Result of the 1st Worldwide Internet Voting System

Kwangjo Kim

International Research center for Information Security(IRIS)

ICU, Korea

Abstract

In this paper, after designing an efficient and secure Internet voting protocol (called as "votopia") based on modified Ohkubo *et. al.*'s scheme [8] under Public Key Infrastructure (PKI), we have implemented this system and served via the Internet to select the Most Valuable Players and Best Goal Keepers of 2002 FIFA World Cup Korea/Japan™. The sketch of voting protocol, practical implementation and voting result are described.

I. Introduction

As new services like e-commerce, e-cash, e-stock and e-books, *etc.* using cryptographic primitives is becoming popular over the Internet, the possibility of Internet voting also attracts of great interest. If the Internet voting is sufficiently easy and comfortable, many people can easily participate in voting over the Internet. As the previous works on Internet voting, the state of California [1] has initiated a shadow election test of Internet voting system for the public election in Conta Costa County. Caltech-MIT joint project [12] has started in 2000 to develop reliable and uniform US voting machine due to the panic that threatened the 2000 American presidential election in Florida [11].

In this paper, we design and implement an Internet voting system (called as " votopia") as one of the best practices of *cryptography everywhere* to select top 10 Most Valuable Players and Best Goal Keepers among 32 national soccer teams participated in the 2002 FIFA World Cup Korea/Japan™, which was jointly hosted by Korea and Japan from June 1st to 30th 2002.

This paper is organized as follows: In Section II, we review cryptographic requirements of electronic voting system discussed in the open literature Section III introduces the overall sketch of system design. Section IV describes real implementation of servers and clients, Java cryptographic library and voting results. Finally, concluding remarks will be made in Section V.

II. Cryptographic Requirements

Many extensive researches [2, 4, 5, 6, 7] on electronic voting have been conducted and an extensive list of cryptographic requirements for electronic voting is available. In general, we can classify the cryptographic requirements of electronic voting system into the two parts.

■ Basic Requirements

- Privacy: All votes should be secret.
- Completeness: All valid votes should be counted correctly.
- Soundness: Anyone cannot disturb the voting.
- Unreusability: All voters can vote only one.
- Eligibility: Anyone who is eligible can vote.
- Fairness: Noting can affect the voting.

In general most electronic voting system as well as paper voting system must meet these basic requirements at least.

■ Extended Requirements

- Walk-away: The voter need not to perform any action after voting.
- Robustness: The voting system should be successful regardless of partial failure of the system.
- Universal verifiability: Anyone can verify the validity of the whole voting process.
- Receipt-freeness: Voter should not be able to prove his or her vote to a buyer. Voter does not have any receipt for the vote to prevent vote-selling.

We aim at designing and implementing the Internet voting system to be suitable for practical use. Since universal verifiability and receipt-freenees are conflicting requirements, we ignored to implement them. Our design mainly focuses ourselves to provide high efficiency and low communication to Internet users satisfying with all the basic requirements including walk-away and robustness. This will enable that more voters from any place can join votopia at any time during permissible period of voting.

III. System Design

In this Section, we sketch the system design and main protocol step of votopia. It is quite natural assumption that all the voters can 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 ElGamal cryptosystem[3], Schnorr digital signature[10], and Schnorr blind signature. This ensures that the overall security of votopia is based on the difficulty of solving discrete logarithm only.

1. PKI

Public key cryptography plays an important role in providing security services such as confidentiality, authentication, digital signatures, and integrity by using a pair of keys: public and private. The public key can be known to anyone, but the private key is kept secret by its owner. For the public key cryptography to be widely used in applications, the ability to verify the authenticity of public key is required. This can be achieved by the use of certificate, which provides a means to bind a public key to its owner. The certificate contains certification information such as owner's name, the associated public key, and validity period issued by a trusted CA, *etc.* whose standard format is X.509v3. But votopia uses its own simplified certificate providing the limited period of validity for a client to consume less memory.

2. Voting Protocol

Votopia consists of five basic entities; voter V_i, admin(*AS*), bulletin board(*BB*), counting server(*CT*) and certification authority. For the voting protocol, we choose OMAFO99 [8] due to its typical implementation, but extend their scheme by replacing the Mix-net[4] by the Internet to build an anonymous channel.

Votopia has three main stages: registration, voting and counting as most voting system does. Before initiating these stage, the system parameter including key pairs of each servers except a voter should be generated and distributed by PKI. All of parameters related to registration information of each voter will be passed through a secure channel. The security of network channel can be guaranteed by using J/SSWEB that provides more secure channel rather than SSL[17] during a web page connection.

▪ Notation

$B()$: Blinding function

C_i: V_i's Certificate

RA: Registration Authority

v_i: vote value by V_i

$UB()$: Unblinding function

WS:: Web Server

▪ Registration Stage

(R1) V_i accesses *AS* via *WS* to download a registration form and inputs his information required for certificate issuing. The information is encrypted with *AS*'s public key and is sent to *AS*. Then *AS* checks that V_i has the right to vote after decrypting the Information. If V_i doesn't have the right, *AS* gives an error message. Otherwise, *AS* gives V_i the right to download key generation applet.

(R2) After downloading a key generation applet and generating key pairs, V_i keeps his private key in safe storage and sends his public key to AS to request C_i.

(R3) AS requests C_i issuing to CA. CA issues a certificate to V_i stores C_i in his/her safe area or CA can keep C_i in DB instead of V_i.

■ Voting Stage

(V1) After downloading a login applet to enter voting stage, V_i provides authentication data (ID and password). AS checks whether the voter has already voted or not. If V_i had already voted, AS rejects the authorization. Otherwise, AS gives V_i the right to download the voting applet.

(V2) After downloading the voting applet, V_i selects vote v_i of his choice and encrypts v_i with CT's public key of the ElGamal encryption as $x_i = E_{CT}(v_i)$. V_i blinds x_i as $e_i = B(x_i, r_i)$, where r_i is a randomly chosen blinding factor. V_i signs e_i as $s_i = S_i(e_i)$ and sends (ID_i, e_i, s_i) to AS.

(V3) AS verifies the signature s_i of message e_i. If s_i is valid, then AS signs e_i as $d_i = S_A(e_i)$ and sends d_i to V_i. At the end of the voting stage, AS announces the number of voters receiving AS's signature, and publishes the final list as (ID_i, e_i, s_i).

(V4) V_i retrieves the desired signature y_i of ballot x_i by $y_i = UB(d_i, r_i)$. V_i checks whether y_i is AS's signature for x_i. If this check fails, V_i claims it by showing that (x_i, y_i) is invalid.

(V5) V_i sends (x_i, y_i) to BB via an anonymous channel (*i.e.*, the Internet).

■ Counting Stage

(C1) CT verifies the signature y_i of x_i. If the verification fails, CT claims that y_i is not a valid signature of x_i and exclude the vote from further steps of the counting stage.

(C2) CT decrypts ballot x_i and retrieves vote v_i as $v_i = D_{CT}(x_i)$. CT store the voting results to DB.

(C3) After the period of voting is finished, CT publishes the voting results by using BB.

IV. Implementation

In order to implement votopia efficiently, software products by Korean security industries have been chosen and their functions have been extended to meet the objectives of votopia.

Votopia used the CA server by KSIGN[14], one of CA vendors in Korea, and the Java crypto library J/LOCK and J/SSWEB by STI[16]. InsolSoft[13] provided the web interface for voters and SECUi.COM[15] provided its firewall SECUiWall 2.0, the security management of all servers and the network. Imai laboratory at the University of Tokyo and NTT did check correctness and vulnerability of votopia.

1. Servers

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. The main part of AS and BB have been developed by using JSP, JDK1.2, and Java crypto library. Oracle DB is used by AS to manage a large number of informations of all voters. BB also uses 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, Sybase, Microsoft, *etc.* Also, CT is implemented in JAVA language.

The information of all servers is summarized as below :

- AS, BB, CT, CA : 2 Sun V.880, Enterprise 3000, Enterprise 6500; Solaris 2.8
- DB : Oracle 8.0 on Compaq Alpha EV 6.7; Tru64 Unix
- Firewall : Compaq Deskpro EN; FreeBSD Unix
- L4 Switch : CSS 11800

2. Client

All clients must get the voting applet which is a downloadable program code and is executed in a web browser of a voter supporting Java, which contains necessary information to support the actual candidate selections. The voter does not need to download any code ahead of time. The voting applet needs permission to open connections to multiple addresses and to access a secret file containing voter's private key. A simple and secure way to achieve this is using the functionality of signed applet in JDK which allows safe downloading and execution of the applet. Because Java applet is running inside sandbox, we believe that system security must be guaranteed to a reasonable level. The current voting applet is limited to Window OS on PC because the location of the secret key can be stored safely. The key size of ElGamal cryptosystem and Schnorr digital signature are fixed to 512 bit for fast computation to a client side. In Appendix, test printout of a client is logged.

3. Java Cryptographic Library

Votopia tried to utilize the existing crypto-library in C language implemented by NTT[10], which was once used to implement an electronic voting system. But all applications of votopia are running in Java, Java-based cryptographic library J/LOCK by STI was used instead. The J/LOCK library includes all the classes and interfaces for keys, encryption, decryption and digital signature. The cryptographic primitives such as ElGamal public key cryptosystem, Schnorr digital signature scheme, and Schnorr blind signature scheme have been implemented using Java in addition.

4. Performance Test

To get ready to receive votes from world wide Internet users, votopia has been installed in high-performance servers and a benchmark test has been carried out to check the possible concurrent number of users. We assume that most action of an Internet user is to connect to a web site, look for the information of candidates and register their personal information for voting. Using a well-known performance test tool, we gradually increased the number of user under the hypothetical condition. The result indicated that votopia can serve about 1,000 concurrent users.

5. Voting Result

Voting was conducted in two stages : preliminary and main voting stage[17]. The preliminary voting stage lasted for 14 days from June 1st to the midnight of 14th 2002 to select top 10 MVP and Goal Keepers among the candidates representing all 32 national teams. The number of voters in preliminary voting stage is 903 from 35 countries. Most voters (95%) are from Asia. Among them, the number of male and female voters are 686 and 217 respectively. On the other hands, the main voting stage started from June 15th to 30th 2002. The number of voters has increased to 3,662 from 31 countries. Among them, the number of female voters are 2,512 (67%) much higher than the preliminary voting stage. The detailed results are posted at the web page[28]. The total number of hits to the web page was 39,738 in a month.

V. Concluding Remarks

We have designed and implemented the Internet voting system using PKI to the first time over the world. Votopia successfully served as an Internet voting system by allowing all netizens to vote for the top 10 MVPs and Best Goal Keepers during 2002 FIFA World Cup Korea/Japan^{TM}. If we can use the smart card interface to each voters, the confidentiality and authentication of eligible voters will be improved. Also mobile voting via such as PDA, cellular phone and *etc.* will be studied. More detailed information will be available in the full paper version.

Acknowledgement

The author would like to be very grateful to Mr. Hyunrok Lee for his help in preparing for this paper and express great thanks to all volunteers of their joining votopia from Korea and Japan. Also, the anonymous voters all over the world via the Internet are very much appreciated for their contributions to the successful votopia.

References

[1] The BELL Newsletter on Internet Voting, The Bell, Vol.1 No.4, Safevote Inc., Aug. 2000.

[2] J. C. Benaloh and D. Tuinstra, *Receipt-free secret ballot elections*, Proc. of 26th ACM STOC, pp.544-553, 1994.

[3] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, Advances in Cryptology-Crypto'84, LNCS Vol.196, pp.10-18, Springer-Verlag, 1985.

[4] A. Fujioka, T. Okamoto and 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.

[5] B. Lee and K. Kim, *Receipt-free electronic voting through collaboration of voter and honest verifier*, Proc. of JW-ISC2000, pp.101-108, Jan. 25-26, 2000, Okinawa, Japan.

[6] M. Maichels and P. Horster, *Some remarks on a receipt-free and universally verifiable mix-type voting scheme*, Advances in Cryptology-Asiacrypt'96, LNCS Vol.1163, pp.125-132, Springer-Verlag, 1996.

[7] V. Niemi and A. Renvall, *How to prevent buying of voters in computer elections*, Advances in Cryptology-Asiacrypt'94, LNCS Vol.917, pp.164-170, Springer-Verlag, 1994.

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

[9] B. Schoenmakers, *A simple publicly verifiable secret sharing scheme and its application to electronic voting*, Advances in Cryptology-Crypto'99, LNCS Vol.1666, pp.148-164, Springer-Verlag, 1999.

[10] C. P. Schnorr, *Efficient Identification and Signatures for Smart Cards*, Advances in Cryptology-Crypto'89, LNCS Vol.435, pp.235-251, Springer-Verlag, 1990.

[11] M. I. Shamos, *What's happening in Florida ? Bugs in Computerized Voting*, CMU Distinguished Lecture, Nov., 2000.

[12] CALTECH-MIT/Voting Technology Project, Dec, 2000, *http://www.vote.caltech.edu/*

[13] Insol Soft, *http://www.insolsoft.com/index2.html*

[14] KSIGN Co., Ltd. KSignCA. *http://www.ksign.com*

[15] SECUi.COM *http://www.secui.com*

[16] Security Technology Inc. (STI), J/LOCK, *http://www.stitec.com*

[17] Draft of SSL 3.0 Specification by Netscape. *http://wp.netscape.com/eng/ssl3/*

[18] Votopia 2002 FIFA World Cup Korea/Japan^{TM} Homepage. *http://mvp.worldcup2002.or.kr/*

Appendix Sample printout of a voting client

- Voter's ID : tank01
- tank01's private key

x: b18a89184ca7c39a564bc8a3951fd31f7c7c4aa2

p
:c16cbad34d475cc5396695d694bc8bc47c598c23b5a9d7c5cc
c82d65b6827d44c95378484730c0bff1f4cb56f47c6c51054bc8
9200f30d43dc4fef9624d4665b

q: b7b810b58c0934f642878f360b96d7cc26b53e4d

g
:4c53c726bdbfbba6549d7c731939c6c93a869a27c5db17ba3c
ac589d7b3c003fa735f290cfd07a3cf10f35155f1a2ef70335af7
b6a5211a1103518fba44e9718

- ElGamal Encryption

Vote : 10000001421000000149

Tag : dfa2b05b80327197

Encoded vote vi which is a message for ElGamal encryption :

31303030303030313432313030303030313439dfa2b05b8
0327197

Random number k for ElGamal encryption by using Counter's public key :

13a256f141daabc0218b3bf9a7d38a6f42f3d1b7

$G(=g^k \bmod p)$:

5c09b2c9f30a3cfa6ca6f759dc5ffa6b41d14db36cfa3ba032
35395009c47bc96a7060549fc29d87776621a038f0382ff11acf
4701f152b439ef6b3d25b8d75a

$M(=m*(y^k) \bmod p)$:

4b1bacf8d9b62dc25a6c694706f06839bb6b4c592aadac586
cf66b3dbc89c633b2aa12b626fec745f5cb289d1a7b853bc714
c28de29325dd1234a1fb988338f8

Encrypted $vi(ev)$:

8400404b1bacf8d9b62dc25a6c694706f06839bb6b4c592aa
dac586cf66b3dbc89c633b2aa12b626fee745f5cb289d1a7b85
3bc714c28dc29325dd1234a1fb988338f800405e09b2c9f30a3
cfa6ca6f759dc5ffa6b41d14db36cfa3ba03235395009c47bc96
a7060549fc29d87776621a038f0382ff11acf4701f152b439ef6b
3d25b8d75a

- Blinding encrypted $vi\ (ev)$

Random commitment $\mathcal{A}$ for blinding given by signer :

d0f610890ae68f7dc30c2e092ec0b8e5f1eef78fe2e6de22c5
d9d3c9722d32d7b8258a82c6e5c64c14c9fd02d8ca33b45975c
0834e8664cad420cf46b6ee742

Message to be blinded :

8400404b1bacf8d9b62dc25a6c694706f06839bb6b4c592aa
dac586cf66b3dbc89c633b2aa12b626fee745f5cb289d1a7b85
3bc714c28de29325dd1234a1fb988338f800405e09b2c9f30a3
cfa6ca6f759de5ffa6b41d14db36cfa3ba03235395009c47be96
a7060549fc29d87776621a038f0382ff11acf4701f152b439ef6b
3d25b8d75a

Blinding factor u :

67a351f610de9a0aecdbe101a1eaad65081ec911

Blinding factor v :

87e0ff425c9a290839c07cf1b447ff9b63af46b6

$r'(=\mathcal{A}*g^u*y^v \bmod p)$:

6dcca3fff1b0a8ad35cec23db88bac58fecec0d822dffbf27b
3f8cafa37a1493c6a9ca29c8f278c7dc47afd0df6acd6d0f5899
1237598542f43749fd4020f3bd

$e'(=hash(r', msg) \bmod q)$:

9cb0ccf2f8c11b8cfbcd67f98601bef690253717

$e(=e'-v \bmod q)$:

14cfcdb09c26f284c20ceb07d1b9bf5b2c75f061

Blinding data $\mathcal{C}\,(=e)$:

14cfcdb09c26f284c20ceb07d1b9bf5b2c75f061

- Schnorr Signature

Message for Schnorr sig. :

14cfcdb09c26f284c20ceb07d1b9bf5b2c75f061

random factor k of Schnorr signature :

e9ba90c0365f43d5ce66f8df8172f51edce80aa0

$r(=g^k \bmod p)$:

9c40ffea40f8b64d07bea68be21ba356e988d4672a6127f73ed26002eab138532a2715045a1b71fbe9d6b72e16aa2c88193b85896e97706ba0a117834bb8717b

Schnor sig. factor $e(=hash(r, msg) \bmod q)$:

1e880df55d4456658f61e9642354332c1b1d741d

Schnor sig. factor $s(=k-e*x \bmod q)$:

3daa4fb08702f94e2e7924cb8afd4a0bcda0f35b

- Message to admin2 $eai(=(s, e)\|\mathcal{C}\|\mathcal{A})$: ae0054001e000674616e6b30310014f944c14a23bd17587da41678d9e200bf2c2898\eb00320030002e050200143daa4fb08702f94e2e7924cb8afd4a0bcda0f35b00141e880df55d4456658f61e9642354332c1b1d741d001414cfcdb09c26f284c20ceb07d1b9bf5b2c75f06100400d0f610890ae68f7dc30e2e092ec0b8e5f1eef78fe2e6de22c5d9d3c9722d32d7b8258a82c6c5c64c14c9fd02d8ca33b45975c0834e8664cad420cf46b6ee742

- Message from admin2, that is, admin's blind signature $ezc(=admin's\ blind\ sig.(s, e))$

53001d000561646d696e0014f562c7aed63493f04f0cbc4d755299e6def0f59d00320030002e05020014b8c375a0b11b24185f14d48e469371b0cba335be001414cfcdb09c26f284c20ceb07d1b9bf5b2c75f061

- Unblinding

Admin's blind sig. factor $s(=\omega-e*x \bmod q)$:

b8c375a0b11b24185f14d48e469371b0cba335be

Admin's sig. factor $s'(=s+u \bmod q)$:

2a51e02718b40372d081a381703721d4084ed9a6

Admin's sig. factor $e'(=e+v \bmod q)$:

9cb0ccf2f8c11b8cfbcd67f98601bef690253717

Unblinded admin sig. $bs(=admin's\ sig.(s', e'))$: 2e050200142a51e02718b40372d081a381703721d4084ed9a600149cb0ccf2f8c11b8cfbcd67f98601bef690253717

- Message to Bubo $esev(=bs\|ev)$:

b6002e050200142a51e02718b40372d081a381703721d4084ed9a600149cb0ccf2f8c11b8cfbcd67f98601bef690253717008400404b1baef8d9b62dc25a6e694706f06839bb6b4e592aadae586ef66b3dbc89c633b2aa12b626fee745f5cb289d1a7b853bc714c28dc29325dd1234a1fb988338f800405e09b2c9f30a3cfa6ea6f759de5ffa6b41d14db36cfa3ba03235395009c47bc96a7060549fe29d87776621a038f0382ff11acf4701f152b439cf6b3d25b8d75a

- Message on Counter

Unblinded admin sig. $bs(=admin's\ sig.(s', e'))$: 2e050200142a51e02718b40372d081a381703721d4084cd9a600149cb0ccf2f8c11b8cfbcd67f98601bef690253717

Encrypted $vi\ (ev)$:

8400404b1baef8d9b62dc25a6c694706f06839bb6b4c592aadac586ef66b3dbc89c633b2aa12b626fee745f5cb289d1a7b853bc714c28de29325dd1234a1fb988338f800405c09b2c9f30a3cfa6ea6f759dc5ffa6b41d14db36cfa3ba03235395009c47bc96a7060549fe29d87776621a038f0382ff11acf4701f152b439ef6b3d25b8d75a

Vote Result: 10000001421000000149