A Study on the Secure Online Examination System

DISSERTATION ABSTRACT

A Study on the Secure Online Examination System

Graduate School of

Natural Science & Technology

Kanazawa University

Division of Electrical Engineering and Computer Science

Student Number: 1323112010

Name : **Abdul Wahid**

Chief advisor : **Prof. Masahiro MAMBO**

July 1, 2016

Abstract

Implementation of secure online examination system has been a hot topic in the educational world in the last decade. Issues that should be addressed in the secure online examination system are computer and network security issues of the systems and prevention of cheating by participants. In our research, we provide a website application and a secure network design which prevents cheating by any participant among examinee, administrator, and examiner. Different security features of the online examination system are discussed both from the website application aspect and network design aspect.

Unfortunately, website application and network design cannot meet some security requirements because of several inside and outside attacks and malicious behaviors of bribed, corrupted or unfair examiners and untrusted exam authority, and we construct a particular online examination protocol to prevent them.

We design an online examination protocol based on certificateless signcryption and prove their security properties under the formal analysis using ProVerif software. The proposed online examination protocol has several advantages over existing protocols such that there is no certificate unlike public key infrastructure, no key escrow and lower computational cost by virtue of the signcryption scheme.

Our results show that some of OES problems both of data security issue such that scanning port attack and cheating problem especially by examinee can be handled over the web application and network design system. While some others will be handled by particular OES protocol. ProVerif shows that our proposed protocol is secure under some privacy and authentication properties.

I. Introduction

The examination is one way to measure the success of learning process or obtaining qualified human resources. In the field of training, the exam is intended to measure the level of achievement by students or learners, so that we can determine the level of understandings of the study being taken. In the context of the recruitment of new employees, the exam is intended to obtain qualified human resources.

All of the examination systems including the national exam system in all levels of education, whether it is an exam for students or exams for teachers, have begun to shift from the manual exam system to digital online systems in order to make it more practical and effective. Online examination systems no longer use paper, pencil and are computerized, in which examinees answer test questions through a computer. Assessment is conducted directly by the system, and examinees will receive their results immediately after the exam.

Although the online examination system has its advantages, computerization incurs security problems. Each exam session needs to deal with cheating that could occur. So far, online examination has mostly focused on system security itself, such as the design of access control, defense against attacks, closing security holes in the application such as PHP, SQL and operating system, or applications of encryption. However, there are a variety of cheating methods more crucial in online examination systems than in conventional exam systems.

Cheating usually exploits weaknesses in the implementation of conventional and online exams. Along with the development of information technology, there is also an increase in more diverse and sophisticated cheating methods. An example is the use of spy cameras or modern tools that are modified to make it undetectable by the exam committee.

Aims and Objectives

This research aims to study the problems in Online Examination System described above, especially those which still has not been considered in the previous research. We intend to achieve those aims through four objectives.

1. To identify problems in Online Examination systems (OES).
2. To develop a basic framework of OES.
3. To design a new fast and secure protocol for this framework of OES.
4. To evaluate security aspects of the designed OES protocol. To this end, we evaluate the designed OES protocol under the computational model and formal model.

Contributions

Our research addresses the four objectives outlined above. The dominant aim of this work is to construct a secure Online Examination System which in secure in term of both network system and cheating prevention. We claim the following issues as the contributions derived from our work:

1. We have constructed a basic framework of secure OES which can prevent some network penetration attacks and common cheating methods.

2. We have designed a secure and efficient communication protocol using certificateless signcryption method.

II. OES Problems

OES does not exists without computer network systems and the main problem here is security. Computers and network security problems occur due to the presence of security holes in the system in both of its network design and web program coding. The existence of security hole allows both of inside and outside attackers to access the system by illegally stealing exam questions and answers, making changes to value, or another type of modifications.

In addition to the security issue of the computer and networking systems, other important issue in OES is cheating prevention. There are many techniques that are often used by the examinee to obtain exam answers illegally.

Besides the cheating by the examinee, there are some threats possibly occurs in online examination system such as bribed, corrupted or unfair examiner and untrusted exam authority. Figure 1 shows the diagram of problems of online examination systems.

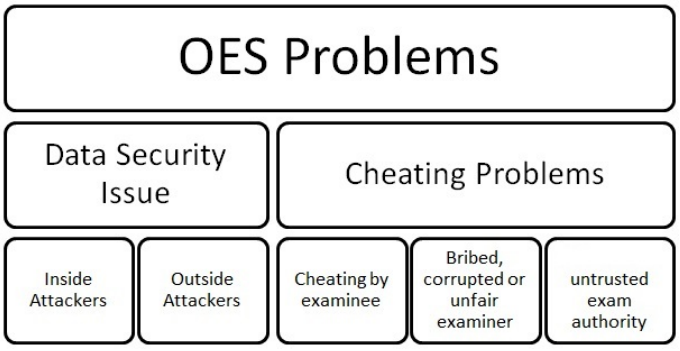

Figure 1: Problems of Online Examination System

III. Proposed Solution

We offer a secure web-based online examination system along with network design so that the system is expected to prevent cheating and network threat, which are either done by the participants taking the exam or by persons inside or outside the system trying to penetrate.

In order to make it easier to design our system, we consider the following situation as a target situation of our OES:

1. In the OES framework, there is a basic computer used by each participant. A large number of participants located in several places take exam at a fixed time and at a fixed axam seat.Limited number of supervisors are in each room during the exams.
2. OES consists of 3 entities which are the examinee, administrator and examiner. Each of this entity has a privileged access to different pages.
3. Examinees take the exam in a secure place or room such as a computer lab or ICT center which has already been set and registered for OES.
4. The examiner executes set-up exam questions from registered place or computer.
5. Whether grading process can be done automatically by the system or manually by the examiner depends on their type of questions.
6. Manual grading will be performed by examiner in a registered place.

Web Security Design

We try to utilize a secure website, which follows the recommendation by [2] about online exam control procedure. This web design consists of three main pages such as Examinee, Administrator and Examiner Board page.

The examinee page consists of 3 sub pages which are Home, Take a Test and View Result. The second page is the administrator page. This page is the most important element of the online test system. In this page, all of the test terms are organized. The third page is examiner board page. It requires user name and password authentication to access it, even though this page is only a viewing mode page. For those who can access this page, they can only view the test results and question analysis with several options.

General Network Security Design

Network design is also one of the main elements of the online examination system. We consider a easier and cheaper way to achieve the goals. We have several points of interest in designing a network for security, which are:

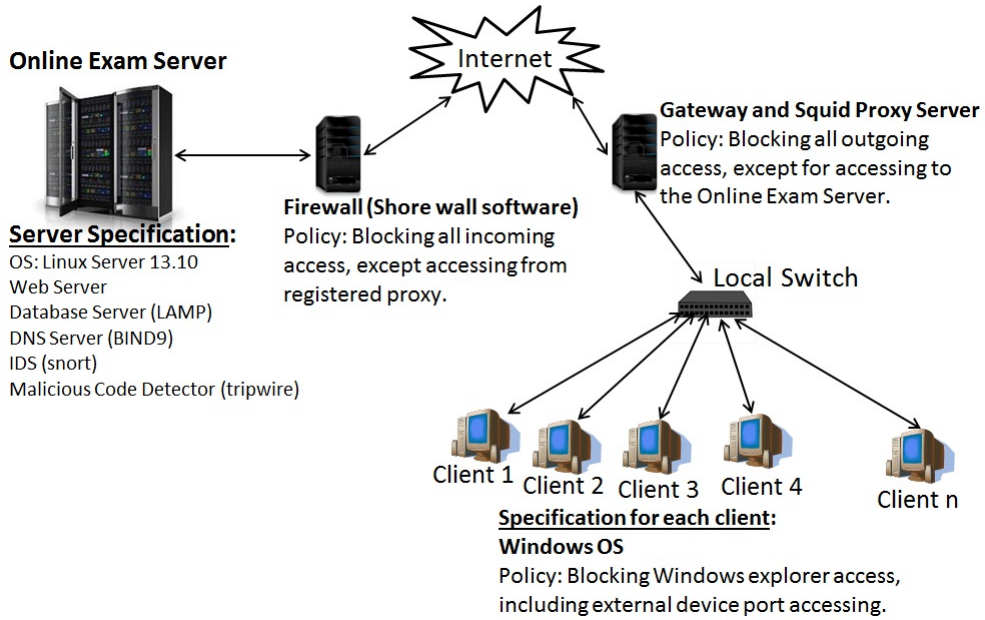

Figure 2: Network design of Online Examination Systems

1. All accesses to the web and OES server database is blocked, except for access from registered proxy.

2. All outgoing accesses of the client, by which the examinee is taking the exam, will be blocked except access to the OES server.

3. The operating system of the client uses Windows OS which will restrict some actions during the examination.

Figure 2 is a block diagram of the online examination system network that our proposed system is based on.

Online Examination System Protocol

Unfortunately, Website application and network design cannot meet some security requirements because of malicious behaviors of bribed, corrupted or unfair examiners, untrusted exam authority and several inside or outside attacks, and we construct a particular online examination protocol to prevent them.

To the best of our knowledge, there are at least three papers that have specifically discussed security protocols of OES. The first paper is from Castella et.,al.[3], the second paper is from Huszty and Petho [4]. And then, Rosario et.,al.[5] tried to construct Remark! in the third paper. They

achieve authentication, verifiability, and conditional anonymity with minimal reliance on trusted parties. This protocol uses multiple servers so that they have a problem of computational cost and time overhead. In addition, there are some problems in the certificate management such as how to design certificate authority, how to handle revocation user and how to manage a key.

In our scheme, we try to address the certificate problems by adopting certificateless cryptography and, in order to increase the efficiency, we adopt signcryption as an alternative solution to the classical signature-then-encryption method. Certificateless signcryption can be a solution for several problems described above.

Our scheme modifies the Elliptic Curve Cryptography based Certificaless Hybrid Encapsulation Key scheme without Pairing and the eCLSC-TKEM to obtain all the advantages of both techniques. The scheme consists of three parts, namely Key Generator Center (KGC), Sender and Receiver.

1. Set-Up Parameter: It is run by the KGC. KGC selects and publishes system security parameters as follows:
   - F_q = Finite field of large prime number q
   - (a, b) = EC value $< q$, satisfy to $4a^3 + 27b^2 \neq 0$ and $q \neq 0$
   - E/F_q = EC over finite field,satisfy to $q : y^2 = x^3 + ax + b \bmod q$
   - G_q = a generator of EC
   - O = infinity point of EC, n is the order of F satisfy to $n.G = O$
   - Hash function $h0 = \{0, 1\}^* \times G_q^2 \rightarrow Z_q^*$, $h1 = \{0, 1\}^{*2} \times G_q^2 \rightarrow Z_q^*$, $h2 = G_q^2 \times \{0, 1\}^* \times G_q^2 \rightarrow Z_q^*$
   - PKG chooses integer $msk \in Z_q^*$ as the master secret key
   - PKG calculate $P_{pub} = msk.G_q$ as master public key.
   - PKG publishes parameters $(F_q, E/F_q, G_q, h0, h1, h2, P_{pub})$ but keeps secret the msk.

2. Set secret value: It is run by each user. User i with ID_i chooses randomly $x_i \in Z_q^*$ and computes public key $P_i = x_i.G_q$

3. Partial private key extract: It is run by KGC. Here, KGC produce the partial private key of every user based on their identity. The KGC processes the user i with ID_i in the following step:
   - Chooses randomly $r_i \in Z_q^*$ and computes $R_i = r_i.G_q$
   - Computes public key $d_i = r_i + msk.h0(ID_i, R_i, P_i) mod q$
   - Sends to user $\langle R_i, d_i \rangle$ in a secure channel
   - User Validate $d_i.G_q = R_i + h0(ID_i, R_i, P_i).P_{pub}$

4. Set Private Key: It is run by each user. User i with identity ID_i performs to set a private key pair $Sk_i = \langle d_i, x_i \rangle$

5. Set Public Key: It is run by each user. User i with identity ID_i performs to set a public key pair $Pk_i = \langle R_i, P_i \rangle$

6. Signcryption Alice is the sender. She wants to send message m to Bob as the receiver with identity ID_B, and a pair public key (R_B, P_B). Alice chooses $l_A \in Z_q^*$ and computes $U = l_A.G_q$, then Alice computes :
   - $Y_B = R_B + h0(ID_B, R_B, P_B).P_{pub}$
   - $SK = h2(l_A.(Y_B + P_B), U, ID_B, R_B, P_B)$
   - $C = E_{SK}(m, ID_A)$
   - $s = (d_A + l_A.h1(m, ID_A) + x_A.h1(m, ID_A)).modq$
   - Alice sends to Bob chipertext $= (C, U, s)$

7. Unsigncryption Bob is the receiver. He receives $= (C', U', s')$ from Alice. Bob computes:
   - $SK = h2((d_B + x_B).U, U, ID_B, R_B, P_B)$
   - $(m, ID_A) = D_{SK}(C')$
   - $Y_A = R_A + h0(ID_A, R_A, P_A).P_{pub}$
   - Verify: Accept if $s.P = Y_A + U.h1(m, ID_A) + P_A.h1(m, ID_A)$ is hold

IV. Evaluation of the Proposed Solution

Web application and General Network Design

We construct a web application and general network in order to prevent some security and cheating during an exam. Table 1 shows a comparison of several online examination systems with our scheme.

Table 1: Features comparison of Online Examination Systems

Features	**Ours**	**SI[1]**	**LG[6]**	**CDS[7]**	**HB[8]**	**IRI[9]**
Browsing Guard	Yes	No	Yes	No	No	No
The Internet Messenger Guard	Yes	No	Yes	No	No	No
Time Limit	Yes	Yes	Yes	Yes	Yes	Yes
Local Data Accessing Prevention	Yes	No	Yes	No	No	No
Ext. Storage Accessing Prevention	Yes	No	Yes	No	No	No
Random Question	Yes	Yes	Yes	Yes	Yes	Yes
Random Scheduling	Yes	No	No	No	No	No
Random Seating	Yes	No	No	No	No	No
Bank Question	Yes	No	No	No	Yes	Yes
Question Analyzing	Yes	No	No	No	No	No
Collusion Prevention	Yes	No	No	No	No	Yes
E-Monitoring	No	Yes	No	Yes	No	No

Yes/No: Feature shown in the left column is/is not held.

Online Examination System Protocol

The time complexity of the proposed scheme is evaluated. Table 2 gives a comparison between the computational costs of our proposed scheme and those of the others schemes, in which the computational costs of verification and symmetric encryption are neglected. Table 3 shows the comparison of cipher text size which will be transmitted from sender to receiver.

Table 2: Computational costs of different schemes

Schemes	Type	Participant	Exp	Div	Mul	Add	ECMult	ECAdd	Hash
Zheng[10]	SC	Sender	1	1	-	1	-	-	2
		Receiver	2	-	2	-	-	-	2
ZI[11]	SC	Sender	-	1	1	1	1	-	2
		Receiver	-	-	2	-	2	1	2
		Receiver	-	-	-	-	4	2	2
WNPZ[12]	CLSC	Sender	4	1	3	2	-	-	4
		Receiver	5	-	3	2	-	-	4
XX[13]	CLSC	Sender	5	-	4	2	-	-	3
		Receiver	5	-	4	2	-	-	3
SB[14]	CLSC-	Sender	-	-	3	2	4	1	4
	TKEM	Receiver	-	-	-	-	6	3	4
WSB[15]	CLSC-	Sender	-	-	2	2	4	2	4
	TKEM	Receiver	-	-	-	1	6	3	4
Ours	CLSC	Sender	-	-	2	2	3	2	3
		Receiver	-	-	-	1	5	3	3

SC: Signcryption, CLSC: Certificateless Signcryption, CLSC-TKEM: Certificateless Signcryption-Tag Key Encapsulation Mechanism, Exp: modular exponentiation operation, Div: modular division operation, Mul: modular multiplication operation, Add: modular addition operation, Ecmult:Elliptic Curve point multiplication operation, Ecadd: Elliptic Curve point addition operation, Hash: One way hash function.

Table 3: Our Ciphertext size comparison

EC-CLSC Schemes	Ciphertext Size
SB[14]	$n_q + n_G + n_{ID} + m$
WSB[15]	$n_q + 2n_G + n_{ID} + m$
Ours	$n_q + n_G + n_{ID} + m$

n_q: The number of bits required to represent an element of F_q, n_G: The number of bits required to represent an element of point EC, n_{ID}: The number of bits required to represent an identity, m: The number of bits in the message being signcrypted.

We use a formal verification program ProVerif to show the correct execution of the protocol. Assuming an attacker in control of the network and

honest principals, ProVerif successfully proves all privacy and authentication requirements. Table 4 reports the execution of ProVerif. Also assuming corrupted principals, ProVerif proves the OES Protocol ensures all the requirements.

Table 4: Summary of privacy and authentication analysis of OES Protocol

Requirements	**Result**	**Honest Roles**
`Question Confidentiality`	True	Examiner, Manager
`Answer Privacy`	True	Examiner, Examinee
`Mark Privacy`	True	Examiner, Manager
`Examiner authorization`	True	Examiner, Manager, KGC
`Examinee authorization`	True	Examinee, Manager, KGC
`Answer authenticity`	True	Examinee, Manager
`Test Origin authentication`	True	Manager
`Test authenticity`	True	Examiner, Manager
`Mark authenticity`	True	Examiner, Examinee, Manager
`Anonymous Marking`	True	Examinee, Manager

V. Conclusion and Future Work

Conclusion

In this study of online examination system, we overcome some security issues of the system and the issue of cheating by all parties by establishing a basic framework. This framework combines the online examination web application, network system configuration, and communication protocol as an integrated system.

In the context of web page application, we combine several techniques for cheating prevention like Fisher-Yates random question, automatic scheduling, and seating arrangement.

In the context of network configuration, the combination of firewall in the server system, proxy and MMC in the client become a security guarantee for the online examination systems, both from attacks by individuals and cheating attempts by examinees.

We implement Certificateless Signcryption based on the elliptic curve which meets all of the basic security needs such as message authentication, integrity, unforgeability, non-repudiation and forward secrecy and solves some another OES problems. Our scheme is more efficient than the previous schemes because our CLSC based on elliptic curve which is more efficient than bilinear pairings and finite field exponentiations used in the previous

CLSC schemes. Besides, our scheme offers shorter ciphertext size than previous CLSC schemes.

At last, we construct an OES protocol scheme based on certificateless signcryption. We show how to model an OES protocol in the applied phi calculus, and define ten relevant security properties, four privacy property and six authentication properties. We analyze the security of our OES protocol scheme under some honest role using ProVerif software. ProVerif shows that our schemes is secure under the formal model analysis.

Future Work

As a future work, we intend to analyze our OES protocol under computational model to ensure our security properties. We can use some software under computational approach such as CyptoVerif.

References

[1] M. Sarrayrih and M. Ilyas, "Challenges of Online Exam , Performances and problems for Online University Exam," Int. J. Comput. Sci., vol. 10, no. 1, pp.439-443, 2013.

[2] G. R. Cluskey, C. R. Ehlen, and M. H. Raiborn, "Thwarting online exam cheating without proctor supervision," J. Acad. Bus. Ethics, vol. 4, pp.1-8, 2011.

[3] J. Castella-Roca, J. Herrera-Joancomarti, and A. Dorca-Josa, "A secure e-exam management system," First Int. Conf. Availability, Reliab. Secur. ARES 2006, pp.864-871, 2006.

[4] A. Huszti and A. Petho, A secure electronic exam system, Publ. Math. Debrecen, vol. 3, no. 4, pp. 209312, 2010.

[5] R. Giustolisi, G. Lenzini, and P. Y. A. Ryan, Remark!: A Secure Protocol for Remote Exams, Secur. Protoc. XXII, LNCS. Springer, pp. 3848, 2014.

[6] S. Liu and Q. Gong, The research on anti-cheating strategy of online examination system, 2011 2nd Int. Conf. Artif. Intell. Manag. Sci. Electron. Commer. AIMSEC 2011 - Proc., pp. 17381741, 2011.

[7] N. Chiranji, C. Depthi, and T. P. Shekhar, A Novel Approach to Enhance Security for Online Exams, Int. J. Comput. Sci. Technol., vol. 2, no. 3, pp. 8489, 2011.

[8] B. Hang, The Design and Implementation of On-Line Examination System, 2011 Int. Symp. Comput. Sci. Soc., no. 1, pp. 227230, 2011.

[9] Z. Islam, M. Rahman, and K. Islam, Online examination system in bangladesh context, Sci. Environ. Technol. , vol. 2, no. 3, pp. 351359, 2013.

[10] Y.Zheng, "Digital signcryption or how to achieve cost (signature and encryption) cost (signature)+cost (encryption)," Adv. Cryptol. Crypto '97,March, pp. 165179, 1997.

[11] Y. Zheng and H. Imai, How to construct efficient signcryption schemes on elliptic curves, Inf. Process. Lett., vol. 68, no. 5, pp. 227233, 1998.

[12] S. Wenbo, K. Neeraj, G. Peng, and Z. Zezhong, Cryptanalysis and improvement of a certificateless signcryption scheme without bilinear pairing, Front. Comput. Sci., vol. 8, no. 4, pp. 656666, 2014.

[13] X. Zheng and X. Yang, Improvement of a Certificate less Signcryption Scheme without pairing, Int. J. Sci., vol. 2, no. 7, pp. 8187, 2015.

[14] S. Seo and E. Bertino, Elliptic Curve Cryptography based Certificateless Hybrid Signcryption Scheme without Pairing, CERIAS Tech Rep. 2013-10, 2013.

[15] J. Won, S.-H. Seo, and E. Bertino, A Secure Communication Protocol for Drones and Smart Objects, in ASIA CCS15, 2015, pp. 249260.

平成２８年８月５日

学位論文審査報告書（甲）

１．学位論文題目（外国語の場合は和訳を付けること。）

A Study on the Secure Online Examination System

（安全なオンライン試験に関する研究）

２．論文提出者　(1) 所　　属　電子情報科学専攻

(2) 氏（ふり）　名（がな）　Abdul Wahid Yunus（アブドゥル ワヒド ユヌス）

３．審査結果の要旨（600～650 字）

平成 28 年 8 月 5 日に第 1 回学位論文審査委員会を開催した。同日に口頭発表を実施し、その後に第 2 回学位論文審査委員会を開催した。慎重審議の結果、以下の通り判定した。なお、口頭発表における質疑を最終試験に代えるものとした。

オンライン試験には、集計処理の負荷の軽減や採点結果の瞬時の提示、更には、紙の取り扱いの負担削減などの利点があり、重要性が高まっているが、オンライン化に伴う安全性の問題など各種の問題が存在するため、安全なシステムの構築が求められている。本論文では、オンライン試験に求められる性質と対策すべき攻撃について整理した後に、ネットワークシステムとその上で動作するプロトコルという 2 つの視点よりオンライン試験のシステムを設計・実装している。前者として、ネットワークセキュリティを考慮したシステム及び受験者への質問の提示方法を、後者として、新しく提案する効率的な証明書不要サインクリプションを用いたオンライン試験プロトコルを構成し、これらの安全性を評価している。特に、後者では、フォーマルメソッドを用いることにより、構成したオンライン試験プロトコルが安全であることを示している。

以上のように、本研究はオンライン試験の構成方法として有益な知見を与えており、当該分野の発展に貢献するものである。よって、博士（工学）に値すると判定した。

４．審査結果　(1) 判　　定（いずれかに○印）　○合　格　・　不合格

(2) 授与学位　博　士（工学）