Secure E-Exam Scheme

Sattar J. Aboud

University of Bedfordshire, Department of Computer Science and Technology, University Sequare Luton, Bedfordshire LU1 3JU, UK

Abstract: ***Secure e-exam is one of the considerable difficult problems in e-learning environment. The exam process for any educational university should involve different security techniques that should be used to protect the exam characteristics in diverse phases. In this paper, we propose a secure e-exam scheme with all of its information is in digital form. We present a system that has to be implemented to get a high standard security.***

Keywords: e-learning, e-exam, encryption scheme**.**

1. Introduction

In e-learning institutions, students and lecturers use Internet on the regular basis to pursue lectures; inquire and answer questions; and post and receive assessments. The e-learning institutions base on exam process by which students maintain the face to face exam in the classroom fixed via the institution under supervised requirements. Such restrictions guarantee the correctness of the exam. Personal exams allow to verifies student identity and ensure exam authorization using conventional method. It means verifying the student *Id* card and checking no person assists him in exam. Check entity *Id* card in the e-exam is a hard problem [1] requires hard solution. But, e-learning universities still require such exam since the personal exam denotes the possible attempt for e-learning universities [2]. In general, distance institutions have not sufficient class facilities for the entire students. Thus, they should rent centers outside the university to let students to take the exam. But, such exam becomes more complicated because it needs to supply with all equipments to ensure that the students are able to complete the exam. Then all exam solutions shall be gathered and passed to the lecturers in order to correct by them. However, enhancing exam scheme has obvious benefits for e-learning universities [3]. To simplify the exam scheme it is needed that all exam steps can be done by computer, thus are turned into e-exams. Observe that we use the word e-exam to denote exam that can be done by the computer. It means that a student uses the computer to hold the exam but in the supervised conditions.

Basically, exam scheme needs to get the high security level, because a correctness of the process guarantees the quality of the institution. Thus, the design of the e-exam scheme must take a security attention. Security in virtual learning was discussed in many studies. The best study of this subject was proposed by [4]. The public key infrastructure is identified as a sufficient tool to give privacy, validity, integrity and undeniable. Consistent with these thoughts, the public key infrastructures is the solutions for the e-learning system [5] notice that the public key infrastructure brings flexibility and scalability to the e-learning system. Concentrating on e-exam scheme, the only published work on this subject is represented by Chadwick [6]. But, the work not included all steps of the exam; it just treats a certain phase with the exam questions are passed between lecturers using secure e-mail relied on the public key infrastructure. Conversely, two proposals for online exams are existed [7]. But, these solutions do not consider the security size, thus it is hard to rate the correctness and security level.

The remainder of this paper is organized as follows. Section 2 clarifies the security properties for e-exam scheme. Section 3 describes the proposed secure e-exam scheme. Section 4 analyzes the security of a proposed scheme. Finally, the conclusions are considered in Section 5.

2. Security Properties

In this section, we describe the security properties for e-exam scheme. These properties are as follows:

Authenticity

1. The student should be certain that the questions and the results are presented by the lecturer.
2. The lecturer should be certain that the exam solution belongs to the authenticate student.

Correction

1. The exam questions must not be changed once it launched.
2. Once an exam time has ended, no answers can be accepted.
3. Once the solution has sent it should not be possible to change it.
4. It must not be able to send more than one exam for each student.
5. The removal of exam must be prevented.

Privacy

1. The exam correction must be blind to get the utmost fairness.
2. The lecturer must not know the student *Id* of the exam solution.
3. The lecturer should be satisfied that the answers belongs to the authenticate student.

Secrecy

1. Exam questions should be reserved private until an exam questions are declared
2. Just authenticate students can be take exam during an exam time.
3. The exam answer should be reserved private until an exam results are declared.
4. The student solutions should be reserved privately; just the lecturer can have access to them.
5. The exam results must only be passed to a student who did an exam.

Receipt

1. The student should get the acknowledgment as the proof that he has did and passed the exam.
2. The student must do an exam alone, thus cheating should be prevented.

3. The Proposed Scheme

In this scheme, we face interactions between three types of participants these are students, lecturer and trusted authority (manager) is an authority who organizes the exam. It runs exam questions, solutions, and results.

3.1 Notations Used

In this paper, we used the following notations:

1. e : public key
2. d : private key
3. m : message
4. s : digital signature
5. h : secure one way hash function
6. Id : exam identifier
7. i : Sub-index identifies the signature value
8. c : encrypted message m
9. j : Sub-index identifies the encrypted value
10. (e_L, d_L) : lecturer's key pair
11. (e_S, d_S) : student's key pair
12. (e_A, d_A) : trusted authority's key pair

3.2 Exam Initialization

The lecturer and the trusted authority should do the following to setup the exam.

Protocol 1

The lecturer should do the following:

1. Find the unique exam Id produced by the following information:
   - x : subject name
   - y : subject code
   - z : semester
   - a : exam date
   - b : fixed time to answer the exam
   - u : exam serial number
2. Suggest the exam questions, q
3. Find the signature of (Id, q, d_L)
4. Find $s_{L,1} = d_L(Id, q)$
5. Encrypt $(Id, q, s_{L,1})$ with trusted authority public key e_A
6. Compute $c_{A,1} = e_A(Id, q, s_{L,1})$
7. Verify $c_{A,1}$ by the key pair (e_L, d_L)
8. Post $c_{A,1}$ to the trusted authority

The trusted authority does the following:

1. Decrypt $c_{A,1}$ by d_A to get $(Id, q, s_{L,1})$
2. Check the signature $s_{L,1}$ with the lecturer's public key e_L
3. Keep $c_{A,1}$ in a secure manner

3.3 Exam Description

The student, lecturer and trusted authority use the protocol 2 to do the following:

Protocol 2

1. The lecturer issues an exam identifier, Id
2. The student confirms himself by the key pair (e_S, d_S)
3. The student requests for an exam Id from the trusted authority
4. The trusted authority does the following steps:
   1) Check if a student is enrolled in the subject, x
   2) Every subject in each semester z has n students enrolled.
   3) This data is kept by the trusted authority
   4) Verify if the present date $a^{'}$ and time $b^{'}$ are in a determined period to answer an exam (a and b are in the Id)
   5) If the checking succeed Then
      1. Decrypt $c_{A,1}$ by d_A to get $(Id, q, s_{L,1})$
      2. Encrypt $(Id, q, s_{L,1})$ with e_S
      3. Compute $c_{S,2} = e_S(Id, q, s_{L,1})$
      4. Post $c_{S,2}$ to the student.
   6) Else, return an error signal to the student
5. The student gets and checks the questions, solves it and posts the answers as follows:
   1) Decrypt $c_{S,2}$ by d_S to get $(Id, q, s_{L,1})$
   2) Check the signature $s_{L,1}$ with e_A
   3) Write down an exam solution, w
   4) Get randomly an answer identifier, g
   5) Find the signature of $(s_{L,1}, g, w)$ with d_S
   6) Find $s_{S,2} = d_S(s_{L,1}, g, w)$
   7) Encrypt $(Id, q, s_{L,1}, g, w, s_{S,2})$ with e_A
   8) Compute $c_{A,3} = e_A(q, Id, s_{L,1}, g, w, s_{S,2})$
   9) Pass $c_{A,3}$ to the trusted authority
6. The trusted authority does the following steps:
   1) Decrypt $c_{A,3}$ by d_A to get $(Id, q, s_{L,1}, g, w, s_{S,2})$
   2) Verify if a present date $a^{''}$ and time $b^{''}$ are in a determined period to answer an exam
   3) Check if a student has sent an exam answer
   4) If the checking succeed Then
      a) Check the signatures $s_{L,1}$ and $s_{S,2}$ by e_L and e_S
      b) Get a present time t
      c) Find the signature of (Id, g, t) with d_A
      d) Compute $s_{A,3} = d_A(Id, g, t)$
      e) The $s_{A,3}$ exam answer receipt, the proof that student has sent the answer
      f) Post $(Id, g, t, s_{A,3})$ to the student
      g) Get randomly the covered answer identifier, $g^{'}$
      h) Find a signature of $(s_{L,1}, g^{'}, w)$ with d_A
      i) Compute $s_{A,4} = d_A(s_{L,1}, g^{'}, w)$
      j) Encrypt $(q, Id, s_{L,1}, w, g^{'}, s_{A,4})$ with e_L

k) Compute $c_{L,4} = e_L(q, Id, s_{L,1}, w, g^{'}, s_{A,4})$

l) Keep securely $(c_{A,3}, s_{A,3}, g, g^{'}, t, c_{L,4})$ as one answer of the exam *Id*

m) Every exam solution is connected to the student who has passed it.

n) Else, return an error signal to the student

7. The student performs the following steps:
   1) Check the signature $s_{A,3}$ using e_A
   2) Keep $(Id, g, t, s_{A,3})$ as the exam receipt

3.4 Exam Grades

The lecturer and the trusted authority use protocol 3 to grade one exam solution.

Protocol 3

1. The lecturer does the following steps:
   1. Confirm himself to the trusted authority by the key pair (e_L, d_L)
   2. Ask for one answer of the distributed exam Id
2. The trusted authority performs the following steps:
   1. Get one exam answer that has not been graded before, $c_{L,4}$
   2. Post $c_{L,4}$ to the lecturer
3. The lecturer performs the following steps:
   1. Decrypt $c_{L,4}$ with d_L to get $(q, Id, s_{L,1}, w, g^{'}, s_{A,4})$
   2. Check the signature $s_{A,4}$ using e_A
   3. Score the answer w by the value v
   4. Find a signature of $(q, Id, s_{L,1}, w, g^{'}, v)$ with d_L
   5. Compute $s_{L,5} = (q, Id, s_{L,1}, w, g^{'}, v)$
   6. Encrypt $(q, Id, s_{L,1}, w, g^{'}, s_{A,4}, v, s_{L,5})$ with e_A
   7. Compute $c_{A,5} = e_A(q, Id, s_{L,1}, w, g^{'}, s_{A,4}, v, s_{L,5})$
   8. Pass $c_{A,5}$ to the trusted authority
4. The trusted authority performs the following steps:
   1) Decrypt $c_{A,5}$ with d_A to get $(q, Id, s_{L,1}, w, g^{'}, s_{A,4}, v, s_{L,5})$
   2) Check the signatures $(s_{L,1}, s_{A,4}, s_{L,5})$ using (e_L, e_A, e_L)
   3) Get $c_{A,3}$ corresponds to $c_{L,4}$
   4) Keep $(c_{A,3}, g^{'})$ and by $g^{'}$ get $c_{A,3}$ connected to $c_{L,4}$ it means the student's solution.
   5) Decrypt $c_{M,3}$ with d_A to get $(q, Id, s_{L,1}, g, w, s_{S,2})$
   6) Encrypt $(q, Id, s_{L,1}, g, w, v, s_{S,2}, s_{L,5})$ with e_S
   7) Compute $c_{S,6} = e_S\ (q, Id, s_{L,1}, g, w, v, s_{S,2}, s_{L,5})$
   8) Keep $(c_{S,6}, Id, g)$ in a secure manner

3.5 Exam Scores

The student gets exam score by applying the protocol 4. The steps of the protocol 4 are as follows:

Protocol 4

1. The student confirms himself to the trusted authority using the key pair (e_S, d_S)
2. The student requests from the trusted authority the score of the answer g
3. The trusted authority does the following steps:
   1. Check if g belongs to the student that has been confirmed
   2. Get $c_{S,6}$ that had been kept
   3. Pass $c_{S,6}$ to the student
4. The student gets the grade v as follows:
   1. Decrypt $c_{S,6}$ with d_S to get $(q, Id, s_{L,1}, g, w, v, s_{S,2}, s_{L,2}, s_{L,5})$
   2. Check the signatures $(s_{L,1}, s_{S,2}, s_{L,5})$ with (e_L, e_S, e_L)

3.6 Exam Revision

The student can request for exam grade revision using protocol 5 as follows:

Protocol 5

1. The student performs the following steps:
   1. Confirm himself to the trusted authority by the key pair (e_S, d_S)
   2. Get randomly one value that is the revision identifier, r
   3. Find the signature of (Id, g, r) with d_S
   4. Compute $s_{S,6} = d_S(Id, g, r)$
   5. Request to review the score of the answer, g
   6. Pass $(Id, g, r, s_{S,6})$ to the trusted authority
2. The trusted authority performs the following steps:
   1. Check the signature $s_{S,6}$ with e_S
   2. Keep $(Id, g, r, s_{S,6})$

4. Security Analysis

Suppose that the trusted authority is uncorrupt, thus the proposed scheme is based on the trusted authority. The trusted authority is protected with standard security tools such as firewalls, IDS, etc...

Authenticity

1. In step 1, 3 of protocol 1 the lecturer signs the exam. The student checks this signature in step 5, 2 of protocol 2, and then makes sure that the exam questions are suggested by a lecturer.
2. In step 3, 4 of protocol 3 the lecturer signs the grade. The student checks the signature in step 4, 2 of protocol 4. Thus, satisfied that grade is suggested by the lecturer.
3. In step 5, 5 of protocol 2 the student signs the exam solution. The trusted authority checks the student's signature in step 6, 4, 1 of protocol 2 and finds the signature of solution in step 6, 4, 6. The lecturer checks the trusted authority signature in step 3, 2 of protocol 3. Suppose that trusted authority uncorrupt, the lecturer has no suspect that the solution has been written by the authenticate student.

Correction

1. In step 1, 3 of protocol 1 the lecturer signs the exam to get $s_{L,1}$. The student finds a signature of $(s_{L,1}, g, w)$ in step 5, 5 of protocol 2 to get $s_{S,2}$. The signatures $s_{L,1}$ and $s_{L,2}$ adopt that the exam questions cannot adjusted once the exam has launched.
2. In step 6, 2 of protocol 2 the trusted authority checks if the exam time has completed, decline any exam solution submission once the time has terminated.
3. The student signs an exam solution in step 5, 5 of protocol 2. Thus, if the solution is amended the signature verification will not pass.
4. In step 6, 3 of protocol 2 the trusted authority checks if the student has sent an exam solution, before and in this situation, an exam solution is rejected.
5. If one exam is removed there is one student that will not get his grade, thus the deletion is detected. Also, a student can prove that he has send an exam, since he can show an exam receipt got in step 7 of protocol 2.

Privacy

1. In step 2, 1 of protocol 3 the lecturer receives exam solution $c_{L,4}$ and then decrypts it in step 3, 1 of the protocol 3 to get $(q, Id, s_{L,1}, w, g^{'}, s_{A,4})$
2. This information does not disclose the student *Id*
3. The signature $s_{A,4}$ satisfies the lecturer that w belongs to the authenticate student.

Secrecy

1. The lecturer encrypts an exam questions in step 4, 5, 2 in protocol 2 using a trusted authority public key. The trusted authority private key is required to get back the exam questions, and this key is limited for the trusted authority. The trusted authority passes an exam questions to the student in step 4, 3, 3 of protocol 2, when a student is enrolled in an exam subject and when the present time and date are in a determined time to solution an exam, steps 4, 1 and 4, 2 of the protocol 2.
2. The lecturer can send the exam answer to the trusted authority using an alteration of protocol 1, thus the answer is encrypted and only can be got by the trusted authority.
3. In step 5, 6 of protocol 2 the student encrypts his solution using the trusted authority public key. However, the exam solution can be got by the trusted authority only. Afterward, the trusted authority encrypts an exam solution by the lecturer's public key in step 6, 4, 7. The lecturer gets the encrypted exam solution in step 3. We conclude that the students' solutions are kept secret, thus only the lecturer and the trusted authority have access to them.
4. The trusted authority validates the student in step 1 of protocol 4 and checks that he is the owner of a solution g in step 3, 1 of protocol 4. When the verification succeeds the trusted authority sends $c_{S,6}$ to the student. The $c_{S,6}$ exam grade encrypted by the student's public key, thus that only the student can get his grade.

Receipt

1. The student gets the receipt in step 7 of protocol 2 as a proof of exam send.

Copy detection is prevented

1. The exam occurs in the supervised condition, thus the copy detection is prevented using traditional means.

5. Conclusions

In this paper, we have proposed a secure e-exam scheme. We have looked at all exam phases and we have recognized different security characteristics that each exam phase should convince. Such information has allowed the scheme to rely on several encryption protocols that provide the high security level for all exam phases. But, the proposed scheme in an initialization phase, students take an exam in the supervised condition. Further study must be aimed to let students to take exams in minimum limited condition.

References

[1] Sattar J. Aboud, "Secure E-Test Scheme", International Journal of Emerging Technologies in Learning (iJET), volume 2, Number 4, 2007.

[2] George Meletiou, Ioannis Voyiatzis, Vera Stavroulaki, C. Sgouropoulou, "Design and Implementation of an E-exam System Based on the Android Platform," pci, pp.375-380, 16th Panhellenic Conference on Informatics, 2012

[3] Mohammad A Sarrayrih, Mohammed Ilyas, Challenges of Online Exam, Performances and problems for Online University Exam , IJCSI International Journal of Computer Science Issues, Volume 10, Issue 1, pp. 439-443, 2013

[4] K. El-Khatib, L. Korba, Y. Xu, and G. Yee, "Privacy and security in e-learning", International Journal of Distance Education, 1(4), 2003

[5] G. Kambourakis, K. D-P.N., A. Rouskas, and S. Gritzalis, "A pki approach for deploying modern secure distributed e-learning and m-learning environments", Computers & Education, Volume 48, Issue 1, pp. 1–16, January 2007.

[6] British Colombia, Electronic Provincial Examinations System User Manual, Grade 10, 11 and 12 e-Administration and Grade 10 and 11 e-Marking, Technical Support – A. Willock Information Systems: 1-866-558-5339 (toll free), Last update: March, 21, 2014.

[7] Naresh.Chiranji, CH.Deepthi, T.P.Shekhar, A Novel Approach to Enhance Security for Online Exams, International Journal of Computer Science and technology, IJCST Volume 2, Issue 3, pp. 85-89, 2011

Author Profile

Sattar J. Aboud, received his Master degree in 1982 and a PhD in 1988 in the area of computing system. The two degrees were awarded from U.K. In 1990, he joined the Institute of Technical Foundation in Iraq as an assistant professor. In 1995 he joined the Philadelphia University in Jordan as a chairman of computer science department. Then, he moved as a professor at the Middle East University for Graduate Studies, Amman-Jordan. Currently, he is a visiting professor at university of Bedfordshire in UK. His research interests include areas like public key cryptography, digital signatures, identification and authentication, and networks security. He has supervised numerous PhDs and Masters Degrees thesis. He has published more than 60 research papers in a multitude of international journals and conferences.