Implementation of an e-Learning System. Optimization and Security-related Aspects

ANTOANELA NAAJI, COSMIN HERMAN
Faculty of Computer Science
“Vasile Goldis” Western University
Arad 310025, Bd. Revolutiei nr. 94-96
ROMANIA
anaaji@uvvg.ro, cosmin@uvvg.ro http://cs.uvvg.ro

Abstract: - Over the last few years, information and communication technologies have been increasingly used in higher education. Likewise, virtual learning environments are largely replacing traditional teaching methods. Implementing complex e-learning systems requires both creating a reliable hardware infrastructure and using high-performance software platforms. This paper presents a few solutions for optimizing these two components, taking into account the changes occurring throughout the use of an e-learning platform, such as: increase in the number of users, web content, data trafficking, exceeding servers' load degree, as well as hardware equipment. At the same time, it presents a few measures for ensuring the security of the information system within which this platform is operated.

Key-Words: - Optimization, security, e-learning system, LMS, Moodle

1 Introduction
The development of information and communication technologies has led, over the last few years, to the higher education system being reconfigured. Thus, more emphasis is now laid on student-centered education, an objective that can be fulfilled by using these technologies [6]. More and more attention is paid to virtual universities and online communication environments. As such, higher education policies can no longer be defined in a traditional context [10], [11].

In the course of the last years, Romanian authorities have been looking for alternatives, such as new web-based teaching methods, to the classic way of teaching, deeply rooted in the Romanian education system. That is the reason why universities try to develop or to adapt different e-learning environments to the needs of today’s education. The most common system used within Romanian higher education is blended learning, which combines online activities with face-to-face, generally applicative ones.

The University’s e-learning platform is based on the Moodle environment and it was implemented in 2003, following a study on existing open-source, but also proprietary platforms [9], [14].

The use of such platforms requires, in addition to development, optimizing and securing procedures, as regards both the hardware and software. These aspects shall be presented throughout the following chapters.

2 Platform Description
The Moodle platform offers a complete study, assessment and collaboration solution, both for teachers and for students. This solution provides user-friendly tools for creating and publishing courses, to be used by teachers. The infrastructure is based on a well-organized database technology, on a secured server, which has an efficient management of the search and display time for the required information [20].

Generally speaking, servers being used in Learning Management Systems (LMS), particularly for web sites, may have various configurations, ranging from PC desktop to dedicated servers. The university has implemented a reliable hardware structure of professional servers.

Moreover, LMS are usually organized as 2, 3, n – tier architectures, for dividing webpage delivery and database management tasks, for processing transactions and interrogations at database level, etc.

In order to implement the Moodle platform at university level, we had to acquire an appropriate hardware structure, as part of the university’s information system. This structure comprises:
- the firewall server – which secures Internet input and output, filtering suspicious packages, allowing access solely to logged users (by username and alphanumeric password), with high complexity. This server also deals with filtering, to a certain extent, high-risk codes, such as viruses or worms;
- the mail server – which supports the email application, users’ mail boxes, with a large variety of intercommunication, high accessibility, high security, users being easy to configure. This server is outfitted with an extended HDD space, considering the increase in the number of users and stored messages;
- the accounting application server – which hosts the SAP;
- the student management server – which hosts the Academis (University Management System) applications for managing students and their academic and financial situations;
- a Moodle platform server - which hosts online courses that are only available to students, who can access them directly on the Internet. Online exams can only be accessed using the internal network, from all university locations, through VPN (Virtual Private Network) [12].

As regards the software, the platform offers:
• Resources required for continuous education for the University’s students;
• Interactivity between students and teachers;
• Possibility for online testing and assessment;
• Organization of online forums;
• Student-student and student-teacher communication;
• Homework submission;
• Flexible grading;
• The possibility to surf through the webpage with a menu in Romanian, English, French and German;
• Virtual information panel.

3 Optimizing the Hardware and Software Infrastructure

As new versions of the platform were released and as they were installed on the university servers, we had to make some improvements, among which: developing the hardware infrastructure, optimizing the database, organizing students per specializations and years of study, developing additional modules, etc. [8], [15], [17].

3.1. Developing the hardware infrastructure

This development was necessary because of the increase number of users simultaneously connected to the platform, the web content, the number of online tests, which led to the overloading of the server’s physical charge.

Considering the reliability standard of the servers’ hardware and software resources, which recommends that the average load should be maximum 50%, it was decided to improve the hardware and software infrastructure of the information system [16].

The implemented structure is scalable, the servers’ hardware and software performance can be periodically improved, depending on average functioning parameters.

Since the elements influencing a server’s performance include: the hardware structure in use, the operating system, connection speed, number of simultaneous visitors, the size and type of delivered resources (static, dynamic pages), etc., we periodically monitor the devices’ load degree and the average number of processes being run.

The decision of selecting the servers was made after taking into account benchmark results (SPEC CPU2006) for the same processor series, Intel Xeon [21].

3.2 Optimizing the Database

In order to optimize the database, which is necessary due to its large size, the data were stored from MyISAM format to InnoDB format [3], [4]. One of the advantages of this type of data storage is that it supports much faster transactions. Another important aspect is that it allows “foreign keys”, so that the union of data structures can be made much more dynamically, saving time and resources in supplying requested data. InnoDB also recovers from a crash or other unexpected shutdown by replaying its logs.

Considering that the tables’ dimensions have over 2 million entries, speed and access to information is imperative. External key requests allow us to access the information exactly where it is located in the table. Index clusters are another facility provided by InnoDB.

Table 1 draws a comparison between the two types of data storage.

<table>
<thead>
<tr>
<th>MyISAM</th>
<th>InnoDB</th>
</tr>
</thead>
<tbody>
<tr>
<td>- supports table locking</td>
<td>- supports row locking</td>
</tr>
<tr>
<td>- not very stable when it comes to many requests in a database with a large amount of information</td>
<td>- more stable transactional</td>
</tr>
<tr>
<td>- ideal for a site with fewer requests;</td>
<td>- larger resource consumption</td>
</tr>
<tr>
<td>- compress read-only storage</td>
<td>- ideal for a large amount of data</td>
</tr>
<tr>
<td>- takes less RAM</td>
<td>- data caches</td>
</tr>
<tr>
<td>- does not support data caches</td>
<td>- clustered indexes</td>
</tr>
<tr>
<td>- does not support clustered indexes</td>
<td>- supports hash index</td>
</tr>
</tbody>
</table>

Table 1. Comparison between MyISAM and InnoDB
3.3 Organizing Students per Specializations and Years of Study

This adjustment was made for a better educational resources management, in accordance with each specialization’s curriculum and corresponding exams. Organizing the users was based on the following schema:

Branches → Faculties → Specializations → Form of education (full-time or distance learning) → Years of study → Groups

Compared to the standard version of Moodle, in which the users could be organized only in groups, the following fields were added to the registration form: branch, faculty, specialization, form of education, year, group, in order to make user management easier. These fields were automatically added to the database [20].

The new type of organizing was required for setting specific queries regarding faculties, specializations, etc. and also for a better organization of online exams.

Initially, users were identified by means of a username consisting of a succession of numbers and a randomly generated password. Currently, the username consists of the user’s social security number.

3.4. Implementing additional modules

For the platform to be more useful and complex, additional modules were implemented. They do not occur in the standard version, requiring special installation and configuration. Problems arise regarding the set of files codes and set of fonts. The following modules were implemented and designed:

- Glossary - improved (new words added);
- Photo gallery – used Gallery2 and enhanced for Moodle;
- Text translator – used Google translator (9 languages);
- Virtual classes – used BigBlueButton (Google Code).

In the case of other modules such as: Timer, Appointment, Blog, Calculator rate, special configurations were designed for the server (Linux Debian). As with most plugins, modules and blocks, Romanian is not an available language option, so we had to perform a translation [20].

Another implemented module was virtual information panel, particularly useful for displaying the information needed by students, such as: timetables, various notices, lists for student groups, etc. Its implementation was based on the Moodle forum, but restricted to student and teaching staff access, appearing on the menu only after log-in.

4 Aspects Regarding the Security of an e-Learning System

4.1 Network-level Security

For the purpose of ensuring the security of the information system, the first step consisted of creating a private virtual network MPLS IPVPN [1]. This was especially necessary for online testing servers, due to some flood problems that appeared when servers had direct access to the Internet.

The MPLS IPVPN solution is implemented on the MPLS infrastructure, accomplished through permanent, safe and highly accessible connections between university buildings, distributed across the city and the entire country. This facility ensures secured, hierarchical and controlled allocation of resources and information. The MPLS VPN system allows the implementation of dedicated solutions for data, voice, videoconference or secured intranet and extranet applications, or of dedicated software for centralized management.

MPLS technology entails a high security standard at the level of the provider’s network, eliminating the need for purchasing equipment for routers and encrypting data among our locations.

The following services are installed and configured:

- VPN MPLS IP service on a dedicated channel between the main node and the other locations;
- Installation and configuration of a closed-circuit telephone system between all locations, with a support of fax transmission, without any monthly subscription costs, ensuring unlimited conversations;
- Establishing hierarchical priorities for diverse traffic categories, according to the needs;
- Dynamic bandwidth allotment for Internet access from the main node to the other locations, so that Internet bandwidth unused by locations would be available for use from the IT Department;
- Capacity-use graphs for each sub-network, in real time;
- Monitoring, notification and alert applications within the main node for all sub-networks in the locations;
- E-mail hosting with unlimited mail addresses, unlimited aliases and unlimited domains, with antivirus facilities, SPAM blocks and an interface for administrating mail domains, accounts and aliases;
- Administration and maintenance of systems in all locations;
- Centralized data backup services which runs on the data backup server.

The developed solution is complete and seeks to maximize performance, optimize costs and proactively monitor the infrastructure of LAN, VPN, MPLS networks or Internet, using proper equipments administered by us. Regarding the software, we have used both open-source and proprietary solutions, which are very reliable.

Thus, we have succeeded in minimizing the required bandwidth by analyzing and proactively monitoring the traffic, with a priority for the services of the infrastructure, depending on their importance, headquarters and branches. The proactive monitoring was extended to work stations and servers, seeking to ensure both their availability in the network and the availability of services provided. Considering the fact that the services are supervised 24/7, priorities are assigned to them according to the order of requests.

Figure 1 shows an example of traffic monitoring graphs per location.

Fig. 1. Traffic and bandwidth between April 2009 and April 2011

Network usage reports help us to monitor traffic and potential anomalies. Proactive monitoring reports inform immediately if an element of data transmission infrastructure, work stations, servers or services provided by them has any problems or does not work within normal parameters. The information system can be integrated with a VoIP system for transmitting alarms directly to the mobile phone.

Using these graphs, apart from a traffic monitoring tool, also an indicator for establishing infrastructure management, which also involves taking appropriate decisions for optimizing this infrastructure.

Following the analysis the existing traffic, we have implemented a self-balancing system for it, between the main node and the other subsidiary locations, so that, each location allots up to 4Mb, 2Mb up and 2Mb down. The total bandwidth is 45 Mb. In case the band is not used, it is automatically allotted to the main node, which will re-allot resources.

Since, in each location, there are several laboratories and offices, i.e. computers, the traffic can be monitored differentially on each of these by using the Linux command iptraf, run on the main router [7]. An example of traffic monitoring is shown in Figure 2.

![Figure 2. Example of traffic monitoring on the IP](image-url)

As regards server security, we are permanently concerned with intranet data security, the security of transmitted information, the security of services provided for students and teachers. The information security solution is structured per several levels [7], [13].

**Level 1**
Firewall – the first protective device in any security system, filtering internet or intranet content depending on the known characteristics of applications being used. The firewall level is used in both directions of data transmission, efficiently protecting computers at internet port levels.

**Level 2**
IPS and DoS – We use the most advanced and up-to-date techniques, in real time, for detecting and preventing cyber-attacks and attempts to intrude upon computers and servers located either in the university campus, or in the offices of faculties. Denial of Service sensors detect and interrupt cyber-attacks of any type, i.e. tcp syn flood, tcp port scan, tcp source/destination session, udp flood, udp scan, udp source/destination session, icmp flood, icmp sweep and icmp source/destination session, which threaten online data transmission. Intrusion
Prevention System protects Windows, Linux, BSD, Solaris and MacOs operating systems, as well as BO, DCERP, DHCP, DNP3, DNS, FTP, H323, HTTP, ICMP, IM, IMAP, LDAP, MSQL, NNTP, P2P, POP3, RADIUS, RPC, RTSP, SCCP, SIP, SMTP, SNMP, SSH, SSL, TCP, TELNET, TFN and UDP protocols against take over targeted computers.

**Level 3**  
AntiVirus and AntiMalware - Since laboratories are used by many students, we use definitions of viruses that are updated in real time; the system scanning Internet traffic provides full protection. The antivirus application scans all transited files through possible infested Internet protocols, namely HTTP, FTP, IMAP, POP3, SMTP, IM and NNTP, while the anti malware engine scans against Adware threats, BHO, Dial, Download, Game, HackerTool, Hijacker, Joke, Keylog, Misc, NMT, P2P, Plugin, RAT, Spy and Toolbar.

**Level 4**  
Web Filter and Application Control – We have the possibility to allow or to prohibit 75 categories of sites and 20 types of web applications in the campus, laboratories or offices, in order to obtain a customized content on the Internet.

**Level 5**  
Spam Filter – Since unwanted SPAM messages make up to 80% from the total number of emails transacted on the Internet, we make sure that they are filtered directly from the e-mail server, and thus do not reach the e-mail utility. We use cutting-edge technologies and global information, updated in real time. The service is addressed to the most widespread e-mail protocols, namely IMAP, POP3 and SMTP. In addition to calculation algorithms of the SPAM score, we also apply marks to messages, using IP, URL, CheckSum, HELO DNS, filters, sending/return e-mail address and key words. Thus, we have succeeded in minimizing this recurring problem.

**Level 6**  
Data Leak Prevention – We have also applied a system for analyzing the entire internet/intranet traffic, in order to detect, block or intercept the transmission or reception of documents, chat messages or confidential data, according to pre-established SLA criteria and internal security standards. We check email, http, ftp, nntp and messenger protocols, with the possibility of assigning sensors or creating templates for content, subject, sender, recipient, web addresses, size, type and transfer content or attached file.

### 4.2 Platform Security

Considering that the Moodle platform also supports online exams, securing it is very important.

Thus, platform administration is organized per levels of permission and usage rights - administrator, teacher (tutor) and student. The platform administrator has full permission rights, teachers have the right to create and manage courses (tests), to grade tests and deal with feedback, whereas students have only the right to access courses or exams they were registered to.

The access to the two components is made based on a username and password, the same which the student receives upon enrolling into the 1st year of study to access the student management system. This securing is supplied by the file server which provides secure, fast and manageable Internet connectivity. The server includes a firewall that is extensible to various levels, characterized by dynamic package filtering. The high-performance cache speeds up web access, also saving time from bandwidth, and is scaled for an efficient and dynamic load balancing. Flexible management tools offer policies on several levels for users, applications, destinations, timetables and types of content.

In order to ensure online exam security, in the sense of making it impossible to access exams from another location than the one decided by the teacher, an IP range corresponding to that particular location is introduced in their configuration.

### 5 Conclusions

With the development of new web technologies, we are considering to upgrade the e-learning platform from version Moodle 1.9.12.* to version Moodle 2.0.* [2] even if this version was only launched 6 months ago and the compatibility of modules between 1.9 and 2.0 is only partly resolved. Thus, we will use this version, which benefits from a much more dynamic structuring of resources and content. Technologies such as jQuery, Ajax MySQL InnoDB are among the most common technologies currently being used in any LMS [5], [18], [19].

For a future development of the platform we intend to implement Web 2.0 modules which are very interactive, using content like sounds, videos and animations. Web 2.0 is a standard that encompasses intercommunication technologies and software and hardware interconnection, multimedia applications, 3D technology, social networks, blogs,
microblogs, videoblogs, podcasts, videocourses, wikis and RSS [22].

For better user management, we seek to synchronize databases corresponding to Moodle and the university management system applications.

If it will be necessary, we will upgrade the hardware structure on which the applications run. As regards the assurance of information system security, it will be adapted according to upcoming standards.

References: