Model of user identification of electronic informational-educational environment

N M Kovalnogova, S S Sokolov and A P Nyrkov
Admiral Makarov State University of Maritime and Island Shipping, 5/7, Dvinskaya st., Saint-Petersburg, 198035, Russia

E-mail: SokolovSS@gumrf.ru

Abstract. This article describes the electronic informational-educational environment (EIEE) of a university, components of IEEE, categories of users, a model of user identification.

1. Introduction

Today, E-learning and Distance Learning Technologies (hereinafter DLT) are widely used in world practice. In Russia the background of E-learning and DLT application is regulated by a number of the legal regulations.

According to Federal Law №273, ‘The Education Act of the Russian Federation’ of 09.12.2012, when implementing educational programs, the university uses different educational technologies including E-learning and DLT. The university should provide suitable conditions for the functioning of the electronic information-educational environment (hereinafter EIEE) while implementing educational programs applying E-learning and DLT. The university EIEE includes electronic information resources, electronic educational resources, a complex of information and telecommunication technologies and technological resources. Besides, it provides a full-scale mastery of educational programs by students irrespectively of the students’ location.

Thus the main purpose of the university EIEE establishment is the information support of the educational process in accordance with the requirements for the educational programs implementation.

The information support of the educational process means the following:

• provision of a day-and-night access (via the Internet) to educational materials;
• provision of the opportunities for students to do self-study exercises, perform tasks, prepare for certification;
• provision of opportunities for teachers to render the professional mentoring support for students (through various means of communication);
• organization of the information exchange between lectors and students;
• publication of information for students (about checks and examinations, ways of reporting results);
• storage and structuring of educational material;
• provision of the electronic document flow;
• management of the educational process, etc.

To achieve these objectives, the university EIEE should include many components, which have different software/hardware platforms supporting different data transmission technologies, support different standards for creation and processing of documents. These university EIEE components can be used within the local network, geographically-distributed network, or on the Internet.
The university EIEE includes the following components: web-sites supporting different Content management systems (CMS), Learning Management Systems (LMS), Learning Content Management Systems (LCMS), Electronic Library Systems (ELS), control automation systems of the educational process, different Enterprise Resource Planning (ERP) systems or Product Lifecycle Management (PLM) systems, Customer Relationship Management (CRM) systems, Decision Support Systems (DSS) and etc.

All these EIEE components can be grouped according to architecture, a degree of automation, a data processing nature, a scope of application, an accessibility level of the information they contain.

EIEE users are divided in two categories: internal and external. The internal category includes staff, lectors, students (which in their turn are divided into students of different levels and forms of education). External users are applicants (enrollee), parents, partners, supervisory organizations (government), etc. The same users may have different roles (defining their rights) in the university EIEE components or may not have any roles at all.

2. The model of user identification

To construct a model of user identification the following notations are introduced into EIOS:

1. \( C_i \) – i-class of EIEE components.
2. \( S_j \) – j-component in i-class.
3. \( a_{ij} \) – l-ID attribute of the user definable in a j-component of an i-class.
4. \( A_i = \{a_{i1}, a_{i2}, ..., a_{in} \} \) – set of identity attributes of the user definable for a j-component of an i-class.
5. \( A = \{A_{11}, A_{12}, ..., A_{1r}, A_{21}, A_{22}, ..., A_{2r}, ..., A_{q1}, A_{q2}, ..., A_{qr} \} \) – set of all identity attributes for all the EIEE components of all classes.

The user may be authenticated by presenting at least one of the following entities:

• something that the user knows (a password, personal ID, a cryptographic key and etc.);
• something that the user owns (a personal card or other device of a similar purpose);
• something that is a part of the user (voice, fingerprints, etc., that is, one’s own biometrics).

For each attribute \( a \in A \) domain \( V_a \) is defined.

\[ 2^{|V_a|} \] – the total number of possible domain values of attribute \( a \).

Thus the model of user identification can be represented by couple \((A, V)\).

A set of tuples \( K_a \) will be treated as a set being is a direct product of attribute values domains \( \{a_1, a_2, ..., a_n\} \):

\[
K_a = \prod_{i=1}^{n} V_a
\]  

Let \( D_m \subseteq A \) be as a set of attributes determining a separate m-category of users, and \( K_{D_m} \) be a set of tuples of this category.

This way there is a following rule:

\[
f : K_{D_m} \rightarrow K_A
\]

representing a mapping of the set of tuples \( K_{D_m} \) on \( K_A \), which gives (associates) a unique element of the set of \( K_A \) to each element of the set of \( K_{D_m} \).

Taking into account the necessity and importance of user identification by a specific attribute, which depends on the user’s category, the class of EIEE components and the component itself, the domain value that is included into any tuple from set \( K_{D_m} \) can have three levels of definition:

1. Explicitly defined.
2. Has value ‘null’ not defined at the moment.
3. Has value ‘x’, that is, should not be defined at all.

So, equation

$$K_{D_m} = \{ K_{D_m} (V_{D_m}) | V_{D_m} \in V, D_m \subseteq A \}$$

(3)
can be viewed as a decomposition of set $K_A$, which will determine the user category with respect to the components of EIEE and methods of user identification. The attribute values of the model of user identification can change during EIEE development. They can become outdated (can be removed), can be updated (software update of the platform), new components can appear, the types of identification can be changed. In this case, it will be appropriate to update the classification of the components.

In addition to user identification by a particular attribute the identification can happen by a number of alternative signs.

Let $a_i$ and $a_j$ be pairwise alternative signs, $a_k$ be signs having no alternative analogues, then true identification $\text{True}(I)$ is possible in case of validity of the following expression:

$$\text{True}(I) = (a_i \& a_j \& \ldots \& a_k) \& ((a_i \vee a_k) \& (a_j \vee a_k) \& \ldots \& (a_m \vee a_n)),$$

(4)

where $n$ – number of signs not having alternative analogues, $m$ – number of signs having alternative analogues.

Let us make a partition of EIEE into two nonintersecting and independent sets of classes of components (it can be justified including a separation of the information of the open and restricted access) according to the following rules:

1. The first set should consist of pairwise incompatible classes of components.
2. The second set should consist of mutually independent classes of components.

In this case, the total probability of true identification will be determined by expression:

$$P = \sum_{i=1}^{n_1} \sum_{j=1}^{m_1} P_{k_{i,j}} (a) + \prod_{j=1}^{m_1} P_{k_{i,j}} (a) + \prod_{i=1}^{n_2} \sum_{j=1}^{m_2} P_{k_{i,j}} (a) + \prod_{i=1}^{n_2} P_{k_{i,j}} (a).$$

(5)

where $n_1$ – the number of pairwise incompatible classes of components in the first set involved in identification, $m_1$ – the number of independent classes of components in the aggregate in the first set involved in identification, $n_2$ – the number of pairwise incompatible classes of components in the first set involved in identification, $m_2$ – the number of independent components in the aggregate in the first set, involved in identification

3. Testing of the model

The model of user identification was tested in one of the Admiral Makarov State Universities of Maritime and Inland Shipping Campuses (in the laboratory of electronic information-educational technologies named after prof. U.M. Kulibinov).

Testing took place in the form of an experiment, within the framework of which three main user groups were chosen: students (three student groups comprising 60 people), lecturers (8 people working with these three groups of students in this laboratory) and the staff (5 people including a director of the laboratory and administrators of the EIEE components, who provide a technical support).

As part of the experiment we examined the work of the users with the following EIEE components:

- 54 PC (in the laboratory);
- 1 mobile access device;
- 3 university web-sites (access via the Internet);
- 1 Learning Management System (distant learning system, hereinafter DLS ‘FARVATER’) (access via the Internet);
- 1 Learning Content Management System (‘Educational portal’) (access via the Internet);
- 1 Electronic Library System (ELS) (the access to ELS is only within university campus LAN; the access to the ELS web-catalog is via the Internet);
• 1 automation system of the educational process management (access is only within university campus LAN);
• 1 decision support system (the client program working in laboratory LAN);

Due to the fact that the selected categories of users have different access rights to selected EIEE components, they were assigned to the methods of authorization of different complexity using various means of authentication.

The base of the experiment was represented by a matrix of allocation of access rights to EIEE components for different users categories under a predetermined set of attributes taking into account the fact that a specific value from the set is predefined for each user/attribute pair (the attribute value is specified, the attribute value is not specified, the attribute value should not be specified).

Thus temporary guest accounts were created for the students working with PCs, temporary personal accounts – for lectors, permanent staff personal accounts – for staff. Furthermore, in order to confirm the authenticity, the staff have to produce a special key, because a hardware-software module of the trusted boot (or a fingerprint when accessing from a mobile device) was installed on PCs belonging to the staff. A fingerprint attribute for access was selected to increase the number of possible user attributes.

In LMS (DLS ‘FARVATER’) and LCMS (‘Educational portal’) special requirements for the password complexity were introduced in order to ensure data security. The complexity includes the use of a minimum number of characters, the use of the letters of different cases, the simultaneous use of letters, figures and special symbols. The level of the password complexity and the frequency of its update depend on the category of users: the highest level is for the staff (administrators of the EIEE components, a tech support team), a lower level is for lectors, and the lowest is for students.

The results of the experiment have shown that the presented model of user identification is adequate and can solve the assigned tasks of:
• forming EIEE users categories;
• partition of EIEE into various locally isolated segments for discrete identification;
• building of a transparent system of access isolation (including a mandatory access control);
• preliminary inspection of compliance (before implementation) of the taken measurements on information security to the claimed requirements (taking into account the necessity of information rating).

4. Conclusion

Improving the quality of education and ensuring equal access to educational resources and services for all citizens are the main aims of educational system today. Development of EIEE and forming mechanisms and prerequisites for the integration of information technology into the everyday educational and scientific practice is a key of integration to an information society.

Information security of EIEE of the educational institution is very important: the number of threats is growing every day, the number of EIEE components is changing, software platforms become outdated.

Data security of EIEE components is provided by EIEE components of the proper software and hardware as well as by organizational and technical measures. The basis for information protection against an unauthorized access is implementation of the principles of access control to resources.

The provision of the correct implementation of the differentiating policy of access to resources is impossible without correct identification of users.

The application of the identification model allows users to control the use of EIEE components.

References
[1] Nyrkov A, Belousov A and Sokolov S 2015 J Modern Appl. Sci. 9 162–76
[2] Chernyi S, Zhilenkov A, Sokolov S and Titov L 2015 J Metallurg. and Min. Ind. 7 66–73
[3] Nyrkov A, Sokolov S, Chernyi S and Mamunts D 2015 J Metallurg. and Min. 7 521–24
[4] Chernyi S 2015 J Metallurg. and Min. 7 60–65
[5] Kovalnogova N and Sokolov S 2015 Electronic informational-educational environment of university complex Maritime educ.: trad., realities and prosp. 157–63
[6] Pastuscshak T, Sokolov S, Kovalnogova N and Mankovskaya A 2014 J Inf. Tech. 9 40–46
[7] Boriev Z, Sokolov S and Nyrkov A 2015 J Materials Science and Engineering 91