Transparent Elections

Ben Adida
Harvard

November 2nd, 2006
Wellesley College
Does e-voting need paper trails?

By Anne Broache
Staff Writer, CNET News.com
Published: October 31, 2006, 4:00 AM PST
Does e-voting need paper trails?
By Anne Broache
Staff Writer
Published: October 12, 2023

State sued over lack of paper trail for ballots
By AMAN BATHEJA
STAR-TELEGRAM STAFF WRITER
Does e-voting need paper trails?

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

Wed Nov 1, 2006 6:37am ET
Does e-voting need paper trails?

By Anne Broache

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

© Nov 1, 2006 10:54 pm US/Pacific

California E-Voting Machine Allows Multiple Votes

Allen Martin
Reporting
Does e-voting need paper trails?

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

California E-Voting Machine Allows Multiple Votes

OCTOBER 31, 2006
Hugo Chavez in the Voting Machine
Does e-voting need paper trails?

By Anne Broache
Staff Writer,
Published: October 31, 2006

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

© Nov 1, 2006 10:54 pm US/Pacific

California E-Voting Machine Allows Multiple Votes

Allen Martin
 Reporting

OCTOBER 31, 2006
Hugo Chavez in the Voting Machine

Originally published October 26, 2006

Your vote will count
Hype over hacking shouldn't shatter confidence

By Paul DeGregorio
McCLATCHY-TRIBUNE
How We Got Here
How We Got Here

http://www.cs.uiowa.edu/~jones/voting/pictures/
How We Got Here
How We Got Here
How We Got Here

http://www.cs.uiowa.edu/~jones/voting/pictures/
How We Got Here

http://www.cs.uiowa.edu/~jones/voting/pictures/
How We Got Here
2 Months Ago: Princeton Report

- Diebold touch-screen runs executable code loaded from memory card
- All audit logs modified to be consistent
- Can spread virally by memory card.

[VOTE STEALING CONTROL PANEL]

Select the race and candidate to fix:
President of the United States

<table>
<thead>
<tr>
<th>Candidate Name</th>
<th>Votes So Far</th>
</tr>
</thead>
<tbody>
<tr>
<td>George Washington</td>
<td>9 (90%)</td>
</tr>
<tr>
<td>Benedict Arnold</td>
<td>1 (10%)</td>
</tr>
</tbody>
</table>

Set the final outcome: Percent for "Benedict Arnold"

75%

OK  Cancel

[FHF2006]
But not just DREs...
We can do better

Beyond DREs and Paper Trails, there is a **third option:** transparent elections

Direct, end-to-end verification by voter. No need to trust equipment.

We should be talking about it.

Let's take a look at the past...
Why is Voting so Hard?
The Point of An Election

“The People have spoken.... the bastards!”

Dick Tuck
1966 Concession Speech
The Point of An Election

“The People have spoken.... the bastards!”

Dick Tuck
1966 Concession Speech

Provide enough evidence to convince the loser.
Secret Ballot vs. Verifiability

but it wasn't always so...
Secret Ballot vs. Verifiability

but it wasn’t always so...
Secret Ballot vs. Verifiability

but it wasn't always so...

Voting System → convince Alice
Secret Ballot vs. Verifiability

Voting System

convince

Alice

but it wasn't always so...

Carl the Coercer
Secret Ballot vs. Verifiability

Voting System

Alice

convince

Carl the Coercer

but it wasn’t always so...
1892 - Australian Ballot

VERIFICATION changed SIGNIFICANTLY

http://www.cs.uiowa.edu/~jones/voting/pictures/
The Next Harvard Prez!

SOURCES: HARVARD WANTS CONDOLEEZZA RICE OR BILL CLINTON FOR NEXT PRES...

The Ballot Handoff

Alice the Voter
The Ballot Handoff

Alice the Voter
The Ballot Handoff

Clint...
The Ballot Handoff

Clint

the Voter

Alice the Voter
The Ballot Handoff

Alice the Voter

Clinton

Rice
The Ballot Handoff

Alice the Voter

Black Box
Chain of Custody
Chain of Custody

Vendor

/*
 * source
 * code
 */
if (...
Chain of Custody

Vendor

/*
 * source
 * code
 */
if (...
Chain of Custody

Polling Location 3

Voting Machine 2

Vendor 1

/*
 * source
 * code
 */

if (...
Chain of Custody

1. Vendor
   /* source code */
   if (...

2. Voting Machine

3. Polling Location

4. Alice
   Polling Location
   Voting Machine
   Ballots
Chain of Custody

Vendor
/*
 * source
 * code
 */
if (...)

Polling Location

Alice

Voting Machine

Ballot Box Collection
**Chain of Custody**

1. **Vendor**
   - /* source code */
   - if (...)

2. **Voting Machine**

3. **Polling Location**

4. **Alice**
   - Paper Trail Bypass

5. **Ballot Box Collection**

6. **Results**
Chain of Custody

Voting Machine

Vendor

/*
 * source
 * code
 */

if (...)

Polling Location

Paper Trail Bypass

Alice

Black Box

Results

.....
The Cost of Secrecy
The Cost of Secrecy

Scavenged ballot box lids haunt S.F. elections

Erin McCormick, Chronicle Staff Writer
Monday, January 7, 2002
The Cost of Secrecy

Scavenged ballot box lids haunt S.F. elections

Erin McClelland

Helicopter Crash Delays Afghan Vote Count

Helicopter Sent to Pick Up Afghan Ballots in Remote Province Crash-Lands, Delaying Vote Count
The Cost of Secrecy

Scavenged ballot box lids haunt S.F. elections

Helicopter Crash Delays Afghan Vote Count

Absentee ballots 'lost' in Florida

Nearly 58,000 absentee ballots for the US presidential election may never have reached Florida's Broward County voters, who had requested them more than two weeks ago, election officials said.
Scavenged ballot box lids haunt S.F. elections

Erin Mcc
Monday, 3

Helicopter Crash Delays Afghan Vote Count

Absentee ballots 'lost' in Florida

October 28, 2004 09:28 IST

Nearly 58,000 absentee ballots for the US presidential election may never have reached Florida's Broward County election officials said.

Mexico Presidential Election Ballots Found in Dump

RAW STORY
Published: Thursday July 6, 2006
Is Secrecy Important?
Is Secrecy Important?

“Secret ballots and transparency in government are mutually exclusive concepts.”

Lynn Landes - Nov. 2005
Is Secrecy Important?

“Secret ballots and transparency in government are mutually exclusive concepts.”

Lynn Landes - Nov. 2005

http://votebymailproject.org
Is Secrecy Important?

“Secret ballots and transparency in government are mutually exclusive concepts.”

Lynn Landes - Nov. 2005

http://votebymailproject.org

Thursday, July 27, 2006

San Diego task force recommends by mail voting

The City of San Diego is considering all mail balloting for special city elections, the Union Tribune reports.
Is Secrecy Important?

“Secret ballots and transparency in government are mutually exclusive concepts.”

Lynn Landes - Nov. 2005

http://votebymailproject.org

Thursday, July 27, 2006

San Diego task force recommends by mail voting
The City of San Diego is considering all mail balloting for special city elections, the Union Tribune reports.

In U.S., more opt to vote by mail
Number of absentee voters in some states at a record high

By Brian Knowlton / International Herald Tribune
Published: November 1, 2006
Actually, it is.

Secret Ballot implemented in Chile in 1958.

“the secrecy of the ballot [...] has first-order implications for resource allocation, political outcomes, and social efficiency.”

[BalandRobinson 2004]
Transparent Voting
Transparent Voting achieves verifiability \textit{and} secrecy without depending on equipment correctness.

\textbf{HOW} do we do this...

\textbf{LET's RETURN,} for inspiration, to how things were done in the early days of voting.
Public Ballots

Bridget: Clinton

Carol: Rice
Public Ballots

Bridget: Clinton
Carol: Rice

Alice
Public Ballots

Alice: Rice
Bridget: Clinton
Carol: Rice
Public Ballots

Alice: Rice
Bridget: Clinton
Carol: Rice

Tally
Rice........2
Clinton...1
Encrypted Public Ballots

Alice: Rice
Bridget: Clinton
Carol: Rice

Tally
Rice: 2
Clinton: 1
Encrypted Public Ballots

Alice: Rice  
Bridget: Clinton  
Carol: Rice

Tally: Rice........2  
Clinton...1

Alice verifies her vote
Encrypted Public Ballots

Alice: Rice
Bridget: Clinton
Carol: Rice

Tally: Rice.........2
Clinton...1

Alice verifies her vote
Everyone verifies the tally

Alice v
Cryptographic Techniques

things that sound impossible but, in fact, aren’t.
Public-Key Encryption
Public-Key Encryption

Keypair consists of a public key $pk$ and a secret key $sk$. 
Public-Key Encryption

Keypair consists of a public key $pk$ and a secret key $sk$. 

"Condoleezza Rice" $\rightarrow$ ENCRYPT $\rightarrow$ pk
Public-Key Encryption

Keypair consists of a public key $pk$ and a secret key $sk$.

Encrypt

$pk$

Decrypt

$sk$

"Condoleezza Rice"
Zero-Knowledge Proof

DO DEMO before showing this slide.
Zero-Knowledge Proof

**Vote For:** Clinton

---

*DO DEMO before showing this slide.*
Zero-Knowledge Proof

DO DEMO before showing this slide.
This last envelope likely contains “Clinton”
Zero-Knowledge Proof

Open envelopes don’t prove anything after the fact.
Mixnet

TALLYING: we want to shake things around. Like shaking the ballot box.

but.... we have to do more than reorder things, because in the digital world, encryptions are unique and thus recognizable.
Mixnet

TALLYING: we want to shake things around. Like shaking the ballot box.

but.... we have to do more than reorder things, because in the digital world, encryptions are unique and thus recognizable.
Mixnet

\[ c = \text{Enc}_{pk_1}(\text{Enc}_{pk_2}(\text{Enc}_{pk_3}(m))) \]
Mixnet

c = \text{Enc}_{pk_1}(\text{Enc}_{pk_2}(\text{Enc}_{pk_3}(m)))

Each mix server “unwraps” a layer of this encryption onion.
Verifying a Mixnet

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002
Verifying a Mixnet

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002
Verifying a Mixnet

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002
Verifying a Mixnet

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002
Verifying a Mixnet

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002
Verifying a Mixnet

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002
Verifying a Mixnet

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002
Verifying a Mixnet

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002
Verifying a Mixnet

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002
Verifying a Mixnet

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002
Verifying a Mixnet

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002
Verifying a Mixnet

make sure no path is revealed.
50% chance of detecting a single cheated vote.

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002
Putting It Together
Putting It Together
Putting It Together

Encrypted Vote
Putting It Together
Putting It Together

Alice

Encrypted Vote

anonymization

Encrypted Vote

Encrypted Vote
Putting It Together

Alice

Encrypted Vote

anonymization

Encrypted Vote
Putting It Together

Alice

anonymization

Encrypted Vote

Results
Putting It Together

Results

anonymization
Transparent Elections

- Alice verifies that her vote made it all the way to the tally.
- No dependence on any equipment.
- Ballot secrecy is enforced.
Transparent Elections

- Alice verifies that her vote made it all the way to the tally.
- No dependence on any equipment.
- Ballot secrecy is enforced.

Anyone can Audit.
Questions?