Security Aspects for e-Learning Portals

Natalia Miloslavskaya, Vladislav Petrov and Alexander Tolstoy
The National Research Nuclear University «MEPhI», 31 Kashirskoye shosse, Moscow, Russia

Keywords: Distance Learning, e-Learning, e-Learning Portal, Information Security, Security Subsystems.

Abstract: Many safety problems are facing e-Learning portals (EP) developers to make it a trusted tool for e-Learning. The paper gives motivation of security implementation expedience for EP including a brief overview of typical attacks against EP. Further a generalised EP structure as a protection object is created and the key security requirements and functional security subsystem components of a secure EP are developed. In conclusion a real example of the secure EP on the basis of "DOCENT" distance learning system (DLS) by the Russian company UNIAR being used in the National Research Nuclear University «MEPhI» is shown.

1 INTRODUCTION

Today many educational institutions have their corporate information and telecommunication networks – Intranets, intended to integrate parties, processes and information within them. In general an Intranet uses the Internet-based technologies to facilitate communication and access to information with a common entry – portal (Jonas, 2008). At the Universities it usually contains a part designed especially for supporting e-Learning – an e-Learning Portal (EP). As an amalgamation of hardware and software applications, it provides a personalized single point of access to educational applications, content, parties and processes through one common user Web interface. The EP accumulates data from diverse internal and external sources, provides access to data by all users, presents information in the format appropriate for each of them, provides underlying services for such an applications as storage, processing, search, collaboration, workflow and security and also guarantee performance and availability. As a traditional portal, the EP has no client software dependencies beyond a Web browser.

The EPs have different specific aims and focus on guiding students through a structured learning experience and providing the necessary human factors support to increase the effectiveness of the portal as a means of an educational material delivery. The EP is a thematic guide to quality-controlled information and knowledge on the Internet, focusing on education and lifelong learning. Many of Distance Learning (DL) needs could be solved via the EP usage: permanent uniform administration and management over the whole educational process through a web platform; modern learning infrastructure accessible anywhere and anytime; cost-effective training through DL interfaces; personalised single point-of-access desktop to DL resources and applications; access to pedagogical resources through the possibility of referring to high-quality on-line resources from multiple sources through content syndications; effective integration of computer technology use into classroom curriculum in order to improve students' learning and achievement; communication and collaboration through e-mail, videoconferencing and threaded discussions. DL teachers have an access to relevant information for educational decision-making and are able to prepare and enter into the system lessons from home. The EP supports testing of students' abilities as they follow the courses, so include various forms of assessment. Assignment and examination materials and results must therefore be presented in a personalised and confidential way.

Unfortunately all of the listed objects and processes can become a target of unauthorized access by malefactors having various goals – to steal training materials and tests, to obtain a certificate without any real training, to arrange substitution while passing test and so on.

In DL both remote students and universities have direct security concerns. Thus problems of development, integration and maintenance secure subsystems supporting DL is highly urgent for many educational institutions.

Miloslavskaya N., Petrov V. and Tolstoy A..
Security Aspects for e-Learning Portals.
DOI: 10.5220/0004940204270432
In *Proceedings of the 6th International Conference on Computer Supported Education* (CSEDU-2014), pages 427-432
ISBN: 978-989-758-020-8

2 RELATED WORKS

Problem of DL and security were discussed by various scientists during more than a previous decade. The necessity for securing online DL because of its use of the Internet as a communication medium was proved by (Furnell, Karweni, 2001) yet in 2001! They listed the following typical information security (IS) threats in DL content: malicious software such as viruses, worms, Trojan Horses, Denial of service attacks, masquerading, spoofing, fraud, data theft and so on.

The paper's authors experience in solving security problems in DL as a whole and for progress testing can be found in (Diatchenko, Miloslavskaya, Tolstoy, 2001), (Miloslavskaya, Tolstoy, 2003) and (Miloslavskaya, Tolstoy, 2004). But till now the given problems are still up-to-date.

At present not only data security should be supported – capturing of students' personal information and their privacy are becoming a source of growing concern (Siciliano, 2013). In (Kavun, Sorbat, Sorbat, 2012) authors consider the security aspects that are directly relevant to DLS and identify major elements of them (or subsystems-services): security mechanisms as identification and authentication and services like Web site, e-mail and ftp server. DLS should have adequate tools to protect content, personal data, copyrights and passwords from disclosure, attacks on its integrity and "denial of service" (DoS) attacks.

The given problems are thoroughly examined in many scientific works, conferences (like IEEE Symposium on Security & Privacy 2013, May 19-22, USA, San Francisco) and specially devoted to these issues The Open Web Application Security Project (OWASP) [http://www.owasp.org].

3 GENERALIZED EP STRUCTURE

Different EP structures should be generalized to pick out main DLS objects and processes requiring protection. The EPs consolidate, manage, analyse and distribute information across the identified learning community (not necessarily only University students, but also short term trainees, possible from another countries). Content Management Systems (CMS) process, filter and refine "unstructured" data and information, often restructure it and store it in a centralized/distributed repository. Business Intelligence tools access data and information and through querying, reporting, on-line analytical processing. Data Mining and Analytical Applications provide a view of information both presentable and significant to the end user. Data Warehouses and Data Marts are integrated, time-variant, non-volatile collections of data supporting applications. Data Management Systems perform extraction, transformation and loading, clean data, and facilitate scheduling, administration and metadata management for data warehouses and data marts. The Learning CMS (LCMS) is an environment that consolidates planning, building and evaluation of the learning/educational process and covers the tools for creating, arranging and consolidating content parts. As it can be seen even all the modern information and network technologies are used for EP functioning support.

Proposed general model of EP structure from Infrastructure, Learning Services and Applications viewpoints is represented in Figure 1.

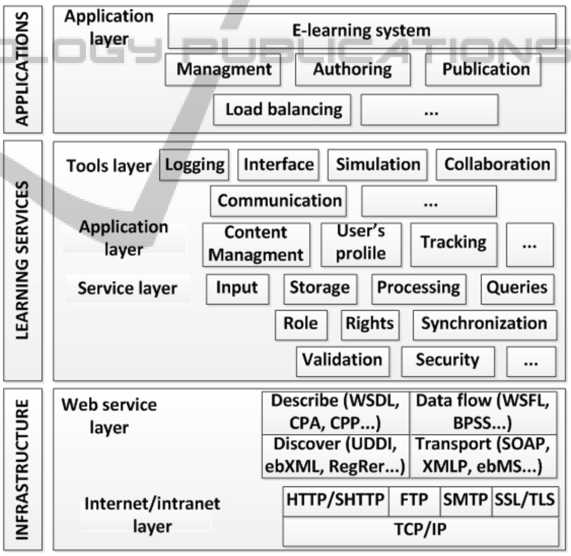

Figure 1: EP structure.

The Internet layer and its information flow protocols are used at EP Infrastructure. The EP utilizes HTTP/SHTTP for data transfer and FTP for uploading the materials. The SSL/TLS protocols are intended for session protection while an author or an administrator works with the resources. The SMTP (or ESMTP which is better from the security point of view) is used in the EP e-mail system. The SOAP, which is in the Web service layer of the Infrastructure, is used for making the data into packages and forwarding it to external sources. Data flow management protocols are also included in the model as well as discover and describe services.

Learning services, used in EP at higher levels, can be divided into the three groups – common services (for data processing), common applications (for DLS resources management) and tools layer (for logging, interfaces and communications). Applications' layer contains DLS itself, its management and different supporting subsystems (such as publishing and authoring).

4 TYPICAL ATTACKS AGAINST EP

Generally as a typical information system and a classical Web application any EP is subjected to all typical attacks on it. A quick search in the National Vulnerability Database [http://nvd.nist.gov] shows the following problems in DLS:

- SQL injection in search_result.asp in Pre Projects Pre E-Learning Portal allows remote attackers to execute arbitrary SQL commands via the course_ID parameter;
- PreProjects Pre E-Learning Portal stores db_elearning.mdb under the web root with insufficient access control, which allows remote attackers to obtain passwords via a direct request;
- directory traversal in user_portal.php in the Dokeos E-Learning System 1.8.5 on Windows allows remote attackers to include and execute arbitrary local files via a ..\ (dot dot backslash) in the include parameter;
- Multiple cross-site scripting (XSS) in Blackboard Learning System 6, Blackboard Learning and Community Portal Suite 6.2.3.23, and Blackboard Vista 4 allow remote attackers to inject arbitrary Javascript, VBScript, or HTML via data, vbscript and malformed javascript URIs in various HTML tags when posting to the Discussion Board;…

Main types of attacks on DLS can be divided into attacks on the DLS components and attacks on the participating parties – instructor/curator/ administrator and trainees. Here are some examples.

There is a possibility when trainees will try to get a certificate of successful training completion without studying all the provided educational material. To do this they will have to successfully pass exams/test/quizzes, but they may not be having sufficient knowledge on the subject. In that case the DLS interaction data and evaluation code can be potentially exposed (for example using a sniffer intercepting network traffic) and analyzed by a cheater to beat the test. The data collected through the DLS use interface can be analyzed offline. A malicious person can reconfigure DLS settings (of course under certain circumstances).

In practice all Web client-server architecture components (servers, clients and channels) are susceptible to very many old and modern security threats (executable because some vulnerabilities are still alive). For example two most widespread attacks on Session ID are XSS (it allows abducting Session ID from lawful users) and "phishing" (it lures the unsuspecting user to a fake web site looking and acting like trustworthy site).

CGI scripts usage is the next Web server threat, as far as many of CGI scripts contain program errors, which can be used as loopholes by malicious persons. In turn Java and JavaScript usage is one more problem to be concerned with. Unlike CGI scripts Java code is run on a client side and that is why cannot damage a Web server, but can contribute troubles to a client. Ensuring secure usage of Java and JavaScript is based on a browser used by a client. Many of these problems appear as a result of the errors in Java interpreters used by the browsers.

Plus possibility of theft and substitution of cookies – a small data piece sent from EP and stored in a trainee's web browser while the user is browsing that EP. Cookies can store passwords and forms a trainee has previously filled out, such as an address or a credit card number. The authentication cookie's security generally depends on the security of the issuing website (EP) and the trainee's web browser, and on whether the cookie data is encrypted. Security vulnerabilities may allow a cookie's data to be read by a hacker, used to gain access to user data or to the EP (with the user's credentials).

There is also a problem of construction of secure authentication and authorization subsystems while integrating several automated systems into a portal. As the majority of modern DLS are SCORM compliant (Sharable Content Object Reference Model) it is justified to look at SCORM security requirements. SCORM has no specific provisions to provide for content, sessions and test security. How to ensure that users are authenticated is also out of SCORM scope. So is ensuring that users cannot tamper with the software on their computer while experiencing SCORM content. The higher the stakes in a test, the more incentive there is for some learners to cheat. The Tin Can API is the newest, more secure version of SCORM, but it does not solve old DL security problems. The Tin Can API developers outline one of its advantages – Oauth usage. The National Vulnerability Database highlighted several records concerning Oauth vulnerabilities being found in 2012-2013:

- XSS in some IBM WebSphere Application Server (WAS), when OAuth is used, allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors;
- Cross-site request forgery (CSRF) in the omniauth-oauth2 gem 1.1.1 and earlier for Ruby allows remote attackers to hijack the authentication of users for requests that modify session state;
- DaoAuthenticationProvider in some VMware SpringSource Spring Security does not check the password if the user is not found, which might allow remote attackers to enumerate valid usernames via a series of login requests;
- tmhOAuth before 0.61 does not verify that the server hostname matches a domain name in the subject's Common Name or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate;
- Content Security Policy (CSP) functionality in some Mozilla Firefox, Firefox ESR, Thunderbird, Thunderbird ESR and SeaMonkey does not properly restrict the strings placed into the blocked-uri parameter of a violation report, which allows remote web servers to capture OpenID credentials and OAuth 2.0 access tokens by triggering a violation and so on.

On the other hand another technologies used in the EP (such as sharing documents, support for virtual, distributed working teams, usage of different communication tools and protocols, data repositories, publishing systems etc.) need protection against their own specific types of threats leading to different local and remote attacks. For example besides many basic possibilities many EP solutions have tools for students' works publishing that essentially increases risk of distribution of data containing malicious code: viruses, Trojan programs, malicious mobile applications etc.

Another big problem – how do you know that the person taking a test is really the person you are trying to test?

Therefore it is not exaggeration to conclude that at the moment the lack of affordable and reliable ways of authentication of the student in the learning process, and most important, during the distance intermediate and final control of knowledge does not give full confidence in usage of the distance testing system.

It is considered that the DL scenario principally demands attention to the following areas:

- authentication (the right person should present the right login and password to the DLS – no masquerading);
- accountability and access control (of all actions that can influence DLS security);
- confidentiality where it is necessary;
- availability (24/7) of all DLS components;
- protection of communications;
- non-repudiation issues;
- DL server with various data protection.

At present any DL server with all its databases and services can be investigated as a cloud. Its main IS problems are the very typical: data loss and data leakage, account or service traffic hijacking, insecure interfaces and APIs, DoS, malicious insiders, abuse, insufficient due diligence and shared technology vulnerabilities (Samson, 2012).

The given analysis shows that IS threats to EP are still exist and are not solved yet.

5 EP SECURITY SUBSYSTEM

Thus EP application must include robust security. EP application, such as that required by the consumer self-service solution, must include robust security. It means more emphasis on the EP resources' and clients' information security including such an important items as privacy, content integrity, recognition, accessibility, confidentiality, availability etc. It is reasonable to elaborate implied EP security requirements and a complex approach to their realization in the form of an information protection subsystem as an integral (build-in) part of a secure EP.

The majority of traditional universities can typically be seen to have a number of protection measures in place, such as anti-virus software, scanning and monitoring tools, prevention of unauthorized software installation, IT usage policy etc. But presence of written, approved, maintained and communicated IS policies for all EP components and users is critical. Without EP Security Policies (EPSP) there is no general DL security framework. They provide guidelines to users on processing, storage and transmission of EP resources and define what behavior is and is not allowed. EPSP consist of policies for user accounts and passwords, remote access, personal information protection and many others.

While many definitions of security mechanisms exist, for the sake of simplicity the list of key EP security requirements should be defined as follows: general security, authentication, fine-granted access control to EP resources, encryption, centralized security events audit (including control, account and analysis resources using and submitted user data verification) and also internal resources' protection.

The EP engine is responsible for the execution and rendering of EP logics. Well-designed EP technologies combine standard processes for inventorying and organizing sources of information, identifying users and owners of that information and establishing rules for granting and controlling access plus flexible administration models for cost-effective and time-efficient management.

The basic subsystems in the overall generalized secure EP are suggested in Figure 2 (it is generic and can be applied to practically all web sites/portals).

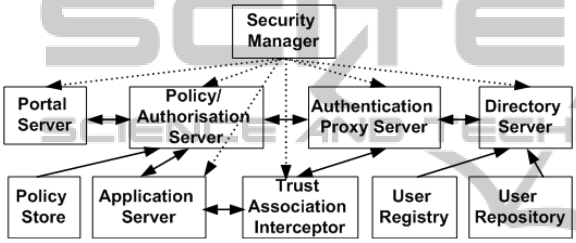

Figure 2: Secure EP Architecture.

The key component is a single, centralized *Security Manager* that activates required Security Services in addition to the other EP subsystems and coordinates all security tools managing a distributed, constantly changing e-learning environment. *EP server (PS)* uses one of the APIs to determine the access rights on a resource and different user interfaces for the learners, authors and DLS administrators. *User registry (UR)* is a database, containing user account information (user's ID and password) and used in the modern Single Sign-On systems. *User repository* is a database, which contains user profile information (name, address, already taught courses, gained certificates, educational schedule, etc.). *Directory server (DS)* provides the information from the UR and the User Repository. *Application server (AS)* is responsible for all basic EP services (including course access, assignments, collaboration and communication software, indexing engines, application gateways, knowledge applications, etc.), one part of which is Security Services. All the requests and responses are directed through the *Authentication proxy server (AP)*, responsible for managing the authentication process. It uses the DS to access the UR. A reverse proxy server is a component that is generally used to perform URL mapping and manage user sessions (for example with SSL/TLS authentication of both a client and a server) in order to protect the DLS Web site's structure from the outside world, but it can also be used for authentication. This would typically locate in a Demilitarized Zone (DMZ) of a University Intranet in front of the EP. The *Policy/authorization server (PAS)* is responsible for the IS management. It maintains the master policy store with authorization and access control data and offloads the tasks of authorization decisions to the PAS when requests are made. The *Policy store (PS)* as a repository of the groups and access control lists is used by the PAS for resources' access control. The *Trust association interceptor (TAI)* is responsible for establishing trust between the AS and the PAS. It validates any request and provides the user ID to the AS obtained from the PAS.

6 SECURE EP IMPLEMENTATION EXAMPLE

There are two possible ways of practical EP security implementation. First one is to buy one of the well-known portal solutions (such as Microsoft SharePoint, Oracle WebCenter etc.), relying on experts' estimations of their security. The second is to create an own EP software with all necessary Security Services and built-in (integrated) security subsystems. Such an approach allows to take into account all necessary security requirements, specific operation and environment from the very first designing stage and to ensure an efficient and holistic secure EP.

Implementing the EP security requires usage of some standard security concepts, for example, encryption (such as SSL/TLS), Virtual Private Networks (IPSec or similar) in University-trainee connection, enhanced protocols (such as ESMTP) and so on. Support for industry (such as LDAP, NTLM, NIS and NDS) and DL standards allows educational institution to easily carry over existing security profiles and meet even the strictest security requirements to their EPs. Monitoring tools used for analysis of all interactions with a Web server (IDS/IPS) should be also stipulated.

The EP made on the basis of the "DOCENT" DLS by the Russian company UNIAR is successfully used at the National Research Nuclear University MEPhI [http://www.mephi.edu] for 10 years. It is the first example of a secure Russian EP created according to the described modular approach (section 5). The "DOCENT" DLS security is provided by its functioning logic. It realizes protection against the most probable attacks. It is supposed that an intruder is an authorized EP user with only a browser (including those used in the mobile phones and pocket PCs). However it is enough for example to read the Web page contents and the entire client side scripts, which for example are not referenced anywhere (for example to the page, where correct answers to the quizzes are shown). He/she can transfer any parameters including forge ones. The EP security subsystem detects all these activities, reacts in an appropriate way and logs any attempts to compromise the EP.

Security subsystem logic consists of several business classes, incorporating all functionality supplied by the described in Figure 2 servers plus logging audit messages about all actions performed by the users. Protection against information substitution and deleting is also implemented via strict access control. The authentication scheme is based on the data, never saved to disk and destroyed if the browser is closed. All administration pages are accessible only through the HTTPS connections. Because the clear-text password can be sniffed the administrators are required to authenticate themselves to the EP with their personal certificates. Payload protection protocols used are SSL/TLS with encryption facilities.

The "DOCENT" DLS is used very effectively in the University's DL process for the University's students, bachelors and masters (as a part of the blended learning), at the short-term training courses and during an assessment of the trainees from the other Russian universities and NRNU MEPhI's partners (when we serve as a certification center). More than 10000 learners of different ages and preliminary education have already experienced all its advantages.

The "DOCENT" DLS is permanently improved. Its first versions suffer from a few typical attacks as data sniffing and DoS attacks. Their analysis showed the need to protect information in almost all stages of DL process. Stronger protection against attacks on EP communication channels and counteraction to DoS and DDoS (distributed DoS) attacks are going to be implemented.

7 CONCLUSIONS

Our many years' experience shows motivation of IS implementation expedience for EP and that to resolve DL IS issues completely and generally is a very hard task. DLS as they use network protocols, operational systems, databases management systems, different network services, Web applications, APIs etc. always inherit their vulnerabilities. A generalised EP structure as a protection object is created and the key security requirements and functional security subsystem components of a secure EP are developed. A secure EP on the basis of "DOCENT" DLS (UNIAR) being used in the NRNU MEPhI is shown.

In any modern DLS proactive EP security against new more and more sophisticated attacks is very welcome, but at present unfortunately nobody knows how to realize it in DL. The only way to reach the higher level of the DLS security is to conduct a full IS risk processing cycle for a concrete DLS in its particular content. After all IS objects, threats, vulnerabilities and risks will be defined and estimated it will be possible to create an adequate DLS security subsystem as it described below.

REFERENCES

Diatchenko, J., Miloslavskaya, N., Tolstoy, A., 2001. *Problems in Designing Secure Distance Learning Systems*. In *Proceedings of the 2st World Conference on Information Security Education WISE2*. Australia, Perth. Pp.147-159.

Furnell, S. M., Karweni, T., 2001. *Security issues in Online Distance Learning*. In *VINE*, Vol 31, Iss 2.

Jonas, X. Yuan, 2008. *Liferay Portal Enterprise Intranets*. Packet Publishing. 408 p.

Kavun, S., Sorbat, I., Sorbat, I., 2012. *Distance Learning Systems and their information security*. In *Business Inform*, Iss 7, pp. 234-239.

Miloslavskaya, N., Tolstoy, A., 2003. *Distance Learning and Virtual Private Networks*. In *Proceedings of the eLearning, eMedicine, eSupport Conference "Viewdet-2003"*. Austria, Vienna.

Miloslavskaya, N., Tolstoy, A., 2004. *Problems of Distance Progress Testing*. In *Proceedings of the EDEN 3rd Research Workshop*. Germany, Oldenburg.

Samson, T., 2012. *9 top threats to cloud computing security*. http://www.infoworld.com/t/cloud-security/9-top-threats-cloud-computing-security-213428 (last access date 18/10/2013).

Siciliano, R., 2013. *Distance Learning Poses Serious Data Security Issues*, http://www.huffingtonpost.com/robert-siciliano/distance-learning-poses-s_b_3938096.html (last access date 18/10/2013).