VOTOPIA - Internet Voting Experience during 2002 FIFA WorldCup Korea/Japan™

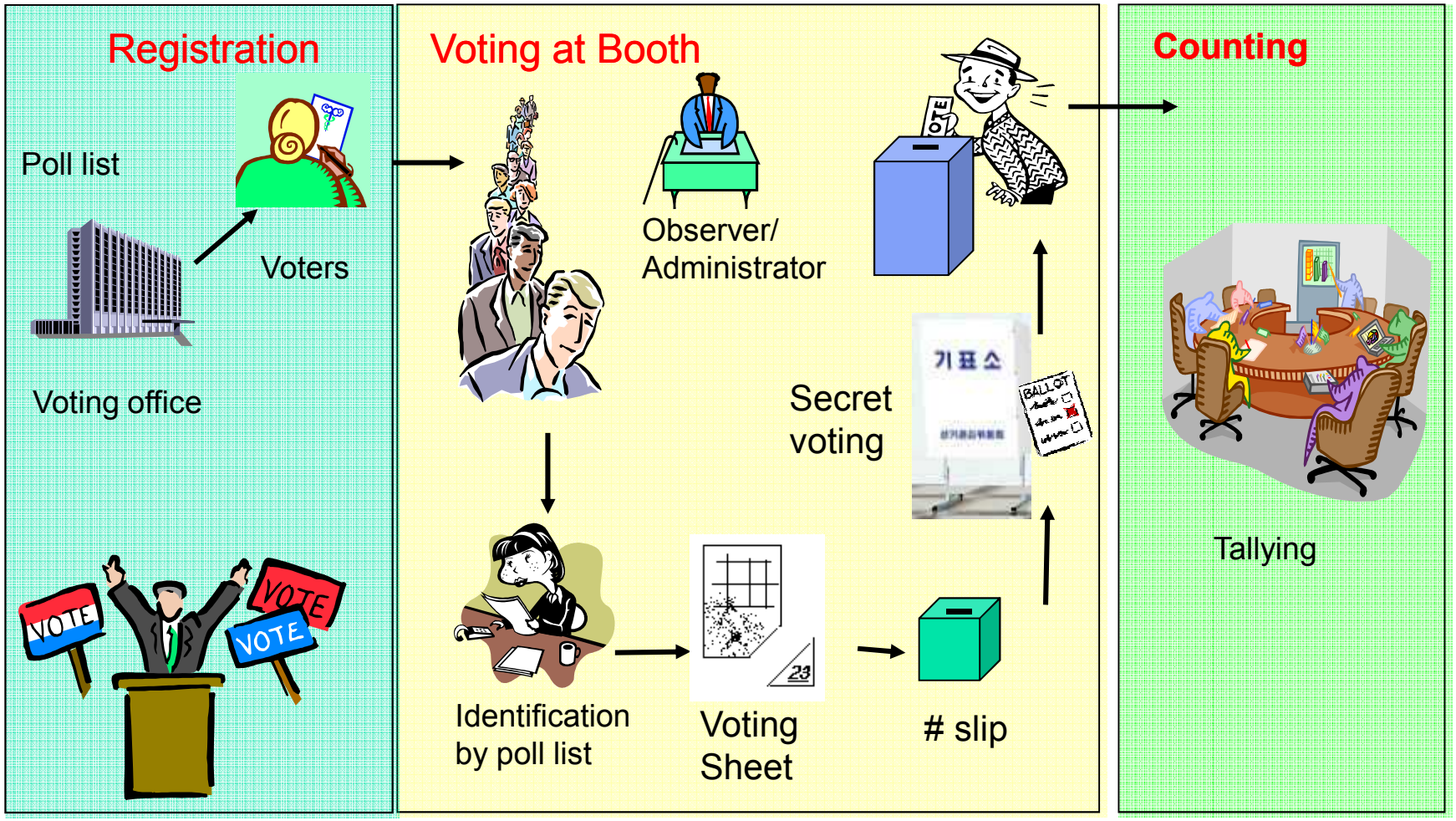
[1] International Research center for Information Security (IRIS)
Information and Communications University (ICU)
[2] Information Security Dept., Joongbu University

Mar. 17, 2005

[1] Prof Kwangjo Kim, kkj@icu.ac.kr
[2] Prof. Byoungcheon Lee sultan@joongbu.ac.kr

Contents

Paper Voting



How to approach E-Voting

- [Idea 1] Voter Interface: Replacing by electronic voting mechanisms for friendliness
  - **User layer**
  - **Touch screen, mouth, *etc.***
- [Idea 2] Leased network connected restricted voting booth
  - **Secure Session Layer**
- [Idea 3] Internet voting
  - **From Kiosk, voting booth, Home or mobile phone**
  - **Encrypted voting over the Internet**
  - **Application Layer**
- [Idea 4] Selective use of paper and electronic voting

Secure Electronic Voting(I)

- **Homomorphic Encrytion**
  - Yes/no vote
- **Blind signature-based**
  - Multiple choice
- **Mixnet-based**
  - anonymous channel
- **Combinations above**

Secure Electronic Voting (II)

- Sensus [92] by Cranor and Cytron
  - **Expanding FOO92**
  - **No walk-away**
- EVOX by MIT based on FOO02
  - **Single administrator[97]**
  - **Multiple administrator[99]**
- Caltech-MIT project
  - **Florida presidential election at Florida 2000**
- Cybervote
  - **Europe 2000 – 2002**
  - **Test voting at Swindon, UK, May 2002**
- Many approaches based on different requirements

Internet Voting - Votopia

- **An international project called "VOTOPIA" was carried out by effective collaboration among some of the prominent Korean and Japanese IT firms and research institutes**
  - Korea: IRIS, KISTI, KSIGN, LG CNS, SECUi.COM, STI, VOCOTECH
  - Japan: NTT, University of Tokyo
- **IRIS, affiliated to ICU, Korea - initiated, managed, and coordinated the project**

Goals of Votopia

- Korea/Japan teams initiated the idea of VOTOPIA* in 2000, in order to show their strong support to the most prestigious mega event "2002 FIFA World Cup Korea/Japan™".
- Advance in Korean PKI
  - 10M broadband Internet users at home
  - 3M certificate holders for Internet banking, e-auction, *etc*.
- Verify secure Internet voting system using cryptographic primitives and show its usefulness as replacement of paper voting.

* VOTOPIA is in no way associated with FIFA and does not intend to violate international legal issues and digital copy rights.

Contributors

- IRIS : Kwangjo Kim, Byoungcheon Lee, Jinho Kim, Myoungsun Kim, Hyunrok Lee, Jaegwan Park, Manho Lee, Wooseok Ham, Jongseung Kim, Hyunggi Choi, Kyuseok Han, 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, Koutarou Suzuki
- ORACLE, SUN

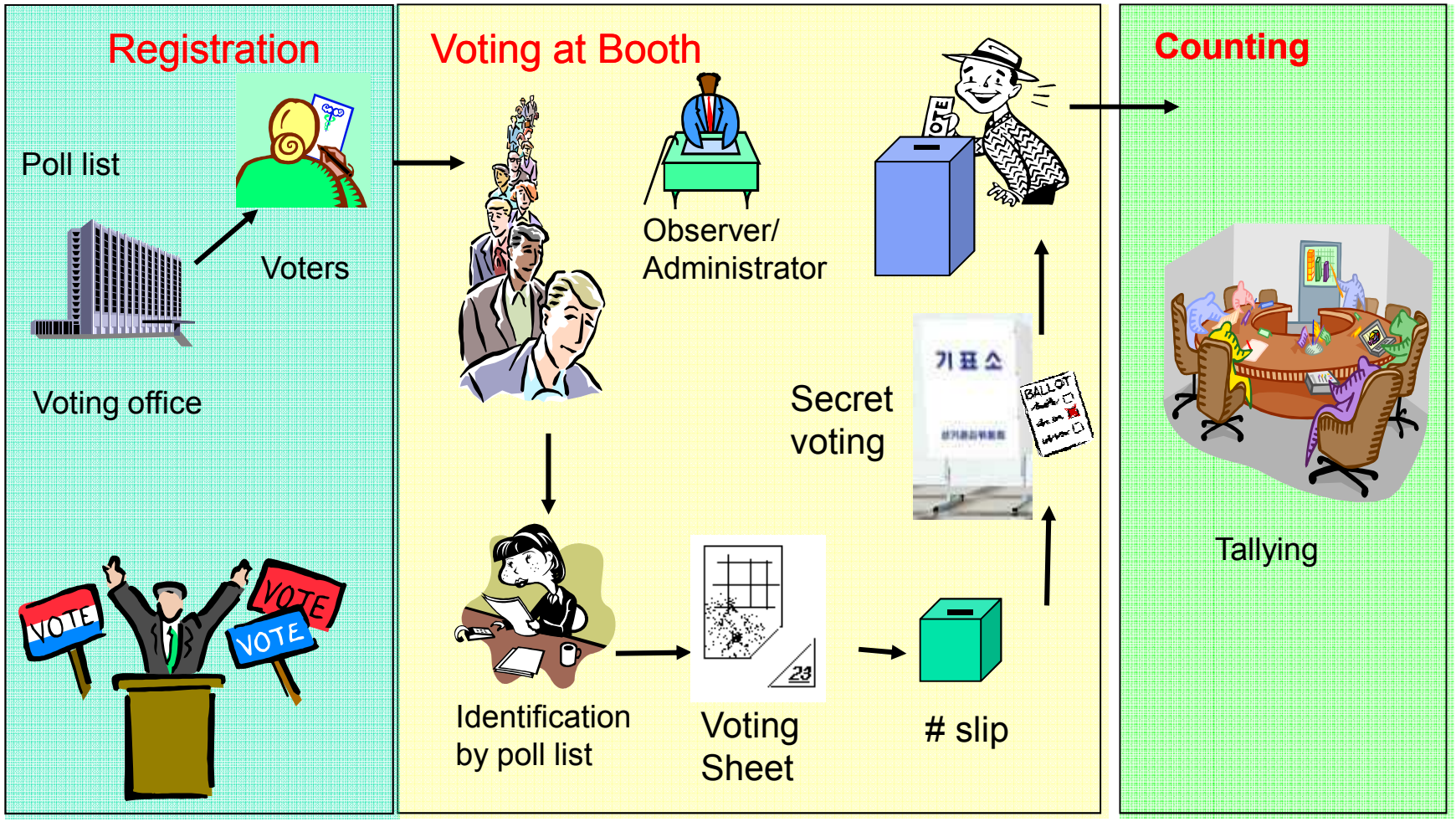
2. System Design (1)

- Type of voting system
  - Remote Internet voting for large scale election
  - based on blind signature under PKI environment
- Authentication of voters
  - Anyone registered once can cast a vote
  - Issue certificate to voters
- Meet basic cryptographic requirements in e-voting
  - ✓ 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

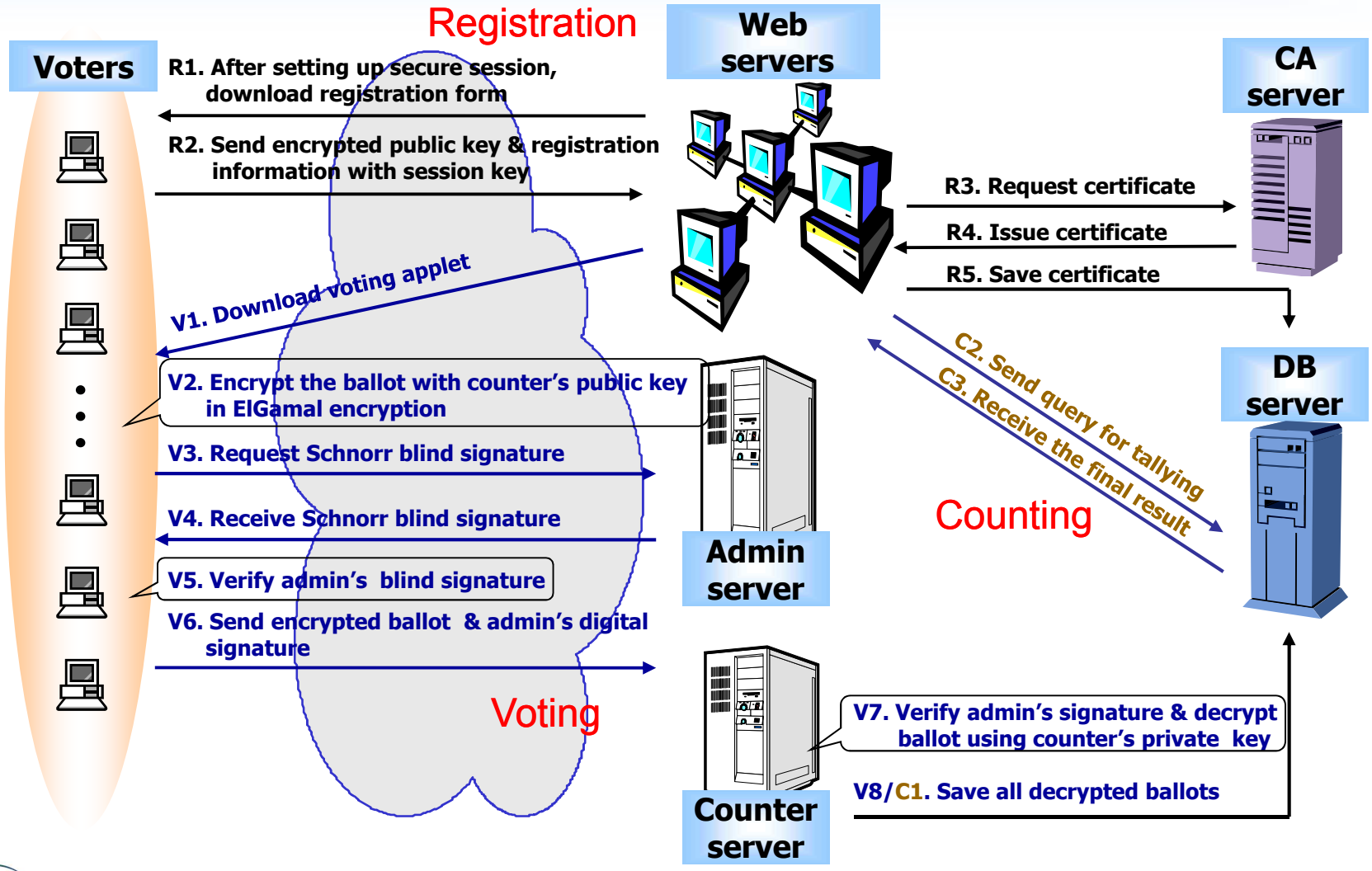
System Design (2)

- Client side
  - Fast and easy, user-friendly web interface
  - No tamper-proof device needed
  - Consider various kind of platforms, OS, browsers, and Internet speed
- Server side
  - Highly secure network and computer system
    - Anti-hacking system (such as DOS attack, *etc.*)
  - Large DB handling
  - Fault-tolerance and high reliability
  - Reasonable processing in registration and voting

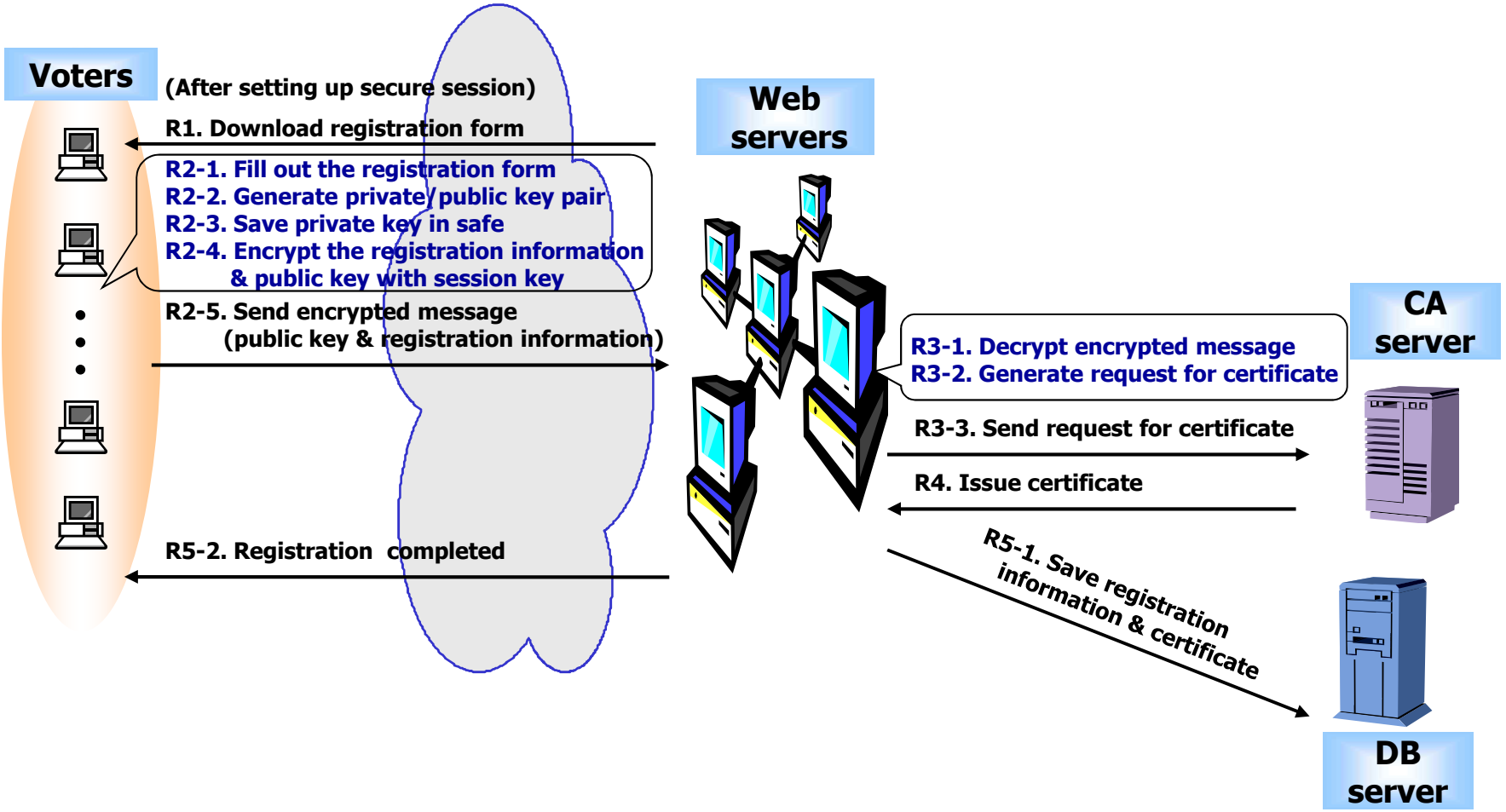
Paper Voting Scenario



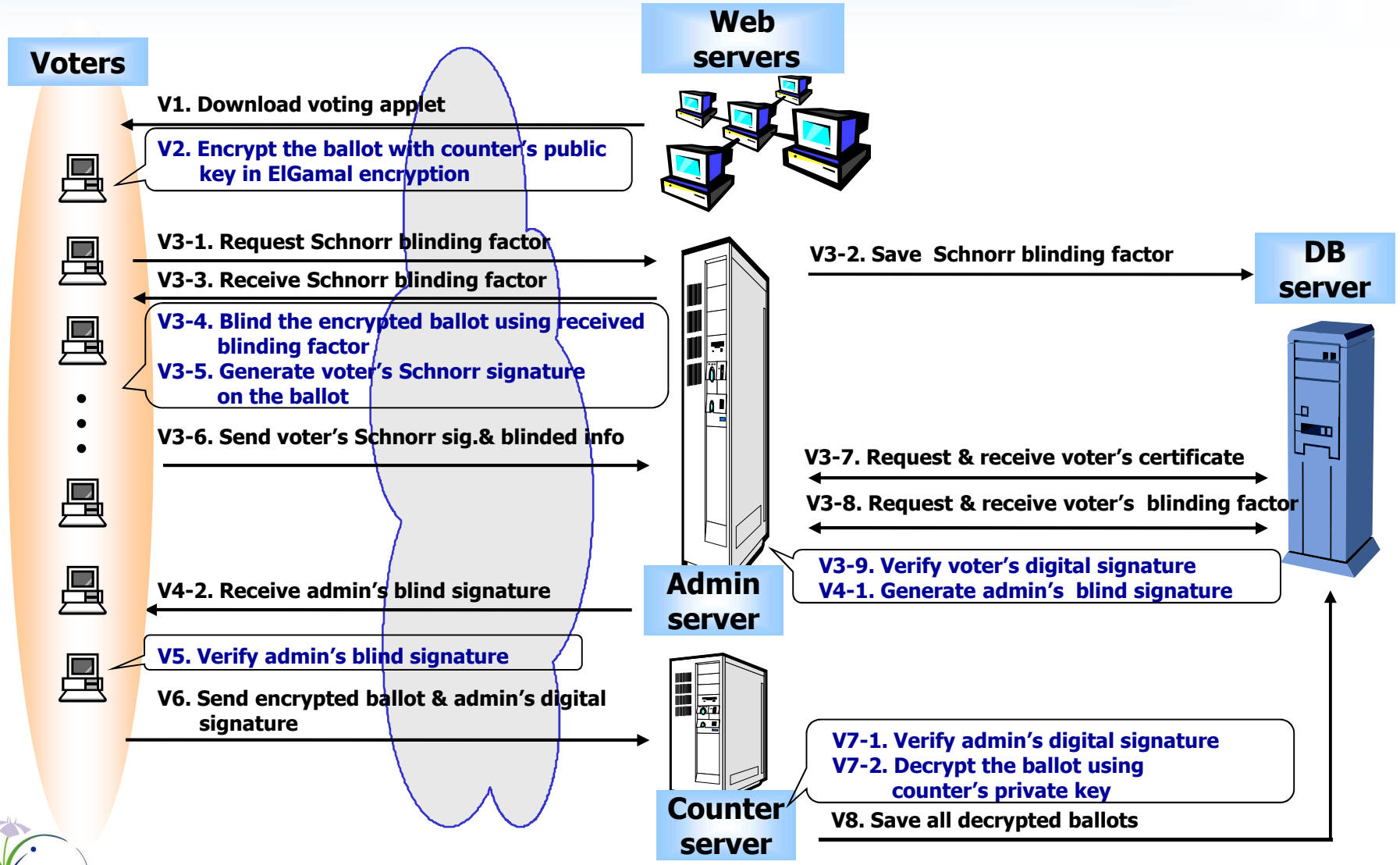
Internet Voting Scenario



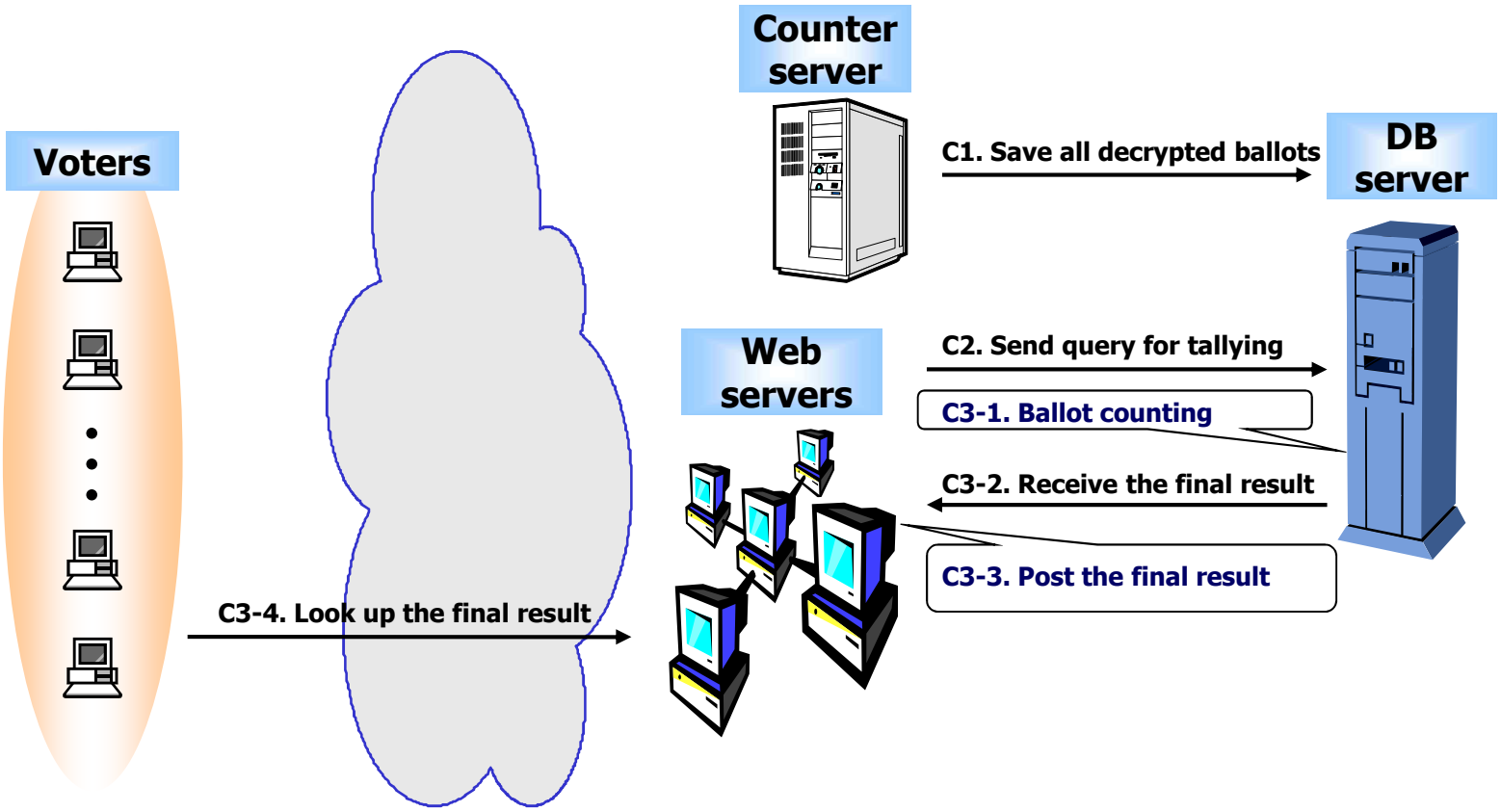
Registration Stage



Voting Stage

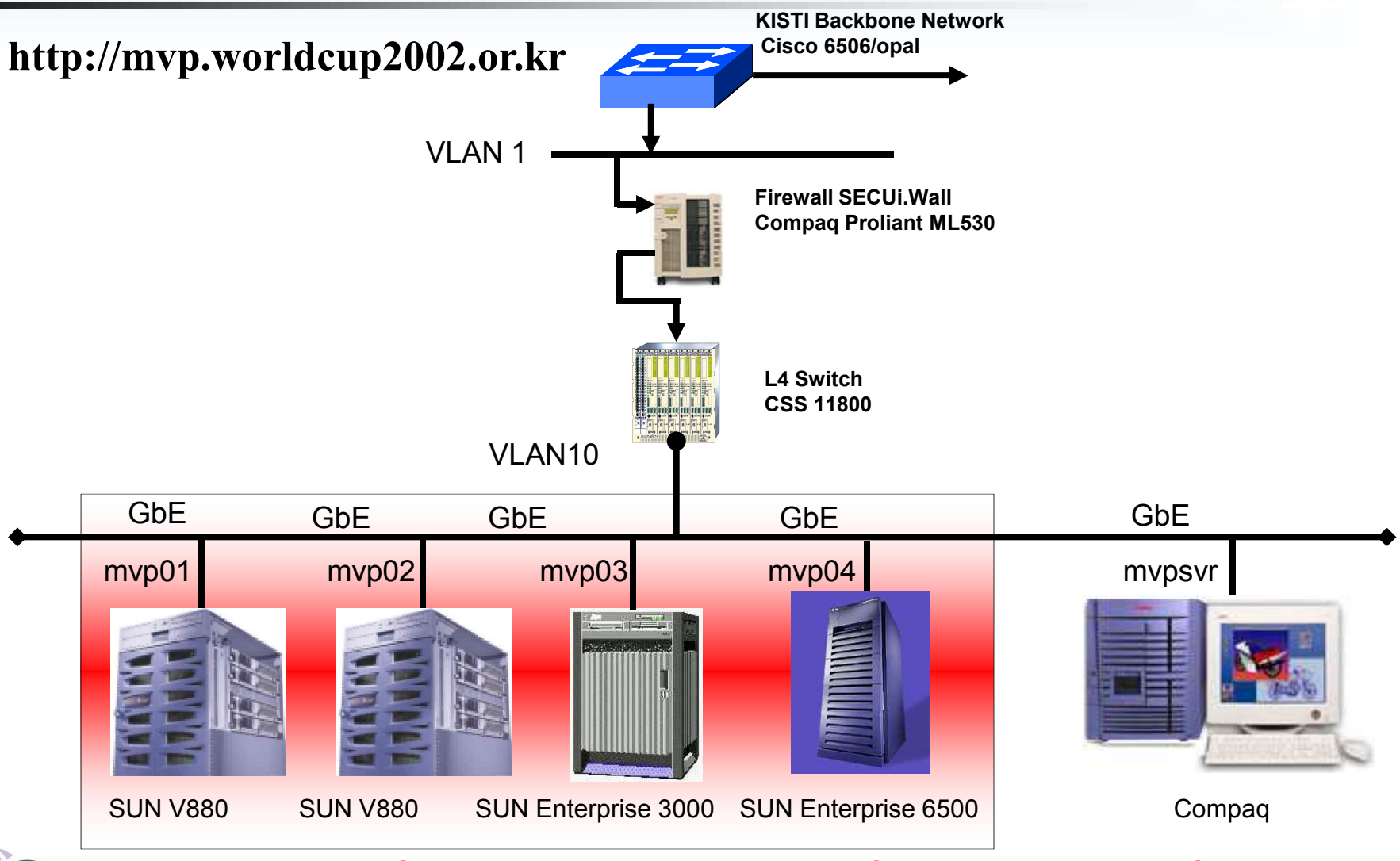


Counting Stage



3. Configuration of Servers (1)

http://mvp.worldcup2002.or.kr

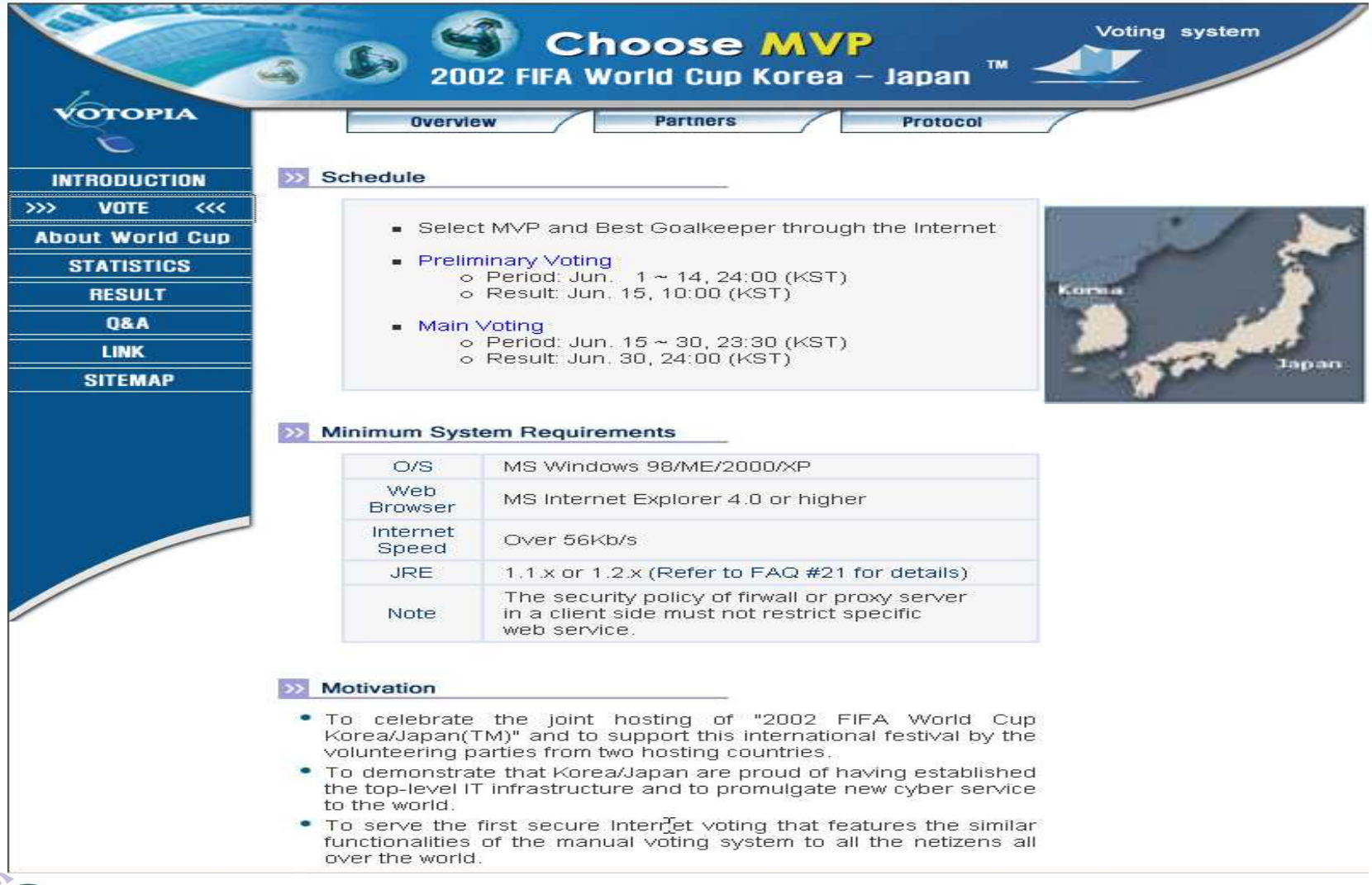


Configuration of Servers (2)

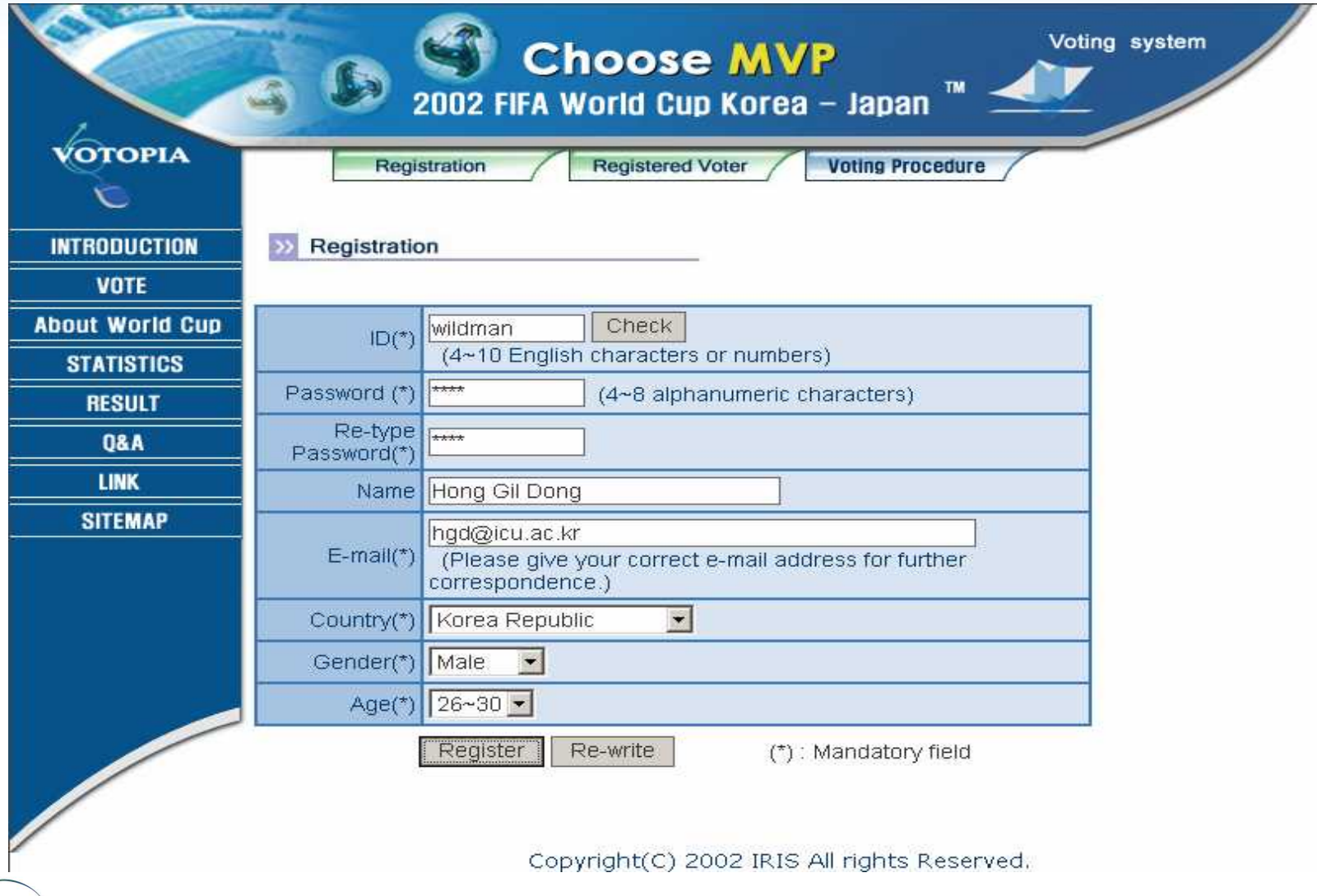
Implementation Details

- 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
  - ElGamal encryption & Schnorr (blind) signature
  - Simplified X.509v3 certificate issued by CA server

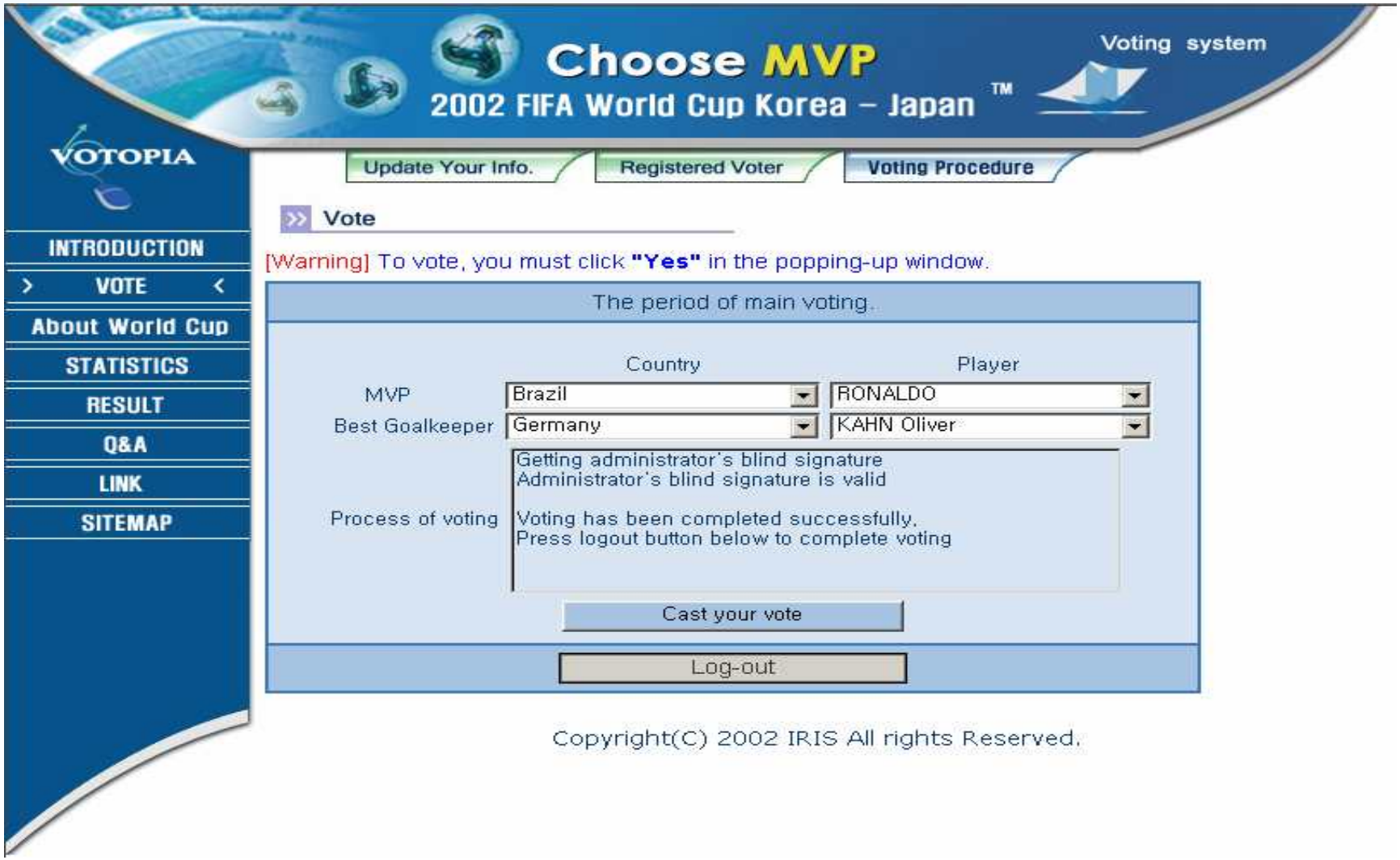
Homepage (http://mvp.worldcup2002.or.kr)



Registration Page



Voting Page


Choose MVP
2002 FIFA World Cup Korea – Japan ™
Voting system
VOTOPIA
Update Your Info.
Registered Voter
Voting Procedure
INTRODUCTION
VOTE
About World Cup
STATISTICS
RESULT
Q&A
LINK
SITEMAP
Vote
[Warning] To vote, you must click "Yes" in the popping-up window.
The period of main voting.
Country
Player
MVP
Brazil
RONALDO
Best Goalkeeper
Germany
KAHN Oliver
Process of voting
Getting administrator's blind signature
Administrator's blind signature is valid
Voting has been completed successfully.
Press logout button below to complete voting
Cast your vote
Log-out
Copyright(C) 2002 IRIS All rights Reserved.

4. Voting Result

- 2 times voting to select MVP and Best GK
  - **Preliminary vote**
    - Period: Jun. 1 ~14
    - Candidates: 32 teams
    - Notification: June 15 10 AM
  - **Main vote**
    - Period: Jun. 16 ~ 30
    - Candidates: 16 teams
    - notification): June 30 12 PM
- One team has 20 players and 3 GKs

Data Size & Voting Time

- **Data Size**
  - Applet for SSL Connection at *R1*
    - 207 KB
  - Voting Client Applet at *V1*
    - 215 KB
  - Voter's Registration Information at *R2-1*
    - Avg. 50 Bytes
  - Key Size : Security / Performance Trade-off
    - Voter : 256 bit ElGamal Encryption & 512bit Schnorr Signature
    - Administrator : 256 bit Schnorr Blind Signature & 512bit Schnorr Verification
    - Counter : 256 bit ElGamal Decryption
- **Voting Time (*V1 - V6*)**
  - Avg. 2 (or 3) min. under Pentium III 100M LAN (or 56K modem)
  - Including Admin's & Counter's Server Computation Time : avg 195 msec

Sample Vote (1)

Voter's ID : tank02

tank02's private key

Private Key *x*: 9fa840a6974fc04810db89b73461bb8d561a20bd

Security Parameters:

p **:**
c16cbad34d475ec5396695d694bc8bc47e598e23b5a9d7c5cec82d65b6827d44e95
378484730c0bff1f4cb56f47c6e51054be89200f30d43dc4fef9624d4665b

q **: b7b810b58c0934f642878f360b96d7cc26b53e4d**

g **:**
4c53c726bdbfbba6549d7e731939c6c93a869a27c5db17ba3cac589d7b3e003fa735
f290cfd07a3ef10f35155f1a2ef70335af7b6a5211a1103518fba44e9718

Admin's public key

Public Key *y*:
c0ace983c8c4346b99b54e96505f94b7b2ba25d6764c16fcb9f239cbc447402f

Security Parameters:

p **: f668a94f0ce284e30ce284e30776b59b319fec12ba069d10c56498e2bd0cb42f**

q **: e3109c1fd13c8d637f6c39e6c0a6e9dfc0a6e9df**

g **: a7688634018f161c62de5014ca99e983759fb4f67b575bbc4b51d32392177a40**

Sample Vote (2)

Counter's public key

Public Key *y*:
b6fbabc9259a1267fcde3a82ebc060781c9404b7caf4c07837fb86b1054207fb
Security Parameters:
***p* : e204679a6b62fe446b62fe440c0bfea01223d98b7b65a6b1095962b41d502d21**
***q* : ad9c0afead1c2e24900e4799ddcade6bddcade6b**
***g* : 329d730dea5e5cff79b9a46968414e16ec610dbdd3e1b7d090aec0bdef310411**

Message from Admin1(*tildeA*):
2004d4c5ff693b20ad4574a062c1eb80d6e2e0d79639f755cd9e4de14593f9ceec

Vote : 100000014310000000160
Tag : 4277bb955fad5f86

Encoded vote(*vi*) : 313030303030303134333130303030303136304277bb955fad5f86

Message for ElGamal encryption :
313030303030303134333130303030303136304277bb955fad5f86

Sample Vote (3)

Random number k for ElGamal encryption :
4af1c2911bd5f59789307fd12366436e68dbd0ae

G(=*g^k mod p*) :
316aafb99ed1a7565e09d795a1c4bc1bc884f5069b3e3af12c61976bd929cd35
M(=*m*(y^k) mod p*) :
9f88bcf0128a500c218c8fbde13a21ca8eae32caa58ac9339d8c3a5eaa79489d

Encrypted *vi*(*ev*) :
4400209f88bcf0128a500c218c8fbde13a21ca8eae32caa58ac9339d8c3a5eaa79489 d0020316aafb99ed1a7565e09d795a1c4bc1bc884f5069b3e3af12c61976bd929cd3 5

Blinding encrypted *vi*
Random commitment *tildeA* for blinding given by signer
4d4c5ff693b20ad4574a062c1eb80d6e2e0d79639f755cd9e4de14593f9ceec

Message to be blinded
4400209f88bcf0128a500c218c8fbde13a21ca8eae32caa58ac9339d8c3a5eaa79489d00 20316aafb99ed1a7565e09d795a1c4bc1bc884f5069b3e3af12c61976bd929cd35

Sample Vote (4)

Blinding factor *u* : 1a35c544169b7df3cde2488f5ae6179ad3c50ea7
Blinding factor *v* : e1254df36ad334dc92e7f5c75224f2b77b179924

***r'(=tildeA * g^u * y^v)* :**
8ac9e4f8917d0961a017b0706bb2cc9145161dab9b01322849ce97878ffb67d5
***e'(=hash(r',msg)mod q)* : 2c81051411f5826f47fa9825b579bb6eb97bf01d**
***e (= e'-v mod q)* : 2e6c5340785edaf6347edc4523fbb296ff0b40d8**

Blinded *ev(tildeC=e)* : 2e6c5340785edaf6347edc4523fbb296ff0b40d8

Message for Schnorr Sig. : 2e6c5340785edaf6347edc4523fbb296ff0b40d8
random factor *k* of Schnorr Sig. : b09bd1ea81f8f91c2ec9cc8a805b4150ced8bf37
***r(=g^k mod p)* :**
a04164bfc61f673d77d29aae45fb503394823bbf96bb1407acdbbf2a76069313204ae
1cf8e9fc8862f3d07c27ac2f6dc529d47d5e06f2450715a1a5034c996ff

voter's sig. (s,e) of message *tildeC*
Schnorr Sig. factor *e (= hash(r,msg) mod q)* :
3b6226900a5333f29f8c0ca99b1c0c5aeee5a1c7
Schnorr Sig. factor *s (= k - e*x mod q)* :
12ed689be782fbcae8d8f823226997769fc469d0

Sample Vote (5)

Message to admin2 (*eai=(s,e)|tildeC|tildeA*) :

8e0054001e00066b6d616e3232001490a9ab12dc8f91be844dc57575ff741f6565bab300320030002
e0502001412ed689be782fbcae8d8f823226997769fc469d000143b6226900a5333f29f8c0ca99b1c
0c5aeee5a1c700142e6c5340785edaf6347edc4523fbb296ff0b40d8002004d4c5ff693b20ad4574a
062c1eb80d6e2e0d79639f755cd9e4de14593f9ceec

Message from admin2, that is, admin's blind signature (*ezc*) :

53001d000561646d696e001411cc6504f02e79e6811c8046cf13ebb47d4f6e6600320030002e0502
00148bcd80bd228501354422eacf5032171ee491725000142e6c5340785edaf6347edc4523fbb296f
f0b40d8

Unblinding

Admin's blind sig. factor *s (= omega-e*x mod q)* : 8bcd80bd228501354422eacf5032171ee4917250

Admin's sig. factor *s' (= s+u mod q)* : a603460139207f291205335eab182eb9b85680f7

Admin's sig. factor *e' (= e+v)* : 2c81051411f5826f47fa9825b579bb6eb97bf01d

Unblinded admin sig.(*bs*) :

2e05020014a603460139207f291205335eab182eb9b85680f700142c81051411f5826f47fa9825b57
9bb6eb97bf01d

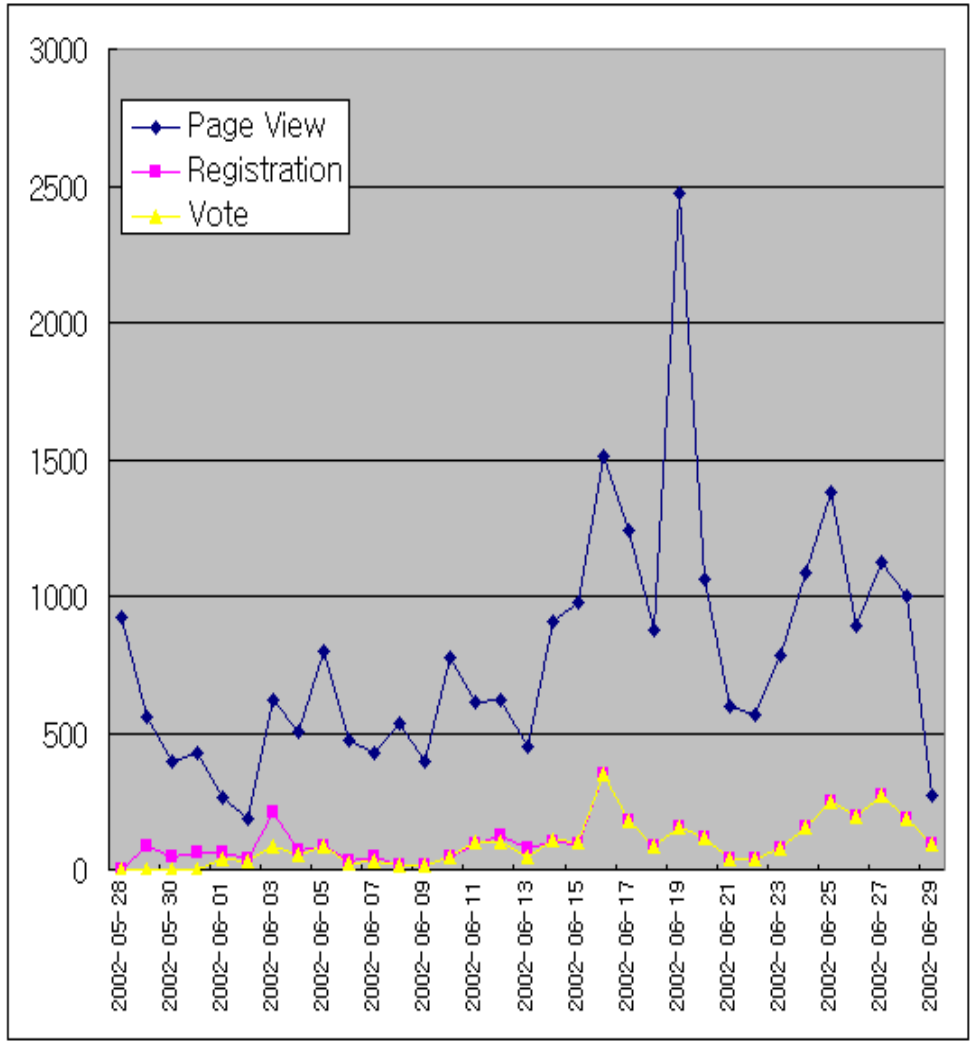
Message to Bubo(*esev=bs||ev*)

76002e05020014a603460139207f291205335eab182eb9b85680f700142c81051411f5826f47fa982
5b579bb6eb97bf01d004400209f88bcf0128a500c218c8fbde13a21ca8eae32caa58ac9339d8c3a5
eaa79489d0020316aafb99ed1a7565e09d795a1c4bc1bc884f5069b3e3af12c61976bd929cd35

Vote Result : 10000001431000000160

Daily Access Record

	Page View	Registration	Vote
27-May	1137	209	0
28-May	925	0	0
29-May	559	85	0
30-May	394	50	0
31-May	428	59	0
1-Jun	263	59	39
2-Jun	186	42	34
3-Jun	622	210	89
4-Jun	502	70	57
5-Jun	798	85	82
6-Jun	476	33	25
7-Jun	423	44	32
8-Jun	533	19	17
9-Jun	393	14	15
10-Jun	772	47	48
11-Jun	610	94	99
12-Jun	617	124	102
13-Jun	453	80	48
14-Jun	910	104	105
15-Jun	973	92	100
16-Jun	1508	346	346
17-Jun	1240	180	180
18-Jun	878	82	82
19-Jun	2474	154	154
20-Jun	1060	113	113
21-Jun	597	38	37
22-Jun	568	39	39
23-Jun	784	77	78
24-Jun	1086	154	155
25-Jun	1380	247	246
26-Jun	889	194	194
27-Jun	1125	270	271
28-Jun	1002	188	187
29-Jun	275	93	94
Total	26840	3695	3068



IIS Attack Monitored in Error.log File at Apache Server

[Thu Jul 4 23:59:48 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/msadc/..%5c../..%5c../..%5c/..?../..?../..?../winnt/system32/cmd.exe

[Thu Jul 4 23:59:48 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/scripts/..?../winnt/system32/cmd.exe

[Thu Jul 4 23:59:48 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/scripts/..유../winnt/system32/cmd.exe

[Thu Jul 4 23:59:48 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/scripts/..뾎../winnt/system32/cmd.exe

[Thu Jul 4 23:59:48 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/scripts/..%5c../winnt/system32/cmd.exe

[Thu Jul 4 23:59:48 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/scripts/..%2f../winnt/system32/cmd.exe

[Fri Jul 5 01:06:56 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/c/winnt/system32/cmd.exe

[Fri Jul 5 01:06:56 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/d/winnt/system32/cmd.exe

[Fri Jul 5 01:06:56 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/scripts/..%5c../winnt/system32/cmd.exe

[Fri Jul 5 01:06:56 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe

[Fri Jul 5 01:06:56 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe

[Fri Jul 5 01:06:56 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/msadc/..%5c../..%5c../..%5c/..?../..?../..?../winnt/system32/cmd.exe

[Fri Jul 5 01:06:56 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/scripts/..?../winnt/system32/cmd.exe

[Fri Jul 5 01:06:56 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/scripts/..유../winnt/system32/cmd.exe

[Fri Jul 5 01:06:56 2002] [error] [client 210.107.135.145] File does not exist: /user/mvp/public_html/scripts/..뾎../winnt/system32/cmd.exe

of Typical Hacking (Filtered by IDS) (1)

Type of Hacking

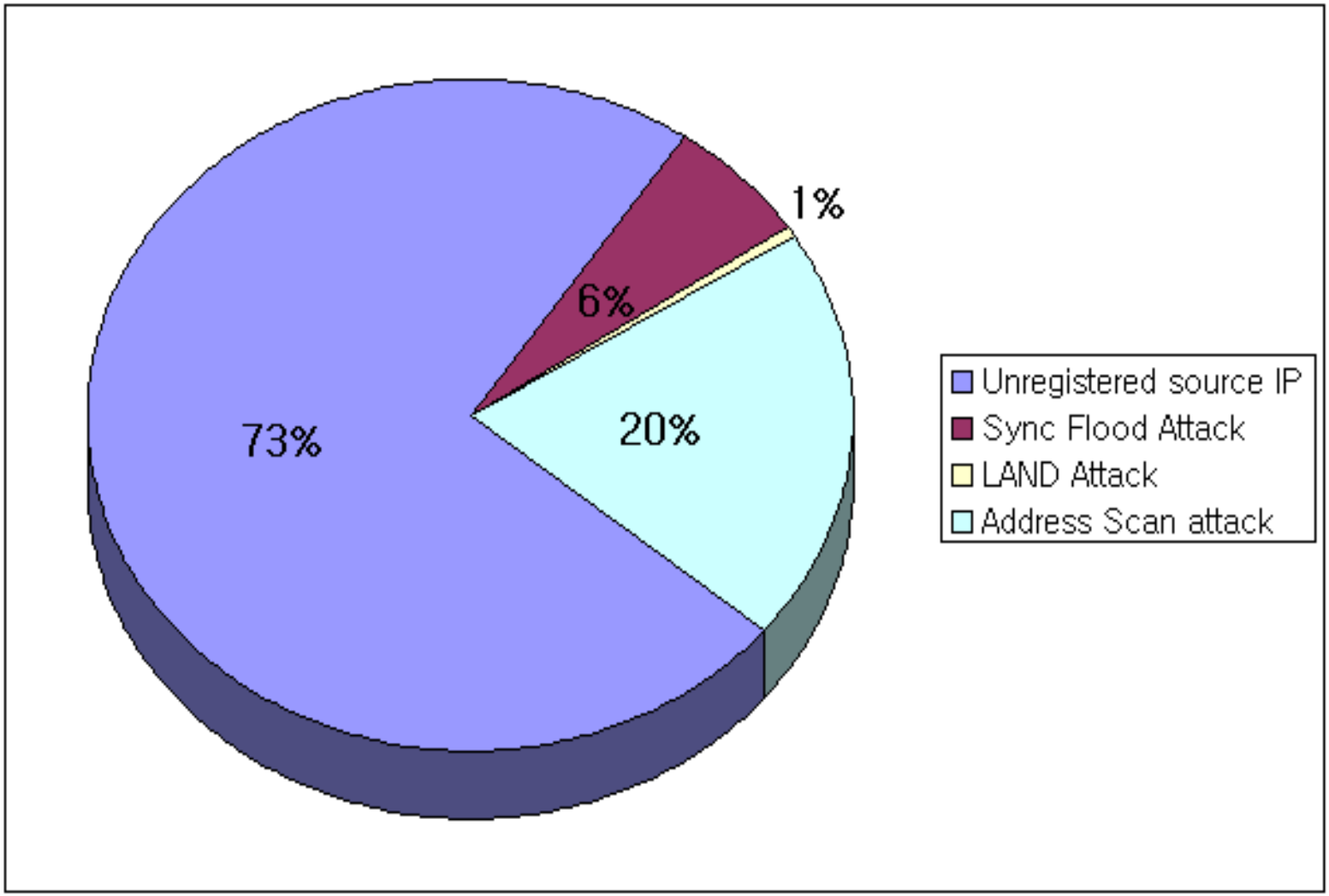
Date

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
28-May	0	0	0	10	0	0	1	0	0	0	0	4	0	0
29-May	0	0	0	7	0	0	1	0	0	0	0	3	0	0
30-May	0	0	0	6	0	0	0	0	0	0	0	4	0	0
31-May	0	0	0	1	0	0	0	0	0	0	0	2	0	0
1-Jun	0	0	0	5	0	0	1	0	0	0	0	3	0	0
2-Jun	0	0	0	3	0	0	0	0	0	0	0	3	0	0
3-Jun	0	0	0	8	0	0	0	0	0	0	0	3	0	0
4-Jun	0	0	0	3	0	0	0	0	0	0	0	1	0	0
5-Jun	0	0	0	3	0	0	0	0	0	0	0	2	0	0
6-Jun	0	0	0	3	0	0	0	0	0	0	0	6	0	0
7-Jun	0	0	0	1	0	0	0	0	0	0	0	4	0	0
8-Jun	0	0	0	3	0	0	0	0	0	0	0	0	0	0
9-Jun	0	0	0	4	0	0	0	0	0	0	0	3	0	0
10-Jun	0	0	0	2	0	0	0	0	0	0	0	4	0	0
11-Jun	0	0	0	7	0	0	0	0	0	0	0	2	0	0
12-Jun	0	0	0	17	0	0	4	0	0	0	0	11	0	0
13-Jun	0	0	0	9	0	0	0	0	0	0	0	1	0	0
14-Jun	0	0	0	13	0	0	0	0	0	0	0	1	0	0
15-Jun	0	0	0	11	0	0	1	0	0	0	0	3	0	0
16-Jun	0	0	0	31	0	0	0	0	0	0	0	1	0	0
17-Jun	0	0	0	17	0	0	2	0	0	0	0	7	0	0
18-Jun	0	0	0	14	0	0	1	0	0	0	0	2	0	0
19-Jun	0	0	0	16	0	0	2	1	0	0	0	1	0	0
20-Jun	0	0	0	23	0	0	3	0	0	0	0	4	0	0
21-Jun	0	0	0	6	0	0	0	0	0	0	0	3	0	0
22-Jun	0	0	0	6	0	0	0	0	0	0	0	1	0	0
23-Jun	0	0	0	11	0	0	4	0	0	0	0	2	0	0
24-Jun	0	0	0	9	0	0	1	1	0	0	0	1	0	0
25-Jun	0	0	0	11	0	0	1	0	0	0	0	2	0	0
26-Jun	0	0	0	16	0	0	0	0	0	0	0	2	0	0
27-Jun	0	0	0	12	0	0	3	0	0	0	0	2	0	0
28-Jun	0	0	0	35	0	0	3	0	0	0	0	1	0	0
29-Jun	0	0	0	8	0	0	0	1	0	0	0	1	0	0
Total	0	0	0	331	0	0	28	3	0	0	0	90	0	0

Type of Hacking

1. Mail Bomb Attack
2. PORT Scan attack
3. Internal source IP
4. Unregistered source IP
5. Unsolicited ICMP reply
6. Inconsitent fragmentation
7. Sync Flood Attack
8. LAND attack
9. Ping of death packet
10. ICMP unreachable packet
11. Source route option
12. Address Scan attack
13. Targa/NewTear/Nestea attacl
14. UDP flood attack

of Typical Hacking (Filtered by IDS) (2)



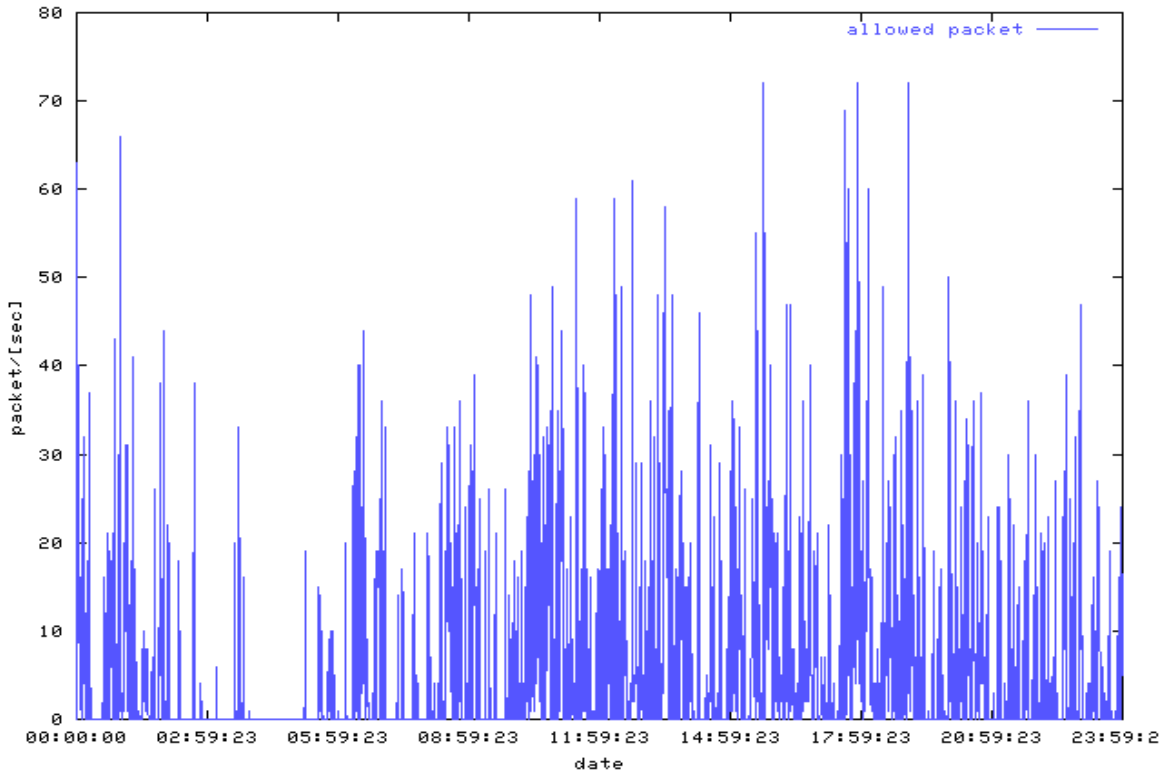
Packet Control (by Firewall) (1)

- **Allowed Packet (Jun. 7th , 2002)**

Allowed Rule ID	# of Allowed Packet
3	37334
5	205078
9	284195
10	0
12	2175
13	0
17	2031

Disallowed Rule ID	# of Disallowed Packet
1	79840

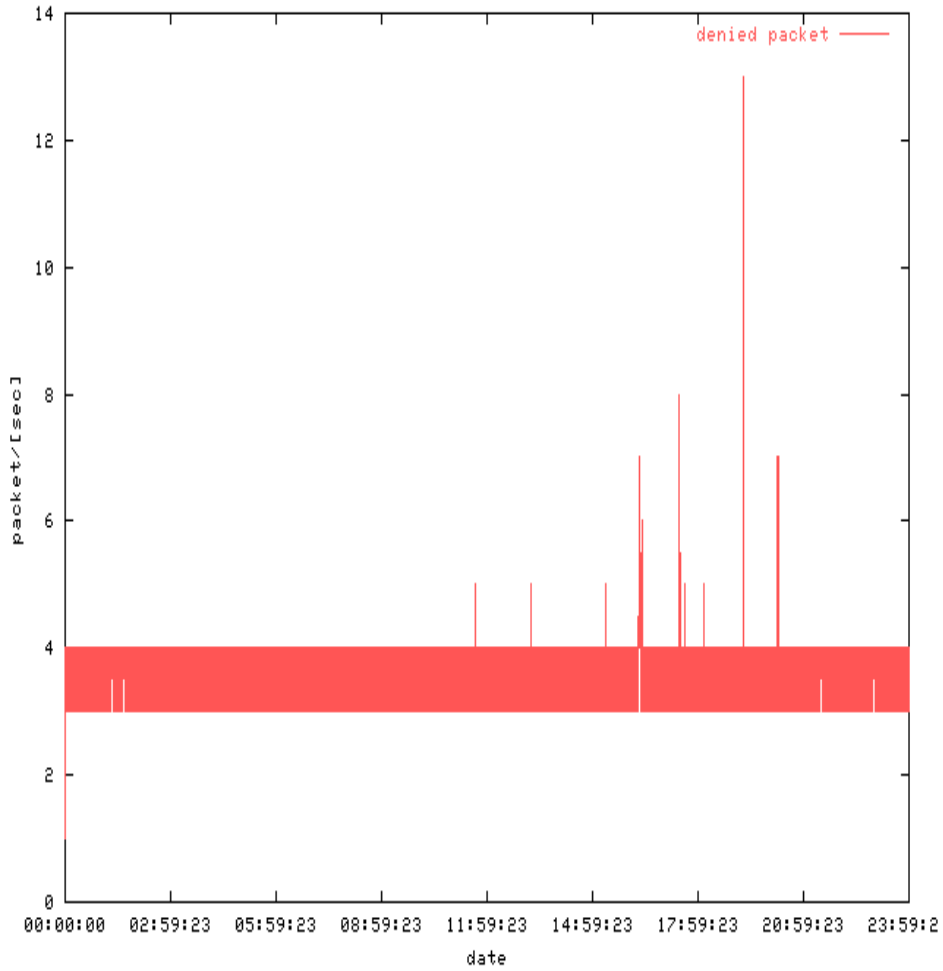
Total Packet	Allowed Packet	Disallowed Packet	Unit
610653	530813	79840	[ea]



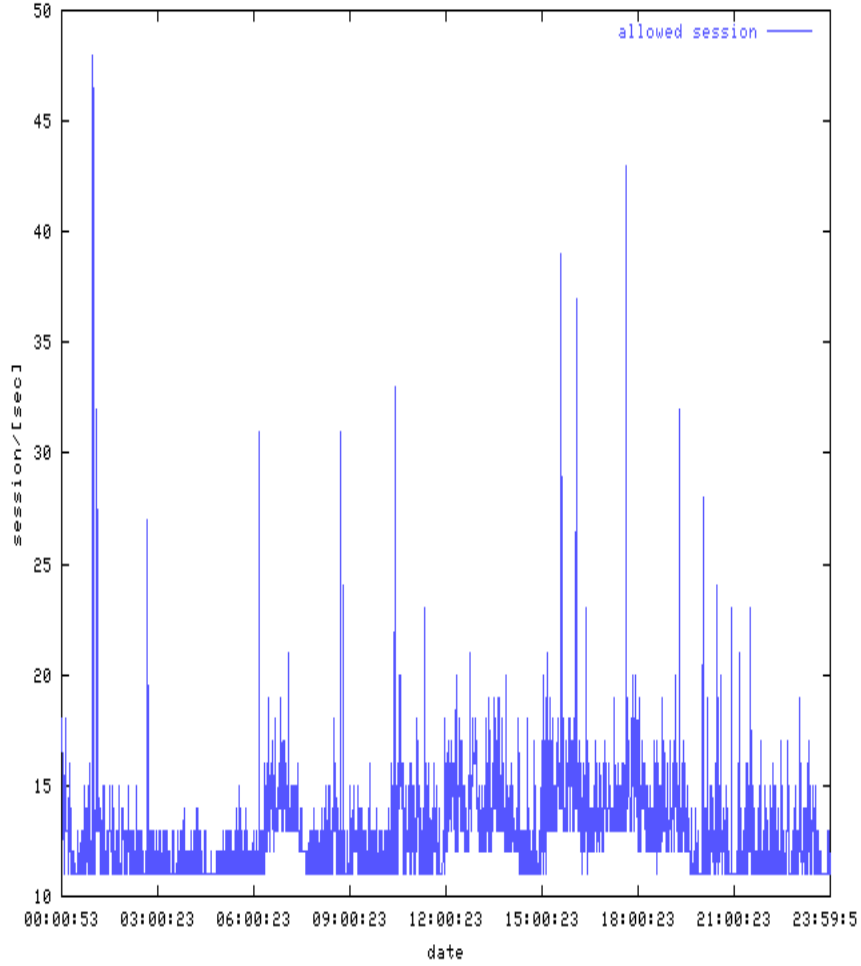
Allowed Packet

Packet Control (by Firewall) (2)

- **Disallowed Packet & Session (Jun. 7th , 2002)**

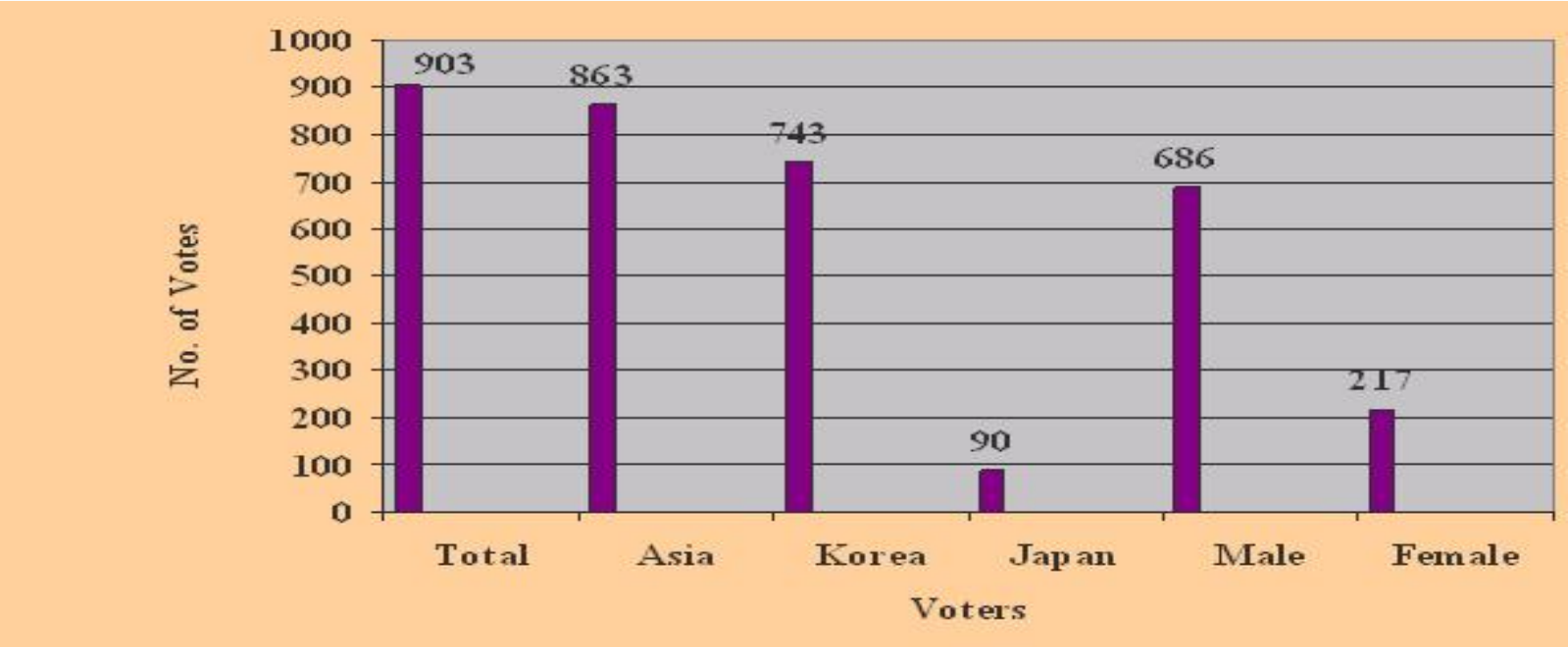


Disallowed Packet



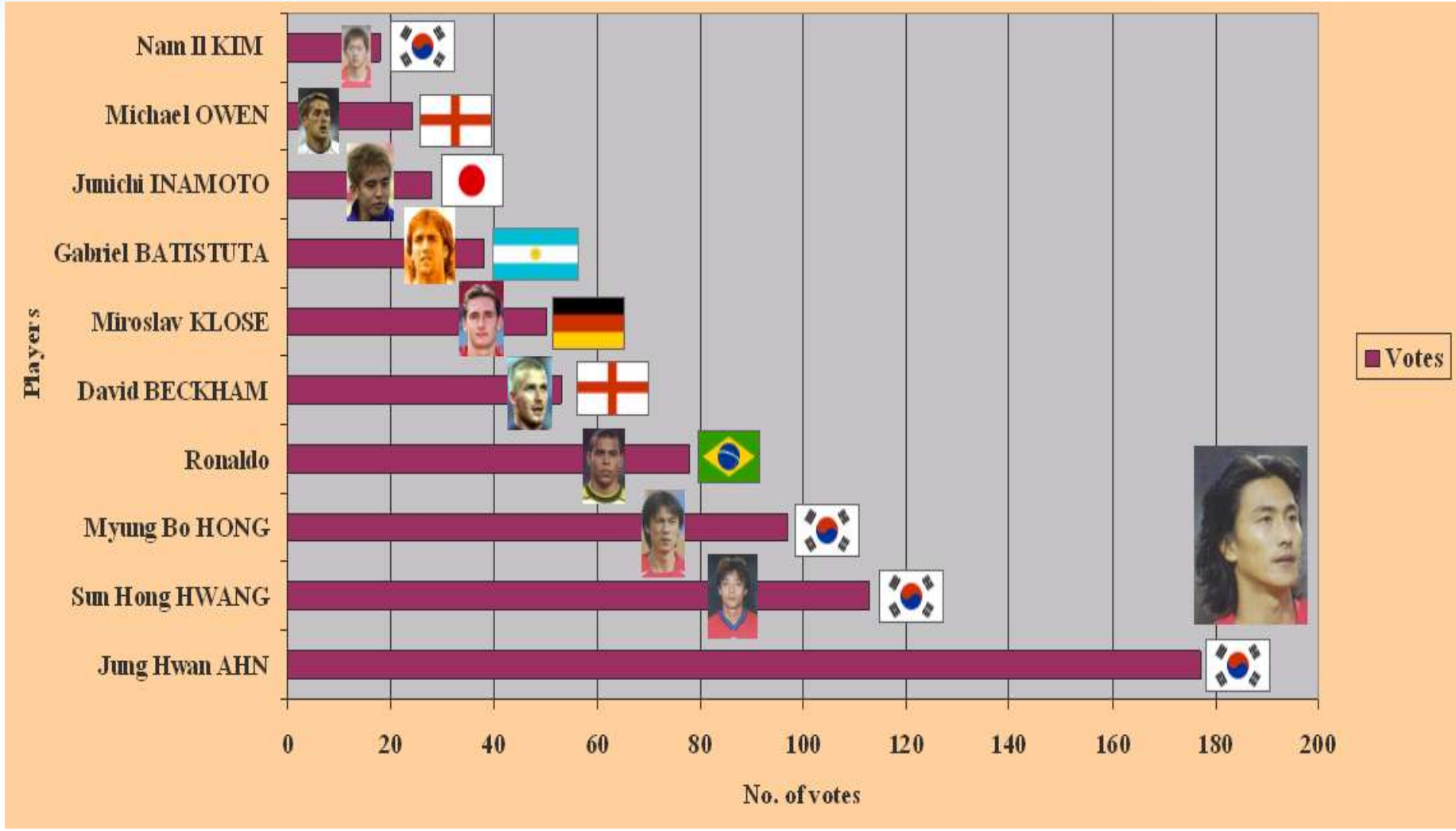
Allowed Session

Statistics of Preliminary voting

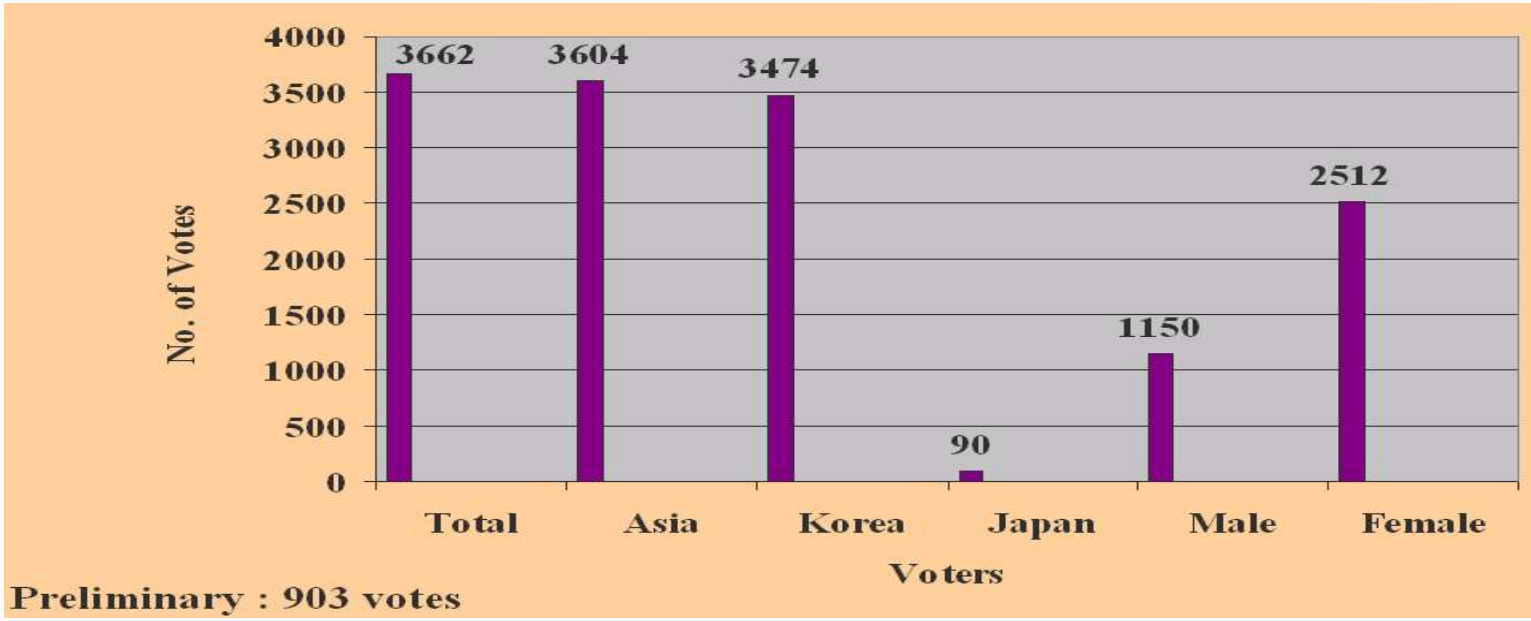


- **Age:**
  - Below 10 yrs: 9 (1.0%), 11~ 20 yrs: 200 (22.1%), 21~30 yrs: 454 (50.3%), 31~40 yrs: 176 (19.5%), 41~50 yrs: 49 (5.4%), 51~60 yrs: 7 (0.8%), Above 61 yrs: 8 (0.9%)
- **Continents:**
  - Asia: 863 (95.6%), Europe: 16 (1.8%), North America: 10 (1.1%), Oceania: 4 (0.4%), South America: 6 (0.7%), Africa: 4 (0.4%)

Top 10 MVPs in Preliminary Voting



Statistics of Main Voting



■ **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%)

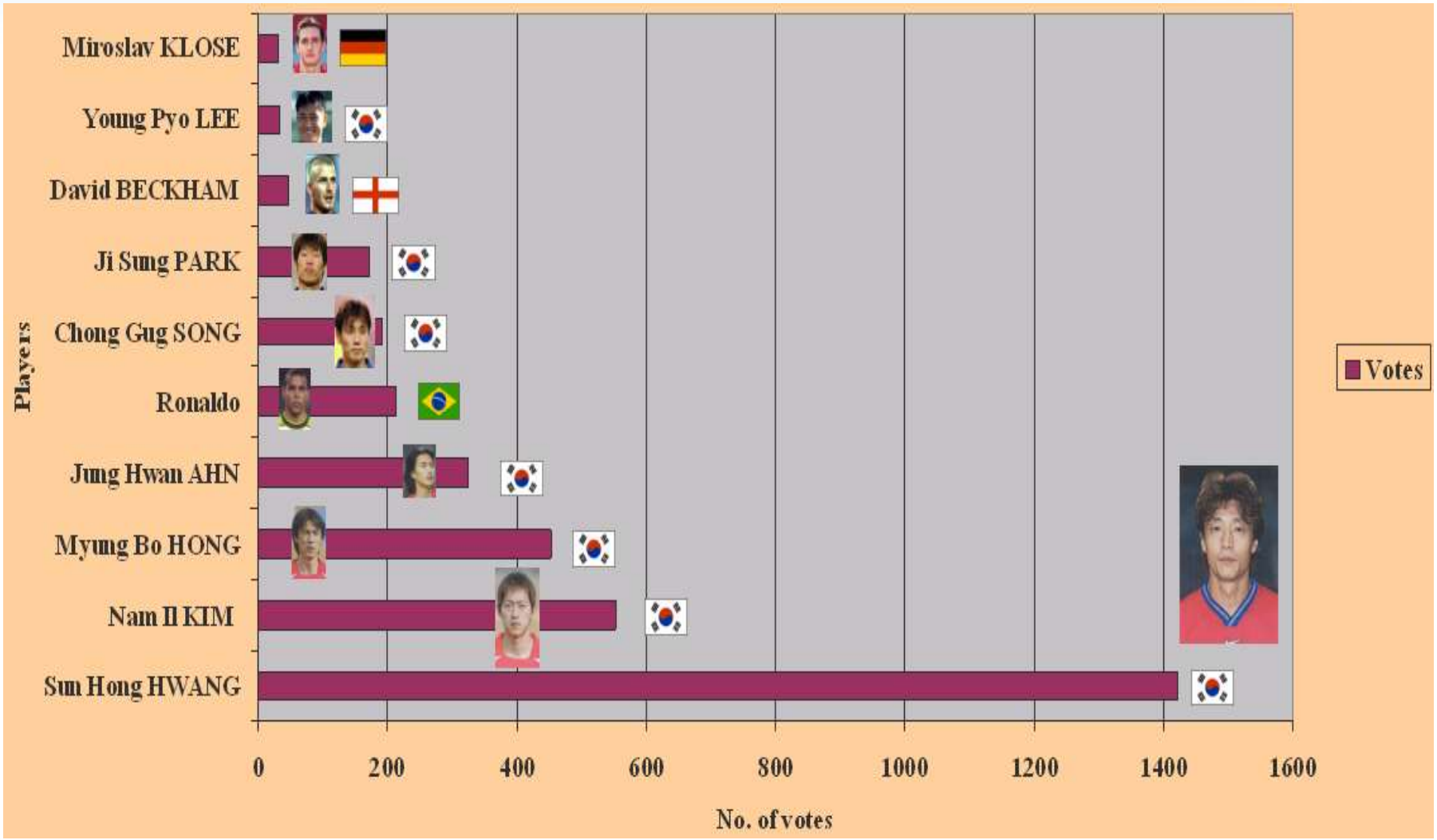
■ **Continents:**

- 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*.

Top 10 MVPs in Main Voting



5. Concluding Remarks

- **Lessons we learned**
  - Need Performance/Security Trade-off
  - Proper anti-Hacking mechanisms with double screening
    - Firewall (H/W), Intrusion Detection System (S/W)
  - S/W Portability
    - Platform independent by Java
  - Hard to meet all the security requirements
  - Multiple voting with different ID's due to weak identification
- **Further Works**
  - Extensions
    - Strong authentication (bio-identification), Mobile Internet voting
    - Pilot project on Absence voting or I-polling by open source
    - Public discussion on security requirements (receipt-freeness, verifiabilility?)
  - Overcome Non-technical Problems (Digital Divide, Political Consensus, legal issue, *etc*.)

Appendix A: E-Voting Research in ICU(1)

- **Receipt-free voting**
  - Byoungcheon Lee and Kwangjo Kim, “Receipt-free Electronic Voting Through Collaboration of Voter and Honest Verifier”, Proceeding of JWISC2000, pages 101-108, Okinawa, Japan, Jan. 25-26, 2000.
  - Byoungcheon Lee and Kwangjo Kim, "Receipt-free electronic voting scheme with a tamper-resistant randomizer", ICISC2002, LNCS 2587, pp. 389-406, Springer-Verlag, 2002.
  - Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, Jeongmo Yang and Seungjae Yoo, "Providing Receipt-Freeness in Mixnet-Based Voting Protocols", *ICISC 2003*, LNCS 2971, pp. 245--258. Springer-Verlag, 2003.
  - Riza Aditya, Byoungcheon Lee, Colin Boyd and Ed Dawson, "An Efficient Mixnet-Based Voting Scheme Providing Receipt-Freeness", *Trustbus 2004*, LNCS 3184, pp. 152--161. Springer-Verlag, 2004.

E-Voting Research in ICU(2)

- **Implementation issue**
  - Riza Aditya, Byoungcheon Lee, Colin Boyd, Ed Dawson, "IMPLEMENTATION ISSUES IN SECURE E-VOTING SCHEMES", The 5-th Asia-Pacific Industrial Engineering and Management Systems Conference (APIEMS 2004), ANA Hotel, Goldcoast, Australia, Dec. 12-15, 2004.
- **Real world voting**
  - Kwangjo Kim, Jinho Kim, Byoungcheon Lee, and Gookwhan Ahn, "Experimental Design of Worldwide Internet Voting System using PKI", SSGRR2001, L'Aquila, Italy, Aug. 6-10, 2001.
  - Kwangjo Kim, Jinho Kim, and Byoungcheon Lee, "No More Panic in Florida: Reality or Dream?", Rump Session of Crypto2001, UCSB, Aug. 21, 2001.
  - Kwangjo Kim, "Experiences of Internet voting based on PKI", International Conference on Number Theory for Secure Communications, SASTRA Deemed University, India, 2003.12.20~12.21
  - Kwangjo Kim, "Killer Application of PKI to Internet Voting", Proc. of IWAP2002, Taipei, Taiwan, Oct 30- Nov.1 2002.
  - Kwangjo Kim, "Lessons from Internet voting during 2002 FIFA WorldCup Korea/Japan(TM)",
    DIMACS Workshop on Electronic Voting - Theory and Practice
    Rugters Univ, NJ, USA. May 26 - 27,2004

App. B: Int'l Collaboration in secure E-voting

- **VOTOPIA project with NTT, U. of Tokyo, Japan**
  - Prof. Imai/Dr. Okamoto, 2001.4~
  - E-voting experiment during 2002 FIFA WorldCup Korea/Japan™
- **Collaboration with QUT, Australia**
  - Prof. Byoungcheon Lee, 2003.7.~2004.6.
  - E-voting research
- **Collaboration with MIT, USA**
  - Prof. Kwangjo Kim, 2005.3.~2005.5.
  - MIT-CALTECH e-voting project

Thank you for your attention

Q&A