Review

E-learning security issues and challenges: A review

Adetoba B. T.1*, Awodele O.2 and Kuyoro S. O.2

1Department of Computer Science, Yaba College of Technology, Yaba, Lagos, Nigeria.
2Department of Computer Science, Babcock University, Ilishan, Ogun State, Nigeria.

*Corresponding author. E-mail: tiwabj@yahoo.com

Accepted 07 May, 2016

E-learning is an online or electronic learning platform which refers to a new method of learning that depends solely on the Internet in its execution. The Internet as the backbone of any system is inherently insecure. Many institutions are adopting the use of e-learning due to some of its benefits such as lower cost, faster delivery, more effective learning and lower environmental impact; without much consideration to issue of security. However, e-learning system requires a well secured environment for it to function. Security of e-learning system is one of the key factors to ensure effective delivery of content on the web. This paper is a review on e-learning, security issues and challenges, and point out the current or recent research in area of e-learning security.

Key words: E-learning, E-learning security, Internet.

INTRODUCTION

The development and application of Information Communication Technology (ICT) in education has resulted in e-learning or electronic learning which has brought about a significant improvement in learning, and at the same time given equal opportunities to everyone to become learners. E-learning also known as online learning, distance learning, virtual learning, etc are all forms of learning that take place outside a traditional learning environment and can be alternatives for learners who are not able to study in a traditional environment for various reasons. With advancement in technologies and increased use of smart phone, mobile learning has also become very popular and has given more opportunities for learners to learn anywhere and anytime (Ally, 2007). E-learning involves the use of ICT tools in order to support the learning process, whereby knowledge or information can be accessed using the communication technology (internet).

The number of student participating in online learning has dramatically increased over the years (Allen and Seaman, 2014). This increase indicates that e-learning is becoming a popular alternative to the traditional face to face learning (Pastore and Chellman, 2009). Many higher institutions of learning have also embarked on e-learning in order to increase revenue and to take advantages of its benefits. Statistics from the National Center for Education, U.S. Department revealed that in Year 2012, 925,495 students enrolled exclusively in distance education courses at private, for-profit institutions, which indicates that 35% of all students enrolled solely online (Akanegbu, 2012). This shows that e-learning has become a powerful medium and a main building block of teaching and learning in many higher institutions of learning. Therefore it needs to be secured and protected against possible attacks.

E-learning like any other e-system depends solely on the internet for sharing and distribution of information. The internet as the backbone of any e-system is inherently insecure resulting in serious security threat which includes software attacks (worms, viruses, macros, denial of service), espionage, acts of theft, hardware failure, and compromises to intellectual property (copyright, piracy, infringement). Unfortunately, very few efforts have been made to rectify this situation. Security in an e-learning environment should be given more attention to avoid this threat and to ensure a safer learning environment. Also, security is needed within e-learning environments owing to the fact that, knowledge
is important and has become a key for personal success. In e-learning, deriving useful information is amongst the main assets of any organisation.

Amongst security issues in e-learning are protection against manipulations (i.e. from either student or insider), user authentication, and confidentiality. However, as e-learning functionality is expanding, information must be actively protected to avoid the loss of confidentiality, availability and integrity. Security of information is very crucial, therefore sensitive information should be restricted only to few well defined groups, for example, learning materials for certain groups, e-result for certain individuals and copyright protection of intellectual properties. Moreover, it is difficult to verify whether or not an assignment was completed and submitted by a valid student or whether some form of cheating takes place.

E-learning like any other e-services has similar characteristics such as: accessibility through the internet, the service consumed by a person through the Internet, and the fee that must be paid by the consumer for using the e-services.

The functionality and security threats to e-learning have common features with other e-services, and the management approaches could also have common characteristics. For any institutions and organisations to protect and maximise return on their investment in learning technology, content and services, the systems they use must be interoperable, usable, manageable, and durable (Alwi and Fan, 2010). Previous studies have shown that there are barriers to a more wide-spread adoption of online education (Allen and Seaman, 2014). The reason behind such barriers is not the high costs or the greater level of tasks which need to be carried out, but rather the security aspect. Take for instance; it is difficult to verify the identity of a person to know whether or not he/she is a genuine student or an impostor when asked to submit assignment online. The identity and the secure content are difficult to maintain. Finally, security issues in e-learning have only been addressed mostly by security technologist; for instance a technical framework on access control, authentication and accountability, protection of communications, non-repudiation issues and learning resource provider server protection (Alwi and Fan, 2010). This paper reviewed e-learning security issues and challenges and point out current or recent research in area of e-learning security.

RELATED WORKS

A number of security issues were raised in previous studies regarding security in e-learning systems. May and George (2011) focused on privacy and security issues in e-learning and came up with some issues such as Protection of personal data, anonymous use, address and location privacy, authentication, digital right management, etc. The work mentioned that learners are concerned about the protection of their sensitive data while technology providers are finding ways of securing the learning environment and also the storage of learner’s data.

Levy (2011) discussed user authentication as an important issue to consider in e-learning security. The work shows that with varying software and hardware requirements, policies and strategies should be put in place to ensure appropriate authentication of the learner.

Chen and He (2013) highlight some security issues in online learning systems which includes identity theft, impersonation, and inadequate authentication. Saleh and Wahid (2015) also mentioned authenticity, access control, confidentiality, integrity, availability, and non-repudiation as various sources of e-learning security threats.

Barik and Karforma (2012) also discussed various security risk or threat in e-learning. Some of which includes confidentiality violation, integrity violation, denial of service, etc. and providing remedies to minimise all these risk.

From the above literature, it can be seen that the security issues in e-learning can be categorised under the following:

(1) **Availability:** In e-learning, availability is the assurance that the e-learning environment is accessible by authorised users, whenever it is needed. Availability can be divided into two: Denial of Service attack (DoS – an attack that stop access to authorized users of a website, so that the site is forced to offer a reduced level of service or, in some cases, ceases operation completely) and loss of data processing capabilities. The e-learning 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. Failing to fulfill this will have a huge impact on e-learning users and providers (Alwi and Fan, 2010).

(2) **Integrity of Information:** This is the protection of data from unauthorised changes (i.e. only authorised users or processes are allowed to 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, masqueraders, unauthorised user activity, unprotected downloaded files, LANs, and unauthorised programs (e.g., Trojan horses and viruses), simply because each of these threats can lead to unauthorised changes to data or programs.

(3) **Confidentiality:** This is the protection of information in the system so that unauthorised persons cannot gain access.

(4) **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.
(5) Authorisation: Authentication checks whether or not the authenticated person has right or privilege to access the contents of the system (Assefa and Solms, 2009).

From various studies conducted, it has been discovered that, in order to avoid all security attacks on the e-learning environment, controlling access is paramount and one way of achieving this is through the authentication and authorisation process.

E-LEARNING SECURITY CHALLENGES

E-learning security plays a very important role in e-learning systems development despite its huge benefits. There are numerous challenges faced by learners, Higher learning Institutions and e-learning service providers in today’s internet age. Some of these challenges include:

(a) Interoperability of applications: Despite current technological advances in e-learning, emerging trends are demanding a greater level of interoperability for components, systems, applications, and environments which are often developed for a particular institutions or organization and provide very similar functionalities (Cardenas and Sanchez, 2005).

(b) Standardization and compatibility: are vital for both e-learning service providers and end users (learners) to be able to inter-change components in the market. These are very important where different e-learning systems must interact with one another.

(c) Security policy and enforcement Mechanism: The security policy is defined as the set of laws, rules and practices that regulate how an organization manages, protects and distributes sensitive information. Once the security policy is defined, it must be captured and followed at application runtime via an enforcement mechanism which represents the set of centralized and distribute software to ensure that the security policy is maintained and never violated.

(d) E-learning Infrastructure: This refers to Hardware, Software and connectivity required for e-learning development and implementation (Taurus et al., 2015).

POSSIBLE ATTACKS ON E-LEARNING SYSTEM AND COUNTERMEASURES

Bokhari et al. (nd) mentioned some possible attacks and countermeasures associated with e-learning system and summarised them into the following categories:

(1) 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.

(2) 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.

(3) 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. Strong encryption methods should to be used to counter confidentiality attack.

(4) Authentication attack: The attack is to gain access to system information by using stolen passwords, key or credentials or an attack device pretending as 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 includes 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 Biometric based security should be considered.

(5) Authorization attacks: 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.

(6) Countering non-Repudiation: To counter the problem of non-repudiation, digital signature can be used and Audit trails should be created

CURRENT RESEARCH IN E-LEARNING SECURITY

E-learning system will be more secured and more user-centered if new technologies are adopted. Some recent research trends are listed as follows:

(a) Development of Personal Learning Environment (PLE): Personal Learning environment is a learning environment that helps learners take control of and manage their own learning needs (Van Harmelen, 2008). It integrates a number of “web 2.0” technologies such as blogs, wikis, twitter, face book, etc. to connect individual learner to his/her own learning needs and interest thereby achieving learning goals (i.e. learning is tailored to meet individual learners need). A report from the American Institute of Research (AIR), 2013 about the
next wave of K12 education reform talks about the opportunities, promises and pitfalls in the design and development of PLE. They concluded that PLE can increase academic success and college and career readiness provided certain requirements are met. Attwell (2007) also concluded that PLE is a new trend or development (i.e. a significant move forward) and an answer to the future education and learning problem.

(b) Biometric Authentication System: Biometric authentication system has been proposed to be the next option for future e-learning users (Wang et al., 2013). Biometrics refers to the use of identification mechanism that distinguishes an individual based on his/her physiological and behavioral characteristics (Asha and Chellappan, 2008). Recent research have shown that biometric is becoming a principal method of securing any e-system. Biometric system can be unimodal (a single biometric feature of person identification) or multimodal biometric systems (i.e. several biometric features at the same time). Alotaibi and Argles (2011) proposed a biometric authentication system, Finger ID, which requires a fingerprint scan and human interaction to utilize a service. Meanwhile, Song et al. (2013) also proposed another method that uses brain wave and eye movement to authenticate users of online learning systems.

(c) Security for Online Assessments: One major component in e-learning is the assessment which accounts for a significant part of teachers’ workload, especially in situation where we have large student groups (i.e. in developing countries). High quality assessments are those consistent with a high level of reliability and validity. Online assessment is very important to ascertain students’ progress (Reeves, 2000; Meyer and Zhu, 2013). Previous research has shown that 73.6% of students think that cheating in an online environment is easier than in traditional classroom setting (Guyette and Piotrowski, 2009). Therefore, improving the security of e-learning will improve the security of online assessments, and this should not be neglected. Some models have been proposed but have their advantages and disadvantages. New models need to be developed to secure online learning assessment.

Security is an important factor in e-learning system. The goal of security for e-learning is to maintain the confidentiality of data or information, integrity of information and availability of e-learning resources at a certain level while keeping their usability acceptable for learners.

CONCLUSION

E-Learning offers a lot of opportunities for the expansion of education and learning beyond the classroom, particularly, in developing countries. The major challenge in e-learning today is the issue of security. Lack of attention to security issues in e-learning is a problem because important issues of student and staff privacy are at stake and also online learning credibility is at stake. Security elements, such as availability, integrity and confidentiality should be given more attention in order to prevent security breaches before it is too late.

REFERENCES

