

Security Issues Concern for E-Learning by Saudi Universities

Shakeel Ahmed *, Khalid Buragga **, Ashwani Kumar Ramani***

* Department of Computer Science, ** Department of Information Systems, CCSIT, King Faisal University, Saudi Arabia.

*** School of Computer Science, DAVV, Indore, India

shakeel@kfu.edu.sa, kburagga@kfu.edu.sa, ramaniak@yahoo.com

Abstract—Emergence of the information age and the growth of Internet and communication technologies in Saudi Arabia have changed the way of teaching and learning process.

The education community in Saudi Arabia believes that the legacy methods of teaching are not able to create a good impact on the E-Learning capability of Saudi learners while compared with that of E-Learning. The emergent of E-Learning has created a buzzword of virtual university worldwide. E-Learning is available to anyone, anywhere in the world; all that a learner needs is the access to internet with Web browser.

Increase in the number of Saudi universities and a large number of internet users in Saudi Arabia have provided a number of benefits to students at the university level. Due to the close relation between E-Learning and WWW many of the security problems in E-Learning are similar to ones of the general WWW. A lot of work has been done in the development of infrastructure for universities and e-contents but security issues are also to be taken seriously, issues like ethical learning practices plagiarism, violation of privacy, vandalism, theft, and spying into the cyberspace, personal integrity and accountability. This paper will discuss some of the issues in an E-Learning environment particularly in Saudi Arabia. It will also attempt to provide suggestions and possible solutions to some of these problems.

Keywords— E-Learning System, Saudi Universities, WWW, Security issues, plagiarism

I. INTRODUCTION

It is well known fact that no country can develop without a proper infrastructure for education. Considering human development as the core of real development Saudi Arabia is undertaking massive initiatives to overhaul its education system by adapting E-Learning environment. A record budget of SR137.6 billion (\$36.7 billion) was allocated in the Fiscal Year 2010 for education and training [1]. The main focus of the government is on Education; priorities include increased student enrollments and new universities. Currently, the Saudi government offers more than 60,000 scholarships to Saudi students around the world [2].

There has to be innovative ways of imparting education as per the needs of the learner. Kingdom's ratio of 15 students to every teacher is one of the lowest in the world [3], from the statistics of the budget and increase in number of Internet users in Saudi Arabia shown in Table 1. [4]. E-Learning is the

most essential requirement of the current knowledge based Saudi economy.

TABLE1. NUMBER OF INTERNET USERS IN SAUDI ARABIA

YEAR	Users	Population	% Population.
2000	200,000	21,624,422	0.9 %
2003	1,500,000	21,771,609	6.9 %
2005	2,540,000	23,595,634	10.8 %
2007	4,700,000	24,069,943	19.5 %
2009	7,761,800	28,686,633	27.1 %
2010	9,800,000	25,731,776	38.1 %

A large numbers of Saudi universities are offering higher education programs to impart quality education where the students can learn at their ease. Due to the recent development in IT industry new trends of teaching and learning quality education can be provided to large number of people and it will ease the students to learn with their own pace and help them, to learn a lot without much effort.

As, the development of technology grows there are always certain threats [17], to the user and to the application itself and E-Learning is one of them. Developing the infrastructure and the content will create more number of students to register for E-Learning in Saudi Arabia but simultaneously it will create threat for security. Privacy issues has to be analyzed a proper review should be considered for adopting E-Learning, security tools are to be implemented for proper management of E-Learning platform.

II. E-LEARNING: SECURITY ISSUES

E-Learning is the process where learning and teaching are imparted by using all sorts of electronically enabled technologies, both the Information and communication systems coordinate to impart E-Learning. E-Learning system generally is located logically at many locations. E-Learning systems allow multiple users or applications to download, upload and exchange distributed Information from different location of the world.

E-Learning comprises of applications which includes Web-based learning, computer-based learning, virtual classroom, and digital collaboration essentially the computer and network-enabled transfer of skills and knowledge [5]. Content is delivered via the Internet, intranet/extranet, audio or video tape, satellite TV, and CD-ROM. It can be self-paced or

instructor-led and includes media in the form of text, image, animation, streaming video and audio.

The main concern of Saudi universities is to develop infrastructure and e-contents and delivery of these contents to E-Learning system, but the privacy and security concern has also to be considered as integral part of E-Learning systems. The universities have to adopt security technologies and must be put in place to meet the security requirements [6].

The primary concern in E-Learning is the security that can be summarized as under:

A. User Authorization and Authentication

The elementary feature of E-Learning system is the reliable identification of the user because it is the basis for Access control to the E-Learning system. The degree of authorization can be classified based on two basic categories viz users with or without proper authorization.

The Authorization is usually is granted only to registered students and even their access is generally restricted to a certain subset of the E-Learning material based on the billing if E-Learning is offered on billing basis and on the level of learning of the registered student which will allow him to either to move to the next level or have a revision of the previous session. It is not possible to correctly identify a student if he is interacting from a distance location. Therefore physical security may be required to handle such issues.

B. Entry Points

There are many “entry points” in E-Learning system [6] since by definition E-Learning communication system is an entity which exists in many physical/logical locations simultaneously also E-Learning systems allow multiple users or applications to download, upload and exchange distributed information.

A system can be attacked only through its “entry points” [6]. Designers can limit the security risks by reducing the number of entry points but E-Learning system cannot be implemented using this since there are a large number of multiple users from different geographic locations.

C. Dynamic Nature

The other challenge is the dynamic nature of these systems where there are dynamic sessions where any process may join or leave the group sessions at anytime. Security is also concern with each particular member process, a strict session has to be maintained and the credentials are to be verified to control both at the session level and at the participant site [16].

D. Protection against Manipulation

One of the issues of E-Learning is manipulation from the side of the students the system must be secured against manipulation. There are many possible solutions where any manipulations can be protected by using the techniques of encryption, digital signatures, firewalls, etc. These mechanisms are needed to prevent manipulations from a third side but one needs additional mechanisms against manipulation from the side of the legitimate users.

E. Confidentiality

Due to the fact that learning material by its nature must be distributed to the outside, industrial espionage and data theft are not major problems in E-Learning. The user should obtain access only to authorized contents and those persons who are not the legitimate users must not be able to gain access to the system.

F. Integrity

Integrity is that only authorized users are allowed to modify the contents which include creating, changing, appending and deleting data and metadata and the attacks on integrity are generally the attempts made to actively modify or destroy information in the E-Learning site without proper authorization.

G. Availability

The E-Learning material e-content, data (or metadata) are to be made available to the learner at the specified session when the user log on to the system for their session at the period of time, if the required material is not available the learner will lose interest and not get the at most use of E-Learning system. Mainly there are two types of attacks viz blocking attack and flooding attack, e.g.: Denial of Service, Node attacks, Line attacks, Network infrastructure attacks [6].

H. Non-Repudiation

Non-repudiation is the last step in information security where the learner have to be provided with E-Learning services without any possible fraud such as when computer systems are broken in to or infected with Trojan horses or viruses, to deny the works or changes done by them in the system [8] [9].

III. COUNTER MEASURES TO SECURITY ATTACKS

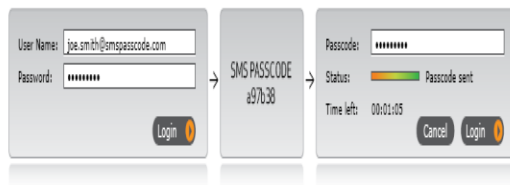
Some of the possible measures that can be applied to Saudi Universities to counter the security threats are:

SMS Information Security, Biometrics Information Security, Token Based Information Security Mechanism, Access Control List (ACL) Mechanism, Digital Signature Information Security Mechanisms can be used to enforce the Identification and Authentication of Information Security Service in universities offering E-Learning.

1) SMS (Short Message Service) Information Security Mechanism

Most of the students in Saudi Arabia have a mobile phone as a means of communication, this can be an added advantage to the universities offering E-Learning system, where a student is first authenticated with a user id and password, the E-Learning system generates a special password for the session and sends SMS message to the registered mobile phone in the E-Learning system. The student enters this password in order to authenticate his identity as shown in Figure 1. By which security can be implemented and this improves the protection against the modern threats on today's Internet.

Figure 1: SMS Pass code login scenario



2) Biometrics Information Security Mechanisms

Biometrics comprises methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. According to which all the students are required to enroll their physical or behavioral traits, which is stored in the database which is encrypted from any modifications. As shown in Figure 2. The sensor collects the data and the preprocessed data is passed on to the Biometric system where the system check to perform. When a student's logs on to the sessions his identity is checked with the database stored templates when a matching is found the content is delivered to the student the Biometric scanning can be done either by using the fingerprint scanned enabled keyboards or mouse or a combination of both, Digent offers a wide range of mouse including IZZIX FM 1000, IZZIX FD1000 [12].

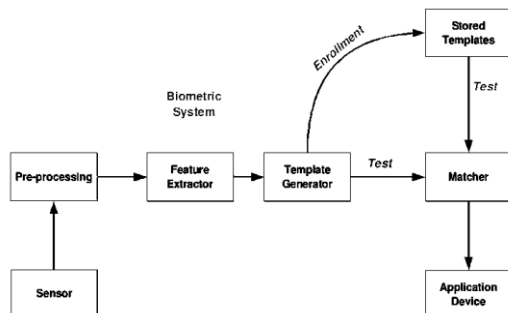


Figure 2. Biometric System Diagram

3) Token Based Information Security Mechanisms

A security token called sometimes as hardware token, hard token, authentication token, USB token, cryptographic token, or key fob may be a physical device that an authorized user of computer services is given to ease authentication [13].

Saudi universities can provide students with Security Tokens to prove student's identity electronically. The token can be used in addition to or in place of a password to prove that the student is who they claim to be. The token acts like an electronic key to access E-Learning System.

4) Access Control List (ACL) Mechanism

Access control list provides the access to the resources found in the system or the web server. Any access control will have two components for successful functioning of the system [14]. In an E-Learning environment the student has to have access to the resources they are intended for there are configuration tools that allows to grants which user have access to which resources and a means to authenticate the users to identify them properly, which can be controlled by using the one of the three most popular methods for authenticating and controlling access to the users in a web

scenario. They are the host based access control, basic authentication, and access through SSL / TLS client certificates [14].

5) Digital Signature Information Security Mechanisms

Digital Signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later [15].

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact this feature can be easily applied to E-Learning system and any changes to the documents can be verified whether the intended user has tried to make any modifications to the e-content.

6) Security from Passive Attacks

The measures discussed above can be used to detect the Active attacks, the Passive attacks can be prevented by adopting cryptographic algorithms on the basis of security and performance requirements of e-contents so that the users cannot understand the message, Cipher and authentication are two important concepts in cryptography. By cipher, the eavesdropping can be avoided and confidentiality which is the inverse concept of eavesdropping can be achieved [10].

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 [11].

IV. CONCLUSIONS AND FUTURE WORK

This paper highlighted how important it is to ensure that information within the E-Learning environment is to be secure. We have discussed need of securing E-Learning systems, basic security requirements of an E-Learning system, some of the possible attacks on the E-Learning systems and counter measures to deal with these attacks.

The future scope of our work is to both protect the active attacks and passive attacks by designing and implementing cryptography algorithm by encryption and decryption of data to make data secure.

REFERENCES

- [1]. Riyad Capital Monthly Economic Report February 2010, Issued February 27, 2010, by Khan H. Zahid, Riyad Capital.
- [2]. Qorvis Communications, LLC on behalf of the Royal Embassy of Saudi Arabia. Dec 2009.
- [3]. Education in the Kingdom an Overview, Ministry of Education, KSA Corporate Brochure7
- [4]. <http://www.internetworldstats.com/me/sa.htm>

- [5]. N. Manoehehr, "The Influence of Learning Styles on Learners in E-Learning Environments: An Empirical Study," *Computers in Higher Education Economics Review*, vol. 18, no. 1, 2006, pp. 10-14.
- [6]. Nickolova and Nickolov, 2007 Nickolova, M., Nickolov, E., 2007. Threat Model for User Security in E-Learning Systems. In: *International Journal on Information Technologies and Knowledge*, vol. 1, 2007.
- [7]. El-Khatib, K., L. Korba "Privacy and Security in E-Learning." *International Journal of Distance Education*, 2003
- [8]. Weippl, Edgar R. "Security in E-Learning" *Advances In Information Security*, Vol. 16, 2005, XVIII, 185 P. 43
- [9]. Sorene Assefa & Prof. Von Solms "An Information Security Reference Framework for e-Learning Management Systems (ISRF-e-LMS)", *Proceedings of 9th WCCE*, 2009
- [10]. Yoshihito Takahashi, Tomomi Abiko, et al "An Ontology-based e-Learning System for Network Security" *Proceedings of the 19th International Conference on Advanced Information Networking and Applications - Volume 1*, 2005
- [11]. Gary C. Kessler "An overview of cryptography" <http://www.garykessler.net/library/crypto.html>
- [12]. Bayometric, Inc., 2009, <http://www.bayometric.com/products/griaule-fingerprint-sdk.htm>
- [13]. Security token" http://en.wikipedia.org/wiki/Security_token
- [14]. Tutorial on using Access Control List <http://www.dotnet-guide.com/accesscontrol7.html>
- [15]. Tutorial on Digital Signature http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211953,00.html
- [16]. Mitja Kolšek. "Session Fixation Vulnerability in Web-based Applications." Dec. 2002.
- [17]. E. Kritzing & S.H. Von Solms "E-Learning: Incorporating Information Security Governance" *Issues in Informing Science and Information Technology Volume 3*, 2006