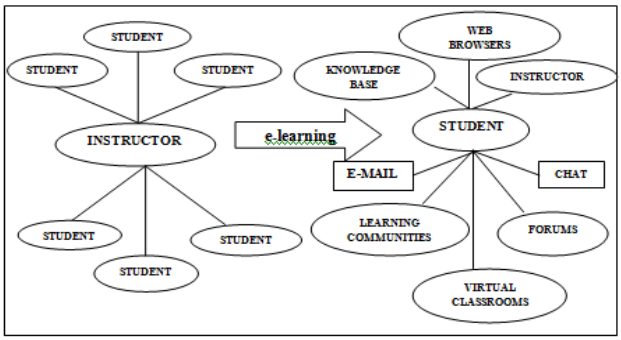

Fig. 1. Transition from learning to e-learning.

Major features involved in introducing e-learning involved:

- *Personalization*: The learning topics can be selected based on student interest, student aptitude and educational level, and societal need.
- *Interoperability and reusability*: e-Learning systems with different environments and contents from multiple authors had the ability to work together. Learning content can be reused in multiple applications and environments regardless of the tools used to create them.
- *Flexibility*: Courses could be designed in a variety of forms based on standard style sheets. Different forms of layout could be available depending on the purpose of the course and the preferences of the learner.

Most e-learning innovations and institutions have focused on course development and delivery, with little or no consideration to privacy and security and even focus on the protection of personal information of a learner in an e-learning system is rarely stressed upon.

II. SECURITY CONCERNS IN E-LEARNING

e-Learning aims are concerned with providing teaching and e-learning to everyone. Ensuring the availability and integrity of information is the main goal in relation to e-learning security. Sharing of information, collaboration and interconnectivity are core elements of any e-learning system and hence, data must be protected in order to maintain confidentiality, integrity and availability. Protecting against data manipulation, fraudulent user authentication and compromises in confidentiality are important security issues in e-learning [3]. Many definitions of computer system security and basic categorization have been proposed by different researchers, most of them following the three-layer model, presented in figure 2.

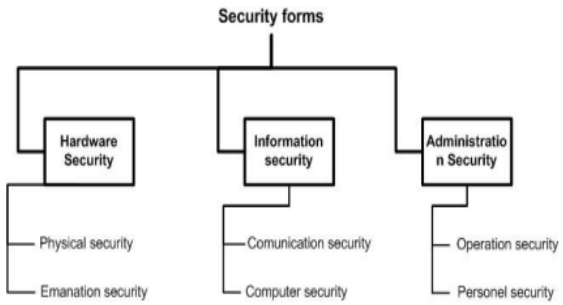

Fig. 2. Forms of security [4].

The issues of security includes: user authentication /authorization, protection of private information from unintended access, and protection of data integrity (guarding against data corruption by attackers). Hence, securing the e-learning environment requires avoiding the four types of threat, which are fabrication, modification, interruption and interception. e-system are vulnerable to a range of security threats [5]:

- *Authentication* – broken authentication and session management; insecure communication.
- *Availability* – denial of service.

Namita Singh, "e-Learning security concerns and measures", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 139-141, 2015.

- *Confidentiality attacks* – insecure cryptographic storage; insecure direct object reference; information leakage and improper error handling.
- *Integrity attacks* – buffer overflow; cross site request forgery; cross site scripting; failure to restrict URL access; injection flaws; malicious file execution.

Though the focus rests on vulnerabilities and risks specific to e-learning, yet all the components of e-learning system such as web services, server computer systems, client computer systems, database systems can also be vulnerable to network attacks.

III. PROTECTION MEASURES IN AN E-LEARNING SYSTEM

To design a secure e-learning system it is not sufficient to choose strong authentication and encryption system and to implement new security solutions only in response to actual attacks that have recently occurred. A system can't be made "secure" in general, it may be secured against specific attacks. A secure e-learning system must address the issues of security as part of an organized process in the design phase.

A. Network-level Security

For the purpose of ensuring the security of the information system, the first step consists of creating a private virtual network so as ensure secured, hierarchical and controlled allocation of resources and information and by installing firewalls and anti-virus software's. Authorized access through firewall will prevent unauthorized access to a corporate network from outside the organization. Technically, a firewall is a specialized version of a router and must work on the principle that allows all traffic from the inside to the outside and vice versa to pass through the firewall. Network security area can be therefore divided into three layers.

- Network hardware security
- Computer hardware security
- Operating system security

B. Implementing Security Management (ISM)

Most of the information systems have not been designed to be secure. There are four main elements of information security within e-learning environments, including ensuring e-learning information security governance, creating e-learning information security policy and procedures, implementing e-learning information security counter measures, and monitoring the e-learning information security countermeasures. Educational institutions should implement cyber security approaches to manage their information security risks as part of existing governance structures. While implementing information security measures an e-learning platform should be tested for external intrusion issues. Institutions need to identify the 'controls' of data in order to establish clear lines of secure information sharing in a distributed environment.

C. Security Policies

Security policies and mechanisms in online learning must support authentication, authorization, confidentiality, and accountability [6]. Authentication refers to the validation of a person's identity before the access is assigned. Authorization defines what rights and services a person can access after the authentication process is passed. Confidentiality means that some specific information or data cannot be disclosed to anyone who is not authorized. Accountability refers to the methodology by which users' resource consumption information is collected for billing, auditing, and capacity-planning purposes [7].

D. Using Digital Right Management and Cryptography

One of the major strategies to be implemented to reduce risks associated with e-learning assets is digital right management [8]. Digital Right Management (DRM) makes the system safer for its contents [9]. e-Learning system is working either in a distributed network or in Internet where multiple rights associated with learner, instructors content providers, administrators etc come into play as content and services are created, distributed, aggregated, disaggregated, stored found and used. Different cryptographic tools and techniques are also needed for the implementation of security in Internet based transactions. Cryptography not only protects data from theft or alteration, but can also be used for user authentication. Generally three types of cryptographic schemes are used to accomplish these goals: Secret Key or Symmetric Key Cryptography, Public Key or Asymmetric Key Cryptography and Hash Functions [10]. Denial of Service sensors (DoS) detect and interrupt cyber attacks of any type which threaten online data transmission. Intrusion Prevention System protects Windows, Linux, BSD, Solaris and Mac Os operating systems to take over targeted computers

IV. CONCLUSION

Ensuring the availability and integrity of information and material within e-learning environments requires that countermeasures, such as security technology hardware and software, need to be implemented. The demand for e-learning has changed the way in which Higher Education conducts its core business of providing courses to various learners. The increase in popularity of eLearning systems, with large dependence on the Internet has resulted in the appearance of new threats in the security of information stored in the systems. Through the mode of this paper an attempt has been made to identify data security threats existing in e-learning platforms and it is believed that the primary issues faced in an e-learning system can be met by building secured, standardized e-learning environments, as well as centralized application management.

REFERENCES

[1] Dr. M. U. Bokhari, Dr. S. Kuraishy, and S. Ahmad, "Security concerns and counter measures in e-Learning systems," available at : http://www.academia.edu/3662527

[2] K. K. Jain and L. B. Ngoh, 'Motivating factors in e-Learning- a case study of UNITAR," Student Affairs Online, [Online], vol. 4, no. 1, pp. 21, 2008.

[3] I. Bandara, F. Ioras, K. Maher, "Cyber security concerns in e-learning education," *Proceedings of ICERI2014 Conference*, Seville, Spain, 2014.

Namita Singh, "e-Learning security concerns and measures", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 139-141, 2015.

[4] R. Grzybowski, "Security of information in university elearning systems," *Proceedings of Journal Of Applied Computer Science*, vol. 19 no. 2, pp. 7-18, 2011.
[5] N. Rjaibi, L. B. A. Rabai, A. B. Aissa, and M. Louadi, "Cyber security measurement in depth for E-learning systems," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, issue 11, pp. 1-15, 2012.
[6] R. G. Cardenas and E. M. Sanchez, "Security challenges of distributed e-learning systems," *In Advanced distributed systems*, Springer Berlin Heidelberg, pp. 538-544, 2005.
[7] K. Song, S. M. Lee, and S. C. Nam, "Combined biometrics for e-learning security," ISA 2-13, ASTL, 21, pp. 247-251, 2013.
[8] Z. F. Zamzuri, M. Manaf, A. Ahmad, and Y. Yunus "Computer security threats towards the e-learning system assets," *Communications in Computer and Information Science*, vol. 180, pp. 335-345, 2011.
[9] Banerjee Sanjay and Karforma Sunil "Pros and Cons of the credit card and e-money business models "ACM 2008.
[10] G. C. Kessler, An overview of cryptography, http://www.garykessler.net/library/crypto.html.

Namita Singh, "e-Learning security concerns and measures", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 139-141, 2015.

ISSN: 2454-1532

Namita Singh, "e-Learning security concerns and measures", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 139-141, 2015.