

Identifying and Protecting eLearning Systems From Corrupt Use and Plagiarism

Emil Marais and Basie von Solms

Academy for Information Technology
University of Johannesburg
Johannesburg, South Africa
emar@rau.ac.za, basie@rau.ac.za

David Argles

Electronics and Computer Science
University of Southampton
Southampton, United Kingdom
da@ecs.soton.ac.uk

Abstract

eLearning systems are becoming the main support medium in education. To enable an eLearning system to protect the academic integrity of the education provider, it is critical to address security issues and to protect the integrity of the system. (von Solms, 2004) eLearning systems have unique security issues and therefore require additional checks and balances to protect the integrity of the system. Not all of these issues are addressed by web security research although a well-designed system will be more secure. In this paper, security issues specific to eLearning systems will be identified and solutions to these problems given. Current commercial systems and security research do not address these issues competently and therefore these issues need to be addressed. In this paper, data obtained from practical assignment submissions showing that plagiarism is a problem in eLearning systems will also be presented. The problem can be minimized by applying the solutions presented in this paper and including certain tools and reporting functions that enable course administrators to be alerted of corrupt use. From the data presented in this paper, we will show an alarming number of users submitting similar assignments that can be proven to be copied from only a few sources. These copy groups are not desirable in an eLearning system

where we want to make sure that students do their own work with summative assessments. The security issues acknowledged in this paper have been identified from experience working with different eLearning systems that provide the primary support for several programming courses. eLearning systems are an excellent tool to ease the administration burden of the course presenter and to provide support for students but we need to address the issues identified in this paper to allow it to take the place of conventional assessments while protecting the integrity of academic information.

1. Introduction

eLearning systems ease the course administration burden of presenting a course and provide tools to present the information in an orderly and clear way. Although commercial and experimental systems have vastly improved over the last 5 years and have become learning portals they still lack certain tools to ensure academic integrity. We will start by looking at the results obtained when allowing learners to remotely submit their assignments without any control of where and when they can submit. The only restriction was a cut-off date that had to be adhered to. Thereafter methods to limit the corrupt use of eLearning systems will be discussed and lastly.

2. The Extent of Cheating in eLearning Systems

Corruption in eLearning systems is a big problem as shown in an earlier article by the authors where the conclusion was that an auditing function needs to be integrated into current eLearning systems to create an easy way for course administrators to audit submissions. (Marais, 2006) The data shown here has been obtained by auditing practical submissions for a second year programming course. A copied programming assignment is where the code is 80% or more exactly the same as another assignment as determined by a similarity checker. The implementation of this checker is not discussed in this article as it is not the focus of this article. Figure one shows the amount of copiers.

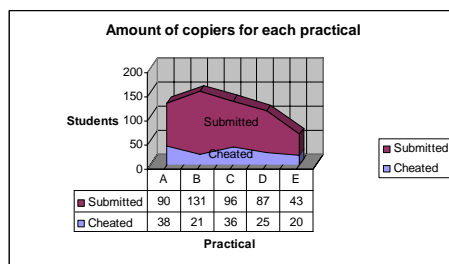


Figure 1: Amount of copied practicals.

This data was obtained by auditing a class of 190 students and only including the students that submitted practicals. Expressed as a percentage the following results were obtained:

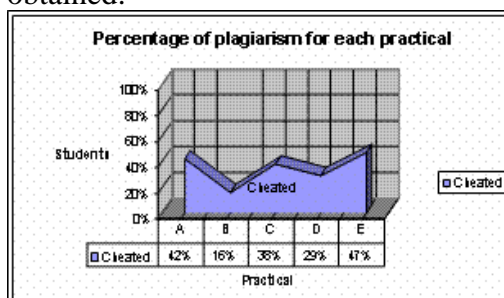


Figure 2: Percentage of copied practicals.

This is unacceptably high and needs to be addressed. It was also seen that there are

distinct groups that copied from each other. In a group an original author and the copies of his/her practical were identified.

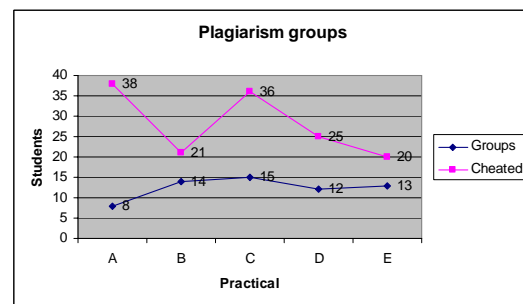


Figure 3: Amount of plagiarism groups.

The same problem is present with online assignments where students submit online assessments or e-assessments in the eLearning environment. To prove there is corruption is somewhat more difficult but this article discusses how corrupt use can be minimized or even avoided. The e-assessments are slightly different from the submission of assignments in two important aspects that are:

- E-assessments are normally done in a controlled environment.
- It is difficult to impossible to check two assessments for copying.

With a controlled environment is meant that the assessment has to be taken without:

- Help from another student.
- No books or Internet sources may be consulted.

Therefore we need to secure the e-assessment environment.

3. Securing the e-assessment Environment

This section will identify the security issues in eLearning environments that are relevant to e-assessments.

3.1 Correct/supervised Location of e-assessment Practical Submission

It is important to be sure that a test is taken at the correct location. eLearning

systems rely on a communication medium that connects all the computers to give them access to the intranet and Internet. This unfortunately implies that the web-based clients can also access other services other than the eLearning server as shown in figure 3 below:

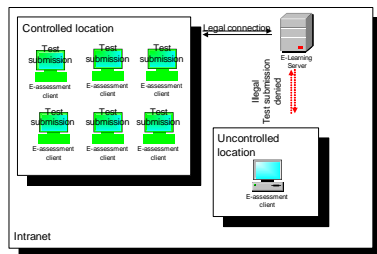


Figure 3: Controlled and uncontrolled environments

As can be seen from figure 3 only students in the controlled environment are allowed access while a student trying to make a submission from an uncontrolled location is denied access. The reason for blocking such a student is that the student in the uncontrolled environment could be helped by another person or use material not available to other students taking the test. Even worse a student can write the test and leave the venue where after he/she can log into the server again at another location and submit a practical for another student or correct his own.

WebCT is one eLearning system that currently provides a subnet mask to allow traffic only from a specific subnet to the assessment server (Walton, 2005). This is similar to using a firewall to distinguish different users. Unfortunately this is not foolproof as IP (Internet Protocol) addresses can be spoofed, the network environment needs to be laid out correctly for it to work and remote administration tools can be used to control a machine in a legal location from an uncontrolled environment, this scenario will be discussed in a later section. The next level of security that is also supported by WebCT is to password protect the

assessment. A password is set that needs to be entered before the assessment can be retrieved. The password has to be verbally given to the students or physically entered by the invigilator/s. Here again the security it provides is not sufficient as any cell phone or bugging device can be used to leak the password outside of the controlled e-assessment location.

The solution is to use several of the following techniques:

- An IP range instead of only a subnet mask.
- Inputting the number of students and letting the password only allow that many students to login before the password is automatically changed.
- Having a tracking console to monitor connections.
- Monitoring the network traffic for anomalies.

Only allowing a specific IP range decreases the likelihood of machines in an uncontrolled location to gain access to the e-assessment but this is not the ultimate solution.

By only allowing the required amount of students to login to then make their submission also decreases the chance of anybody logging in twice or from another location. If a password is set to gain entry into the e-assessment only people at the test location will be able to hear the password if verbally given in the controlled environment. If the password is sent by cell phone to another student he/she would not be able to login as the password would have changed as soon as the amount of students at the location has logged in. Unfortunately the implementation of this is more cumbersome as students always come in late and machines stall etc. This creates an administration burden/nightmare for the invigilator.

By having a login tracking console the lecturer can monitor the connections to the

server but this requires the constant monitoring of the environment that again introduces an administrative burden.

By only allowing network traffic that matches the pattern of the majority of connections from clients, makes it possible to determine if a student's login is from a legal test submission location. If they were in another location the traffic would most likely take another route and could have different response times etc. Unfortunately this is also not the ultimate solution but is only one more level of achieving a higher level of security.

3.2 Test Visibility

When writing a practical test the students need to be separated sufficiently that they cannot copy from each other. Another way of deterring students from copying from each other is to set two tests that are placed at alternating desks in the test location or randomizing test questions.

3.3 Avoiding Electronic Corruption

The integrity of the eLearning server can be violated by electronic corruption. Electronic corruption is any means whereby a student, malicious person or program changes information on the server, makes use of resources not specified in the test (writing the test outside the test location where the student can have access to books or the Internet) or helps another student by communicating with a fellow student.

As an example we need to deny a student from logging in twice, thereby doing a double submission for him/her and then for another person. To accomplish this, the server has to deny two logins originating from the same IP address. If non-static IP addresses are used the student could reboot his/her machine to get another IP address but to solve this loophole the lecturer could set the eLearning server to not accept new

connections for the duration of the e-assessment. If a student's machine stalls, the invigilator could have an override function to allow a student at his/her discretion. Commercial products do not cater for the detection of a double submission. The problem of a double submission is illustrated in figure 4 below.

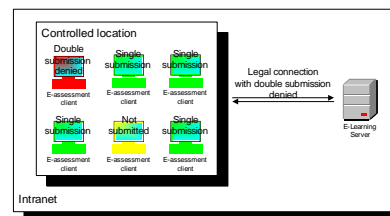


Figure 4: Double submission

An even worse scenario is where a student completes his test and then reboots his machine telling the invigilator the machine broke. When the invigilator helps the student log in again he/she can use another person's login to complete another student's test by using the knowledge of the just completed test. Controlling double submissions could prevent this problem but if the student is moved to another computer the exploit could still exist.

When a test is taken it should also not be possible to go to a website that contains information giving the student an unfair advantage. To deter this kind of corruption, the following approaches can be taken:

- Controlling the routing table on the workstation.
- Enabling monitoring software on the workstation.
- Locking the student in the test environment.

When the routing table is controlled on the workstation only traffic to the e-assessment server is allowed. To deter a student from manually changing the routing table the second approach could be used in conjunction with this method.

If monitoring software is installed on each workstation the e-assessment can then

be monitored to see if other sites are being accessed or if the machines routing table has changed. Monitoring software can also be used to scan for high ports being opened that could indicate that a remote administration tool or other communication tools are being used. If these conditions exist a message can be sent to the invigilator to investigate the matter. Denying access to other sites and the controlling of the routing table is shown in figure 5 below.

Figure 5 also illustrates how monitoring software can be used to detect the remote controlling of an e-assessment submission in a legal location from an uncontrolled location.

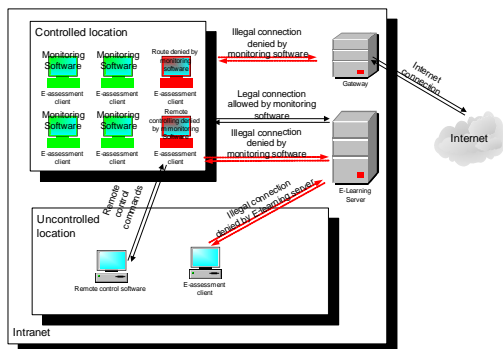


Figure 5: Monitor software running on the computers to limit corrupt use.

When a student is locked in the e-assessment environment he/she will not be able to access other sites but here again the student could reboot the system and claim the machine stalled.

4. Conclusion

The exploits identified in this paper is unique to e-assessments and need to be addressed to be able to make sure that a fair assessment has been taken. Therefore the solutions suggested in this paper brings us closer to ensuring fair use on eLearning systems.

5. References

- Marais E., Minnaar U., Argles D., 2006, "Plagiarism in eLearning systems: Identifying and solving the problem for practical assignments", *The 6th IEEE International Conference on Advanced Learning Technologies*, pp 822-824, Netherlands.
- Walton S., KS3 ICT Onscreen Test Project, Qualifications & Curriculum Authority, *BETT 2005*, http://www.qca.org.uk/downloads/6967_ks3_ict_bett_2005.pdf, Accessed on 9 July 2005.
- von Solms B. 2004, "Information Security Governance In ICT-Based Educational Systems", *Discourse*, Year 32 Volume 1.