Prerendered User Interfaces
for
Higher-Assurance Electronic Voting

Ka-Ping Yee
accessibility folks

computers = flexible

security folks

computers = vulnerable
accessibility folks

electronic voting = empowerment

security folks

electronic voting = hazard
1 Accessibility vs. security.
vendors

transparency = liability

security folks

transparency = reliability
1 Accessibility vs. security.
2 Proprietary interests vs. transparency.
Insert Card to Begin Voting
AccuVote TS

MFC

Windows CE

> 31 000 lines of C++

{ millions of lines of C++ }
1 Accessibility vs. security.
2 Proprietary interests vs. transparency.
3 Too much code to verify.
AccuVote TS

- > 31 000 lines of C++
- election rules
- ballot layout
- visual style
1. Accessibility vs. security.
2. Proprietary interests vs. transparency.
3. Too much code to verify.
4. Code changes too frequently.
Paper Voting

- Election office
- Design
- Paper ballot
  - Cast
  - Anonymous marked ballots
  - Tally
- Election results

Voter
Paper Voting

1. Voter
2. Election Office
3. Design
4. Paper Ballot
5. Cast
6. Anonymous Marked Ballots
7. Tally
8. Election Results
Electronic Voting

voter

election office

computer

ballot definition

DRE device

vote records

computer

election results

ballot design software

DRE voting software

vote tallying software

source

compiler

libraries

source

compiler

libraries

source

compiler

libraries
Electronic Voting

- Voter
- DRE device
- Ballot definition
- Vote records
- Computer
- Election office

- Ballot design software
- DRE voting software
- Vote tallying software
- Compiler
- Libraries
- Source
Anonymous vote records

Election office

Computer

Ballot definition

Voter

DRE device

Anonymous vote records

DRE voting software

Published in advance

Computer

Vote tallying software

Published after election

Election results

Source

Compiler

Libraries

Source

Compiler

Libraries
Electronic Voting

Voter

DRE device

Naveen Sastry
hardware isolation

Ka-Ping Yee
prerendered user interface

ballot definition

anonymous vote records

DRE voting software

David Molnar
anonymous, tamper-evident ballot storage

Arel Cordero
random selection for auditing

election results
Conventional Ballot Definition

<table>
<thead>
<tr>
<th>Contest</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>title</td>
<td>Mayor</td>
</tr>
<tr>
<td>max selections</td>
<td>1</td>
</tr>
<tr>
<td>options</td>
<td>Tom Bates</td>
</tr>
<tr>
<td></td>
<td>John Boushell</td>
</tr>
<tr>
<td></td>
<td>Shirley Dean</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contest</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>title</td>
<td>School Board</td>
</tr>
<tr>
<td>max selections</td>
<td>2</td>
</tr>
<tr>
<td>options</td>
<td>Karen Hemphill</td>
</tr>
<tr>
<td></td>
<td>Merrilee Mitchell</td>
</tr>
<tr>
<td></td>
<td>Joaquin Rivera</td>
</tr>
<tr>
<td></td>
<td>Kalima Rose</td>
</tr>
<tr>
<td></td>
<td>John Selawsky</td>
</tr>
</tbody>
</table>

UI widgets

font data

layout manager

text renderer

---

2006 General Election, City of Berkeley, California
November 2, 2006

**Mayor** (page 1 of 1)
This contest has 4 boxes. Choose ONE box.
Touch a box to select or deselect.

- Tom Bates
- John Boushell
- Shirley Dean
- write in a candidate

Your ballot is not yet recorded. Press NEXT PAGE to continue or REVIEW AND FINISH to review your choices and cast your ballot.

PREVIOUS PAGE  NEXT PAGE  CLEAR THIS CONTEST  REVIEW AND FINISH
Mayor (page 1 of 1)

This contest has 4 boxes. Choose ONE box.

Touch a box to select or deselect.

- Tom Bates
- John Boushell
- Shirley Dean
- write in a candidate

Your ballot is not yet recorded. Press NEXT PAGE to continue or REVIEW AND FINISH to review your choices and cast your ballot.
Prerendered Ballot Page

Mayor (page 1 of 1)

This contest has 4 boxes. Choose ONE box.

Touch a box to select or deselect.

- Tom Bates
- John Boushell
- Shirley Dean
- write in a candidate

Your ballot is not yet recorded. Press NEXT PAGE to continue or REVIEW AND FINISH to review your choices and cast your ballot.

PREVIOUS PAGE NEXT PAGE CLEAR THIS CONTEST REVIEW AND FINISH
options

- Tom Bates
- John Boushell
- Shirley Dean

Your ballot is not yet recorded. Press NEXT PAGE to continue or REVIEW AND FINISH to review your choices and cast your ballot.
Prerendered Ballot Page

Mayor (page 1 of 1)

This contest has 4 boxes. Choose ONE box.

Touch a box to select or deselect.

- Tom Bates
- John Boushell
- Shirley Dean

- write in a candidate

Your ballot is not yet recorded. Review your choices and cast your ballot.

PREVIOUS PAGE | NEXT PAGE | CLEAR THIS CONTEST | REVIEW AND FINISH
Write-in Candidate for Mayor

Use the keyboard above to enter the name of the candidate you wish to write in. Press ACCEPT to vote for this candidate or CANCEL to not vote for this candidate.
Write-in Subpage

character entry
subtargets

Write-in Candidate for Mayor

Use the keyboard above to enter the name of the candidate you wish to write in. Press ACCEPT to vote for this candidate or CANCEL to not vote for this candidate.
Write-in Subpage

Write-in Candidate for Mayor

Use the keyboard above to enter the name of the candidate you wish to write in. Press ACCEPT to vote for this candidate or CANCEL to not vote for this candidate.
Write-in Subpage

2006 General Election, City of Berkeley, California

Write-in Candidate for Mayor

Q W E R T Y U I O P -
A S D F G H J K L |
Z X C V B N M

CLEAR

Wed / backspace
subtargets

Use the keyboard above to enter the name of the candidate you wish to write in. Press ACCEPT to vote for this candidate or CANCEL to not vote for this candidate.

CANCEL THIS WRITE-IN

ACCEPT THIS WRITE-IN
Write-in Subpage

cancel / accept subtargets
Write-in Candidate for Mayor

Use the keyboard above to enter the name of the candidate you wish to write in. Press ACCEPT to vote for this candidate or CANCEL to not vote for this candidate.
Prerendered Ballot Page

Mayor (page 1 of 1)

This contest has 4 boxes. Choose ONE box.

Touch a box to select or deselect.

- Tom Bates
- John Boushell
- Shirley Dean

MARIE CURIE

Your ballot is not yet recorded. Press NEXT PAGE to continue or REVIEW AND FINISH to review your choices and cast your ballot.
Prerendered Ballot Page

character slots

write-in

Mayor (page 1 of 1)

Touch a box to select or deselect.

- Tom Bates
- John Bouchell
- Shirley Dean

Your ballot is not yet recorded. Press NEXT PAGE to continue or REVIEW AND FINISH to review your choices and cast your ballot.

PREVIOUS PAGE  NEXT PAGE  CLEAR THIS CONTEST  REVIEW AND FINISH
Your ballot is not yet recorded. Touch any box to change your selection for that contest or measure, or press NEXT PAGE to continue reviewing your choices.
Prerendered Ballot Page

Review Your Selections (page 1 of 2)

Mayor
(vote for 1)

School Board
(vote for up to 2)

no selection has been made

✔ Tom Bates

no selection has been made

no selection has been made

Your ballot is not yet recorded. Touch any box to change your selection for that contest or measure, or press NEXT PAGE to continue reviewing your choices.

PREVIOUS PAGE   NEXT PAGE
Ballot Definition Format

ballot model
- contest
  - int max_sels
  - int max_chars
- subpage
  - subtarget
    - int action
- page
  - target
    - int action
    - int page_i
    - int contest_i
  - option
    - int contest_i
  - write-in
    - int contest_i
  - review
    - int contest_i

image library
- layout
  - background
    - int width
    - int height
    - byte[] pixels
  - slot
    - int left
    - int top
    - int width
    - int height
- sprite
  - int width
  - int height
  - byte[] pixels
Voting Machine Software

- **display**
- **touch sensor**
- **video driver**
- **event loop**
- **navigator**
- **ballot model**
- **vote recorder**

Connections:
- Display to video driver
- Touch sensor to event loop
- Event loop to video driver
- Navigator to vote recorder
- Vote recorder to ballot model
- Ballot model to navigator

Resources:
- Image library
- Ballot model
- Navigator
- Image library
- Display
- Touch sensor

Inputs:
- x, y
- slot

Outputs:
- Selections
- Cast vote records
How much code?
How much code?

<table>
<thead>
<tr>
<th></th>
<th>everything</th>
<th>UI only</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccuVote TS</td>
<td>&gt;31 000</td>
<td>&gt;14 000</td>
</tr>
<tr>
<td>our prototype</td>
<td>293</td>
<td>255</td>
</tr>
<tr>
<td></td>
<td>100×</td>
<td>55×</td>
</tr>
</tbody>
</table>

Python features used:
- one standard library module (SHA-1)
- one collection type
- very few built-in functions
How much code?

- ballot loader: 126 lines
- event loop: 13 lines
- navigator: 94 lines
- video driver: 22 lines
- vote recorder: 38 lines
Accessibility

- earphones
- keypad
- sound library
- audio driver
- event loop
- navigator
- ballot model
- vote recorder
- selections
- cast vote records
1. Accessibility vs. security.
2. Proprietary interests vs. transparency.
3. Too much code to verify.
4. Code changes too frequently.
1. Decouple UI design from security. Open participation in ballot review.
2. Isolate code to be disclosed.
3. Reduce the trusted code by 10 to 100x.
4. Put security responsibility in a VM.
Goal:

an order of magnitude reduction in voting-specific trusted software

similar or better accessibility and usability

compared to the state of the art.
Thank you!

http://zesty.ca/voting

Ka-Ping Yee
ping@zesty.ca