ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Enhanced Security for Online Exams Using Group Cryptography

Shaik Abdul Muneer
Assosiate Professor,
Department of Physics,
Osmania College (Autonomous), Kurnool.

G.Mahaboob Basha
Assosiate Professor,
Department of Physics,
Osmania College (Autonomous), Kurnool.

ABSTRACT:

Online exam is field that is very popular and made many security assurances. Then also it fails to control cheating. Online exams have not been widely adopted well, but online education is adopted and using allover the world without any security issues. An online exam is defined in this project as one that takes place over the insecure Internet, and where no proctor is in the same location as the examinees. This project proposes an enhanced secure filled online exam management environment mediated by group cryptography techniques using remote monitoring and control of ports and input. The target domain of this project is that of online exams for any subject's contests in any level of study, as well as exams in online university courses with students in various remote locations. This project proposes a easy solution to the issue of security and cheating for online exams. This solution uses an enhanced Security Control system in the Online Exam (SeCOnE) which is based on group cryptography with an e-monitoring scheme.

INTRODUCTION:

Education has expanded rapidly. Even so, the off-line test is usually chosen as the evaluation method for both off-line education and online education. The se- curity of online examinations remains a problem. In some cases, the person writing the exam on a networked computer is moni- tored by a proctor at some predetermined location. But, the requirement for an exam location goes against the accessibility, the major attraction of e-learning or distance learning. The requirement may also negate the cost savings generated by e-learning or pose obstacles for remote students. Simplification and automation of educational processes are other benefits of online educatio, and online exams inherit these advantages.

To remove the requirement for human intervention in secure online exam management so as to capitalize on the advantages of online processes, this paper proposes a solution to the issue of security and cheating for online exams. This solution uses an en- hanced Security Control system in the Online Exam (SeCOnE) which is based on group cryptography with an e-monitoring scheme. The cryptography supports enhanced security control for the online exam process, as well as authentication and in- tegrity. The e-monitoring provides a proctor function to remote examinees to prevent cheating, and thus removes the require- ment of having to go to a fixed location. The target of this paper is online exams for mathematics or English contests in middle or high school, and exams in online university courses with stu- dents at remote locations. This paper addresses the problem of administering an online exam at a fixed time with the same ques- tions for all examinees, just like an off-line exam, but without re- stricting the physical location of the examinees. As the SeCOnE system enables many kinds of tests to be given online, it can pro- vide teachers with better evaluation standards for students and may contribute to improving the quality of education.

Requirements For A Secure Online Exam

The requirements for a secure online exam are as follows.

- Accessibility Online exams should be possible without re- gard to location and time.
- Monitoring The absence of proctoring on online exams may relax the examinees and encourage cheating. Therefore, it is necessary for an online exam manage- ment system to have some monitoring method to prevent and to detect cheating.
- Management Online exam management includes

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

problem creation, problem sheet distribution, answer sheet collec- tion, marking, grade posting, and handling of appeals. The cost savings of online exams mitigate the burden of exam enforcement and induce many examinees located at very remote sites to participate in the exam. Educators can ob- tain more objective standards for evaluation. The automatic management of exams lets the examinees know their exam performance very quickly. Online exams permit both edu- cators and examinees to achieve their objectives efficiently.

An online exam should also have the following features.

- Authenticity The identities of the examinee, examiner, marker, and proctor should be all authenticated and veri- fied at every step in the online exam process, because it is difficult to identify them "face-to-face" online.

Existing System:

- Different cheating patterns exists in current system including copying the answers of others, exchanging answers, searching the Internet for answers, using the data and software saved on the student's local computer and discussing the exam by e-mail, phone, or instant messaging.

Disadvantages:

1) Level of communication between teachers and students decreases.
2) The tendency to cheat by students increases.
3) The system must rely on students' honesty or their having an honor code

Proposed System:

- This project proposes a solution to the issue of security and cheating for online exams. This solution uses an enhanced Security Control system in the Online Exam (SeCOnE) which is based on group cryptography with an e-monitoring scheme.
- The cryptography supports enhanced security control for the online exam process, as well as authentication and integrity. The e-monitoring provides a proctor function to remote examinees to prevent cheating, and thus removes the requirement of having to go to a fixed location. The target of this project is online exams of any type and exams in online university courses with students at remote locations.
- Project proposes administering an online exam at a fixed time with the same questions for all examinees, just like an off-line exam, but without restricting the physical location of the examinees. As the SeCOnE system enables many kinds of tests to be given online, it can provide teachers with better evaluation standards for students and may contribute to improving the quality of education.

Advantages:

1) Online exam management system having some monitoring method to prevent and to detect cheating.
2) Without regard to location and time.
3) Avoid intercepting or interfering with communications during an online exam.

An Enhanced Security Control In The SeCOnE System:

A. Architecture of the SeCOnE System

As shown in Fig. 1, all entities in the SeCOnE system per- form their roles as members of either group G_A or G_E. S_S re- ceives the problems and the right answers from C_T, and then distributes the problems and collects the answer sheets from C_E. A proctor monitors the examinees through C_P using the mon- itor data in S_M. Through C_E, an examinee belonging to G_E and managed by A_E, can take the online exam. The group agents A_A and A_E create a set of public and private keys [20] for each group. They distribute this set of keys to their group members at each exam, and exchange the public keys with each other. The public key of each group is used for secure intergroup commu- nications.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

For secure communications among group members, they use the symmetric keys created by the Diffie-Hellman key exchange [21].

B. Equipment

The examinees' computers should be equipped with We- bcams and microphones. High-quality Webcams are readily available now and are constantly improving [22], [23]. There- fore, the use of Webcams in online exams is not considered unreasonable.

C. The SeCOnE System Software

The SeCOnE system software is divided into two parts de- pending on the role, that is, whether it is on the client side C_A, or server side C_E. The operating system of the examinees' computers and the proctor's computer is assumed to be Windows XP or Windows 2000. However, the program semantics are not confined to Win- dows because the APIs to control the examinee's computer and to handle the multimedia data are also available in Linux and Unix environments.

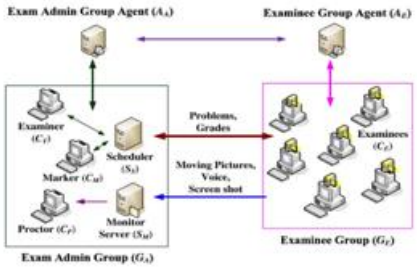

Fig. . The system architecture of SeCOnE.

1) Server Side:

•Scheduler S_S

As shown in Figs. through the Examiner/Ex- aminee management module, S_S obtains the temporary identity of the examiner $T(i)$ from A_A directly when an online exam is set up. The identity is encrypted with the symmetric key $KS[S_S A_A]$ shared by S_S and A_A. To input the problems, the right answers, the exam duration, and the time assigned for each problem, the examiner is verified through C_T with $T(i)$ by the Exam Setup Man- agement module in S_S.

Through the Problem/Answer Management module, the problems, the right answers, and the time allocated to the problems are saved in the database (DB), which is accessed only by S_S. When $C_E[S(i)]$ connects to S_S with its identity, $S(i)$ and its IP, $IP[S(i)]$, the Examiner/Examinee management module.

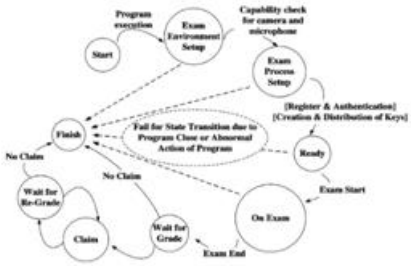

Fig. . Online exam client state transition diagram.

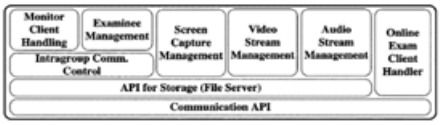

Fig. . Monitor server architecture.

Sends them to A_A and requests the verification of the ex- aminee. As $S(i)$ is encrypted with $KPR[A_A]$, $C_E[S(i)]$ cannot know its identity nor can S_S verify the examinee. After the verification, S_S saves $S(i)$ and $IP[S(i)]$ in the DB and sends $IP[S(i)]$ to S_M. Then, it sends the prob- lems and the time assigned for the exam to $C_E[S(i)]$ through the Exam Process Management module. According to the exam management policy of the SeCOnE system, at the end of the exam or earlier, the answer sheets submitted by the examinees are delivered to the Exam Process Management module, which saves the answers in the DB, then the Grade Management module marks them with the correct answers provided by C_T. The grades are also kept in the DB. The an- swer sheets marked by S_S can be referenced by C_M through the Grade Management module when subjec- tive questions are included in the problems. The grades are distributed to the C_Es after all the examinees have submitted their answer sheets. If an examinee, whose identity is $S(i)$, is not satisfied with his or her grade $G[S(i)]$, he or she sets up an appeal $C[S(i)]$ to S_S through the Exam

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Process Management module. The claim is delivered to C_M through the Claim Manage- ment module, and a regrading is initiated. The Time Control module manages the exam time, and the Exam State Management module checks the states of all C_Es according to Fig. 4. The Authentication Management module is responsible for the integrity checking of the communication messages and the examinee authentication. The inquiries from the examinees during the exam are managed by Question management. Inquiries are saved in the DB first so that C_Q can provide the replies for them one by one. When the replies are checked by the Question Management module, they are immediately transmitted to the C_E, which sent out the questions. Secure intragroup communication goes through the Intragroup Communication Control module in S_S. This module manages the symmetric keys shared between S_S and the other members in G_A.

•Monitor Server S_MAs shown in Fig. , when the Examinee Management module in S_M receives the examinee's IP from S_S, it prepares a directory to save the monitor data of the examinee in a file server. The module also verifies the examinee by comparing the IP with that from A_A as shown in Fig. 2. The monitor data are saved with the reference photos for the examinees from A_A; the photos were taken when A_E authenticated the exam- inees. During or after the exam, a proctor connecting S_M through C_P can verify an examinee by comparing the stored reference photo and the monitor data. TheOnline Exam Client Handler module notifies the ports to which video, audio, and screen captures of C_E are sent. Then, the three types of the monitor data are managed through the Video Stream Management, Audio Stream Management, and Screen Capture Management modules, respectively. Before the exam starts, a proctor should connect to S_M through C_P and test.

CONCLUSION:

This paper describes how the SeCOnE system provides both a secure online exam management and a scheme for the preven- tion and detection of cheating using e-monitoring. The measures for preventing and detecting cheating proposed in this paper cover cheating methods identified for the online exam process via computer or Internet, although it may not address all possible cheating methods. This paper is targeted towards exams admin- istered through the Internet at a fixed time with one problem set, but without any restriction on the exam location. A powerful feature is that SeCOnE can be applied to an exam administered at different times. In this case, the examiner should prepare as many problem sets as there are exam times, in order to prevent cheating during the exam. One overhead cost for this system is in the preparation of the equipment, such as Webcams and microphones, to monitor and to authenticate the entities. A net- work load due to monitor data transfer and the storage is another overhead to be considered, but this is not a major obstacle when data compression is used and more monitor servers are prepared.

REFERENCES:

1. Golden Gate University [Online]. Available: http://www.ggu.edu/cy- bercampus/DegreesCourses/ClassSchedule
2. Univ. Phoenix Online [Online]. Available: http://online.phoenix.edu/ Degree_Programs.asp
3. New York University [Online]. Available: http://www.scps.nyu.edu/ areas-of-study/online/
4. C.-R. Jordi, H.-J. Jordi, and D.-J. Aleix, "A secure E-exam manage- ment system," in Proc. 1st Int. Conf. Avilabil., Reliab. Security, 2006.
5. TOEFL [Online]. Available: http://www.ets.org/bin/getprogram.cgi?Source=toefl&newRegURL=&test=TOEFL&greClosed=new&greClosedCountry=China&browserType=Other&toeflType=&redirect=&t_country1=group_Korea%28Rok%29
6. C. C. Ko and C. D. Cheng, "Secure Internet examination system based on video

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

monitoring," Internet Res.: Electron. Netw. Appl. Policy, vol. 14, no. 1, pp. 48–61, 2004

7. The Blackboard Northern Illinois Univ. [Online]. Available: http://www.blackboard.niu.edu/blackboard/
8. C. Rogers, "Faculty perceptions about e-cheating during online testing," J. Comput. Sci. Colleges, vol. 22, no. 2, pp. 206–212, 2006.
9. D. L. McCabe, L. K. Trevino, and K. D. Butterfield, "Cheating in aca- demic institutions: A decade of research," Ethics Behav., vol. 11, no. 3, pp. 219–232, 2001.
10. W. L. Goffe and K. Sosin, "Teaching with technology: May you live in interesting times," J. Econom. Educ., vol. 36, no. 3, pp. 278–291, 2005.
11. J. C. Adams and A. A. Armstrong, "A Web-based testing: A study in insecurity," World Wide Web, vol. 1, no. 4, pp. 193–208, 1998.
12. D. Agarwal, O. Chevassut, M. R. Thompson, and G. Tsudik, "An in- tegrated solution for secure group communication in wide-area net- works," in Proc. IEEE Symp. Comput. Commun., 2001, pp. 22–28.