International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 21 Issue 3 – APRIL 2016.

Security Attacks and Threats in E-Learning

R.Priya[#1] and J.Jayanthi[*2]

[#]*PG Student, Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India*

[*] *Assistant Professor, Department of Information Technology, Sri Ganesh College of Engineering and Technology, Puducherry, India*

***Abstract*— E-learning is a smarter way of learning environment by which it deepens the knowledge skills. As it is an online based application system it is easily susceptible to various attacks and threats. It is vital to detect and realize the attacks and threats that occurs on the application. Nowadays, information security plays a vigorous role in each and every field since everything becomes online. The exposure of internet and its loopholes leads to various attacks in day to day approaches. It is difficult to build an application without loopholes but due to the security consciousness it can be controlled to an assured range. This paper explains about the various security attacks that are possible in an E-learning environment at user side, network and server side.**

***Index Terms*—E-learning, E-learning issues, Information security, Security.**

I. INTRODUCTION

E-learning can be defined as the smart way of learning environment with the help of growing technologies that are interconnected with the web by which it enriches the knowledge skills. Learning is considered to be a constant process. Progressive growth of e-learning methodologies increases the learning and provides identical chance to each of them to be a good learner. With the help of various transforms of technology now learning becomes an easier way to all. E-learning includes everything in the form of electronic such as learning online courses, online assessment, online video classes, electronic study materials etc. Also, the e-learning does not require any classrooms like traditional learning that is learning can be done anywhere and anytime. The learner needs system, mobile or laptop should be connected to the internet and passion to learn these are simple requirements of e-learning. Currently, e-learning gained its more attention in educational organization due to its creativity, animation, text, audio, video etc. The e-learning types are as follows:

- Synchronous
- Asynchronous

In synchronous e-learning the learner and the trainer will present in online at a time and connected with each other from various places. Both will have an interactive session also exchange their ideas through video conferencing, webinars etc. In asynchronous e-learning the learner and the trainer will not to be present in online at a time the learner can learn anytime by downloading e-materials also it is in the form of self-study with the help of internet viz studying from blogs, forums, e- materials.

Information security gained its importance in almost each and every fields around the sphere. The organization must understand the importance of their assets and protect them without considering the cost. Also, there should not be any compromise in security issues. If the security issue occurs, it should be monitored thoroughly without any ignorance sometimes the occurred issue may be false negative. The information once uploaded in the web is endlessly unprotected to various security issues. The information that are related to e-learning background specifically which may be private, preserve, trusted should be safeguarded from wide open threats and attacks since many e-learning environment are vulnerable, scattered and interrelated.

The pillars of information security are confidentiality, integrity and availability. There should not be any compromise because if anyone of them is subjected to be vulnerable the entire environment is collapsed.

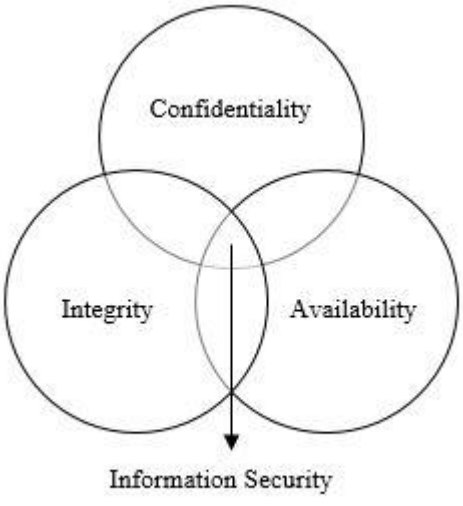

Fig. 1 Pillars of Information Security

Confidentiality ensures that the information is protected and cannot be accessed by divulged illegal persons. But nowadays these type of information are most frequently attacked.

Integrity confirm that the information is not tampered or modified throughout the network by unauthorized persons. Thereby, it ensures that the information is reliable and unaltered.

Availability describes that the information that are easily accessed to the authorized persons when it is needed.

I. Impact and Security Measures of CIA

Pillars of Information Security	Impact of CIA Information	Security Measures
Confidentiality	Loss of secrecy, gains illegal information access	Enabling cryptographic techniques, encryption algorithm, access control list, and proper authentication
Integrity	Tampered, modified, not reliable	Enabling hashing, message digest and digital signature
Availability	Distributed Denial of Service attack	Periodical back up of the information

The basic security definition in information security are

- Threat
- Vulnerability
- Attack

Threat is indicated as the possible event in order to damage the system such as an attack. It is considered to be a danger to the system. The threat may be or may not be true.

Vulnerability is a flaw or weakness of the arrangement made by a system that causes vulnerable to an attack.

Attack is an exploit which is done in contrast to the system in order to cause damage to the target. An attack can be successfully done when all the security aspects that are made available to the system are compromised. If the threat and vulnerability issues that are not properly identified and rectified that may leads to severe impact to the system.

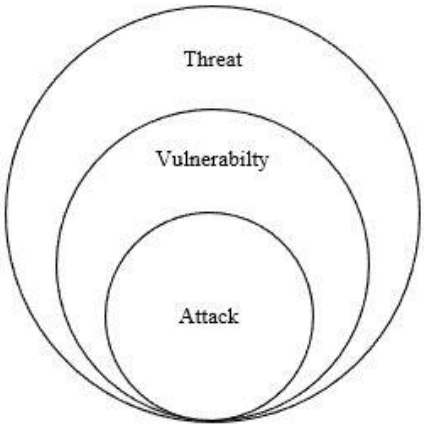

Fig. 2 Basics terms of Information Security

II. RELATED WORK

II. Overview of Literature Survey

PAPER TITLE NAME	YEAR	AUTHOR	ISSUES ADDRESSED
Information Security in an E-learning Environment	2006	E. Kritzinger [1]	Its purpose is to distinguish between traditional, online learning with the security issues such as illegal access to E-Learning information. To protect the E-Learning system from attack it provides solution in both technical and practical level.
Computer Security Threats Towards the E-Learning System Assets	2011	Zainal Fikri Zamzuri et al.[2]	The assets of E-Learning that are subjected to security threat are addressed. The assets of E-Learning were investigated and assessed against the threat model such as STRIDE Model.
E-Learning Security Vulnerabilities	2012	Ciobanu (Defta) Costinela-Luminița et al. [3]	The E-Learning vulnerabilities and threat are addressed. The confidentiality issues that are tackled in E-learning and Moodle were exhibited.
E-Learning and Security Threats	2012	Ateeq Ahmad et al. [4]	It focuses on the fundamental security threats that are related to E-Learning systems. It also provides some of the security measures for it.
SQL Injections Attack and Session Hijacking on E-Learning System	2014	Sum Keng Chung1et al. [5]	It gives the overview of various attacks that are performed in online. They analyzed SQL injection, Session hijacking as a case study and they proposed the solution for these two attacks.

III. SCENARIO AND SECURITY CONCERN IN E-LEARNING ENVIRONMENT

The basic scenario of e-learning environment are as follows:

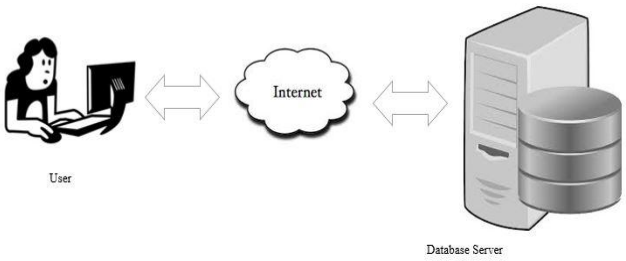

Fig. 3 Scenario of E-Learning Environment

The user access the e-learning material via internet for educational purposes. The developed environment contains three portions such as

- User
- Internet
- Database Server

The user is one who access the material for studying, learning, downloading and submitting the assignment. Also, the user can request the material to the server.
Internet is a type of medium through which the e-learning material is shared. It acts like a bridge between user and server.
Database server is a server through which the materials are accessed by the user. The server responds to the user needs accordingly through which the request has been made.

A. Security Threats in E-Learning Environment

The security threats that are possible in e-learning environment is

- Virus
- Worm
- Trojan horse
- Malware
- Adware
- Spyware
- Rootkit

A computer virus is a malicious programs that are intended to cause damage to the system. It attaches itself to the individual files or a set of files which may cause malicious activity. The written malicious code or scripts may severely affect the system. They may look like small blocks of code causing malicious activity such as occupying large amount of hard disk space, corrupting files and folders, slow start up. They itself create the replica and spreads over the entire system.

A worm is a malicious program which creates replication of itself and outspread to the network of computers that are interconnected into it. The network is considered as the medium for the worm to outspread. The impact of worm leads to data corruption, remote listening.

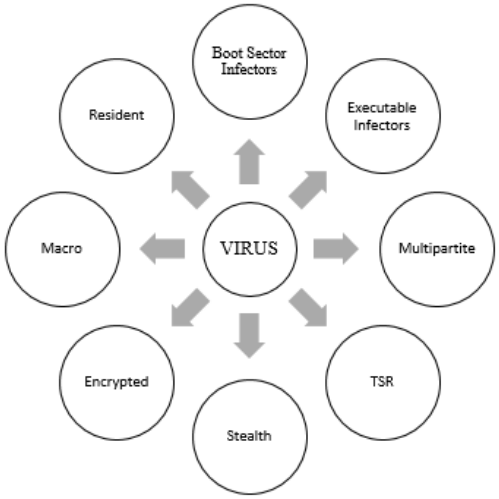

Fig. 4 Types of viruses

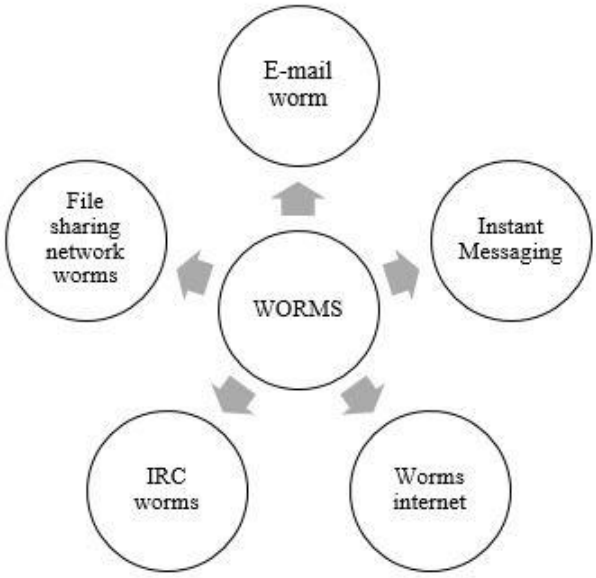

Fig.5 Types of viruses

Trojan horse is a malicious type of malware which executes like a legitimate program but pretend to execute malicious activities such as remote listening, illegal access to the system, data theft, also it creates a back door to the attacker to enter into the system.

Malware is a malicious program intended by malicious software which cause harmful impact or unsolicited activities that are executed in the computer.

Adware is a malicious program that are inserted into the advertisement that are pop up often if the user makes a click on it may lead to identity theft by grabbing credentials from users or it may download other malicious software.

Spyware that executes like a software and the main intention of it is to collect fact about the individual person or institution the monitored details will be redirected to the attacker or system that are connected. The impact of spyware may lead to monitoring of the system.

Rootkit is a malicious software that are executed at the time of boot up. They are very hard to identify since they get initiated Earlier when operating system boots up. They includes installation of unseen files, malicious user accounts. They are interrupted by network connections.

B. Cyber Security Attacks in E-Learning Environment at User side

- Phishing
- Cross side scripting
- Click jacking
- Content Spoofing
- Brute force attack
- Authentication attack

Phishing is an endeavor to gain user's private credentials. It is widely spread and done through the email links. The attacker will deliver the phished E-learning website links to large number of users. The users who are unacquainted of this type of cyber-attack may succumb into this lure. The appearance of the phished website looks more or less similar to the legitimate E-learning website. The attacker gains huge profit by demanding the grabbed user's credentials.

Cross side scripting is also known as XSS attack. It is one of the well-known attack that occurs in web application. In this attack, the genuine E-learning webpage is injected with malicious scripting code by the attacker. The malicious code is executed when the user clicks on to the link. This link will readdresses to the spurious E-learning webpage and takes the user identifications. By the grabbed credentials the attacker may deface the user profile.

Click Jacking alter is UI redress attack [6]. The user opens the E-learning webpage, the attacker performs the emerge on the legitimate E-learning webpage such that you have won the Free Online course material which cost rupees of several thousand if the user clicks on to that pop up it will readdress to the bogus website and it informs the user to avail that free course you must enter your credentials such as username, password, bank account details. The users who are all unconscious of this type of attack will enters their credentials which will leads to severe impact. Moreover the attacker uses attractive words to click on that pop up.

Content Spoofing ruses a user to trust that the appearance and content looks exactly same as the legitimate website and from an attacker.

Brute force attack uses the trial and error process to acquire the user credentials.

Authentication attack aims to crack and abuse the validation process that a website uses to authenticate the uniqueness of a user.

C. Cyber Security Attacks in E-Learning Environment over the internet

- Sniffing
- DOS
- DDOS
- Spoofing
- Replay attack

Sniffing is considered to be one of the common attack in the network. As many of the E-Learning website uses individual login id and password for each and every user who have registered into their website. The sniffer captures the entire communication by using sniffing tools. If the website does not uses encryption of username and password then task the sniffer is very easy because it does not contains any encryption.

Denial of Service attack can be performed on the network to overload the specific target and thwarting the genuine user to accessing the particular target or application.

Distributed Denial of Service attack can be performed with multiple systems and internet that are connected and thwarting the genuine users to accessing the particular target or application.

Spoofing attack is done by malevolent party by mimicking an unveiling attack for larceny details or access control sidestep.

Replay attack are done on the network in which the attacker secretly sniffs the exchange of information between the users and server to gain the valid evidence.

D. Cyber Security Attacks in E-Learning Environment at Database Server

- SQL Injection
- LDAP Injection
- Weak Authentication

SQL injection involves injection or placing of structured query language statements to remove the existing content they are injected into the database and dumped by the malicious attacker query statements. The gainful SQL injection attack may allow the attacker to view the data, leakage of sensitive details, alter the data, causing damage to the stored data and make it inaccessible.

LDAP is expanded as Lightweight Directory Access Protocol [7]. It is a type of attack which negotiates and abuses the vulnerability that are present in the web application by generating the LDAP statements which are given as the input by the user. By altering the LDAP statement that are present in the E-Learning web application may leads to illegal access, permitting the attacker to deface the web application content.

Weak Authentication may leads to many type of attacks such password guessing, dictionary attacks, illegal access to contents. To safeguards and to avoid leakage of data it should be enabled with strong security measures.

IV. CONCLUSION

In this paper, the specific security attacks that are address at user side, network, and server side are defined. The progress of E-learning must be executed by using highly accepted security standardization. The E-Learning web application must involve the security measures such as proper sanitization of the user input, privileged access, authentication, authorization and permissions. The exchange of information between user and server must be encrypted by using secure communication channel. Moreover, the application must built the security traits throughout the entire communication.

REFERENCES

[1] E. Kritzinger, "Information Security in an E-learning Environment" in Education for the 21st Century — Impact of ICT and Digital Resources: IFIP 19th World Computer Congress, TC-3, Education, Deepak Kumar, Joe Turner, Eds. US: Springer, 2006, pp 345-349.

[2] Zainal Fikri Zamzuri , Mazani Manaf , Adnan Ahmad , Yuzaimi Yunus "Computer Security Threats Towards the E-Learning System Assets" in Software Engineering and Computer Systems: Proc. Of the Second International Conference, ICSECS, Part II, Jasni Mohamad Zain, Wan Maseri bt Wan Mohd , Eyas El-Qawasmeh, Eds. Berlin: Springer, 2011, pp 335-345.

[3] Ciobanu (Defta) Costinela-Luminița, Ciobanu (Iacob) Nicoleta-Magdalena, "E-learning Security Vulnerabilities" Procedia - Social and Behavioral: 4th World Conference on Educational Sciences (WCES-2012) Sciences, Vol. 46, pp. 2297 – 2301, February 2012.

[4] Ateeq Ahmad, Mohammed Ahmed Elhossiny, "E-Learning and Security Threats," International Journal of Computer Science and Network Security, vol.12, no.4, April 2012.

[5] S. K. Chung, O. C. Yee, M. M. Singh and R. Hassan, "SQL injections attack and session hijacking on e-learning systems," Computer, Communications, and Control Technology (I4CT), 2014 International Conference on, Langkawi, 2014, pp. 338-342.

[6] https://www.owasp.org/index.php/Clickjacking

[7] https://www.owasp.org/index.php/Testing_for_LDAP_Injection_(OTG-INPVAL-006)

R.Priya pursuing her M.Tech (Information Security) in Computer Science and Engineering from Pondicherry Engineering College, Puducherry. She completed her B.Tech degree in Information Technology from Sri Ganesh College of Engineering and Technology, Puducherry. Her research interest is Information Security.

J.Jayanthi, Assistant Professor, Department of Information Technology, Sri Ganesh College of Engineering and Technology, Puducherry. She received her B.Tech degree in Information Technology from IFET College of Engineering, Anna University and completed her M.E degree in Computer Science and Engineering from Arunai Engineering College, Anna University, Chennai. Her research interest are in Computer Organization and Architecture, Networking.