Problem of Trust in e-Learning Environment

Vladislav Petrov, Natalia Miloslavskaya, Victor Gorbatov and Anatoliy Durakovskiy
The National Research Nuclear University «MEPhI», 31 Kashirskoye Shosse, Moscow, Russia

Keywords: Distance Learning, e-Learning, Information Security, Problem of Trust, Trusted e-Learning Environment.

Abstract: The problem of trust and methodological approaches to resolve it for one of the most widespread types of open information systems – an e-Learning environment (ELE) – are discussed. For that purpose the state of trust implementation in distance learning (DL) is analyzed and its peculiarities are shown. An information security (IS) threats model for ELE is proposed. The methodological foundations of trust building for ELE are described. The results obtained allow to determine the goals and objectives for further research, including in particular the formulation of the task of developing a formalized (unified) model of building trust for learning management system (LMS) information resources using an integrated (complex) approach to IS insurance.

1 INTRODUCTION

Technological IT advances are considerably modifying traditional forms of activity, in particular, in the field of educational services. E-learning systems (ELS), using distance learning technologies (DL) for achieving the best possible performance, became an integral part of the modern educational process as its specific form or a separate part of broader blended educational process. Teaching Internet-based technologies are widely represented on the market of IT products and are commonly used by educational institutions in practice.

However, despite of a particular attention to the technological component of insuring information security (IS) while applied to DL, there is still a number of outstanding issues obligatory in implementation of ELS. At present the main goal, in our opinion, is a solution of the so-called problem of trust and building a trusted e-Learning environment (TELE).

In accordance with the terminology set for the IS field a concept of "building trust" in ELS can be defined as a fulfilment of the generally known triad of IS requirements:

- availability of ELS resources that seems not to require special comments;
- confidentiality/privacy of ELS resources in accordance with the law or another restrictions. For example, the personal data provided by ELS users should have such a property in the Russian Federation. The necessity to fulfil this requirement determines the current development period of the technological component of IS ensuring in ELS;
- integrity of ELS resources as no no-authorized modification provides legal value of learning outcomes on the basis of their trustworthiness and/or non-repudiation from these results.

Which properties and in what combination are required to perform depends on the IS threat and intruders models designed for the specific protected object.

The paper shows that the above mentioned problem of trust, due to the peculiarities of its fulfilment for the third condition, still not having a satisfactory solution, at least, on the existing market of IT products.

The remainder of the paper is organized as follows. Section 2 analyses the state of trust implementation in DL. Section 3 shows the peculiarities of trust in DL. An IS threat model for e-Learning environment (ELE) is proposed in Section 4. The methodological foundations of trust building for ELE are discussed in Section 5. In conclusion main results of the work are shown and future research is pointed out.

2 RELATED WORKS

Many of the tasks of securing information systems

Petrov V., Miloslavskaya N., Gorbatov V. and Durakovskiy A..
Problem of Trust in e-Learning Environment.
DOI: 10.5220/0005477604240429
In *Proceedings of the 7th International Conference on Computer Supported Education* (CSEDU-2015), pages 424-429
ISBN: 978-989-758-107-6

(ELS as an example), in particular maintaining confidentiality of their information assets, are performed by applying user identification, authentication and authorization mechanisms, providing the legal nature of their interaction with the system. However, even this aspect is difficult to be adjusted in DL in terms of anywhere recognized international norms and laws. Today only one methodological document – the international standard ISO/IEC 24703:2004 – Information technology – Participant identifiers (ISO/IEC 24703:2004) and its Russian harmonized analogue GOST R ISO/IEC 24703-2011 – can be specified, where only data types used to identify the participants of the educational process are defined. And aspects of ensuring IS, in particular, the personal data security concerning participants' identifiers usage as well as their authentication are beyond the scope of this standard.

There are a lot of research works devoted to investigations relating to different aspects of IS in ELE. But none of them considers the trust in DL as a systemic problem of IS in the above mentioned goal-setting.

The necessity of IS ensuring for DL while using the Internet as an open type communication was investigated in (Furnell and Karweni, 2001). But the paper does not provide a description of the specific approaches to the problem solution.

Other researchers (Nickolova and Nickolov, 2007), (Eibl, 2010) confined only to build up the so-called threat models or a list of potential dangers.

The majority of works (Weippl, 2005), (Ullah at al, 2012), (Kumlander, 2008), (Inaba, Watanabe and Kodate, 2003) are connected with the study of the issues on effective legal access control, in other words of such a service which guarantees the right to use the system only by its authorized users. That is, the problem of countering unauthorized access in its traditional understanding was solved, including using of biometric identification/authentication for DL process participants and monitoring compliance with the passage of various kinds of control activities.

All these definitely important aspects of ensuring IS for DL, in particular, the access restriction for illegal users, nevertheless, do not realize all the above mentioned conditions for trust building as a complex problem. For example, the possibility of countering action against such a real threat as a non-verbal substitution of a legal trainee on the distance progress testing procedure with his consent. Traditional access control mechanisms do not provide an effective mechanism to counter the known IS threat called masquerading. The reason is that a signature carrier (for example token) and the software that generates these signatures can be considered as alienable. And this fact does not enhance the level of trust in ELS.

3 PECULARITIES OF DISTANCE LEARNING AS AN OPEN SYSTEM

An additional aspect, in a certain way complicating comprehension of the problem of trust, is the fundamentally open nature of ELE. The traditional understanding of ELE as an open system is based on the definition suggested by the Committee of IEEE POSIX 1003.0 (1003.0-1995 – Guide to the POSIX(R) Open System Environment). It is concerned as a computer environment that implements an open interface specifications and services (environment services). This environment supports the data formats sufficient to provide the following properties:

- extensibility is the system ability to add new application functions or to modify some functions from the amount of already performed without modifying the rest of the subsystems;
- scalability is the system ability to increase its productivity while expanding resources;
- portability is the ability to transfer the system to a more advanced hardware and software platforms while their upgrading or replacement;
- interoperability is the system ability to interact with other systems, if necessary, referring to information resources (databases, knowledge bases, and etc.) of these systems or performing specific tasks using their computing resources when their own resources are insufficient;
- integration is the ability to combine several systems/databases/applications for different purposes in a single multifunctional system/data store/multi-tier client/server architecture.

Such a common representation of the open system, created on the basis of a cloud-based technology according to SaaS model (Software as a Service) (Docebo.com), (ProProfs.com), is widely used in DL and other network technologies implemented in the Intranet, Internet, or their combination shown in Figure 1.

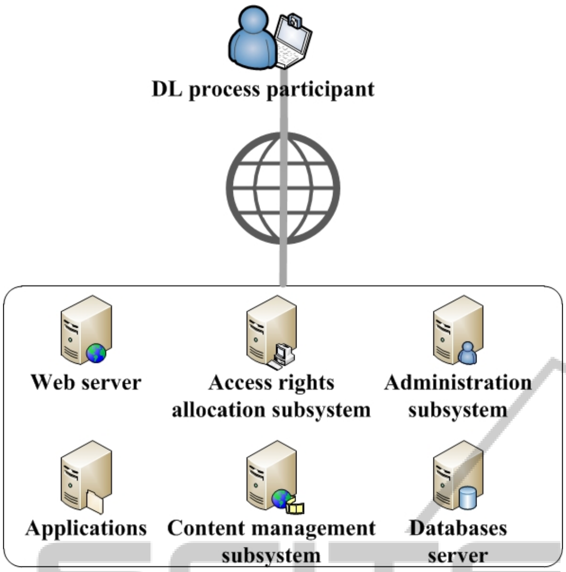

Figure 1: Typical LMS's structure.

It is interesting to note that such a learning management system (LMS) service deployment model as a public cloud, in other words an infrastructure for free mass use, is frequently used in the technology of cloud computing applied here to DL purposes. Such an infrastructure may be in ownership, management and maintenance of commercial, academic and government organizations (or of any combination thereof). The public cloud physically exists in the jurisdiction of the owner (server provider) and the problem of integrated security compliance of information resources (the problem of trust) becomes more obvious than in the untrusted environment in the setting of local installation (Miloslavskaya, Petrov and Tolstoy, 2014), (IITO UNESCO, 2013).

In that context *trust is a (positive) decision on the admissibility of interaction with an IT system and acceptance of the results of its functioning*.

We formally define the open trusted IT environment as a set of hardware and software, providing creation, application and development of the system in accordance with its purpose and having a full set of software, design and in-line documentation, including program source codes meeting IS requirements and confirmed by certificates of compliance audit reports) by the relevant legislative regulation systems.

Analysis of some sources (Hameetha Begum, Sheeba and Nisha Rani, 2013), (Gunasekar and Anirudh, 2011), (Wenan Tan et al, 2012) showed that the use of the public cloud as a basis for ELE is not safe in the context of our definition of trust. There are currently no generally recognized requirements to cloud IS assurance, in particular a detailed (particular) IS threat model for cloud computing environments, as well as verification mechanisms able to unambiguously define a user. The reason is that even using of integrated circuit card or USB key does not warrant that the access has been gained by the very legitimate user because they are a removable media of key information. Consequently, the use of the cloud infrastructure has high risks and more limited access control capacities. Therefore, one of the main problems of cloud computing is the users' trust formation in above mentioned goal-setting in relation to cloud providers and their possibilities to form TELE.

4 IS THREATS MODEL FOR E-LEARNING ENVIRONMENT

Analysis of (Miloslavskaya, Petrov and Tolstoy, 2014), (Najwa Hayaati Mohd Alwi and Ip-Shing Fan, 2010) shows that none of the IT products available at the LMS market (both cloud-based and local) does not currently warrant the necessary IS level for LMS resources as it is provided by usage of the specific information protection tools (IPT). However, if consider the existing research papers on IS threats in DL (Nickolova and Nickolov, 2007), (Najwa Hayaati Mohd Alwi and Ip-Shing Fan, 2010), then the major threats are described there in some detail including those using users' (DL process participants) software. Nevertheless, the list of IS threats described there is not complete. So, it can be said that the question of regulation of requirements to DL process participants' (users') working stations/computers/mobile devices (WS) has not been discussed up to date. The absence of such requirements to the DL process leads the DL participants and LMS (educational institution) interaction environment to objective distrust. For example, during e-assessment (progress testing) the DL process participants have a possibility to use third-party Internet-resources that are not permitted within the traditional progress testing activities.

Thus the extended set of key IS threats is represented as follows:

1) an unauthorized access to LMS information resources, including an unauthorized access to the answers to the control data (tests, quizzes, etc.).

2) a possibility of LMS breaking by hackers as well as legal users in order to substitute the author's answers to the progress testing and, as a

consequence, changing/replacement of the testing results.

These IS threats are realized in the form of attacks against LMS server in order to progress testing data compromise, unauthorized copying of learning materials and personal data theft or attacks against DL instructor/teacher WS in order to obtain data/edit the results of academic performance rating, spoofing of user identity while accessing ELE and interference at all DL stages (Miloslavskaya, Petrov and Tolstoy, 2014), (Siciliano, 2013).

The IS threats model for TELE in case of vulnerabilities allowing LMS's IS violation is shown in the Table 1.

Table 1: IS threats model for TELE.

Reasons – Absence of trust in	IS threat – Violation of	Description
WS	Integrity, availability and confidentiality of LMS (with its resources) and WS	Use of undocumented features of custom and malicious software with the purpose of substitution of access permission, information leakage and modification and performing attacks against WS and LMS
LMS information (including progress testing data) transfer paths	LMS resources integrity and confidentiality and DL process participants' privacy	Capturing information circulating between DL process participants with the purpose of compromise both authorization and progress testing data
Authenticity of DL process participants	DL process participants' privacy	Substitution of legal DL process participants for falsification of progress testing results

The result of both intentional and unintentional actions of any intruder is a violation of LMS properties and, as a consequence, the distortion of the real (true) information: deletion, substitution and modification of rights, system's hacking, the replacement of progress testing results, etc. All this information is described in a separate document entitled "Intruders' Model". The model contains a formalized intruders' classification, including description of their experience, knowledge, available resources needed for IS threats implementation, possible motivation of their actions and IS threats implementation techniques used by the given intruders.

The extended IS threat model analysis leads to a conclusion that the current situation with ensuring IS for DL is far away from ideal. In other words DL process participants do not have trust in DL process. One of the main reasons is the fact that the main DL process participants – trainees – can be interested in falsification of their progress testing results. And as it follows from analysis of the Table 1, actually all existing DL information-sharing environment and its basic structure do not meet above mentioned requirements of building trust (Figure 2).

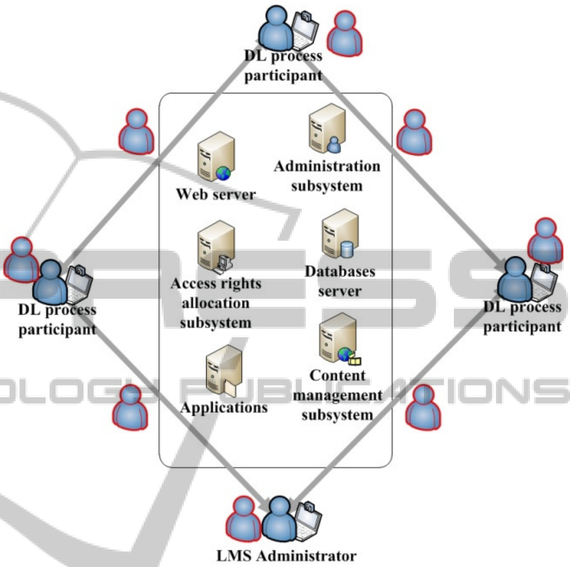

Figure 2: Typical LMS structure with intruders (in red) and their attacks' objects.

5 METHODOLOGICAL BASIS FOR BUILDING TRUST IN E-LEARNING ENVIRONMENT

Thus, the scenario of above mentioned trust building in ELE requires essential attention to all of the following areas: upgraded (non-traditional) user identification and authentication; access control; and connection protection and et al (Miloslavskaya, Petrov and Tolstoy, 2014).

In order to determine the methodological approaches for building TELE for the new DL forms, some necessary conditions in terms of well known IS requirements (such as availability, confidentiality and integrity) to LMS information resources (assets) can be formulated.

Definition 1. TELE is determined as the automated information system with a typical document of compliance setting IS requirements. That means the fulfillment of a set of the following conditions:

- the presence of the reference software and operating systems with control and differentiation of starting processes and tasks;
- the presence of certified IPT and cryptographic protection facilities;
- building of trust in circulating information;
- the presence of a complete set of software and hardware documentation prepared in accordance with applicable standards;
- the presence of an environment support system at all stages of the life cycle from software design process to compliance evaluation certification.

Definition 2. The relatively trusted ELE means an ELE that does not fulfill at least one of the conditions of Definition 1.

Definition 3. The untrusted ELE means an ELE that does not fulfill the first three conditions of Definition 1.

Limitation 1. The relatively trusted ELE for DL process participants is considered as one of the untrusted ELE components.

For normal TELE functioning a property precluding the possibility of implementing a variety of IS threats $\mathrm{Th} = \{\mathrm{Th_i}\}$, emerging and ongoing in interaction with this environment via untrusted LMS channels, should be carried out. DL process participant's WS is a collection of finite disjoint sets of trusted $\{\mathrm{ET}\}$ and untrusted $\{\mathrm{EUnt}\}$ components being distributed across hierarchical layers of embedded components $\mathrm{L_i}$, where $\mathrm{i} \in [0, \mathrm{N}]$, and $\mathrm{L_0}$ is a basis component of this hierarchical structure, in which the physical access to hardware resources of DL process participants in distributed ELE is delegated by the corresponding means.

Based on that the following statements can be introduces.

Statement 1. A component $\mathrm{L_1}$ realized only by the trusted computing facilities can be allocated in TELE. Therefore, the computer environment built on $\mathrm{L_0}$ will be protected from all hypothesized IS threats Th.

Statement 2. The components $\mathrm{L_i}$, where $\mathrm{i} \in [2, \mathrm{N}]$, are not safe or/and are untrusted by definition, as meanwhile realization of both external and internal unauthorized access is possible, during which the properties of confidentiality, integrity and availability for WS of DL process participants can be violated.

Statement 3. Trusted components of an arbitrary component are functioning within this component's security boundaries and must interact with neighboring components via secure interfaces.

Statement 4. To ensure availability and integrity the component $\mathrm{L_1}$ must support recursive methods of control, management, integrity monitoring of the trusted components constituting $\mathrm{L_i}$, where $\mathrm{i} \in [1, \mathrm{N}]$, and information circulating between the components. For all the components $\mathrm{L_i}$, where $\mathrm{i} \in [0, \mathrm{N}]$, an access differentiation model of software components to protected resources must be supported.

The above conditions allow to correctly formulate the non-existent at the moment task of developing a formalized (unified) model of building trust for LMS information resources based on an integrated approach to IS insurance. Formulation and solution of this problem will be the subject of our further research.

6 CONCLUSIONS

Thus the task of building trust in ELE can be formulated on the basis of the criterion of "Three trusts" when it is necessary to provide the widespread trust in all three key DL elements:

- WS of DL process participants;
- information transfer channel between DL process participants that will allow to introduce an additional authentication parameter such as biometrical characteristics for DL process participant;
- upgraded authenticity of DL process participants including usage of biometric methods.

Compliance with these requirements may be achieved through the use of some biometric characteristics or their combination. They should have the fewest false positives and do not require further action by the user, and additional technical support.

The implementation of this criterion in LMS by combining the known mechanisms of organizational and technical IS ensuring allows to significantly reduce the probability of having false progress testing results and to detect messages and items non-repudiation violation in a single TELE among all DL process participants.

While beginning the research the authors have already tested a variety of methods and means supporting the implementation of the given criteria. The results obtained are a testimony to the fact that we can achieve different compromise levels between openness and a desired trust level. The future work is connected with the search of an acceptable more rational approaches.

REFERENCES

1003.0-1995 – Guide to the POSIX(R) Open System Environment (OSE). IEEE Standard.

Docebo.com. *Discover Docebo's Features An ecosystem of features and modules to extend your LMS.* https://www.docebo.com/elearning-platform-saas-lms/ (last access date 22/03/2015).

Eibl, C.J., 2010. *Discussion of Information Security in E-Learning, Dissertation, Doktor der Ingenieur-wissenschaften (Dr.-Ing.),* Universität Siegen, Siegen, Germany. http://dokumentix.ub.uni-siegen.de/opus/ volltexte/ 2010/444/pdf/eibl.pdf (last access date 22/03/2015).

Furnell, S.M., Karweni, T., 2001. *Security issues in Online Distance Learning, VINE,* Vol. 31, Iss: 2, pp.28-35.

Gunasekar, K., Anirudh, C., 2011. *Analysis of security issues in cloud based e-learning.* http://bada.hb.se/ bitstream/2320/9271/1/2011MAGI23.pdf (last access date 22/03/2015).

Hameetha Begum S., Sheeba T., Nisha Rani S.N., 2013. *Security in Cloud based E-Learning.* International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 3, Iss. 1, pp. 270–278.

IITO UNESCO, 2013. *Information and communication technologies in education:* Monography / Ed. Badarcha Dendeva. Moscow, IITO UNESCO, 2013 (in Russian).

Inaba, R., Watanabe, E., Kodate, K., 2003. *Security Applications of Optical Face Recognition System: Access Control in E-Learning.* Optical Review, Vol. 10, Iss. 4, pp. 255–261.

ISO/IEC 24703:2004 — Information technology — Participant identifiers.

Kumlander, D., 2008. *Soft Biometrical Students Identification Method for e-Learning*. Advances in Computer and Information Sciences and Engineering, pp. 114–118.

Miloslavskaya, N., Petrov, V., Tolstoy, A., 2014. *Security Aspects for E-Learning Portals.* In *Proceedings of the 6th International Conference on Computer Supported Education (CSEDU 2014)*. Spain, Barcelona. pp. 427–432.

Najwa Hayaati Mohd Alwi, Ip-Shing Fan, 2010. *Information Security Threats Analysis for E-Learning.* Technology Enhanced Learning. Quality of Teaching and Educational Reform. First International Conference, TECH-EDUCATION 2010, Athens, Greece, May 19-21, 2010. Proceedings. pp. 285–291.

Nickolova, M., Nickolov, E., 2007. *Threat Model for User Security in E-Learning Systems.* International Journal of Information Technologies and Knowledge, Vol. 1, pp.341–347.

ProProfs.com. *SaaS elearning platform: features & benefits.* http://www.proprofs.com/c/e-learning/saas-elearning-platform-features-benefits/ (last access date 22/03/2015).

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 22/03/2015).

Ullah, A., Xiao, H., Lilley, M., Barker, T., 2012. *Using Challenge Questions for Student Authentication in Online Examination.* International Journal for Infonomics (IJI), Vol. 5, Iss. 3/4, pp. 631–639.

Weippl, E.R., 2005. *Security in E-Learning*, Springer US.

Wenan Tan, Jingxian Li, Anqiong Tang, Tong Wang, Xiaoming Hu, 2012. *Trust Evaluation Model Based on User Trust Cloud and User Capability in E-Learning Service.* Communications and Information Processing. International Conference, ICCIP 2012 Aveiro, Portugal, March 7-11, 2012 Revised Selected Papers, Part I, pp. 583–590.