Design and Implementation of Internet Voting System to the Worldwide Level

August 28, 2001

IRIS (International Research center for Information Security)

ICU (Information and Communications Univ.), Korea

kkj@icu.ac.kr

Kwangjo Kim
Contents

1. Introduction
2. Requirements
3. Voting Scheme
4. System Configuration
5. Implementation
6. Application
7. Summary
1. Introduction

Why do we consider Internet voting?
- Anyone can vote using internet
- Anywhere from home, office, overseas, etc.
  -> Solution for the problem of decreasing the participation rate in manual voting

What are the problems in Internet voting?
- Strong security requirements: anonymity, privacy, completeness, fairness, receipt-freeness, etc.
- No perfect secure system
- PKI is not ready.
Motivations

- **Our motivation and contribution - “Votopia”**
  - Prompt cryptographic voting techniques to the real life
  - Demonstrate public awareness of PKI
  - Satisfy most of security requirements
  - First trial of Internet voting to the worldwide scale such as 2002 FIFA World Cup Korea /Japan
  - Participation based on volunteership

- **Similar trial – “CyberVote”**
  - Remote Internet voting with fixed and mobile internet tech.
  - 3-year R&D program funded by European Commission
2. Requirements - cryptography

- Basic requirements
  - **Privacy**: All votes must be secret
  - **Completeness**: All valid votes are counted correctly
  - **Soundness**: The dishonest voter cannot disrupt the voting
  - **Unreusability**: No voter can vote twice
  - **Eligibility**: No one who isn’t allowed to vote can vote
  - **Fairness**: Nothing can affect the voting

- Advanced requirements
  - **Walk-away**: The voter need not to make 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 vote
  - **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)
Requirements – Security & Performance

- **Server side**
  - Network and computer security
    - Anti-hacking such as DOS attack
  - Large memory and communication bandwidth
  - Fault-tolerant and high reliable
  - Reasonable time of registration and voting

- **Client side**
  - Fast and Easy
  - Web Interface
  - No tamper-proof device provided
  - Various kinds of platform and browser
3. Voting Scheme

- **FOO92 Scheme**
  - Fujioka, Okamoto, Ohta, “A Practical Secret Voting Scheme for Large Scale Elections”, Auscrypt’92
  - Features: Blind signature + Mix-net + Bit commitment

- **Implementation examples**
  - Sensus : L.F. Cranor, Washington Univ.  
    http://www.ccrc.wustl.edu/~lorracks/sensus
  - EVOX : M.A. Herschberg, R.L. Rivest, MIT  
    http://theory.lcs.mit.edu/~cis/voting/voting.html

- **OMAFO99 Scheme**
  - Improved version of FOO92
  - Features : Blind signature + Mix-net (hybrid-mix) + threshold encryption
OMAFO99 scheme

System overview

(1) Voter Authentication
(voting + encryption + blind signature)

(2) Voting
(voting + encryption + signature)

(3) Opening
(Threshold decryption)
4. System Configuration

Registration stage : 0, 1
Voting stage : 2, 3
Counting stage : 4, 5, 6

System Configuration Components:
- **Voter**
- **Admin Web Server (RA)**
- **Mix Server**
- **BB Server**
- **Tally Server**

Key Stages:
1. Certificate Issue
2. Blind Sig.
3. Ballot Casting
4. Mixing
5. Tallying
6. Counting Results
Registration stage

1) Access Web Page

2) Down

3) Registration
   ID & Passwd, name, etc ...

4) Encrypted Data

5) Check & Store

6) Down

7) Key Generation
   8) Private key

9) Public key

10) Registered Info + public key

11) Certificate Request

12) Certificate Issue

13) Certificate

Admin Web Server

Voter

RA

DB

CA
Voting Stage

1) Log In
   - ID & Passwd

2) Authenticated Channel

3) Check Double Voting
   - Admin DB

4) If not vote

5) Select Vote. Encrypt by counter key. Blinding.

6) Requests blind sig.

7) Blind Sig.

8) Send blind sig.


10) Ballot Casting

11) Sig. Verify & Store ballot
    - BB DB
    - Admin DB
    - BB Server

Voter

Admin
Web Server

Voting Applet

ID & Passwd

Admin
DB

Wote'01
Counting Stage

1) Mixing
2) Tallying
3) Results
4) Announce

Admin
Web Server

Mix Server

BB Server

BB DB

Counters
Threshold decryption

Wote'01
5. Implementation

- Public-key Infrastructure
  - Needed for “one certificate - one vote” principle
  - simplified X.509v3 for one-time use

- Web Interface
  - User Friendliness

- A huge number of data handling
  - KISTI – Computing Power Support
  - Mix Server and Counting Server
Detailed Implementation

- **Severs**
  - AS,BB : Apache web server and Tomcat to support JSP
  - DB : Oracle DB + JDBC
  - M,T : Implemented in C language

- **Voting applet**
  - Signed java applet to access a secret key and to open connections to multiple addresses
  - Platform : WINDOW98 /+ on IBM PC

- **Cryptographic algorithms**
  - AES
  - ElGamal public key cryptosystem
  - Schnorr type blind signature
2002 FIFA World Cup Korea-Japan MVP Voting System

IRIS
- Project Coordination & System Management
- User Interface
- DB management
- Java Crypto Library

NTT
- Voting system Prototype

InSol
- Verification

U. of Tokyo
- Korean
- Japanese

STI
- SECUi.COM
- PKI service

KSIGN
- Voting Servers
- Backup CA
- Anti-Hacking
- Security Management

KISTI
- Wote'01
6. Application-Votopia

- **2002 FIFA World Cup Korea-Japan™**
  - May 31 ~ June 30, 2002
  - Major cities in Korea and Japan
  - 32 teams from the world

- **Candidates**
  - After 1st round, 16 teams
  - MVP and best goal-keeper

- **Voting period**
  - July 1 ~ 10, 2002 (10 days)

- **Web-page**
  - http://mvp.worldcup2002.or.kr
Example

![Voting World Cup MVP - Microsoft Internet Explorer](image)

<table>
<thead>
<tr>
<th>Country</th>
<th>Players</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MVP</strong> Korea, Republic</td>
<td>Hwang Sun Hong, Kang Chul, Kim Do Hoon, Kim Tae Young, Ko Jong Su, Lee Min Sung, Lee Young Pyo, Park Ji Sung, Park Yong Ho, Seo Jong Ro, Seo Jong Won</td>
</tr>
<tr>
<td><strong>Best Goalkeeper</strong> Korea, Republic</td>
<td>Hwang Sun Hong, Kang Chul, Kim Do Hoon, Kim Tae Young, Ko Jong Su, Lee Min Sung, Lee Young Pyo, Park Ji Sung, Park Yong Ho, Seo Jong Ro, Seo Jong Won</td>
</tr>
</tbody>
</table>

Copyright C&IS All right reserved.
7. Summary

- **Design & Prototyping of Internet voting system**
  - User friendly and secure Internet voting system
  - Applying PKI to the voting system

- **Expected Results**
  - Cyber MVPs of 2002 FIFA World Cup Korea-Japan™
  - Contribution to the development of information security related-industry such as PKI.
  - Valuable lessons to the planned Internet voting systems

- **Left problems**
  - Multiple registration, # of voters,
  - Social engineering, political problem, etc
Questions