PopVote Security & Privacy

Mr. Jazz MA
(IT Manager of Public Opinion Programme)

PopVote

- Topic: CE Election on 25 March
- On-site
  - Voting station

PopVote

- Off-site
  - Website, Mobile

Available on the App Store

ANDROID APP ON Google play

Risk

- Open to public
- Allow public trial
  - 1st stage: 16th – 20th March 2012
  - 2nd stage: 21st March 2012

ID card no. + SMS verification

Protection

- SSL authentication & encryption
- ID & Phone number hashing (SHA-512)
- Virtual keyboard
- CAPCHA validation code

Cloud servers

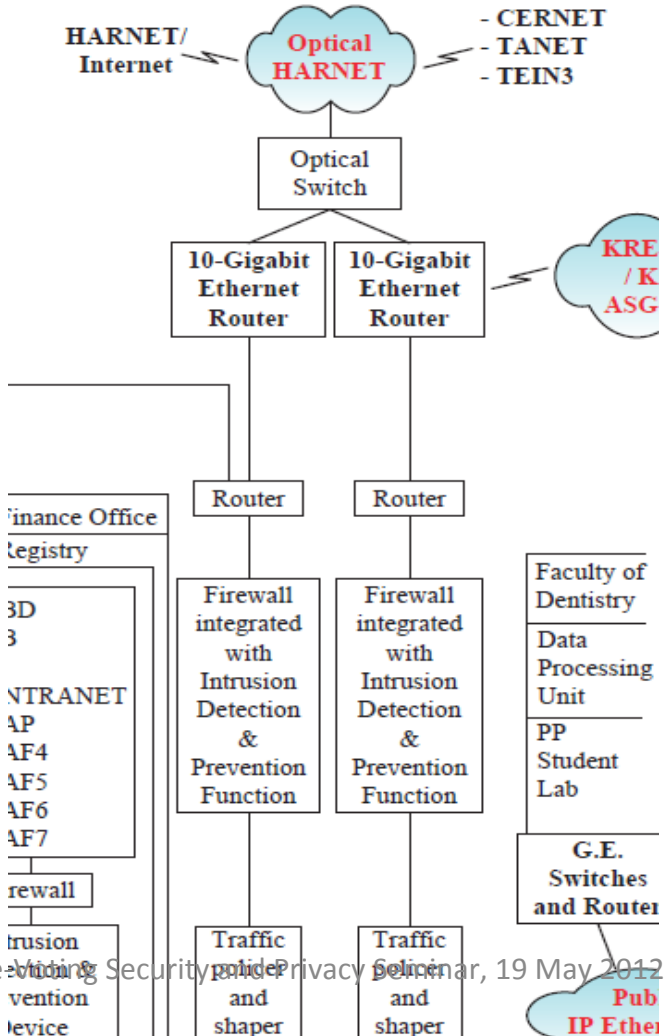
- Off-site request (website, mobile)

Cloud Resources /
Virtual IT Servers

Physical servers

- On-site request (station)

Firewall & IPS

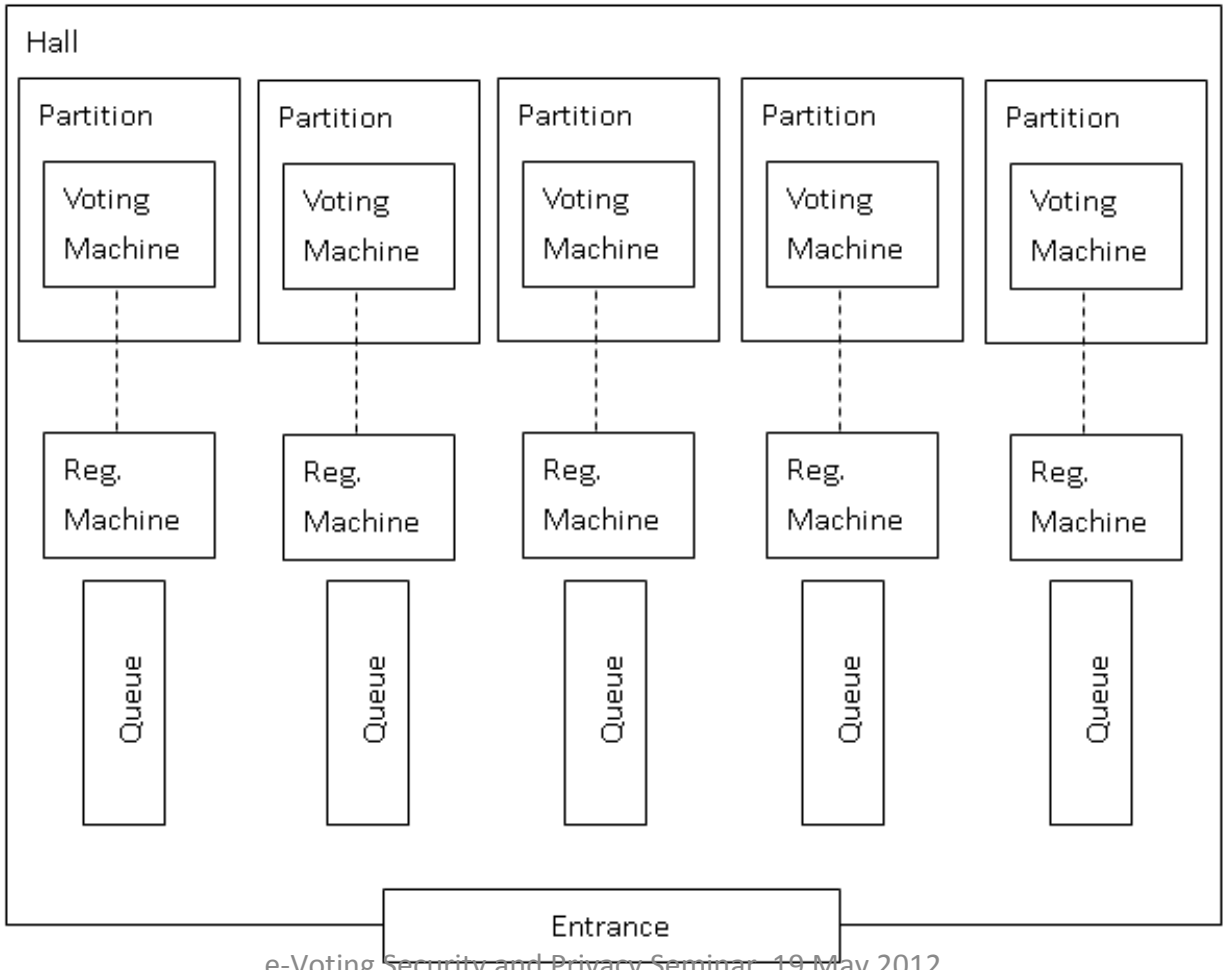


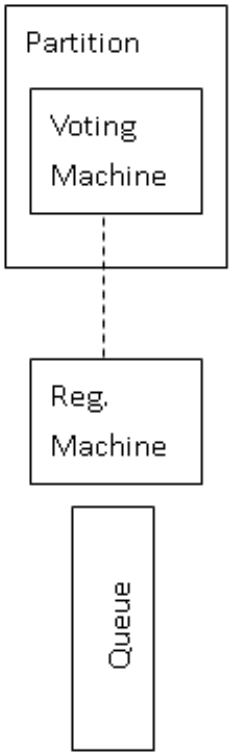
Flow of voting

Flow of voting

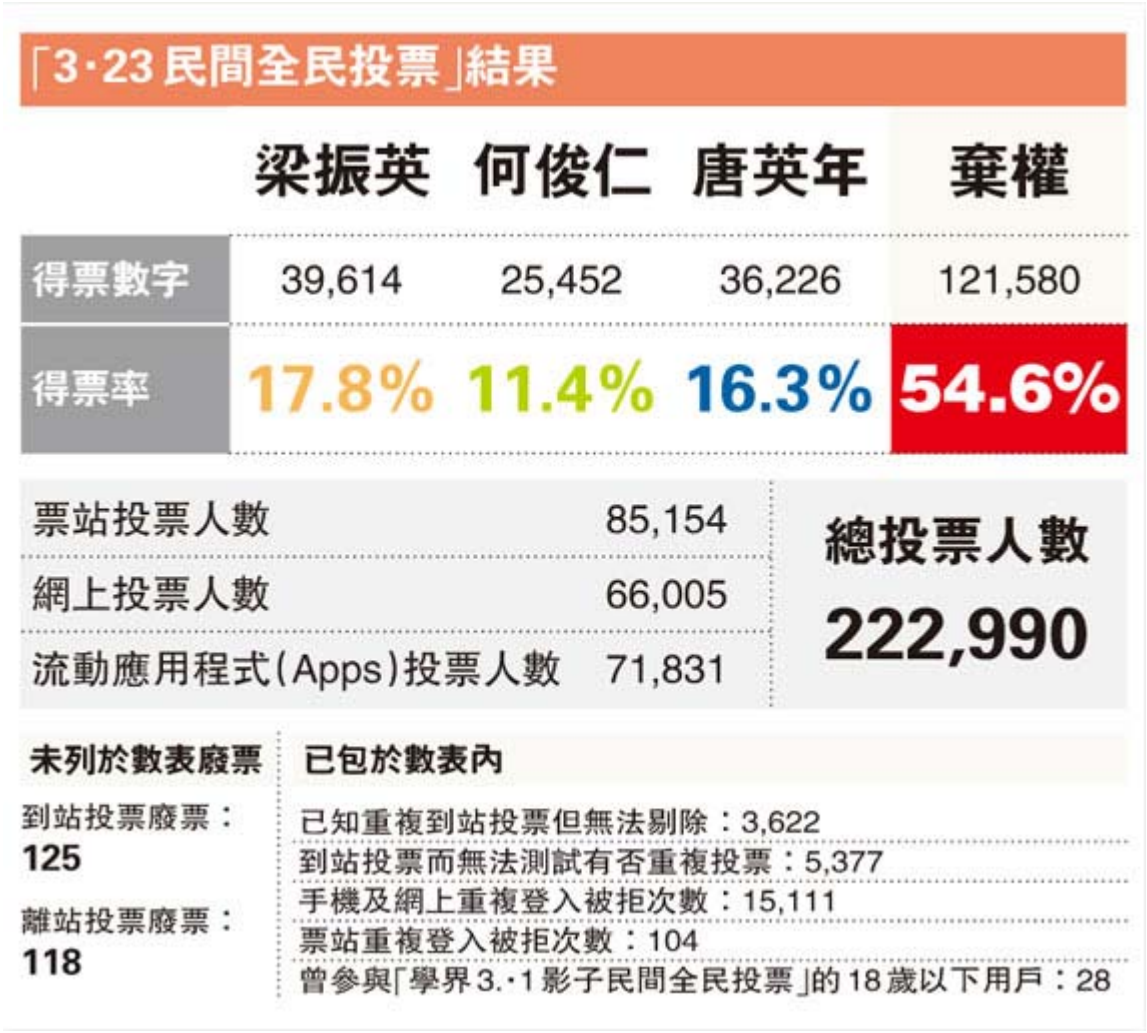
Flow of voting

Voting station




Partition
Voting Machine
Reg. Machine
Queue

- Total number of voters: 222,990
  - Onsite voters: 85,154
  - Offsite website voters: 66,005
  - Offsite mobile app voters: 71,831



「3·23民間全民投票」結果

	梁振英	何俊仁	唐英年	棄權
得票數字	39,614	25,452	36,226	121,580
得票率	17.8%	11.4%	16.3%	54.6%

票站投票人數	85,154
網上投票人數	66,005
流動應用程式(Apps)投票人數	71,831

總投票人數
222,990

未列於數表廢票

到站投票廢票：
125

離站投票廢票：
118

已包於數表內

已知重複到站投票但無法剔除：3,622
到站投票而無法測試有否重複投票：5,377
手機及網上重複登入被拒次數：15,111
票站重複登入被拒次數：104
曾參與「學界3.·1影子民間全民投票」的18歲以下用戶：28

Image from MingPao

Battle & Analysis

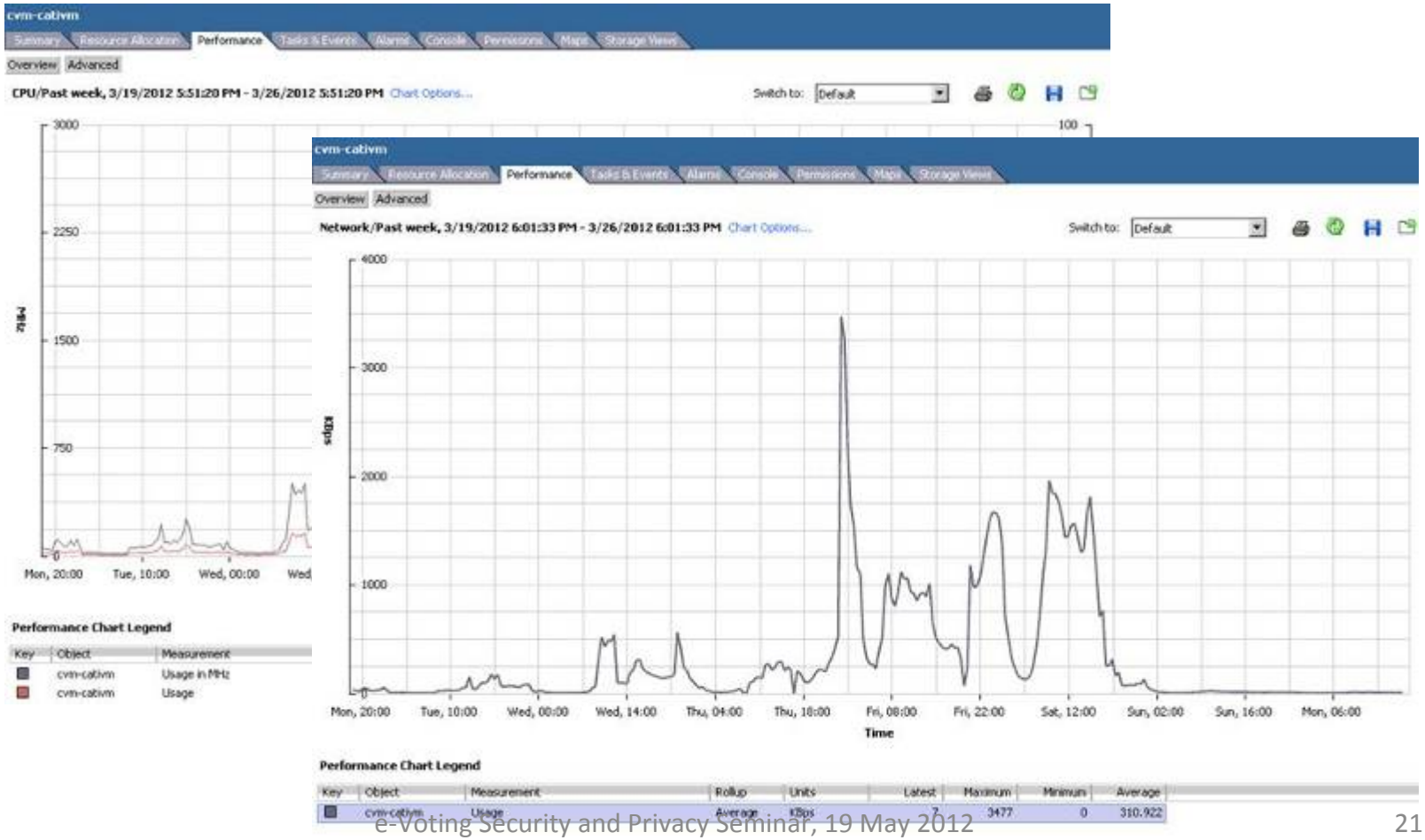
Mr. Jazz MA
IT Manager of Public Opinion Programme

Mr. Kenneth LAM
Manager, Research and Development
3TECH Engineering Limited

Pictures from AppleDaily

Pictures from HKUPOP

Pictures from HKUPOP


cvm-cativm
Summary
Resource Allocation
Performance
Tasks & Events
Alarm
Console
Permissions
Maps
Storage Views
Overview
Advanced
CPU/Past week, 3/19/2012 5:51:20 PM - 3/26/2012 5:51:20 PM
Chart Options...
Switch to:
Default
3000
2250
1500
750
0
MHz
Mon, 20:00
Tue, 10:00
Wed, 00:00
Performance Chart Legend
Key
Object
Measurement
cvm-cativm
Usage in MHz
cvm-cativm
Usage
cvm-cativm
Summary
Resource Allocation
Performance
Tasks & Events
Alarm
Console
Permissions
Maps
Storage Views
Overview
Advanced
Network/Past week, 3/19/2012 6:01:33 PM - 3/26/2012 6:01:33 PM
Chart Options...
Switch to:
Default
4000
3000
2000
1000
0
KBps
Mon, 20:00
Tue, 10:00
Wed, 00:00
Wed, 14:00
Thu, 04:00
Thu, 18:00
Fri, 08:00
Fri, 22:00
Sat, 12:00
Sun, 02:00
Sun, 16:00
Mon, 06:00
Time
Performance Chart Legend
Key
Object
Measurement
Rollup
Units
Latest
Maximum
Minimum
Average
cvm-cativm
Usage
Average
KBps
7
3477
0
310.922

Battle

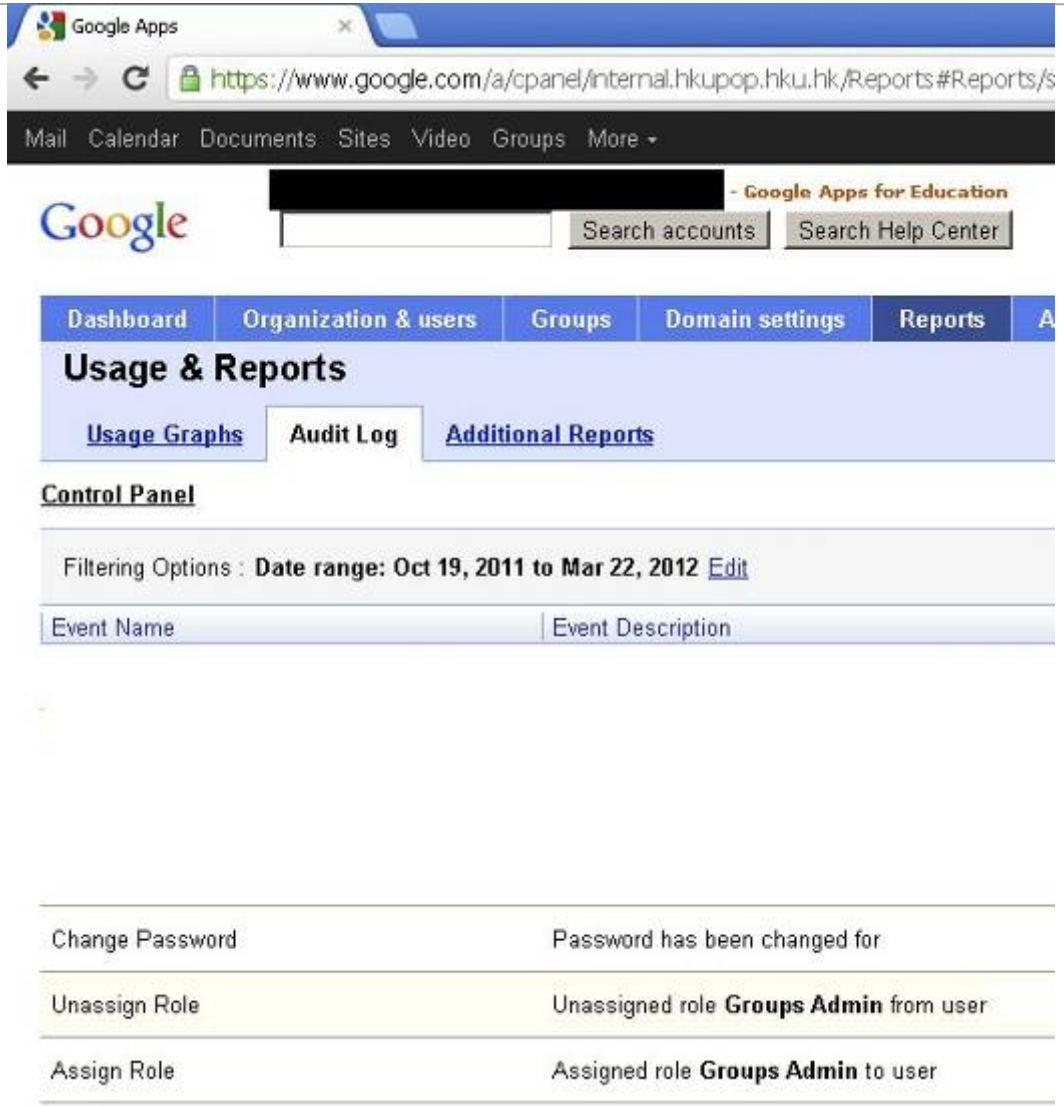
- Suspected DDoS
- 21st March 2012
- 3:52PM
- Over 1million packets

Battle

- Blocked foreign access at ISP level

Battle

- Email accounts being compromised
- 22nd March 2012
- 10:00AM & 8:00PM



Google Apps – Domain management – Reports

Battle

- Email spoofing & virus spreading
- 23rd March 2012
- Attachment :
  “「3.23民間全民投票」階段投票結果.rar”

Battle

- Traced the source from email header

Battle

- Suspected DDoS
- 23rd March 2012

Battle

- Downtime
- 23rd March 2012
- 07:00 – 21:00

Battle

- Checking: Programme code
- Checking: System log analysis
- Action: Block suspected IP
- Action: System optimization
- Other Action: IGP IP Black Hole

Checking: Programme Code

- Review system page flow / data flow
- Quick check of critical (slow) steps
- Identify potential attack points in the system
- Check system log and related source code
- Fine tune program (update source code)

Checking: System Log Analysis

Objective

- Identify problems
- Find attacking source

Checking: System Log Analysis

Log files

- Voting system log
- Web server access log
- Web server error log

Action: Block suspected IP

- Based on the finding of the log checking
- Identified IP addresses
- Block

Action: System Optimization

- Optimize program to reduce loading
- Remove graphic files from the voting pages
- Web server session and connection limit
- Database server optimization
- Update server firewall
- Add new servers to serve on-site voting station

Other Action: IGP IP Black Hole

- Update DNS
- Apply filtering at DNS lookup state
- Not reply IP lookup result to overseas query
- Since HKU Computer Centre has blocked the overseas access, the IGP IP Black Hole service is not used

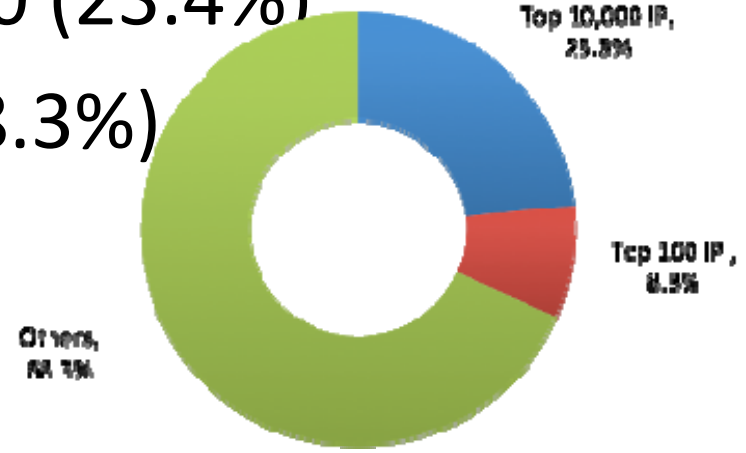
After 24th March, 2012

Web Access Log Analysis

- Hints of DoS attack
  - a large amount of accesses
  - small packet size, exhaust the connection limits
  - a bot running script, so the user agent may not be any browser, e.g. "-"

Web Access Log Analysis

- Total no. of accesses (off-site)
- 23-Mar-2012 & 24-Mar-2012
- Total = 22,441,681 (22.4 million)
- Top 10,000 IP = 5,240,010 (23.4%)
- Top 100 IP = 1,869,722 (8.3%)



Web Access Log Analysis

- Top 1 = 243,174 access
- Acunetix scanner scanning

Web Access Log Analysis

- 1,335,577 access (5.951%) has **size= "-"** (i.e. 0 bytes)
- Attack?
- Congestion?

Web Access Log Analysis

- If useragents is “-“, count=664,199
- Proxy?

e-Voting Challenges

e-Voting Challenges

- Design
- Risks Assessment
- Implementation
- Testing
- Production Environment

Thank You