Technical Overview

David Chaum
Outline of Presentation

• Concept
  (for basic SureVote version)
• User Interface Options
  (and their implications)
• Process Flow Detail
  (multi-server case)
• Variations & Extensions
  (offline, non-geographic, exit devices, control votes, ballot-style security, single-server, etc.)
Simple SureVote Ballot

Ballot #: 52234

<table>
<thead>
<tr>
<th>FEDERAL</th>
<th>FEDERAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRESIDENT AND VICE PRESIDENT OF THE UNITED STATES</td>
<td>UNITED STATES REPRESENTATIVE (CONGRESS) DISTRICT 16</td>
</tr>
<tr>
<td>GEORGE W. BUSH &amp; DICK CHENEY (REPUBLICAN)</td>
<td>MARK FOLEY (REPUBLICAN)</td>
</tr>
<tr>
<td>VOTE CODE: 5216</td>
<td>VOTE CODE: 6965</td>
</tr>
<tr>
<td>SURE CODE: 4784</td>
<td>SURE CODE: 4104</td>
</tr>
<tr>
<td>PAT BUCHANAN &amp; EZOLA FOSTER (REFORM)</td>
<td>JEAN ELLIOTT BROWN (DEMOCRATIC)</td>
</tr>
<tr>
<td>VOTE CODE: 2947</td>
<td>VOTE CODE: 9794</td>
</tr>
<tr>
<td>SURE CODE: 7095</td>
<td>SURE CODE: 5772</td>
</tr>
<tr>
<td>AL GORE &amp; JOE LIEBERMAN (DEMOCRATIC)</td>
<td>JOHN McGuire (REFORM)</td>
</tr>
<tr>
<td>VOTE CODE: 5813</td>
<td>VOTE CODE: 7047</td>
</tr>
<tr>
<td>SURE CODE: 7159</td>
<td>SURE CODE: 6927</td>
</tr>
</tbody>
</table>

SURE CODE: 4104
Overall Process (overview)
What are the main reasons SureVote is so interesting?

• No machines to trust at precinct!
  – Much higher integrity
  – Much lower cost

• Voter authenticates system and choice!
  – More accuracy
  – Higher voter confidence

• Integrated attendance and remote

• Non-Geographic and permissive voting
User Interface Examples

• Web browser
  (which contests revealed UI)

• Barcode

• Telephone
  (number of contests revealed to UI)

• Human Intermediary

• Touchscreen
  (choices must be revealed to UI)
Web

Ballot #: 78694

<table>
<thead>
<tr>
<th>President and Vice President of the United States</th>
<th>United States Representative (Congress) District #16</th>
</tr>
</thead>
<tbody>
<tr>
<td>George W. Bush &amp; Dick Cheney (Republican)</td>
<td>Mark Foley (Republican)</td>
</tr>
<tr>
<td>Pat Buchanan &amp; Ezola Foster (Reform)</td>
<td>Jean Elliot Brown (Democratic)</td>
</tr>
<tr>
<td>Al Gore &amp; Joe Liberman (Democratic)</td>
<td>John McGuire (Reform)</td>
</tr>
</tbody>
</table>

Vote Code: 2304
Sure Code: 1698
**Federal**

President and Vice President of the United States

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Vote Code</th>
<th>Sure Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>George W. Bush &amp; Dick Cheney</td>
<td>2304</td>
<td>1698</td>
</tr>
<tr>
<td>(Republican)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pat Buchanan &amp; Ezola Foster</td>
<td>7406</td>
<td>2425</td>
</tr>
<tr>
<td>(Reform)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Al Gore &amp; Joe Lieberman</td>
<td>8991</td>
<td>8753</td>
</tr>
<tr>
<td>(Democratic)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Telephone

(Remote or Attendance Voting)

NEXT VOTE

Get Digits
(If no action is taken increment User_Error_Counter)

9999

increment User_Error_Counter

5006 You have entered Vote-Code.... V-V-V-V.
(Accept only # and * during play)

5003 If this is correct press #.
(Accept only # and * during play)

5007 -- if not, please enter Vote-Code again now.

increment User_Error_Counter

5001 You have entered an invalid Vote-Code, please try again.

increment Fraud_Error_Counter

Fraud_Error_Counter < Fraud_Error_Limit-1

5011 The sure-code is: SSSS

Play VoteTONE

Reset Fraud_Error_Counter, User_Error_Counter
Set VoteReviewCounter = votesCompleted * 7

Votes_completed > 1 and Votes_Completed < Total_Votes

Votes_completed > 1 and Votes_Completed = Total_Votes

5009 To review your voting, press star *.
Otherwise, please enter the Vote-Code for your next vote. If finished voting, press pound #.

5012 You have now cast a vote for every office on your ballot. To review your voting, press star *.
If finished voting, press pound #.

# Key pressed during play back of sure-code should repeat sure-code.

REVIEW VOTES

END VOTING
**Human Intermediary**

- Unlike “Assisted Voting”
  - No integrity/influencing vulnerability
  - No privacy exposure
- Expands access
  - Beyond usual disability definition
  - Also includes illiterates
### Touchscreen

**President and Vice President of the United States**

- **George W. Bush & Dick Cheney** (Republican)
- **Pat Buchanan & Ezola Foster** (Reform)
- **Al Gore & Joe Lieberman** (Democratic)
Process Overview

1. Ballot preparation—for all ballots
   - Committing, printing, checking
2. Voting—for each ballot [not detailed]
   - Exchanging SureCodes for VoteCodes
3. Tabulating—for all voted ballots
   - Two passes through trustees, checking
1. Ballot Preparation

i. Commitments to codes are published
   – Pins created by each trustee
   – Shift amounts created by each trustee
   – Trustees each publish commits to all values

ii. Printing of paper ballots
   – Trustees furnish values to printer
   – Printer combines (addition modulo max value)
   – Printer prints codes “rotated” by shift amount

iii. Checking ballots & commitments
   – “Auditors” choose ballots to open at random
   – Trustees open commitments for opened ballots
   – Auditors check consistency
3. Tabulating

i. Computing and publishing proofs
   - Entire batch passes through trustees twice
   - First phase: trustees add in two exponents, one for shift (different per item) one for encryption (same for all items) [no mixing]
   - Second phase: trustees remove encryption exponent and output batch in permuted order [mixing]

ii. Checking proofs
   - Verify that the ballot images output correspond to the originally committed ballots and committed votes
Variations & Extensions

• re-tally
• Online/offline attendance voting
• Non-Geographic
• Write-in and type-in
• Scratch-off printing
  – Indelible ballots
  – Self-shredding ballots
• Control votes & exit devices
• Single & multiple server applications
Re-tally

• Example uses:
  – Permissive registration/contested ballot
  – Court ordered inclusion/exclusion
    (formerly required spoiling precinct)
Non-Geographic

• Example uses of “one big precinct”
  – Early voting (e.g., countywide)
  – Absentee ballot
  – Attendance at non-home precinct
Demand-Printed Ballot

Lois Capps
Barbara Lee
David Dreier
Maxine Waters

9574 6456
Indelible Ballots

Lois Capps 5
Barbara Lee 1
David Dreier 4
Maxine Waters 8

Lois Capps 5
Barbara Lee 1
David Dreier 9574 6456
Maxine Waters 8
Self-Shredding Ballots

Once arrows are scratched off to reveal numbers, choice is permanently destroyed.
|   | A   | B   | C   | D   | E   | F   | G   | H   | I   | J   | K   | L   | M   | N   | O   | P   | Q   | R   | S   | T   | U   | V   | W   | X   | Y   | Z   |
|---|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 7435 | 6583 | 9474 | 3608 | 4765 | 3235 | 6863 |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 8763 | 5643 | 7548 | 7805 | 5427 | 0765 | 4534 |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 6355 | 0654 | 0966 | 8653 | 2595 | 9643 | 8768 |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 8765 | 4673 | 4367 | 6658 | 3409 | 9054 | 6435 |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 9574 | 5645 | 5465 | 4565 | 3443 | 5645 | 4534 |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 6456 | 5465 | 4565 | 5465 | 6544 | 6544 | 3454 |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 5445 | 4876 | 5435 | 1018 | 7654 | 3246 | 4324 |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 9573 | 7653 | 3486 | 0187 | 0865 | 3454 | 3423 |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
Write-In

BALLOT #: 9375343

John Doe

Jose Smith

Write-In

Mandatory Code: W□□□□

Write-In Candidate Name

9574
6456
W345
Ballot-Style Security

• You can take your ballot home!
  – Shredding also possible
Cast/Spoilt Control Votes

- Control votes can lock a ballot
- Control vote can make a ballot spoilt
Counterfoil Printer
Example Exit Device

Before

After
Single-Server System
Multiple-Server Configuration Options

• **Each political party has server**
  – e.g., Democrats, Republicans, etc.

• **Government hierarchy of servers**
  – County has its own server(s)
  – State & Federal can too

• **Monitoring countries have servers**
  – Critical emerging country elections
Conclusion

• Higher integrity & confidence
• Lower cost
• Robust
• Attendance & Remote in real-time
• Non-Geographic
• Permissive re-tally
• Multi-server