MOODLEGATE: SECURING COMPUTER DRIVEN EXAM ENVIRONMENTS

Rodolfo Matos, Jonathan Barber

Computer Centre (CICA), Faculty of Engineering (FEUP), University of Porto (PORTUGAL)
rmatos@fe.up.pt, jbarber@fe.up.pt

Abstract

Moodle installations that are used to make assessments inevitably run the risk of being used to obtain fraudulent results by the students. Such fraud can be mitigated through the use of auditing tools that detect abnormal behaviour, but students continue to attempt to cheat the system despite the knowledge that these tools are active. This article presents a tool that blocks a range of behaviours which could be used by students fraudulently. This result is achieved by implementing access control to any Moodle deployment. The access control is based on the identity of the Moodle user, time and date, computer (or range of computers), and the Moodle resources that are being accessed. By integrating with Moodle, the tool is able to provide a finer level of access control than would be provided by traditional network access control devices such as firewalls. This increases the assurance that the results of Moodle driven exam assessments are accurate.

Keywords: Moodle, quizzes, examination, fraud, cheating, security, prevention, auditing.

1 INTRODUCTION

Computer based examinations are becoming increasingly important because of the benefits they can deliver over traditional paper based methods. These benefits include reduced running costs from material expenses such as paper and printing; lowered management costs from the collection and distribution of completed exam scripts to assessors and evaluating the results; decreased time to evaluate examinations, and simplifying the task of tracking student performance.

Despite the benefits listed above, computer based examinations introduce their own problems, including new opportunities for cheating through the examination system itself.

In this work we examine the problems of cheating through computerized examination systems. We focus on the Moodle platform as it is our institution's e-learning platform. We present a new tool, MoodleGate, designed to protect the Moodle learning management system (LMS) from attempts to cheat during examinations.

1.1 Learning Management Systems

There are many learning management systems (LMS) available. However, in 2012 the market is dominated [1] by BlackBoard (44.8%), Moodle (20.1%), Desire2Learn (11.1%) and Sakai (6.1%). LMSs typically offer both pedagogical and evaluation capabilities in the same package. This integration of functionality presents several benefits. Firstly, users become more familiar with the user interface for both systems – as the same interface is used for both teaching and examinations, this makes it easier and less stressful for students to complete examinations and more likely that staff will not make errors when constructing examinations. Secondly, operational costs (due to installation, maintenance and licensing) are generally be less for a single software package than for two packages. Finally, by integrating pedagogy with evaluation, it should be simpler to monitor the progress of students and so better target future teaching resources.

1.2 Typical LMS Architecture

LMSs are commonly deployed in one of two configurations: either the server is installed on the institution's premises; or the server is installed at a remote location. These configurations have dramatically different scenarios for cheating because of the information available to the LMS about an examinee's computer.

In an on-premises installation the LMS can accurately determine where an examinee's computer is located through its network address. With a remote installation this is not possible as the network

address is normally hidden by the institution network. Indeed, with a remote installation it can be impossible for the LMS to know if students are using different computers or sharing the same device.

Therefore, if it is important that examinees take an exam at a stated location, and that a person can be proved to have taken an exam, then a remote installation may not be appropriate.

1.3 Goals of an Examination

The point of an examination is to assess the ability of the examinee at a point in time without unauthorized assistance or materials. Fraud is therefore the unauthorized use of materials or assistance during the course of an examination. Types of fraud and exemplars are:

1 Unauthorized communication between examinees (e.g. whispering answers).

2 Impersonation (e.g. one student taking an examination for another).

3 Access by examinees to unauthorized material during the exam (e.g. crib sheets).

4 Preventing the running of the examination (e.g. setting off a fire alarm).

Examinees determined to cheat will use any methods that permit the illicit activities listed above. The type of technology used to perform these activities is inconsequential. Crib sheets could be paper based or on-line and accessed via wireless devices; communication between examinees could be via whispering, on-line instant messaging, or Bluetooth capable devices [2]. With mobile phone technology improving and miniaturization continuing, technology will be increasingly used to assist in cheating at examinations.

Besides these examples of cheating, the advent of using LMSs as examination systems presents to additional problem of examinees using the LMS as a method of cheating. It is this problem that the MoodleGate tool addresses.

1.4 Increase in Examination Fraud

A recent study [3,4] characterizing Portuguese University students discovered that the percentage of students that had previously cheated in exams is 69.3%. The same study reports that “copying-favourable environments are associated with a higher propensity to cheat”. This observation is reinforced by the work of Roberts & Wasieleski [5] who report that the use of computer based technology is positively related to misconduct.

Together, these studies show that cheating in the electronic environment of an LMS is a real problem that needs to be addressed. Because dishonest conduct is encouraged when the act of dishonesty is easy and the risk of punishment is low [6], removing opportunities for misconduct through LMSs is important to combat cheating.

1.5 Methods of Cheating via Moodle

Most teachers and administrators of LMSs are not aware of the methods used to cheat, or of how easy it can be to cheat. The following examples of cheating via Moodle have been observed [7,8] and are provided to give examples of the problems that MoodleGate tool is designed to solve:

1 Unauthorized communication

1.1 During an examination, student A logs in with student B's username and password. Student A can now see all the questions and answers of student B and copy the answers.

1.2 If student B is not enrolled in the examination, then student A can use this as a second login and as a means of communicating with collaborators outside the exam environment. As this is an unexpected pattern of behaviour it is often disregarded even if logs are audited by invigilators. This was one of the most frequently observed methods of cheating [7].

1.3 During an examination, Student A and B can communicate by editing their own user profiles. The profiles include a section called “details” which allows text to be written. By frequently refreshing their view of the other student's profile and updating their own profile, this can be used as a form of instant messaging.

2 Impersonation

2.1 During an examination, student A logs in with students B's username and password and can now impersonate student B to complete their exam. If student A is malicious they can sabotage student B's exam. If network restrictions are not enabled in Moodle, then student A doesn't have to be present in the exam room to carry this out.

3 Access to unauthorized material

3.1 Pedagogical material or crib sheets can be saved in other parts of the LMS that are usually out of scope of the examination process logging system. These can then be accessed by the students during examinations.

3.2 Moodle 2.0 introduced the Private Files repository, providing users with an area to store their own files. However, access to this area is not logged by Moodle, is enabled by default, and can not be restricted on a user-by-user basis. This therefore provides a simple way for examinees to store crib sheets.

4 Preventing the examination from running

4.1 The default Moodle configuration allows requests to the system to be made by normal users that cause a very high load on the server [8]. These requests can be made very frequently by simply requesting the same page repeatedly (by pressing and holding the “refresh” key of the web browser). Generating many of these requests causes the server to become overloaded and no longer able to respond normally.

Reactive technologies such as MoodleWatcher [7, 8] provide a real time dashboard of student activities during examinations. However, by design MoodleWatcher is a passive tool that does not enforce good behaviour. Additionally, MoodleWatcher is tightly integrated with Moodle, and so major releases of Moodle require that MoodleWatcher be tested and adjusted so as to work for those releases.

The MoodleGate tool introduced here is a proactive technology that can prevent fraudulent behaviour attempted through the Moodle LMS. It works by restricting the Moodle resources that examinees can access during exams, thus preventing unauthorized communication and materials from taking place through Moodle. By using the network addresses of the computers used by examinees, it can restrict access to Moodle resources based on location.

2 MOODLEGATE OVERVIEW

MoodleGate consists of 3 components:

1 An web-based administrative interface for exam administrators to manage Access Control Lists (ACLs) that define when, where and what Moodle resources the users are allowed to access for an exam

2 A database which stores the ACLs

3 A firewall which consults the ACLs for every request made by a user to Moodle

The firewall is placed in front of Moodle, so that all user requests to Moodle pass through the firewall. Based on the ACLs, the firewall can then specifically allow or deny any activity within Moodle. The administrative interface integrates with Moodle quizzes (examinations) to make it simple for course leaders to administer the ACLs for their quizzes – defining when examinations are taking place, where users taking the exam should be located and what resources the examinees should have access to during the exam.

Here we will describe MoodleGate from the point of view of exam administrators and the examinees.

3 EXAM ADMINISTRATION INTERFACE

After logging on, a course leader is shown a list of quizzes that they are responsible for (Fig. 1). The list shows the time and date of when the examinations are, the course that the examination is assessing and the room that the examination will be held in. The time and date defines when the ACLs are active, the course defines which Moodle users the rules will be applied to, and the room defines which computers will be allowed to take part in the exam.

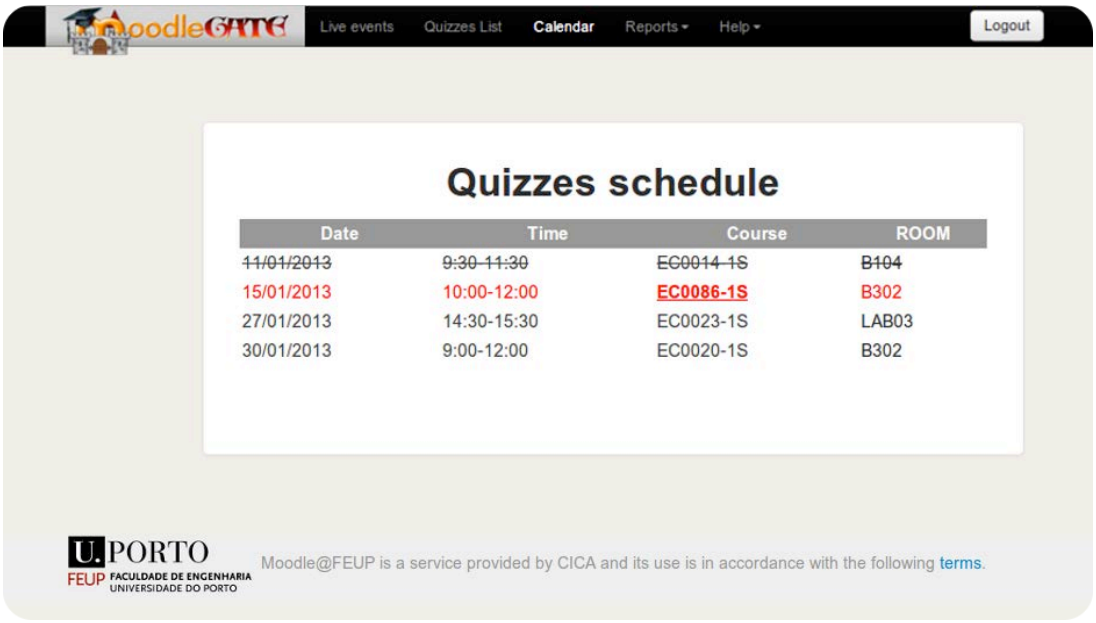

Fig. 1: MoodleGate screenshot illustrating the exam administrators interface and list of examinations.

Each quiz in the list is a link that opens a page to show the exam's details (Fig. 2). These include a link to the list of users enrolled in the quiz and an editor to define which Moodle resources will be accessible during the exam (the whitelist). The list of users provides a simple method to print out an attendance sheet for checking which students are present during an exam. The page showing the exam details page also has an interface for enabling or disabling the ACLs to allow the exam administrator to bypass the MoodleGate restrictions.

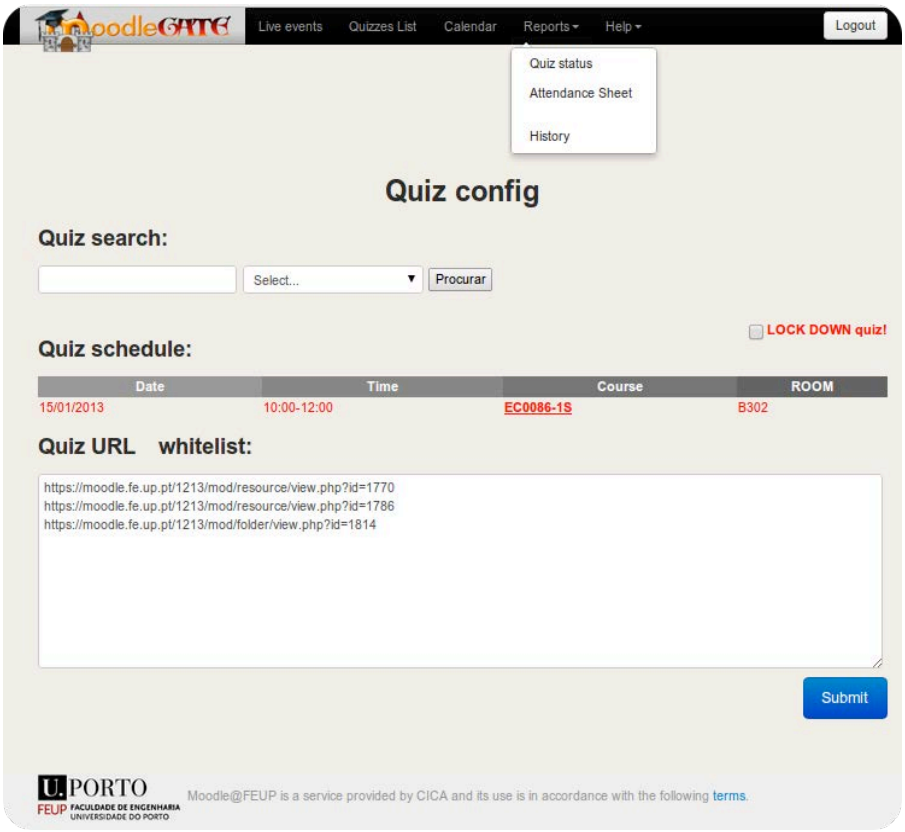

Fig. 2: MoodleGate screenshot illustrating the administrative interface for editing the resources available for an exam.

While the quiz is in progress, a live page shows the status of the examination, including attempts to access unauthorized materials, attempts to log in as an non-enrolled user from within the exam room, and changes in computer by enrolled users. If a user changes computer, they are automatically denied access until the administrator allows them access through this screen.

After the exam is complete an audit log of examinee activity can be generated - using MoodleWatcher [7,8] - showing which computers the users were using, and when and where attempted infractions took place.

4 EXAMINEE INTERFACE

When an examinee accesses Moodle from a computer in an exam room during the time that a quiz is active they are presented with a special MoodleGate login page (Fig. 3). After they login with their usual Moodle username and password, they are shown the list of quizzes that they are enrolled for at that time and location and links to the quizzes.

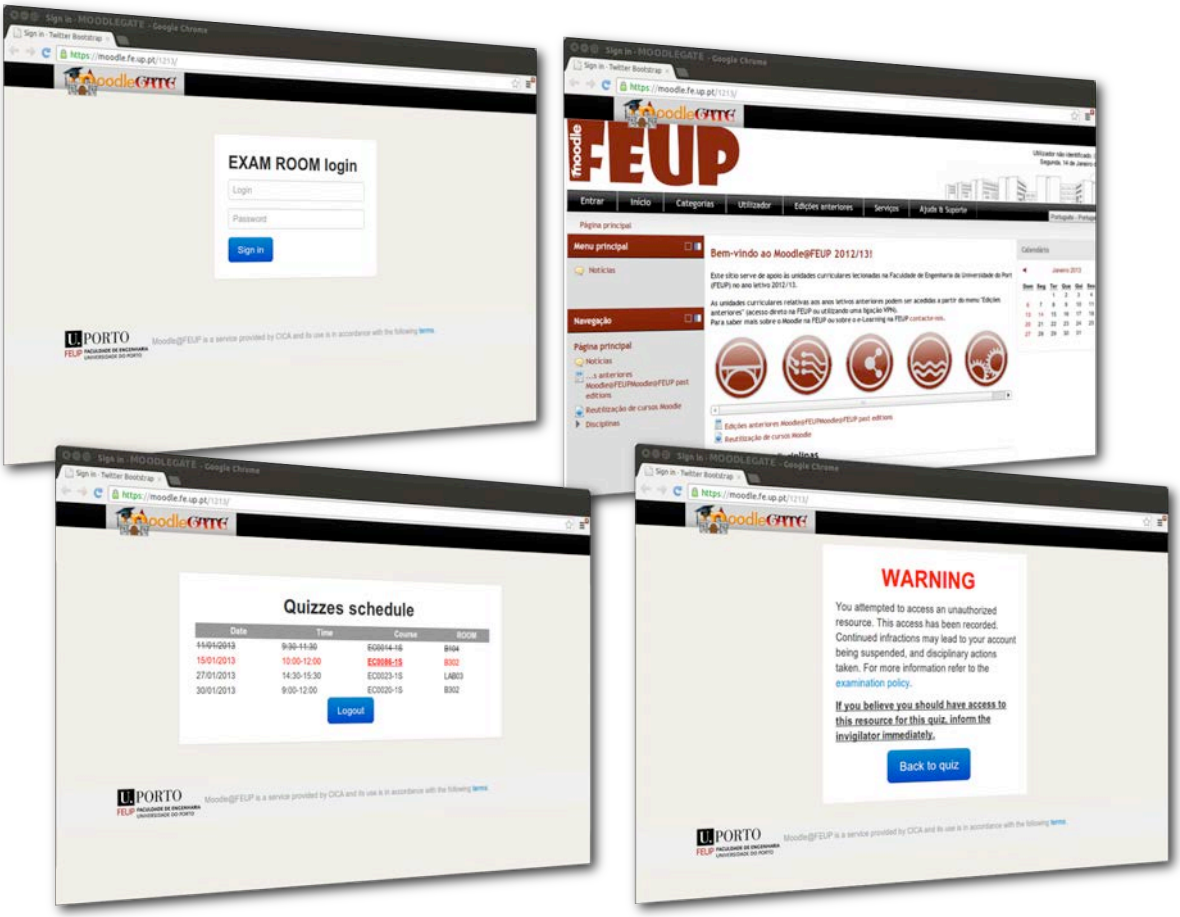

Fig. 3: Screenshots of the interface shown to examinees during an exam; Top left shows the initial login screen, bottom left shows the list of examinations the examinee is enrolled in, top right shows the normal Moodle interface after logging in, bottom right shows the warning issued to examinees if they attempt to access resources not permitted by the quiz whitelist.

During an examination, when the user accesses a Moodle resource that they are not permitted to by the examination whitelist, they are instead shown a warning that informs them that the content they are trying to access is restricted.

If the user is not enrolled in any quizzes, they will not be able to access any resources from an examination location during the time of the quiz.

If a user enrolled in an exam accesses Moodle from outside the exam location, they are shown a warning message that the content they are trying to access is restricted.

If a user that is not enrolled in an exam accesses Moodle from outside the exam location, they can access Moodle as they would normally.

When a user accesses the Moodle content, they are still regulated by the Moodle access control system. MoodleGate therefore provides an additional layer of security to the Moodle system.

5 CONCLUSIONS

MoodleGate increases the integrity of examinations by addressing the points raised in section 1.5 as follows:

1. Unauthorized communication
    1.1. MoodleGate blocks multiple logins from the same computer or student, thus preventing users from sharing login information.
    1.2. MoodleGate prevents students not enrolled in a examination from logging in at an exam location. Additionally, students enrolled in an exam will not be able to access Moodle from outside the exam location. This stops students from outside the examination location from colluding with students taking the exam.
    1.3. By not including the profile resources in the MoodleGate exam whitelist, MoodleGate restricts access to user profiles, preventing them from being used for cheating.
2. Impersonation
    2.1. MoodleGate provides an attendance sheet of the students in an examination and reports the location of the computers that the students taking their examination at. This allows the invigilators to verify their identity.
3. Access to unauthorized material
    3.1. MoodleGate restricts access to all content that is not explicitly allowed through the exam whitelist. By not preventing access to non-examination material MoodleGate prevents students from accessing crib sheets they may have loaded into Moodle before the examination.
    3.2. Because MoodleGate is external to Moodle it can restrict access to Moodle resources that currently have no access controls defined within Moodle. It can therefore restrict access to private files and other, currently unknown, potential methods for sharing materials.
4. Preventing the examination from running
    4.1. Because MoodleGate is external to Moodle it can filter requests to Moodle and therefore prevent access to pages that might cause the server to become overloaded.

In conclusion, MoodleGate helps to prevent fraud during examinations through the mechanisms outlined above, it improves management of examinations by providing a central point management dashboard and an audit trail of attempted infringements. Finally, it eases running examinations by providing an accurate attendance sheet.

6 FUTURE WORK

This paper addresses local installations as described in section 1.2. We plan to extend MoodleGate to allow MoodleGate to be used for remote installations where the Moodle server is located outside off premises.

REFERENCES

[1] http://www.campuscomputing.net/item/campus-computing-2012-mixed-assessments-it-effectiveness (Nov. 2012)

[2] http://www.chinadaily.com.cn/china/2012-06/06/content_15477031.htm (Jan. 2013)

[3] http://www.fep.up.pt/docentes/ateixeira/integridade_academica/11.09.11_Integridade%20Acad%C3%A9mica%20em%20Portugal_relat%C3%B3rio%20s%C3%ADntese.pdf (Sep. 2011)

[4] Teixeira A.A.C.; Rocha M.F. (2010) "Academic misconduct in Portugal: results from a large scale survey to university economics/business students", Journal of Academic Ethics, Springer, 8(1): 21-41.

[5] Roberts, J. A., Wasieleski, D. M. (2012) Moral Reasoning in Computer-Based Task Environments: Exploring the Interplay between Cognitive and Technological Factors on Individuals' Propensity to Break Rules, Journal of Business Ethics 110:355–376

[6] Mazar, N., Ariely, D. (2006) Dishonesty in everyday life and its policy implications, Working paper series, Federal Reserve Bank of Boston 06-3

[7] Matos, R., Torrão S., Vieira T. (2012) "Moodlewatcher: Detection and prevention of fraud when using Moodle quizzes" INTED2012 Abstracts CD (ISBN: 978-84-615-5562-8), INTED2012 Proceedings CD (ISBN: 978-84-615-5563-5)

[8] Matos, R., Torrão S., Vieira T., Carvalho F. (2012) "Moodlewatcher: One year experience of detecting and preventing fraud when using Moodle quizzes" EDULEARN12 Abstracts CD (ISBN: 978-84-695-3176-1), EDULEARN12 Proceedings CD (ISBN: 978-84-695-3491-5)