The Analysis of Security in a Multi-Server E-Learning Environment Based on Moodle and Zimbra Software.

Rafał Grzybowski  
Institute of Information Technology, Lodz University of Technology  
ul. Wólczańska 215, 90-924 Lodz, Poland  
rafalg@p.lodz.pl

Błażej Feret  
Library of The Lodz University of Technology  
223 Wólczańska Street, 90-924 Łódź, Poland  
blazej.feret@p.lodz.pl

ABSTRACT

An increase in popularity of university-wide e-learning platforms which support conventional educational methods and the development of new means of communication, has placed an emphasis on the security of data that is stored in such systems. The discussion on the issue of security in e-learning platforms was begun by M.K. Littman [8] as long ago as 1996. The following article seeks to identify security threats to data existing within a university’s e-learning environment, built on moodle software integrated with the remaining computer systems of the college, including an electronic mail system employing Zimbra technology. Analysis of a database of security infringements for the years 2011 and 2014 combined with insight into user behaviors described in literature identified areas to which systems are most vulnerable to unauthorized data access. Activities undertaken in each of the identified regions have a significant impact on one of three key elements of data security.

KEYWORDS

e-learning, security, university e-learning software, moodle, zimbra

1 INTRODUCTION

The global market for e-courses is developing rapidly, resulting in a commensurate increase in the number of remote learning systems [5][6]. This claim is supported by a report entitled „Tracking Online Education in the United States” [2]. According to said report and also information supplied by [3] the increase in popularity of such e-learning systems that has been observed during the last decade will continue, leading to almost 86% of classes for post-secondary students being completed online. In spite of this significant development, the issue of security in e-learning seems to be receiving relatively little attention in research, as well as in practice. In most instances these platforms are very complicated computer systems connected to the Internet, and thus susceptible to the same security threats as all other networks. Not taking appropriate security measures in e-learning could turn out to be a matter of great concern for both students and lecturers because of the risk of unauthorized access to sensitive data and work results. More information on security infringements can be

Definitions of computer system security and a basic division into categories were introduced by T. Olovsson [1], as a three layer system, represented in figure 1.

In the model proposed by T. Olovsson [1] computer system security has been divided into three categories, which are:

**Hardware Security**, comprising:
- Physical security, as a set of behaviors that protect hardware from external threats such as sabotage, theft, earthquakes or flooding.
- Emanation security, as a set of behaviors that prevent unauthorized broadcasts of data from hardware.

**Information security**, comprising:
- Computer security, as a set of behaviors reinforcing the weak points of the architecture of a given computer system.
- Communication security, as a set of behaviors protecting information while it is being transferred.

**Administration security**, comprising:
- Operation security, as a set of behaviors protecting the elements of a system from weak points in the organization of a system (procedural errors).
- Personnel security, as a set of behaviors protecting the elements of a system from attacks carried out by authorized users.

From the viewpoint of security, remote learning systems have a few unique traits. According to Edgar R. Weippl [4] “E-learning can be considered a special form of e-business. The good involved is digital content that has to be distributed, maintained, and updated. Moreover, the value of this good has to be adequately protected from unauthorized use and modification, without preventing students from using it in a flexible way”. The discussion on the issue of security in e-learning platforms was started by Littman [8] as long ago as 1996. She mentioned that “Internet access to online information can enhance a classroom instruction. However, network connectivity generates security risks for the learning environment”.

The discussion has touched upon these three domains: policy [9], [10], [11], widely understood management of access [4], [12], [13] and also intellectual property [14], [15], [16]. The conclusion taken from studying different areas of this topic indicate, that most authors lean towards marking advanced access management as the panacea for remote learning security threats. The authors of this article analyze the issue of security in a large e-learning platform built on the basis of moodle software. The moodle platform is a globally used LMS Open Source system. As of July 2015, the number of registered moodle installations was estimated at above 49
thousand, with more than 56 million users in 214 countries. Therefore, the topics this article touches upon may lay the groundwork for a broader discussion on security of the moodle platform itself and of its integration with other computer systems at universities.

2 DESCRIPTION OF THE COMPUTER ENVIRONMENT ANALYZED.

Many universities offer computerized remote learning platforms, which support the conventional teaching process by offering educational materials, a space for discussion and information exchange, systems for arranging and carrying out tests or exams, virtual libraries, and many other examples of additional content. University e-learning platforms are built as open, dispersed, multi-server computer systems. These are often integrated with administrative systems of the campus. This combination enables the flow of data containing student information and their authorizations to e-learning applications, which return updates on students’ progress within a given class or subject. Access to sensitive data such as:

- Personal data identifying a student or lecturer
- Type of degree, specialization name, year and number of semesters
- Email address
- Partial and final grades

are the reasons why security has become an important challenge in order to ensure that only authorized people have access to the right information at the appropriate time. The importance of this premise is also emphasized by Cárdenas and Sanchez in [18], as well as Zhang and Cao in [19].

The e-learning platform considered in this article was created within the Lodz University of Technology in the year 2010. Network connections within the system and data streams are presented in figure 2. The bulk of the platform comprises 17 autonomous moodle servers that exchange data via moodle net (mnet) technology. Each server is assigned to a single department of the university. The platform does not have a central user database. The profiles of students and lecturers have been created on servers belonging to the departments and types of degrees of which a given student or lecturer is a part.

![Figure 2. Network connections within the e-learning platform](image)
department was built for the purpose of authenticating users. An electronic mail system built in Zimbra technology was added to the platform for the purpose of enabling versatile campus-wide communication. Both Zimbra and moodle servers use the same LDAP database for authentication. By employing this solution and the Zimbra SSO module all moodle users can check their messages without having to log into another mailing system. The moodle software servicing the platforms was equipped with a number of extensions that adapt it to the principles by which the Lodz University of Technology functions. All of these extensions were produced by IT teams of our university.

In 2013 the platform was thoroughly modernized. The key element in the upgrade was the implementation of elements that allow full integration of data flow with the remaining systems of the university. The most significant change was the creation of a central authentication system based on CAS technology. Network connections after the modernization are presented in figure 3. A thorough analysis of the DSI database of security incidents has shown that the upgrade has increased the probability of security infringements in some areas of the system. This will be described in detail further in this article.

3 SECURITY AREAS IN A UNIVERSITY E-LEARNING SYSTEM

The original version of the system, as described in section 2, was subjected to a security analysis. The results presented in [23] allowed us to formulate the security structure of a university e-learning system, which is shown in figure 4. While this structure was being mapped out, an analysis of the DSI database of security incidents, mentioned in section 2, was performed. The examined platform was hosting about 20 thousand users at that time and was connected to all educational departments of the university.

Results of the aforementioned analysis are presented in table 1. The impact of activities within respective layers was assigned to one of two levels: HI – significant or LO – small effect. This approach allowed a quick identification of threat areas and the need for administrator oversight. Apart from the classification, table 1 contains statistics for the amount of security incidents registered in different areas joined by an identification of incident type (intrinsic or forced).

Because it was impossible to automatically register security incidents in the areas of legal security, communication tools and the application layer, data from the DSI database in these fields was deemed highly undervalued.
After the completion of this analysis it was advised that attention should be focused on preventing security infringements in the areas of: Authentication & Authorization Security, Database Security and Application Layer Security. What should be kept in mind is that activities taken in almost all of the areas have a significant impact on confidentiality of information.

As described in section 2, the year 2013 saw a thorough modernization of the platform which streamlined data exchange with the remaining computer systems of the university. A year after the completed upgrade, the authors of this article decided to carry out an analysis of the DSI database once more in order to evaluate the impact of performed upgrades on the security of data stored in the system.

Data included originated from the time period of the year 2014, during which the number of users reached 25 thousand leading to a fourfold increase in system calls (mouse clicks) relative to the previously analyzed period of the year 2011. Results of the second analysis are presented in table 2.

### Table 1. Significance of security activities in respective areas – 2011

<table>
<thead>
<tr>
<th>Security area</th>
<th>availability</th>
<th>integrity</th>
<th>confidentiality</th>
<th>intrinsic failure</th>
<th>forced failure</th>
<th>no of registered incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network hardware</td>
<td>HI</td>
<td>LO</td>
<td>LO</td>
<td>91%</td>
<td>9%</td>
<td>46</td>
</tr>
<tr>
<td>Computer hardware</td>
<td>HI</td>
<td>LO</td>
<td>LO</td>
<td>81%</td>
<td>19%</td>
<td>127</td>
</tr>
<tr>
<td>Operating system</td>
<td>HI</td>
<td>LO</td>
<td>HI</td>
<td>41%</td>
<td>59%</td>
<td>258</td>
</tr>
<tr>
<td>Legal</td>
<td>LO</td>
<td>LO</td>
<td>HI</td>
<td>3%</td>
<td>97%</td>
<td>86*</td>
</tr>
<tr>
<td>Authentication &amp; Authorisation</td>
<td>HI</td>
<td>LO</td>
<td>HI</td>
<td>14%</td>
<td>86%</td>
<td>361</td>
</tr>
<tr>
<td>Database</td>
<td>HI</td>
<td>HI</td>
<td>HI</td>
<td>58%</td>
<td>2%</td>
<td>9</td>
</tr>
<tr>
<td>Application layer</td>
<td>HI</td>
<td>HI</td>
<td>HI</td>
<td>60%</td>
<td>40%</td>
<td>138*</td>
</tr>
<tr>
<td>Communication tools</td>
<td>LO</td>
<td>LO</td>
<td>HI</td>
<td>0%</td>
<td>100%</td>
<td>72*</td>
</tr>
<tr>
<td>Session management</td>
<td>LO</td>
<td>LO</td>
<td>HI</td>
<td>49%</td>
<td>51%</td>
<td>176</td>
</tr>
<tr>
<td>Course management</td>
<td>LO</td>
<td>LO</td>
<td>HI</td>
<td>0%</td>
<td>100%</td>
<td>465</td>
</tr>
<tr>
<td>Role management</td>
<td>LO</td>
<td>LO</td>
<td>HI</td>
<td>3%</td>
<td>97%</td>
<td>26</td>
</tr>
<tr>
<td>Network management</td>
<td>HI</td>
<td>HI</td>
<td>LO</td>
<td>34%</td>
<td>68%</td>
<td>31</td>
</tr>
<tr>
<td>Configuration management</td>
<td>HI</td>
<td>LO</td>
<td>HI</td>
<td>3%</td>
<td>97%</td>
<td>68</td>
</tr>
</tbody>
</table>

HI - significant effect
LO - small effect
** - Data not representative due to lack of automatic registration method.

### Table 2. Significance of security activities in respective areas – 2014

<table>
<thead>
<tr>
<th>Security area</th>
<th>availability</th>
<th>integrity</th>
<th>confidentiality</th>
<th>intrinsic failure</th>
<th>forced failure</th>
<th>no of registered incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network hardware</td>
<td>HI</td>
<td>LO</td>
<td>LO</td>
<td>94%</td>
<td>6%</td>
<td>88</td>
</tr>
<tr>
<td>Computer hardware</td>
<td>HI</td>
<td>LO</td>
<td>LO</td>
<td>78%</td>
<td>24%</td>
<td>236</td>
</tr>
<tr>
<td>Operating system</td>
<td>HI</td>
<td>LO</td>
<td>HI</td>
<td>32%</td>
<td>68%</td>
<td>282</td>
</tr>
<tr>
<td>Legal</td>
<td>LO</td>
<td>LO</td>
<td>HI</td>
<td>4%</td>
<td>96%</td>
<td>246**</td>
</tr>
<tr>
<td>Authentication &amp; Authorisation</td>
<td>HI</td>
<td>LO</td>
<td>HI</td>
<td>9%</td>
<td>91%</td>
<td>712</td>
</tr>
<tr>
<td>Database</td>
<td>HI</td>
<td>HI</td>
<td>HI</td>
<td>99%</td>
<td>2%</td>
<td>56*</td>
</tr>
<tr>
<td>Application layer</td>
<td>HI</td>
<td>HI</td>
<td>HI</td>
<td>60%</td>
<td>40%</td>
<td>258**</td>
</tr>
<tr>
<td>Communication tools</td>
<td>HI</td>
<td>HI</td>
<td>HI</td>
<td>2%</td>
<td>98%</td>
<td>94**</td>
</tr>
<tr>
<td>Session management</td>
<td>LO</td>
<td>HI</td>
<td>LO</td>
<td>78%</td>
<td>22%</td>
<td>158**</td>
</tr>
<tr>
<td>Course management</td>
<td>LO</td>
<td>LO</td>
<td>HI</td>
<td>0%</td>
<td>100%</td>
<td>765</td>
</tr>
<tr>
<td>Role management</td>
<td>LO</td>
<td>LO</td>
<td>HI</td>
<td>61%</td>
<td>99%</td>
<td>106</td>
</tr>
<tr>
<td>Network management</td>
<td>HI</td>
<td>LO</td>
<td>HI</td>
<td>29%</td>
<td>71%</td>
<td>24</td>
</tr>
<tr>
<td>Configuration management</td>
<td>HI</td>
<td>HI</td>
<td>HI</td>
<td>13%</td>
<td>87%</td>
<td>96</td>
</tr>
</tbody>
</table>

HI - significant effect
LO - small effect
** - Data not representative due to lack of automatic registration method.
*** - Data not fully representative
4 ANALYSIS OF THREAT CHANGE IN RESPECTIVE AREAS OF SECURITY IN THE ANALYZED SYSTEM

An evaluation of changes in threats to information security in respective areas of the analyzed system was created by comparing data from analyses of DSI databases for the years 2011 and 2014, which are presented in tables 1 and 2. These changes may be summarized thus:

It was noted that there had been 42 more security incidents, which accounts for an increase of 91%, in the area of **Network Hardware Security**, which is defined as a set of behaviors designed to ascertain the continued functionality of hardware responsible for dataflow. However, if we allow for the fact that the number of users increased by 25% (from 20 to 25 thousand) and for the almost fourfold increase in platform workload (number of system calls increased by 390%, number of messages sent increased by 219%), we should interpret the higher number of incidents as a decrease in relative threat levels in the area of **Network hardware Security**. A similar trend can be seen in the area of **Computer Hardware Security**, which is defined as a set of behaviors designed to ascertain the continued functionality of elements providing undisturbed dataflow as well as in **Operating System Security**, which is defined as a set of behaviors designed to ascertain the continued functionality of the computer’s operational systems. A rise in the number of incidents was noted in both of these areas, by 85% and 48% respectively, but it is much lower than it would be expected if judged solely on the increase of workload handled by the platform. The three areas mentioned: **Network Hardware Security, Computer Hardware Security** and **Operating System Security** are elements of the Network Security group (Figure 4). Discussion of the results of the 2014 analysis indicate that this area was well designed and its remodeling did not impact security levels. The system is well scaled in terms of security and resistance to errors originating from increased workload.

**In the area of Legal Security**, which is responsible for updating and implementing normative acts of the University so that they are always in compliance with the law of the country, only a slight increase in the number of incidents was recorded. Because of the impossibility of automating the recording of such incidents this area was not evaluated in terms of security threat changes.

**In the area of Authentication & Authorization security**, which is responsible for implementing and oversight of the precise mechanisms of unambiguous authentication of users of the e-learning platform and allocation of appropriate authorizations, a 97% increase in the number of incidents was noted, but at the same time a few percentage points drop in the number of incidents generated within the platform. A higher number of incidents (attempts at unauthorized access) is easily explained by the fourfold increase of workload, which led to a proportional rise in demands for information stored within the system. The decrease of incidents generated within the platform may be attributed to a better structured login system implemented by utilizing the CAS technology and also to the rise of user awareness after several years of gaining experience with the system.

**In the area of Database Security**, which is responsible for foolproof functioning of the
system’s databases and protecting them from damage, a 22% drop in incidents was noted. This is evidence of the stabilization of the database system, good design and appropriate scaling.

In the area of Application Layer security, which is responsible for activities related to the design, execution, implementation and use of applications by the university e-learning platform, as well as Communication Tools Security, which is tasked with the selection of proper communication tools and imposing an appropriate data exchange policy within the platform, data was deemed unrepresentative because of the lack of mechanisms for automated recording of incidents.

However, a large major surprise was the drastic increase of incident numbers in the area of Session Management Security, which is responsible for choosing the most appropriate software for managing sessions within WEB interface applications. The change in the source of incidents is also puzzling. The analysis performed in 2011 showed an even distribution of external and internal session management issues, whereas the 2014 analysis highlighted that 78% of all issues had a source within the platform, which means that they concerned faulty session management and possibilities of unauthorized access granted to authenticated (legal) users who shouldn’t have the credentials otherwise. A study performed during the evaluation revealed that the cause for such a radical shift was the modernization of the platform, as described in section 2 of this article. As mentioned, one of the primary objectives of the upgrade was to implement a central CAS authentication system. In the past users were able to use the electronic mail system without additional logins thanks to the Zimbra SSO module. The drawback was that users had to log out of both the mailing system and moodle module independently, which generated a higher risk to security (because of the possibility of leaving an open e-learning or mailing session). The implementation of the CAS system was supposed to solve this inconvenience and at the same time integrate user authentication with other computer systems of the university. Unfortunately, the mailing system based on Zimbra technology, which has been used since the platforms’ launch, in fact increased the number of security incidents after the introduction of CAS because of its own architecture. The source of the problem which was identified during the analysis is illustrated in figure 5.
A login into the university computer system commences via the central authentication system (CAS). Users begin their work either by launching the moodle platform or the electronic mail system. The university moodle module is fully integrated with CAS, therefore login and logout operations invoke correct communication with the CAS server, which in turn passes on the login/logout message to remaining computer systems. A proper handling of these signals should result in assuring a high security level within the described area. As it was revealed during the study, Zimbra mail services do not process logout signals properly (CAS session termination signals), which generates incidents of unauthorized access to data. The threat scenario presents as the following:

1. A user is logged into the moodle platform
2. While working in moodle the user opens a session of Zimbra electronic mail in a different window or tab of a web browser, which results in a login into the mailing system on behalf of the CAS session opened by moodle.
3. After completing an e-learning session the user logs out of moodle, which results in the CAS server sending a logout and ‘end of session’ message.
4. Unfortunately, at the moment of obtaining a CAS session the Zimbra server launches an autonomous mailing process for the user, which does not recognize the CAS session termination message.

The result of the scenario presented above, creates a situation in which in spite of logging out of the moodle platform a mailing session is still open within the browser (an effect not compatible with SSO rules). Personal computers do not create opportunities for unauthorized data access, but in the instance of computers with multiple users (such as IT labs, research laboratories, free access areas) each following user may gain access to their predecessors mailbox. The only remedy is to close all of the browser windows after logging out of the CAS server. It is a serious oversight and was the reason for such a drastic increase in security incident numbers in the area of Session Management Security. Data in table 2 does not show the full scale of danger in the mentioned area, because it was obtained only from public access computers. It was impossible to gather the data from personal computers belonging to students and employees of the university.

In the area of Course Management Security, defined as a set of behaviors performed by lecturers while managing their courses, a 65% rise in incidents was noted, which was a result of increased use of the platform by lecturers. This growth is comparable with the growth of the number of lecturers who have begun employing the platform in their teaching process since the first analysis.

In the area of Role Management Security, defined as a set of behaviors performed by course administrators while managing the roles of the platform, a 300% rise in incident numbers was noted. The increased use of the e-learning system, which is followed by a tendency among lecturers (course administrators) to utilize the more advanced tools, revealed problems with incorrectly defined access to information stored in the platform - students obtain diminished or
broadened authorizations. Lecturers tend to overlook these missteps because of a lack of time necessary for acquiring the knowledge needed for proper management. An implemented system of intensive training should eliminate these shortcomings in the future. The rise in security incidents has its source in insufficient user knowledge of tools.

In the area of Network Management Security, which pertains to the optimization of data flow within the computer system, an irrelevant drop in security incident numbers was noted. What this means is that the network that was implemented a few years ago is properly designed, scaled and well managed. A similar conclusion can be drawn in the Configuration Management Security Area, defined as a set of behaviors performed during the configuration of the systems’ functionalities. Any recorded changes in incident numbers are minor and are evidence to good stability of configuration management.

5 CONCLUSIONS

The increase in popularity of e-learning systems and their high dependency on the Internet were the reasons behind the emergence of new threats in the field of security of information stored within such systems. This assessment was prepared with the purpose of comparing how the threats change during the functioning of a system and any changes in its configuration and workload. All activities defined in the process of analyzing data from the e-learning platform functioning on the Lodz University of technology present significant impact on one of three key elements of data security. Nowadays one cannot imagine an e-learning platform functioning in isolation from the remaining computer systems of a university or a modern electronic mailing system.

The analyzed platform was built on the basis of Open Source tools, a very popular methodology in recent times. As presented in section 4, even the most advanced e-learning software, although well protected and safeguarded from security infringements, can reveal its data because of oversights in integration with other systems. During an observation of performance of the moodle software that spanned five years, which was utilized in constructing the platform, enough evidence was gathered to support the claim that, if correctly configured, it can be used to build a multi-server e-learning environment, resistant to issues originating from a multiplied workload growth. It also enables satisfactory oversight of security protocols so as to maintain confidentiality of user data in e-learning. Security incidents that involve users who have been granted too broad or too narrow authorization in access to educational content have their source in insufficient knowledge among administrators (lecturers among others) and not in software drawbacks. It is also noteworthy, that a very sensitive point of such multi server platforms is their integration with other computer systems. As described in section 4, even a suitably configured moodle system may produce an opportunity for unauthorized personal data access when paired with another system, which in this instance was Zimbra.

E-learning platforms belong to a very specific type of computer systems, in which data publication must be prevented not only by mechanisms originating in information technology, but also by appropriate normative
acts and education of the systems’ users. The authors of this article will continue researching aspects of identifying potential threats to information security in e-learning systems built with the use of Open Source software, while concentrating on creating tools for implementing and overseeing security protocols within multi server environments.

REFERENCES

