Votopia will be continued…

1st Secure Internet Voting System over the world

To Choose the Most Valuable Player and the Best Goalkeeper in 2002 FIFA World Cup Korea/Japan™

Kwangjo Kim

International Research Center for Information Security
Information and Communications Univ.

Prof. Kwangjo Kim
Votopia – A Secure Internet Voting System - © IRIS
Introduction

- A project carried out by effective collaboration among some of the prominent Korean and Japanese IT firms and research institutes

- InSol: User Interface, DB management
- STI: Java Crypto Library
- LG-CNS: System Testing and Integration
- IRIS: Project Coordination & System Management
- MIC: Voting system C-src Prototype Verification
- KOWOC: Supporters
- Reddevils: Supporters
- U. of Tokyo: Security Management
- NTT: ORACLE DB
- KSIGN: PKI service
- KISTI: Voting Servers
- SECUi.COM: Security Management

Korean: InSol, LG-CNS, ORACLE, KSIGN, KISTI, SECUi.COM
Japanese: STI, IRIS, MIC, KOWOC, NTT, U. of Tokyo

Prof. Kwangjo Kim
Votopia – A Secure Internet Voting System - © IRIS
Contributors

- **IRIS**: Kwangjo Kim, Byoungcheon Lee, Jinho Kim, Myoungsun Kim, Hyunrok Lee, Jaegwan Park, Manho Lee, Wooseok Ham, Jongseung Kim, Hyunggi Choi, Kyuseok Ham, Kukhwan Ahn, Vo Duc Liem, Xie Yan, Fangguo Zhang, etc
- **LG CNS**: Daehun Kim, Seung Pil Hong, Minhyung Kim, Jongyoon Choi
- **Insolsoft**: Sunjoo, Hyun, Mina Jung, Junghan Kim, YongJae Lee
- **KSIGN**: Ki-Yoong Hong, Jadong Ku, Eunsong Lee, Jinsoo Lim, Daesung Ku
- **STI**: Donnie Choi, Daeha Park, Seoungho Heo, Jung Cheol Yoon
- **KISTI**: Younghwa Cho, Jungkwon Kim, Jun Woo, Okhwan Byun
- **SECUi.COM**: Kyongsoo Oh, Moonseok Seo, Wonkeun Hur, Hyunwon Ko
- **MIC**: Hyun Lee, Ee-Hwan Hwang
- **Korean Press (Digital Times, Daily Econimics)**, Reddevils
- **U. of Tokyo**: Hideki Imai, Kazuguni Kobara
- **NTT**: Tatsuaki Okamoto, Atsushi Fujioka, Masayuki Abe, Kouharou Suzuki
- **ORACLE, SUN**
Cryptographic Req’t

Basic

- 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

- 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)
Security & Performance Req’t

- **Server side**
  - Network and computer security
    - Anti-hacking such as DDOS attack, *etc*
  - Large DB handling
  - Fault-tolerance and high reliability
  - Reasonable processing when registering and voting

- **Client side**
  - Fast and easy, user-friendly web interface
  - No tamper-proof device provided
  - Various kinds of platforms, OS and browsers
  - Keep the privacy of all voters at maximum
System Configuration

http://mvp.worldcup2002.or.kr

Voters

Internet

Firewall

CA Server
SUN 6500 / 3000 SUN 880*2

Clustered Web Servers

Admin Server
SUN 6500

DB Server
COMPAQ ES40

Counter Server
(COMPAQ ES40)
Implementation

- **Client**
  - Java1.2, JLOCK+
  - MS Explorer 4.0 on Windows98 /ME/XP/2000
  - Korean, Japanese, English and Chinese

- **Web, DB, Admin, and Counter Servers**
  - Solaris 2.5.4 (SUN OS 5.8), Oracle DB 8.0.6 , JDBC
  - Tomcat3.1, Apache1.3.12, JSSWEB+

- **Encryption and Certificate**
  - 512 bit ElGamal encryption and Schnorr (blind) signature
  - Simplified X.509v3 certificate issued by CA server
Flow of 3 main stages

R1. After setting up secure session, download registration form
R2. Send encrypted public key & registration information with session key
R3. Request certificate
R4. Issue certificate
R5. Save certificate
R6. Send query for tallying
R7. Receive the final result

V1. Download voting applet
V2. Encrypt the ballot with counter’s public key in ElGamal encryption
V3. Request Schnorr blind signature
V4. Receive Schnorr blind signature
V5. Verify admin’s blind signature
V6. Send encrypted ballot & admin’s digital signature
V7. Verify admin’s signature & decrypt ballot using counter’s private key
V8. Save all decrypted ballots

R: Registration
V: Voting
C: Counting
Home Page
(http://mvp.worldcup2002.or.kr)

Choose MVP
2002 FIFA World Cup Korea – Japan

Schedule
- Select MVP and best Goal Keeper through the Internet
- Preliminary Voting
  - Period: Jun. 1 ~ 19, 2002
  - Announcement: Jun. 15, 2002
- Final Voting
  - Period: Jun. 16 ~ 30, 2002
  - Announcement: Jun. 30, 2002

Client Environments
- At least MS Windows 98 and MS Explorer 4.0 or higher

Motivation
- To celebrate the joint hosting of "2002 FIFA World Cup Korea/Japan (TM)" and to support this international festival by the volunteering parties from two hosting countries.
- To demonstrate that Korea/Japan are proud of having established the top-level IT infrastructure and to promulgate new cyber service to the world.
- To serve the first secure internet voting that features the similar functionalities of the manual voting system to all the netizens all over
Registration

[Warning] For the registration and vote, you must click "Yes" in the popping-up window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID(*)</td>
<td>Check (4~10 English characters or numbers)</td>
<td></td>
</tr>
<tr>
<td>Password(*)</td>
<td>(within 4~8 characters)</td>
<td></td>
</tr>
<tr>
<td>Re-type Password(*)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail(*)&amp;</td>
<td>(Please give your correct e-mail address for further correspondence.)</td>
<td></td>
</tr>
<tr>
<td>Country(*)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender(*)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Age(*)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*) : Mandatory field
*This page is for “vote-now”. In case of “vote-later”, you must give ID and passwd.*
Statistics of main voting

Preliminary: 903 votes

- Total: 3662 votes
- Asia: 3604 votes
- Korea: 3474 votes
- Japan: 90 votes
- Male: 1150 votes
- Female: 2512 votes

Prof. Kwangjo Kim
Votopia – A Secure Internet Voting System - © IRIS
Top 10 MVP’s

- Miroslav KLOSE
- Young Pyo LEE
- David BECKHAM
- Ji Sung PARK
- Chong Gug SONG
- Ronaldo
- Jung Hwan AHN
- Myung Bo HONG
- Nam II KIM
- Sun Hong HWANG

No. of votes

0 200 400 600 800 1000 1200 1400 1600

Votopia – A Secure Internet Voting System - © IRIS
Top 10 Best Goalkeepers

Players

1. Gianluigi BUFFON
2. Seigo NARAZAKI
3. Jose Luis CHILAVERTE
4. Brad FRIEDEL
5. David SEAMAN
6. casillas IKER
7. Tony SYLVA
8. Byung Ji KIM
9. Oliver KAHN
10. Woon Jae LEE

Votes

Prof. Kwangjo Kim
Votopia – A Secure Internet Voting System - © IRIS
Other Details

Age:
- Below 10 yrs: 13 (0.4%), 11~20 yrs: 1,725 (47.1%), 21~30 yrs: 1,551 (42.4%), 31~40 yrs: 270 (7.4%), 41~50 yrs: 85 (2.3%), 51~60 yrs: 13 (0.4%), Above 61 yrs: 5 (0.1%)

Continents:
- Asia: 3,604 (98.4%), Europe: 23 (0.6%), North America: 20 (0.5%), Oceania: 8 (0.2%), South America: 4 (0.2%), Africa: 3 (0.1%)

List of nations more than 5 voters:
- Korea: 3,474, Japan: 90, Vietnam: 18, China: 14
- Canada: 8, USA: 7, India: 6, Australia: 6
- France: 5, Netherlands, Brazil, Denmark, England, Germany, Russia, Peru, Taiwan, Indonesia, Finland, Spain, etc.
Highlights

- Registered netizen can cast his vote anywhere, any time
  - Explorer 4.0 or higher on Windows 98/ME/2000/XP
  - Min. 56 Kb/s Internet Speed
  - Minimized personal information by ID/pwd identification

- Web Site Access
  - About 100 votes and 1,000 hits in a day

- S/W Portability
  - Platform independent by Java

- Double anti-hacking mechanism
  - Firewall (H/W)
  - Intrusion Detection System (S/W)
Concluding Remarks

- Successful Internet Voting
  - Acceptable Performance on Client side
  - Comfortable User Interface
  - System Configuration and Daily Auditing

- Best practice of “cryptography everywhere” in 2002
  - It works good but need some time for practical application depending on a number of factors.

- Further Works
  - Authentication (bio-identification), Mobile Internet voting
  - Trial voting for small society (e.g., IACR’s annual voting)
  - Real voting replacements in isolated areas when natural disaster (e.g., heavy rain) happens.