International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-1 E-ISSN: 2347-2693

E-Learning Security Requirements

Meenal Chavan[1] and Poonam Manjare[2]*
[1]UG Student, Dept. of CSE, Sgbau University, Amravati, India
[2]Faculty, Dept. of CSE, Sgbau University, Amravati, India

www.ijcaonline.org

Received: Dec /26/2014 Revised: Jan/8/2015 Accepted: Jan/20/2015 Published: Jan/31/2015

***Abstract*—**The security is very crucial in developing an e-learning system. Emerging standards for distance learning and education influence in a major way the development of e-learning systems. E-learning system must be secured against manipulation from the side of the students and also it protects user's privacy. This paper presents a review of e-learning privacy and security requirements.It investigates the more popular e-learning standards to determine their provisions and limitations for privacy and security. The capabilities of a number of existing privacy enhancing technologies, including methods for network privacy, security management, and trust systems, are reviewed and assessed.

***Keywords*—**E-Learning Privacy, Security Requirements, E-Learning Security

I. INTRODUCTION

The growth of Information and Communication Technology has significant effects on all people around the world. With this growth, people are able to connect with each other, especially through the Internet. These days, the Internet itself is drastically varying the provisions of services and goods, simply because of its features: immediacy, openness, ubiquity, and global reach. The approach of e-learning has become a powerful way to deliver knowledge considering the increase in on-line users. E-learning is a new education concept by using the Internet technology it delivers the digital content, provides a learner-orient environment for the teachers and students. E-learning can be defined as technology-based learning in which learning material is delivered electronically to remote learners via a computer network. E-learning could be seen as a professional level of education but with the advantages of lower time and cost. Some other advantages of e-learning include larger learner population, shortage of qualified training staff and lower cost of campus maintenance, up-to-date information and accessibility. In a typical e-learning environment the lecturers, students and information are in different geographical locations and are connected via the Internet. The e-learning promotes the construction of life-long learning opinions and learning society. E-learning is a broad concept and it consists with different types, namely Synchronous and Asynchronous e- Learning. Both methods have different characteristics and they use different methods to broadcast the learning materials [1-3]. Asynchronous e-learning occurs when students begin and complete their training courses at different times according to their own schedule. Synchronous e-learning allows real-time interaction and raises a sense of community among learners. The security is very crucial in developing an e-learning system. Emerging standards for distance learning and education influence in a major way the development of e-learning systems. E-learning system must be secured against manipulation from the side of the students and also it protects user's privacy. This paper examines privacy and security issues associated with e-learning. It presents the basic principles behind privacy practices and legislation. Security is an important issue in the actual educational context where e-learning increases in popularity and more and more people are taking online courses. The e-learning platforms are today production systems that need to be secured. To achieve a good level of security, there are many important elements that must be taken into account: authentication, access control and data integrity.

II. MOTIVATION

Security and reliability are important quality factors of almost every informatics system used in productive environments. But unfortunately for most programmers such technical realization factors alone do not imply enduring acceptance on client-side without context awareness and sophisticated adaptations to the group of users.

Considering e-learning as enhanced learning with informatics systems, we are confronted with two very contrary disciplines. The requirements for informatics systems can be managed with mostly technically oriented topics like software engineering including software ergonomics, computer networks, database design, or access control mechanisms. The more difficult task is the management of requirements implied by the context, i.e., in this case "learning". Educational research is mostly raising abstract, theoretical topics like theories of learning, activation of learners, or didactic methodologies which leads to requirements that are not technically manageable without further processing. The research project of the author deals with the interrelation of these two disciplines and aims at an implementation of a secure e-learning architecture fulfilling requirements from both disciplines. To achieve this goal, first, certain problems need to be investigated concerning the interdisciplinary in e-learning:

Which discipline is primary and in focus for e-learning?

How do these disciplines interact and imply each other? What is good e-learning if every affiliated discipline has its own criteria?

III. BACKGROUND

This section discuss about the brief background of e-learning. E-learning refers to the use of electronic media and information and communication technologies in education. E-learning is broadly inclusive of all forms of educational technology in learning and teaching. E-learning is inclusive of, and is broadly synonymous with multimedia learning, technology enhanced learning, computer-based instruction, computer-based training, computer-assisted instruction or computer-aided instruction, internet based training, web-based training, online education, virtual education, virtual learning environments which are also called learning platforms, m-learning, and digital educational collaboration. These alternative names emphasize a particular aspect, component or delivery method.

IV. ARCHITECHTURAL MODEL FOR E-LEARNING

Emerging standards for distance learning and education will influence in a major way the development of on-line learning systems. Standardization and compatibility are vital for both e-learning vendors and end users to be able to sell or purchase portable content and inter-changeable components on the market. They are also very important where different e-learning systems must interact with one another.

Figure 1 shows the typical overview of e-learning system. The learner accesses the learning resources and does the activities as instructed. The Moderator acts as a teacher me evaluate and act as moderator of the learners. In the end, there is an evaluation process. Basically, this illustration contains the processes and the databases.

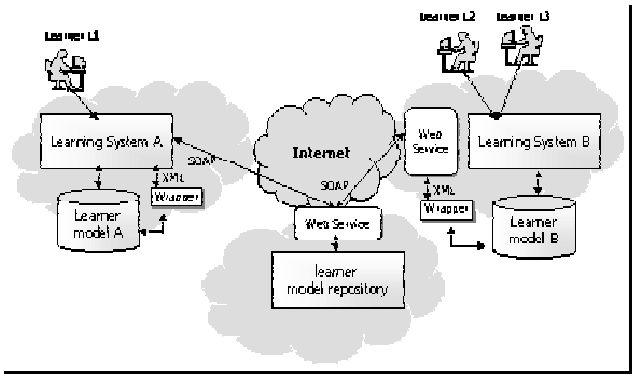

Figure 1: Architecture Model for E-learning

V. THREATS TO E-LEARNING

A loss of an asset is caused by the realization of threats or risks. All threats /risks are realized through the medium of vulnerability. The major threats are as follows-

A. ConfidentialityViolation

An unauthorized party gaining access of the assets present in E-learning system.

B. Integrity Violation

An unauthorized party accessing and tempering with an asset used in E-Learning system.

C. Denial of Services.

Prevention of legitimate access rights by disrupting traffic during the transaction among the users of E-Learning system.

D. Malicious Program.

Lines of code to damage the other programs.

E.Masquerade

Away of behaving that hides the truth by the hackers.

F.Traffic Analysis

Leakage of information by abusing communication channel.

G.Brute-Force Attack

An attempt with all possible combinations to uncover the correct one.

So all participants in E-Learning system must sit for a risk analysis where external IT and security experts could be included. Structuring of thoughts related to risks may be represented by different matrices.

VI. REMEDIES OF RISKS

Participants of E-Learning system face different risks or threats as discussed in the previous section. Following tools or techniques may be imposed to minimize those risks.

A. Access Control Using Firewall

A firewall is a combination of hardware and software security system established to prevent unauthorized access to a corporate network from outside the organization. Technically, a firewall is a specialized version of a router. Apart from the basic routing functions and rules, a router can be configured to perform the firewall functionality, with the help of additional software resources.

Main principle based on the rule is that all traffic from inside to outside and vice versa must pass through the firewall. To achieve this, all access to the local network must first be physically blocked, and access only via the firewall should be permitted. Only the traffic Authorized as per the local security policy should be allowed to pass through. The firewall itself must be strong enough, so as to render attacks on it useless. In practical implementations, a firewall is usually a combination of packet filters and application (or circuit) gateways. One such firewall is shown in Figure-1. So sophisticated firewalls can block some incoming traffic

but permit E-Learning users (may be Students, Teacher, etc.) to the inside to communicate freely from the outside. So it is the duty of all system administrators to earn knowledge and skills to implement firewall, to configure the firewall and to monitor & troubleshoot firewalls.

B. Digital Right Management (DRM) on E-learning Assets

One of the major strategies to be implemented to reduce risks associated with E-Learning assets is digital right management. Shareable asset is the simple resource, such as a static HTML page or a PDF document, or collection of files, such as images and a style-sheet. On the other hand asset of E-Learning system can be defined as E-Learning content (Exam, Notes, Grade), Cryptographic key content, User personal data, Messages between users, Different group membership data, Network bandwidth, Message integrity and Message availability. In this discussion, writers will define E-Learning asset as services provided by E-Learning system such as learning resources, examination or assessment questions, Students' results, user profile, forum contents, Students' assignment and announcement in the E-Learning system. Digital Right Management (DRM) makes the system safer for its contents. 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. That is why digitization is needed. In a general sense, DRM should be used for license agreement and copyright protection or prevents copying.

C. Cryptography

The purpose of confidentiality is to ensure that information and data are not disclosed to any unauthorized person or entity. Also readers must able to rely on the correctness of the course. One of the techniques in this aspect is cryptography. Different cryptographic tools and techniques are needed for the implementation of security in Internet based transactions. There are two types of algorithms in cryptography.

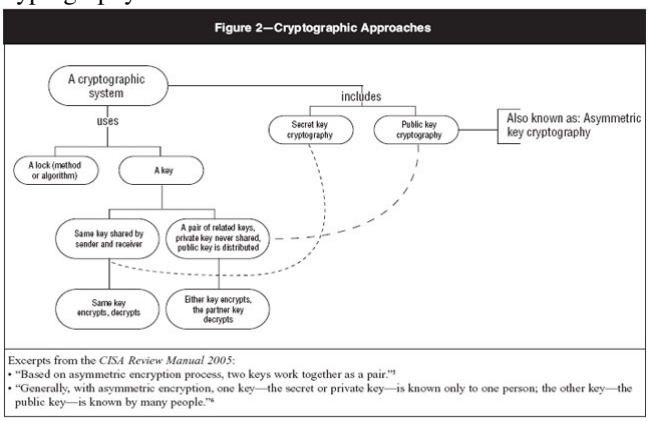

Figure 2: Cryptography Approaches

a)Secret-Key Algorithm:In secret-key algorithms the encryption & decryption key is the same, it requires the sender and receiver to agree on the key prior to the communication, the main function of this algorithm is encryption of data. Examples of such algorithms are Data Encryption Standard (DES), International Data Encryption Algorithms (IDEA), and Advanced Encryption Standard (AES). So only for encryption techniques for E-Learning content we can use these techniques.

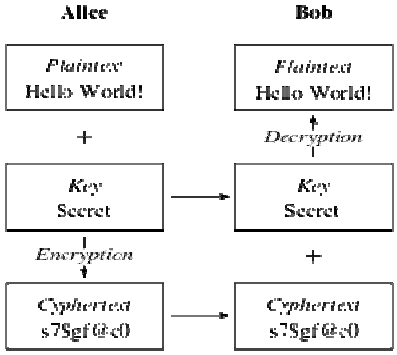

Figure 3: Encryption and Decryption

b)Public-Key Algorithm: Public key cryptosystems, on the other hand, use one key (the public key) to encrypt messages or data, and a second key (the secret key) to decrypt those messages or data. Here three mathematical models are mainly used-Integer factorization, discrete logarithms and elliptic curve. Different public-key algorithms are RSA, El-Gamal, DiffieHellman. We can use these techniques at the time of sending question paper and receiving answer sheets. To authenticate a participant we can use following technologies using public key algorithm

•Digital Signature
•Digital certificate

D. Neural Cryptography

It is a new approach based on artificial neural networks (ANN) for data security in electronic communication. It is once again a cryptosystem, which is based on biological ideas including the network architecture, biological operations and the learning process. So the complexity of the generation of the secured channel is linear with the size of the network. This biological mechanism may be used to construct an efficient encryption system using keys which change permanently. It is very simple and fast to implement in context of possible attack at the time of transferring E-Learning document.

E. Biometric Authentication

Among all authentication techniques like passwords, smart card, Digital signature and digital certificate, there is no guarantee that dishonest Students will keep their password secret. Password might be misused at the time of submission of assignment, receiving question papers,downloading of course materials, etc. where biometric authenticity would

give better security. But this needs a bit more capital investment.

VII. CONCLUSIONS

We presented the risks that may occur by different participants of E-Learning and its counter measure tools/ techniques to minimize those risks. Though in E-Learning only the Student can unlock his private data, rest all challenges remain on how to implement and maintain higher levels of privacy while setting up the learning process. Always the IT department strives to guarantee the availability of services by using redundant hardware like server, routers etc. Another important part that minimizes the risks is logs. Logs are distributed by virtue of the fact that they may be stored by different applications operating on different computers. Details of the transaction including the time of its occurrence would be "logged" and the resulting record will be secured using cryptographic techniques. We can further improve the level of security in E-Learning by applying different other techniques to minimize the risk though no system will be absolutely secured. Readers must be able to rely on the correctness of the content otherwise by reading incorrect or non-relevant content; readers will lose the trust on the texts or will refuse to read for the next time onwards. In future, the concept of m-learning will come in new electronically learning features, however new risks will also occur parallel with M-Learning.

VIII. REFERENCES

[1] F. Graf, "Providing security for e Learning", Computers & Graphics, http://dx.doi.org/10.1016/S00978493 (02)00062-6, vol. 26, no. 2, **(2002)** April, pp. 355365.

[2] Ortigosa, "Sentiment analysis in Facebook and its application to e-learning", Computers in Human Behavior, http://dx.doi.org/10.1016/j.chb.2013.05.024, **(2013)**.

[3] Vladimir I. Zuev, Management Information Systems, Vol. 7 **(2012)**, No. 2, pp. 024-028, Received 12 September 2011 Accepted 24 April 2012 UDC 37.018.43:004.738.5; 371.322:004.

[4] A. YounisAlsabawya, A. Cater-Steel and J. Soar, "IT infrastructure services as a requirement for e-learning system success", Computers & Education, vol. 69, **(2013)** November, pp. 431-451.

[5] V. I. Zuev, "e-learning Security Models", Management Information Systems, vol. 7, no. 2, **(2012)**, pp.024-028.

[6] Karforma Sunil and Ghosh Basudeb ,: On Security issues in e-learning System, " Proceedings' of COCOSY-09 ,University Institute of Technology, Burdwan University ,Jan 02-04,**(2009)**.