Applying PKI for Internet Voting System

Jinho Kim, Kwangjo Kim, Byoungcheon Lee

International Research center for Information Security(IRIS)

Information and Communications Univ.(ICU), Korea

{kman,kkj,sultan}@icu.ac.kr

Abstract

We have designed an Internet voting system applicable for worldwide voting which is based on Ohkubo *et al*'s scheme[9] combined with Public Key Infrastructure (PKI). To the best of our knowledge, this is the first trial to serve secure Internet voting system to the world. In our system, voter's privacy is guaranteed by using blind signature and mix-net, and robustness is provided through the threshold encryption scheme. By employing Java technology, we propose a way of typical implementation for internet voting system. Furthermore, PKI permits worldwide key distribution and achieve "one certificate/one vote" policy. Therefore, anyone can participate in the voting if he gets a certificate from Certificate Authority (CA). By the joint work between Korean and Japanese teams, the implementation aims to select MVPs in 2002 FIFA World Cup Korea-Japan™ in easy and friendly manner for any Internet user to participate and enjoy Internet voting.

I. Introduction

Voting is one of efficient methods for decision making in any society. The research on electronic voting through Internet will play a very important role for the progress of democracy. If a secure and convenient electronic voting system is provided, it will be used more frequently to collect the opinion of eligible voters for many political and social decisions through cyberspace.

In this research, we design Internet voting system using public key infrastructure (PKI). Our proposed Internet voting system satisfies most of important security requirements and has efficiency and flexibility. Although this system is not quite the first trial, we believe it is the first user-friendly, secure Internet voting system using PKI which is open to general people over the Internet. In our system, voter's privacy is guaranteed by using blind signature and mix-net, and robustness is provided through the threshold encryption scheme. By employing Java language suitable for the Internet, we can implement a user-friendly web interface for the voting system and a downloadable voting applet. Furthermore, we use PKI for worldwide key distribution and achieve "one certificate/one vote" policy. Therefore, anyone can participate in the voting if he gets a certificate from CA.

The rest of this paper is organized as follows: In Section 2, we will briefly describe related works done till now. In Section 3, we will discuss the general architecture of our voting system. In Section 4, we will introduce an typical implementation to select MVPs of 2002 FIFA World Cup Korea-Japan™. Finally, concluding remarks will follow in Section 5.

II. Previous Works

Numerous researches have been done to construct secure and efficient voting systems: schemes based on homomorphic encryption [2,5,6,12], schemes based on Mix-net[1,10,11], and schemes based on blind signature[3,7,9]. However, there is no perfect solution satisfying every requirements together with high efficiency. The schemes based on homomorphic encryption are applicable only to yes-no voting. The schemes based on Mix-net cost very much to guarantee that every ballot is opened correctly when the number of voters is large. One of the standard schemes using blind signature was proposed by Fujioka *et al.*[7] (FOO92 in short) in 1992. FOO92 use blind signatures to satisfy the privacy and unreusability property, and the bit-commitment scheme to realize the fairness property. It is efficient in computation and is applicable to multiple choices in very flexible way. But a considerable obstacle caused by using bit-commitment scheme in FOO92 is that all voters have to join the ballot counting process. This means that it is not practical to apply FOO92 for the real world, since each voter must stay until all other voters complete the voting stage. An improved scheme was proposed by Ohkubo *et al.*[9] (OMAFO99 in short) in 1999. They proposed a practical blind signature-based voting scheme that allows voters to walk away once they finish casting their votes.

On the other hands, there have been several practical implementations as a trial for replacing ordinary voting by electronic voting. By Cranor and Cytron[4], a practical, secure and private system called Sensus for polling (conducting surveys and elections) over computer network has been designed and implemented by expanding FOO92. A research group at the Laboratory for Computer Science, MIT, had implemented a system called EVOX[8] based on FOO92. These implementations have same drawback, key distribution that is a traditional problem in cryptography. They assume that all necessary public keys and private keys are generated and stored in a secure way. The assumption can be an obstacle to apply these implementations to the real world. We use PKI to solve key distribution problem. This can be a good way to expand the number of voters easily over the Internet.

III. Internet Voting System

1. Voting protocol

We choose OMAFO99 for our Internet voting system since it is efficient in terms of computation and its typical implementation is available for large scale voting. OMAFO99 inherits most of the security properties of FOO92, but the major differences are the number of talliers and the use of threshold encryption scheme instead of using bit-commitment scheme. The relation between the voter's identity and ballot is sealed by the blind signature scheme. Ballot is sent through an anonymous channel, so no one can violate voter privacy. Unreusability and eligibility also hold under the assumption that no voter can break the blind signature scheme and the ordinary digital signature scheme. The most important improvement is the walk-away property which the voters may leave away after casting their votes. They need not send any information to talliers to open their ballots because they encrypt their votes with the tallier's public key. Furthermore, fairness is also assured because malicious talliers that are less than threshold t can not decrypt the ballots in the middle. Robustness is assured under assumption that the number of colluding authorities don't exceed a predetermined threshold.

2. System Architecture

In this Subsection, we describe overall architecture of our voting system. We assume that the voters trust the admin server completely, and anybody can post, but nobody can erase or overwrite the data once written in the bulletin board. We use some cryptographic primitives such as threshold encryption, digital signature, blind signature, and mix-net. As shown in Fig. 1., Internet voting system

architecture consists of six basic entities: voter, admin, bulletin board, mix server, tally server and certification authority. Throughout this paper we use the following notations:

V_i : voter i, C_i : V_i's certificate

AS: Admin server, M: Mix-server

T: Talliers (T_j denotes the tallier j)

BB: Bulletin board and ballot box.

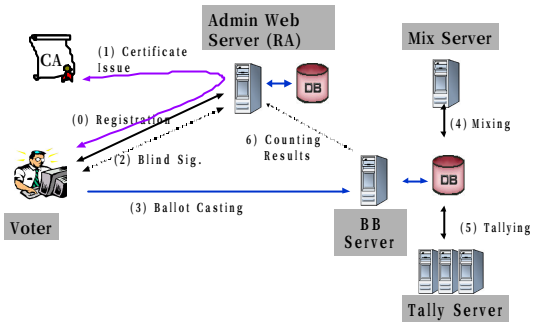

Fig. 1. Internet voting system architecture.

Since, in our system, only a person having certificate can get the right to vote, V_i should register at AS to get C_i before voting. AS is responsible for verifying the voter's right to vote and authenticating the ballot. It must permit only one vote per eligible voter. AS can play the role of a registration authority (RA) when issuing C_i. After successful registration, AS requests CA to issue C_i for each registered person. After receiving C_i from CA and storing it, AS sends C_i to V_i. C_i is issued in simplified form based on X.509v3. After receiving C_i, V_i can vote by using voting applet which is executed in web browser. When the program is downloaded after entering his ID and password, V_i simply needs to click on his choice and click on the "Vote" button. Then, the applet communicate automatically with AS to get AS's blind signature.

Finally, doubly encrypted ballot, V_i's signature, and C_i are posted to BB. BB is used as a public communication channel that can be read by any entity. Each legitimate entity can write message only on its designated section. No entity can erase any information from BB. When receiving encrypted ballot and V_i's signature, BB verifies V_i's signature and store the encrypted ballot to DB.

After the voting time is over, M mixes doubly encrypted ballots by voters and decrypts these mixed ballots. T receives encrypted ballots from M and opens them by using threshold decryption protocol. Finally, T publishes the results by using BB.

IV. Typical Implementation

In order to implement Internet voting system efficiently, we try to use built-in components produced by Korean security industries and extend their functions to meet our objectives. We choose to use the CA server by KSIGN[15], one of CA vendors in Korea, and the Java crypto library J/LOCK by ST[17]. Insol Soft[13] is responsible for web interface for voters and SECUi.COM[16] provides security management of main computer and security measures of network. Imai laboratory at the University of Tokyo is responsible for checking correctness and vulnerability of our system.

1. System Components

AS and BB can be implemented on Unix system using Apache as a web server and Tomcat as a servlet container and JavaServer Pages™ (JSP) implementation. We have developed the main part of AS and BB by using JSP, JDK1.2, and Java crypto library. Oracle DB is used for AS to manage a huge number of information of all voters. BB also use an independent DB to handle ballots. Since JDBC (Java Database Connectivity) and standard SQL queries are used for handling DB, we can use other database systems such as Informix, Oracle, Sybase, Microsoft, and so on. M and T are implemented in C language on a Linux system. We use only one mix server for efficiency.

2. Application

Currently, we are applying our Internet voting system to select MVPs of 2002 FIFA World Cup Korea-Japan™ , which will be held from May 31 to June 30, 2002 at major cities in Korea and Japan. This application aims to demonstrate electronic voting technology to the world in easy and friendly manner with joint work by Korean and Japanese teams. Because this system will be open to general people all over the world via the Internet, a huge amount of data handling are expected. To overcome this bottleneck, KISTI[14] will support computing powers.

V. Concluding Remarks

We have designed the Internet voting system using PKI. To the best of our knowledge, this is the first user-friendly, secure Internet voting system using PKI. Now we have finished to implement our voting system inside LAN. Further works like porting job to supercomputer, system security measures, network security measures, and performance test need to be done. If we succeed in serving the Internet voting system to the world, we can yield very important experiences such as:

- Worldwide level application of cryptographic technology.
- Contribution to the development of information security related-industry such as PKI.
- Typical example of international cooperation between 2 countries: Korea and Japan.
- Many feedbacks and valuable lessons to the planned Internet voting systems, etc.

References

[1] M. Abe, "Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers", Advances in Cryptology-Eurocrypt'98, LNCS Vol. 1403, pp.437-447, Springer-Verlag, 1998

[2] J. Benaloh, "Verifiable Secret-ballot Elections", Ph.D. Thesis, Yale University, Department of Computer Science, YALEU/CDS/TR-561, December 1987.

[3] D. L. Chaum, "Elections with Unconditionally Secret Ballots and Disruption Equivalent to Breaking RSA", Advances in Cryptology-Eurocrypt'88, LNCS Vol. 330, pp.177-182, Springer-Verlag, 1988

[5] R. Cramer, M. Franklin, B. Schoenmakers, M. Yung, "Multi-Authority Secret Ballot Elections with Linear Work", Advances in Cryptology-Eurocrypt'96, LNCS Vol. 1070, pp.72-83, Springer-Verlag, 1996

[6] R. Cramer, R. Gennaro, B. Schoenmakers, "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology-Eurocrypt'97, LNCS Vol. 1233, pp.103-118, Springer-Verlag, 1997

[7] A. Fujioka, T. Okamoto, K. Ohta, "A Practical Secret Voting Scheme for Large Scale Election", Advances in Cryptology-Auscrypt'92, LNCS Vol. 718, pp. 248-259, Springer-Verlag, 1993

[8] M. Herschberg, "Secure Electronic Voting using the World Wide Web", Master's Thesis, MIT, June 1997.

[9] M. Ohkubo, F. Miura, M. Abe, A. Fujioka, T. Okamoto, "An Improvement on a Practical Secret Voting Scheme", Information Security'99, LNCS Vol.1729, pp.225-234, Springer-Verlag, 1999.

[10] C. Park, K. Itoh, K. Kurosawa, "Efficient Anonymous Channel and All/Nothing Election Scheme", Advances in Cryptology-Eurocrypt'93, LNCS Vol.765, pp.248-259, Springer-Verlag, 1994.

[11] K. Sako and J. Killian, "Receipt-free Mix Type Voting Scheme", Advances in Cryptology-Eurocrypt'95, LNCS Vol.921, pp.393-403, Springer-Verlag, 1995.

[12] K. Sako and J. Killian, "Secure Voting using Partially Compatible Homomorphims", Advances in Cryptology-Crypto'94, LNCS Vol.839, pp.411-424, Springer-Verlag, 1994.

[13] Insol Soft, http://www.insolsoft.com/

[14] Korea Institute of Science and Technology Information (KISTI), http://www.kisti.re.kr

[15] KSIGN Co.,Ltd. http://www.ksign.com

[16] SECUi.COM, http://www.secui.com

[17] Security Technology Inc. (STI), http://www.stitec.com