*Sādhanā* Vol. 41, No. 3, March 2016, pp. 317–326 

# Defining the e-learner's security profile: Towards awareness improvement

MARJAN MILOŠEVIĆ and DANIJELA MILOŠEVIĆ*

Faculty of Technical Sciences Čačak, University of Kragujevac, Svetog Save 65, 32000 Čačak, Serbia
e-mail: marjan.milosevic@ftn.kg.ac.rs; danijela.milosevic@ftn.kg.ac.rs

MS received 9 June 2015; revised 10 September 2015; accepted 27 October 2015

**Abstract.** The paper presents an improved e-learner model that supports monitoring of user behavior related to information security. The model is built upon standardized IMS specification, according to literature research and survey conducted among e-learners. It is positioned as key part of an extended LTSA architecture in which the learner data is used to improve learner security position by continuous delivery of important information and adapting security mechanisms. The implementation is considered in Moodle LMS.

**Keywords.** E-learning; security awareness; user profile; security agent; LTSA; IMS LIP; Moodle.

## 1. Introduction

Information technology expansion leads to multiplication of the security threats, especially when it all goes mobile with Internet of Things and Bring Your Own Device (BYOD) philosophy [1]. Also, one does not have to be a hacker in order to compromise someone's data. Rather illustrative example is a FireSheep plugin [2] that enables virtually any beginner to hack an unencrypted session in the same network: very handy if there is an open Wi-Fi hotspot.

Having more and more institutions offering online courses, or even full study programs, information security tends to become important issue in education too [3]. As a form of e-business, e-learning is highly related to security and privacy [4]. Zuev states several categories of threats, such as unauthorized access (unauthorized copying and modification of data, physical access) and law violation (in particular, the laws governing copyrights and other rights) [5]. Still, quite low attention is paid to e-learning security in general [6]. It is stated that a significant number of e-learning platforms do not even have a basic policy defined at all [7]. The remaining question is how many users read it at all.

Security is not just, or even primary, matter of technology: it highly involves organizational and business factors, and that fact has been often neglected [8]. On the other hand, user role is significantly important, since user often presents the weakest point in information system security [9]. The good chance of mitigating risks and avoiding security incidents can be accomplished only with proper introducing users with the risks and threats, as well as with required behavior. That is where the security awareness enters the stage.

The Information Security Forum [10] defines information security awareness as the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization, their individual security responsibilities, and acts accordingly. Information security awareness plays an important role in every organization's information security performance. Raising the awareness level in organization represents a task consisted of many activities, such as: presentation, periodical assessment and policy dissemination, and means a change in culture [11].

In that sense, we shall consider security as a process, not a product [12]. The information security paradigm is therefore cycle-development process, i.e. conducted using the PDCA circle [13], which means it is a constant, never ending endeavor. That also means that the awareness improvement is supposed to be continuous.

In order to conduct appropriate awareness program, it is important to know the users: to build their security profile. That issue is not particularly addressed in context of e-learning – in research known to authors. Therefore the primary goal of this paper is to reveal e-learner's position in context of security and to point to potential ways of improving his security stance and adaptation of security mechanisms in order to be better accepted. The idea is to incorporate user model in a larger e-learning architecture that would further allow automatic proactive security improvement by adaptive dissemination of security policy, thus building the security awareness at user-level. It would be a task performed by a special software component – agent. The model and the agent then would help practitioners in maintaining e-learning system in a continual

*For correspondence

manner, with added user-layer of security. Besides the informational action, additional operations might be performed, such as interface adaptation.

In order to get insight into e-learners' security profile – which is a starting point, the state of the art literature is analyzed. Also, the survey is conducted among students who use e-learning system. The findings are analyzed and the extension to standard architecture and standard learner model is developed. The conceptual model of agent is presented and proposed as extension to the standardized learning architecture.

## 2. Related work

Researchers dealt with matter of user security perception in numerous papers. Mostly it was about home and corporate users, rarely with e-learners particularly.

Zamzuri *et al* analyzed students' perception on e-learning security issues, through STRIDE method [14]. It was shown that students were concerned mostly about data integrity, especially about tampering the assessment results. The second thing they are most concerned about is profile information disclosure.

Shonola and Joy narrowed the research by focusing to m-learning [15]. They showed that in m-learning the client side become very critical, since jeopardizing a device shown up as an serious threat, as well as new malware targeting mobile devices. The numbered threats might repel users and disable the whole process. Authors stated that, beside strong security mechanisms, the education and proper tips providing is crucial for users to get confidence in the m-learning paradigm.

Furnell *et al* [16] analyzed Internet users in general British population. They concluded that the lack of professional sources of information that would raise the security awareness was the main problem for computer novices. Still, the advanced users showed discrepancy among their beliefs of awareness and their real knowledge of security.

Rughiniş and Rughiniş used the large survey dataset from Eurobarometer in order to gain insights of general end-users behaviors in European Union [17]. They managed to cluster the data and got five user profiles: 'explorer', 'reactive', 'prudent', 'lucky' and 'occasional'.

Adams and Blanford pointed out the need for security and usability to get along in e-learning systems [18]. They argued that the poor user-experience of the security control design often leads to unintentional user behavior. Also, the problem found in the e-learning environments is the lack of user support, which eventually makes the system to seem as it works against the user. The need for user-centric design of security controls, based on user feedback and communication between security specialists and end-users was emphasized.

Certain trade-off is present when dealing with security: users tend to evaluate if the effort they make worth the gained benefit. Beautement and Sasse used the economy model to get insights into users willingness to follow the security procedures [19]. They described the compliance budget as capacity of user in bringing effort to gain the security goals. When the budget is spent, users tend to bypass the security in order of getting primary stuff done. With proper monitoring the budget might be kept and users still comply with policies.

Besnard and Arief also analyzed the trade-offs that legitimate users make [20], but stated them in cognitive context. They highlighted several everyday tasks where security may be easily traded for comfort: password complexity, software updates, file sharing and opening mail attachments.

## 3. Gathering relevant data about users

In order to get particular insights into learners' habits and attitudes related to security and privacy, a survey was prepared. We expected to get valuable data that would fulfill gaps of information not found in related research, but which is required for the model building. The survey was supposed to be quite brief and the construction is partly based on the SANS awareness survey template [21].

The survey is conducted at the end of 2013 and beginning of the 2014 at Faculty of Technical Sciences in Čačak. The population consisted of BSc students of engineering, studying in blended mode. The platform used was Moodle, open source learning content management system [22]. A closed-answers questionnaire was used as a survey tool. It was set at the same System.

We did not want to force users to fill the questionnaire in order to eliminate the bias the forced user may add and which may lead to avoiding of admittance about their potentially risky behavior. That is the issue being reported as frequent gap between the intention and real behavior [23]. Therefore, users who filled the survey form, did it voluntary.

The total number of respondents' was 183. Items were grouped in two sections: the first was used in order to acquire general data about System usage and e-learning and the second was used to assess general and e-learning security attitudes and practice.

The section one results are given in tables 1 and 2.

The second section questions and answers are presented in the following tables 3, 4, 5, 6, 7, 8 and 9.

**Table 1.** Types of access.

| How do you access online courses (multiple locations allowed; in %) | | What kind of Internet do you use for accessing courses? (in %) | |
|---|---|---|---|
| From home | 93 | ADSL | 69 |
| From faculty's computer lab | 33 | Wi-fi | 29 |
| From faculty's other PC | 22 | Cable Internet | 18 |
| Via mobile device | 21 | Via mobile phone | 15 |
| From student campus | 9 | Other | 4 |
| From friend's PC | 8 | | |
| From Internet-cafe | 4 | | |
| In other way | 3 | | |

**Table 2.** Extent of usage.

| How frequently do you access online courses (in %) | | State the number of course you are enrolled on (in %) | |
|---|---|---|---|
| Every day | 45 | More than 5 | 31 |
| Several times a week | 47 | 2–5 | 59 |
| Once a week | 5 | One course | 11 |
| Less than once per week | 3 | | |

**Table 3.** Password practice.

| It is OK to disclose password to colleague to let him access the system (in %) | | Describe your password policy (in %) | |
|---|---|---|---|
| I fully disagree | 23 | For every system I use different, strong password | 28 |
| I mainly disagree | 43 | For most systems I use different, strong passwords | 28 |
| I don't have an opinion | 11 | For most important systems I use one strong password, otherwise I use weak password | 23 |
| I mainly agree | 19 | I use one strong password for all systems | 19 |
| I fully agree | 3 | I use one simple password for all systems | 3 |

**Table 4.** Personal security practice.

| | Yes | No or "I don't know" |
|---|---|---|
| My antivirus is running up to date | 81 | 19 |
| My operating system is updated regularly | 68 | 32 |
| Data on my PC is not interesting to hackers | 82 | 18 |

**Table 5.** Site usage policy awareness.

| Did you read the site usage policy? (in %) | |
|---|---|
| No | 15 |
| I just scrolled down | 12 |
| Partially | 25 |
| Mostly | 19 |
| Yes | 29 |

**Table 6.** Profile data disclosure preferences.

| Who is supposed to be able to see your profile data? (in %) | |
|---|---|
| Nobody | 9 |
| Only teacher | 25 |
| Only colleagues from the same course | 20 |
| Only registered users | 27 |
| Everyone | 2 |
| I would like to control the visibility | 17 |

**Table 7.** Attitudes towards potential data loss.

| Imagine that the whole e-learning system is destroyed, including your account and all the files. Which comment most correctly describes your attitude? (%) | |
|---|---|
| A severe problem that might jeopardize my studies | 11 |
| A serious situation, but I'm sure I could manage it | 59 |
| Not a problem, I already got all the data somewhere else | 25 |
| No problem, I got no important data on site | 9 |

**Table 8.** Security education.

| Do you need additional education in information security | |
|---|---|
| I totally disagree | 8% |
| I disagree | 14% |
| I don't have an opinion | 22% |
| I agree | 39% |
| I fully agree | 17% |

**Table 9.** Responsibility towards security.

| Select the appropriate responsibility for security of e-learning system | |
|---|---|
| It is 100% up to institution | 14% |
| 80% institution/20% myself | 23% |
| 50%/50% | 41% |
| 20% institution/80% myself | 9% |
| It is 100% up to myself | 14% |

## 4. Results and discussion

In short, the survey confirmed that e-learners are closest to the "home users" category, one elaborated by Kritzinger and Solms [24].

Survey results are also mostly consistent with research in general public and raise the problems often described by researchers, such as password usage habits [25]. The system is vital for users: they got important materials, news and home works/projects there. On the other hand, as stated, they easily share password with another users, meaning that they have a strong "peer trust". Additionally, they tend to use same password for different systems. Having one password for many systems means that the compromising password at one point, would easily escalate into multiple point problem, so-called "domino effect of password reuse" [26]. It is shown that the care given to the password complexity and disclosure is directly connected to the perception of the system importance [27]. Here we got the discrepancy between care taken about security and the perception of importance.

As stated by Haque *et al* "Unfortunately, password-based authentication is by no means a panacea as far as usability is concerned" [28]. Additional information, gathered directly from the system is that users tend to forget passwords. In November 2014, the E-Learning System log got over 130 thousands of login error lines. With direct communication to users, but also from own experience, authors observed the common case of users accepting browser to save the password and then, after some time (while not having to enter it), while trying to access from another device, they cannot remember the password and cannot use the system.

On the other hand, about half of examinees do not think they should gain security education. The "ambivalent group" is also interesting: the substantial number of students is not sure if they need security education, which also implicate that the level of awareness is quite low.

E-learners do not think their data is of vital interest for hacker. This result may be connected to the effort user would invest into defending their data (the economy factor).

Usage policy is usually a short document stating some basic rules of system usage, users' rights and obligations. Every user is forced to accept it in order to use the system. However, no matter how brief the document is (and this actual one is about 700 words long), it requires some time to read and additional effort is required in order to comply with the rules. Less than half of e-learners actually read the policy. It is clearly that one cannot comply with policy if he did not read it.

When it comes to the profile data, the attitudes are divided and it seems like the aforementioned confusion between security and collaboration takes place. For instance, 25% of examinees think only teacher should see their data. It is then questionable how the communication is supposed to be facilitated between two e-learners if these are not able to know much about each other. For instance – about tags, description, courses they are enrolled in, etc. On the other hand the share of e-learners who would like their profile to be completely publicly available is negligible. We have even recorded a few student requests to delete some posts from publicly available forums in order to protect their identity.

The e-learner security perception of responsibility varies and even 14% do not take any responsibility for security, while the same percent is on the quite opposite side.

The survey confirmed assumptions that e-learners act similar to the ordinary home-users, keeping the common weak points in security. Also, the results revealed features specific for e-learners and their relation to the "e-learning matter", such as security policy or profile data. The key points that should be taken into the user model are further dissemination of all policy elements is needed, with special attention to account management; personal data disclosure option and password management.

The first remaining task is to describe the missing elements and add them to the user profile.

## 5. Learner model and its place in security enhanced standard learning architecture

Learner profile is a paradigm that describes the important aspects of user security behavior. The standards considered issue of user modeling in e-learning. IEEE PAPI model is introduced by IEEE and recommended by ISO. It is highly modular and scalable. The IMS LIP (Learner information package) is partly derived from the PAPI. Unlike PAPI, it includes both data and modeling information that is metadata. The enriched LIP structure is presented in figure 1:

Security issues are not particularly treated in IMS: the only particle dealing with the security is "security key", which identifies passwords for course access and encryption keys. Therefore a need for model upgrade emerged.

In order to enrich it with the security related data, we upgraded package with an additional structure – usersecurity. It is meant to be a foundation to the further developing of security agent that would "do a real job".

Usersecurity is a structure that is supposed to properly represent the important user properties regarding security, which were previously introduced. We recommend a highly flexible structure, formed in manner compatible with the IMS practice, which would allow developers to adapt it to the needs of particular platform and to successfully plug it into a learning architecture. It should provide external access to data important for monitoring of user security practice. The methods for access and update of information are supposed to be implemented in the learning environment and performed by the security agent responsible for the security layer of the learning architecture.

We propose the following elements to be defined: login administration, privacy control and general security capacity. Login administration is supposed to keep track of possible login issues and describe them in a structure. For example, if a user tends to often fail to login, or recover password, or forget to logout, the structure will keep the qualifications as levels of awareness in the particular field.

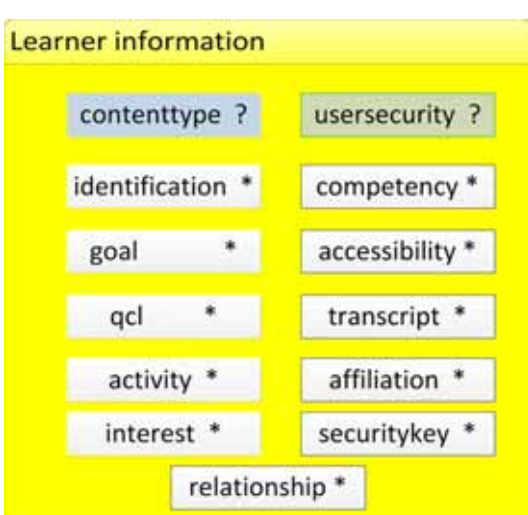


**Figure 1.** Upgraded IMS LIP.

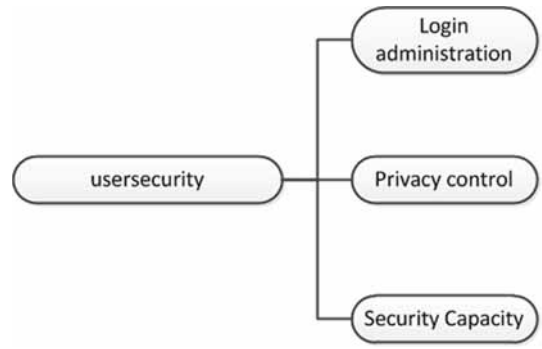


**Figure 2.** Usersecurity structure.

Privacy control keeps a user preference of what personal data is available to which users, in specific context. It is meant to allow user to control the field by themselves, but also to let the system accommodate the data visibility automatically (default option).

The security capacity is a category describing a general security awareness and practice of a user. It is implementation-dependent and might include things like message spamming, bad url guessing, mass downloading, inappropriate content in profile, uploading unsafe files and so on.

The proposed structure of usersecurity is shown in figure 2.

## 6. Standard learning architecture featuring eLearnion agent

E-Learning has been standardized by numerous organizations. Some standards are pointed towards learning process and portability of learning objects solely, while other also treat the context of e-learning, including infrastructure [29]. A great preview of standards featuring e-learner security and privacy is rendered by Jerman-Blažič and Klobučar [30].

IEEE 1484 introduces Learning Technology System Architecture (LTSA), a very generic, high-level e-learning architecture model [31].

In order to implement the security agent, we upgraded the standard architecture to include processes and flows required to improve learner's security. It means a dynamic process which includes constant monitoring of security related data. The architecture already got components and processes useful for agent functions – with the exception that these are meant to be used mostly for learning and not for security, since the standard clearly categorizes security issues as "other design issues". The architecture is upgraded and the new model is shown in figure 3. The security agent built upon is called eLearnion.

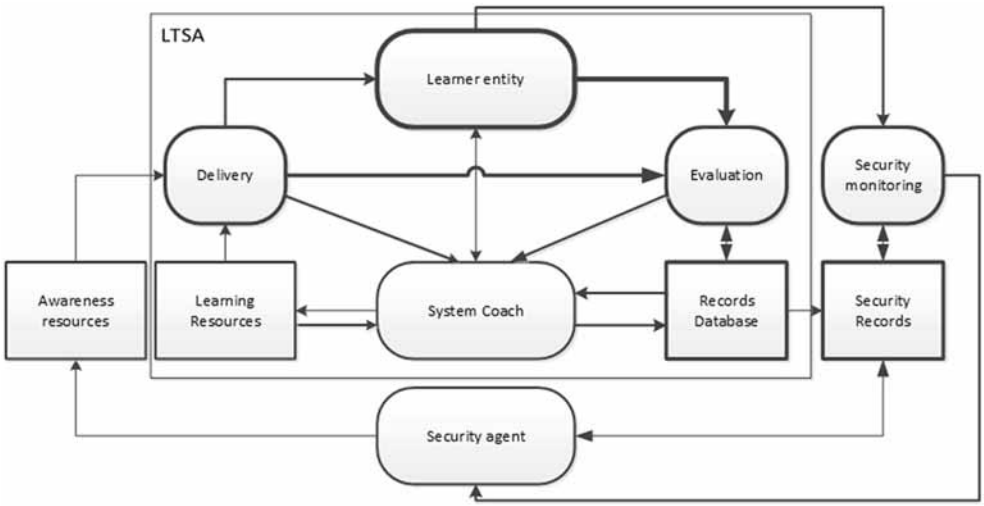


**Figure 3.** The upgraded LTSA architecture.

### 6.1 *Components of eLearnion agent*

The upgraded LTSA has kept its original structure and the security agent and other coupled components are added to it. The behavior related to security is monitored via Security monitoring process. The Security Record (which might be partly based on the general Records Database) keeps the learner information. It is passed to the Security Agent, which then use appropriate awareness resource to deliver content to the learner. The security agent also updates the security record. The agent function is somewhat similar to the system coach, only in security domain. Its role is to manage the delivery of appropriate information to e-learner, to update its security profile and allow other services to use it.

Very important process the agent orchestrates is delivery. The standard describes this process as output producer, which delivers learning multimedia to the learner. In this case, the delivery presents important information (in adequate form) to the learner. It also may adapt the information regularly present by the coach in order to augment its security segment.

eLearnion might incorporate additional functions such as awareness evaluation or security mechanisms adaptation.

### 6.2 *Implementation*

We will discuss implementation of the presented model in popular LMS, Moodle [22]. We chose Moodle because of several reasons:

- it is open-source, so the code is available and also the changes to code are permitted
- it is modular, therefore functionalities can be added as plugins
- Moodle has a large community and is well documented
- we use Moodle at our faculty, so testing and evaluation can be conducted in real system

In order to implement the upgraded LTSA model using Moodle, we should analyze Moodle's architecture and map required resources and processess to the Moodle existing elements and define which elements are supposed to be added.

*Moodle architecture* follows a traditional 3-tier web-application design. In general, Moodle is consisted of core and modules (figure 4). Core got all the basic libraries and defines API that all other components use. Modules may be defined in several categories, such as blocks, activities, repositories and themes. Following the defined procedures of how to create, install and maintain modules, allows their creation in a fully modular and decoupled fashion. On next level, it is administrator's task to install and enable the module and after that there is up to either administrator or teacher to use certain module, depending of its type and purpose. For instance, if a Youtube repository is enabled, then teacher may browse and embed youtube videos directly from Moodle.

User's interaction with the system is performed through web-browser, while choice of particular database and web-server is implementation-dependant and flexible.

We may differentiate various types of modules: course types, authentication types, blocks, activities, reports and so on. It is possible to add many features by fully modular approach, that is – without altering the core. Enabling proper add-in functionality is the recommended way of enriching Moodle with new features. In that way the update process would not overrun any code. However, one may not always do so: if there is a need for modifying certain features incorporated in core, the very core modification is required. These kinds of modifications are declared as "small hacks" and "major hacks".

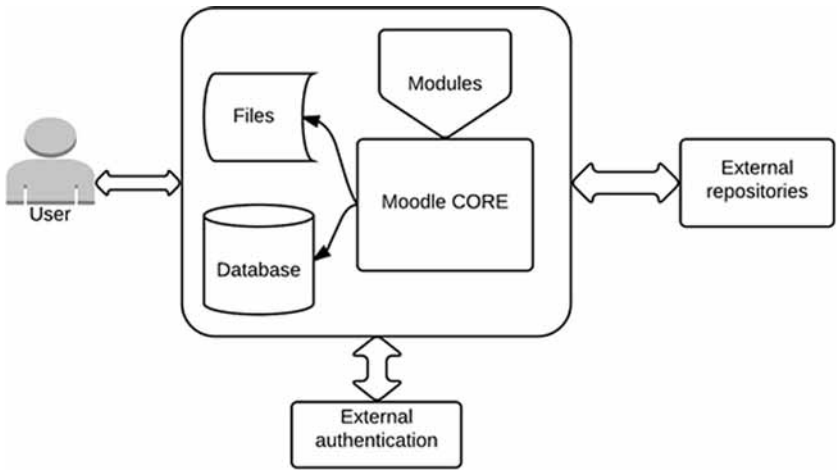


**Figure 4.** Moodle architecture.

In order of implementing the security eLearnion and the companioned architecture, several issues should be considered:

*Profile modification*: additional fields should be added to the existing profile, according to the user model discussed previously. Currently, profile got usual field such as name, place, e-mail, with option of adding custom fields by administrator. The additional fields are updated by the agent.
*Personal data visibility*: user may have various data in his profile and the agent should restrict their visibility according to the privacy value. Granularity of this feature depends on Moodle possibilities, since it recognizes only a few profile sections. Moodle got its profile settings, as well as multilevel permission system, which can be used to achieve data control.
*Gathering data*: Moodle got its native way of collecting data about events in its log. This data can be collected and interpreted or additional events can be caught and processed. Agent is supposed to track the data of interest and then communicate with user and update his profile (the security part).
*Communicating with the user*: This is probably the crucial activity, since its role is to directly affect the user's behaviour related to security and privacy. We realized this part using the block - module that can be positioned on course on site level, and also using the messaging system. The block may contain the following data:

- parts of the security policy
- information regarding general security culture: password creation, closing session, content licencing and so on.
- links to another content: tutorials, tests.

Figure 5 shows a block with link to the test (quiz) that is located on the same system and that is related to the security awareness. User is supposed to click the link and take the test. If he gets good score, then his security capacity will rise. It is not mandatory that user takes the test. That is actually a point in the awareness improvement in this model: the main user's task is to learn and the security awareness is supposed to be informally improved: by taking actions in voluntary manner. For example, if user does not at all click on link and take test, his security parameters will remain and can be updated according to other parameters.

These "other parameters" are based on user's activities, which are monitored. Moodle got its own event/log system. Events are defined and then triggered, which is logged. There are many events already defined and categorized (figure 6).

Existing events and logs that matter for the security agent are failed logins, password recovery attempts, sending too many messages and logging out. Additional events that should be added such as user uploaded a virus and user took an exam (awareness test) or user tried to access restricted site area (resource not allowed by permissions on some level). Agent will act accordingly to monitored behavior. Important parts of communication available in Moodle are mail and personal messages. Personal messages are in the first place meant for user-to-user communication. However,

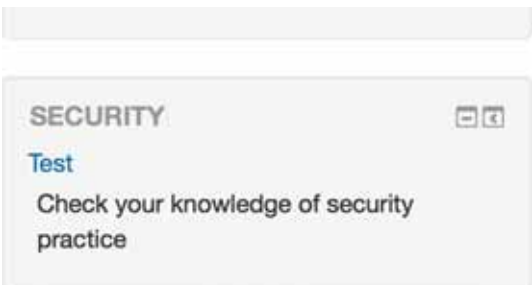


**Figure 5.** Security block.

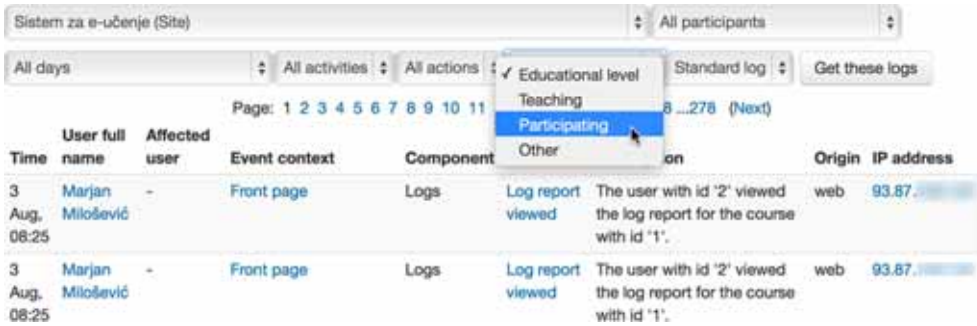


**Figure 6.** Logs and events categories.

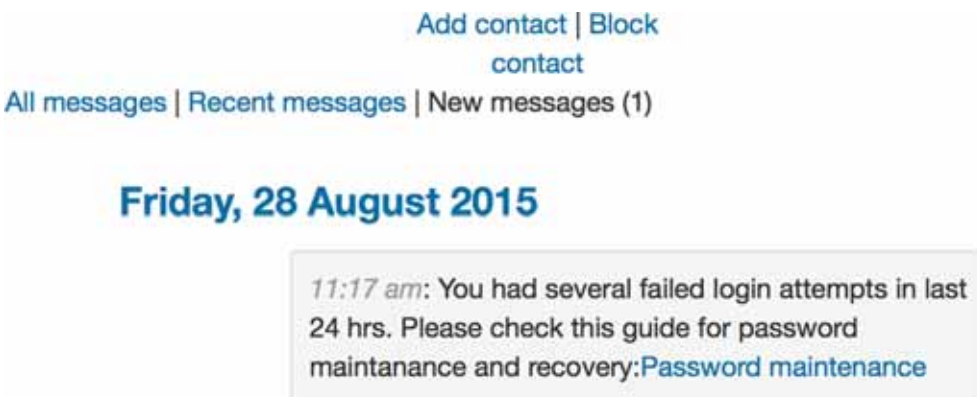


**Figure 7.** Automatic message generated by the agent.

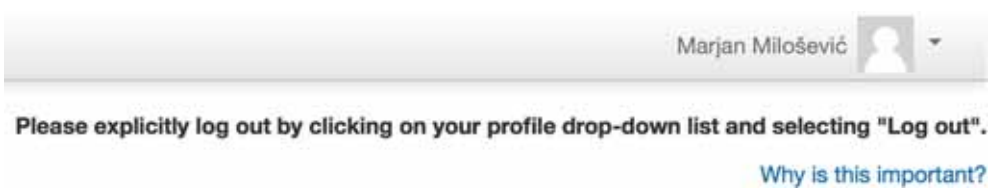


**Figure 8.** Example of interface changing.

messages API provides opportunity of sending arbitrary messages using different modules. Figure 7 shows a message sent by agent when user got login problems. The message is sent automatically after certain number of failed logins occurs. It may be sent by any present module too, such as block.

Messages' content is set in database, in agent's tables. It is optional for user to visit a suggested resource, but if he skips visiting it, the system will keep notifying him again and sending an e-mail with the same content. The approach should not be too aggressive, in terms of obligation. The agent is programmed to sporadically present resources and therefore let the user informally learn about the certain security threats, practice and precautions.

Interface adaptation is done in terms of emphasizing certain standard interface parts and also augmenting interface with additional elements. For example, if agent finds that user has passed some limit in not logging off the Moodle, he may get information through a block (about how is this action important), but also may get emphasized part of interface where he is supposed to actually log off. In the previous version of Moodle, the "Logout" link was visible directly on the front page. In actual version (2.9 at the moment of writing) the logout option is set in the dropdown list. Therefore, it is of little help to emphasize the very option, so this is done by programmatically adding the information on the front page. However, it is added only for certain users (figure 8).

## 7. Conclusions and future work

We found the e-learning user to be very close to model of home Internet user. And one of his features is poor security awareness. The conventional learning management systems suffer from a gap between users and security and we argue that only the continuous user support might promote his security position. A software agent we called eLearnion, which acts according to the augmented e-learner profile, should coordinate that task.

Actual standards do not directly scaffold the idea of raising the e-learner security awareness and support him in activities that correlate with security. Therefore certain adaptations need to be made in order to implement the idea. The user profile is adapted through adding appropriate structure to the standardized IMS LIP model. It is important for the structure to be very flexible, in order to facilitate implementation in various scenarios.

It turned out that standard architecture also did not directly support creation of a security agent, as it was not substantially involved with security. However, there is a way to make a modular approach, which does not jeopardize the basic standard structure, thus bringing the opportunity for practitioners and developers to set it as an addition to the existing system. The agent may be realized in Moodle, but not fully modular, requiring a modification of system's core too.

ELearnion is supposed to be evaluated in a production environment. In the future work, the development and evaluation of eLearnion will be discussed in more detail. Also, the possibilities of adding such module in other distributed architectures will be researched.

## References


[1] Mansfield-Devine S 2014 Mobile security: It's all about behaviour. *Netw. Security* 2014(11): 16–20. http://doi.org/10.1016/S1353-4858(14)70113-8

[2] Buttler E 2010 Firesheep. Retrieved from http://codebutler.github.io/firesheep/

[3] Chen Y and He W 2013 Security risks and protection in online learning: A survey. *The International Review of Research in Open and Distributed Learning*. Retrieved from http://www.irrodl.org/index.php/irrodl/article/view/1632/2725

[4] Weippl E R 2005 *Security in e-learning*. New York, NY: Springer.

[5] Zuev V I 2012 E-learning security models. *Manag. Inf. Syst.* 7(2): 24–28. Retrieved from http://www.ef.uns.ac.rs/mis/archive-pdf/2012-No2/MIS2012-2-4.pdf

[6] Violettas G E, Theodorou T L and Stephanides G C 2013 E-learning software security: Tested for security vulnerabilities & issues. In *2013 Fourth International Conference on e-Learning "Best Practices in Management, Design and Development of e-Courses: Standards of Excellence and Creativity"* (pp. 233–240). IEEE. http://doi.org/10.1109/ECONF.2013.66

[7] Milošević M 2013 Information security in e-learning: The matter of quality. *Preceedings, eLearning conference 2013*, (September): 26–27

[8] Von Solms B and von Solms R 2004 The 10 deadly sins of information security management. *Comput. Security* 23(5): 371–376. http://doi.org/10.1016/j.cose.2004.05.002

[9] Andress J 2014 *The basics of information security*. *The basics of information security*. Elsevier. http://doi.org/10.1016/B978-0-12-800744-0.00008-7

[10] ISF 2003 *The standard of good practice for information security*. Information Security Forum.

[11] Munley M 2004 Moving from consciousness to culture: Creating an environment of security awareness. SANS Institute. Retrieved from http://www.sans.org/reading_room/whitepapers/awareness/moving-consciousness-culture-creating-environment-security-awareness_1439

[12] Schneier B 2000 *Secrets & lies digital security in a networked world*. New Jersey: John Wiley & Sons

[13] BSI 2011 PD ISO/IEC TR 27008: 2011 BSI standards publication information technology — security techniques — guidlines for auditors on information security controls

[14] Zamzuri Z F, Manaf M, Yunus Y and Ahmad A 2013 Student perception on security requirement of e-learning services. *Procedia – Social Behav. Sci.*, 90: 923–930. http://doi.org/10.1016/j.sbspro.2013.07.169

[15] Shonola S A and Joy M S 2014 Learners' perception on security issues in m-learning (Nigerian Universities Case Study). *Exchanges: Warwick Res. J.* 2(1): 102–122. Retrieved from http://exchanges.warwick.ac.uk/index.php/exchanges/article/view/48/162

[16] Furnell S M, Bryant P and Phippen A D. 2007 Assessing the security perceptions of personal Internet users. *Comput. Security* 26(5): 410–417. http://doi.org/10.1016/j.cose.2007.03.001

[17] Rughiniş C and Rughiniş R 2014 Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union. *Comput. Security* 43: 111–125. http://doi.org/10.1016/j.cose.2014.03.008

[18] Adams A and Blanford A 2003 Security and Online learning: To protect or prohibit. In: Ghaui and Claude (Eds.) *Usability evaluation of online learning programs*. IDEA Publishing, pp. 331–359

[19] Beautement A and Sasse A 2009 The economics of user effort in information security. *Comput. Fraud Security* 2009(10): 8–12. http://doi.org/10.1016/S1361-3723(09)70127-7

[20] Besnard D and Arief B 2004 Computer security impaired by legitimate users. *Comput. Security* 23(3): 253–264. http://doi.org/10.1016/j.cose.2003.09.002

[21] SANS 2012 Security awareness survey. Retrieved February 19, 2015, from http://www.securingthehuman.org/media/resources/business-justification/security-awareness-survey.pdf

[22] Dougiamas M 2011 Moodle. Retrieved from https://download.moodle.org/releases/legacy/

[23] Crossler R E, Johnston A C, Lowry P B, Hu Q, Warkentin M and Baskerville R 2013 Future directions for behavioral information security research. *Comput. Security* 32: 90–101. http://doi.org/10.1016/j.cose.2012.09.010

[24] Kritzinger E and Solms S 2010 Cyber security for home users: A new way of protection through awareness enforcement. *Comput. Security* 25(2): 840–847

[25] Florencio D and Herley C 2007 A large-scale study of web password habits. In: *Proceedings of the 16th international conference on World Wide Web - WWW'07* (p. 657). http://doi.org/10.1145/1242572.1242661

[26] Ives B, Walsh K R and Schneider H 2004 The domino effect of password reuse. *Commun. ACM* 47(4): 75–78. http://doi.org/10.1145/975817.975820

[27] Florencio D, Herley C and van Oorschot P C 2014 An administrator's guide to internet password research. In: *USENIX LISA'14* (pp 1–18). Seattle

[28] Taiabul Haque S M, Wright M and Scielzo S 2014 Hierarchy of users' web passwords: Perceptions, practices and susceptibilities. *Int. J. Human-Comput. Stud.* 72(12): 860–874. http://doi.org/10.1016/j.ijhcs.2014.07.007

[29] Anido-Rifón L E, Fernández-Iglesias M J, Caeiro-Rodríguez M, Santos-Gago J M, Llamas-Nistal M, Álvarez Sabucedo L, and Míguez Pérez R 2014 Standardization in computer-based education. *Comput. Standards Interf.* 36(3): 604–625. http://doi.org/10.1016/j.csi.2013.09.004

[30] Jerman-Blažič B and Klobučar T 2005 Privacy provision in e-learning standardized systems: status and improvements. *Comput. Standards Interfaces* 27(6): 561–578. http://doi.org/10.1016/j.csi.2004.09.006

[31] Devedzic V, Jovanovic J and Gasevic D 2007 The pragmatics of current e-learning standards. *IEEE Internet Comput.* (June), 19–27