Open-Audit Elections

Ben Adida
Harvard

(novel work done at MIT, in collaboration with Ronald L. Rivest)

Google
November 16th, 2006
Lloyd Bentsen
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, The Dallas Morning News
Published: October 28, 2020

State sued over lack of paper trail for ballots

By AMAN BATHEJA
STAR-TELEGRAM STAFF WRITER
Does e-voting need paper trails?

By Anne Broache
Staff Writer,
Published: Oct

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 Broach
Staff Writer,
Published: Oct

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?

By Anne Broache
Staff Writer,
Published: Oct 30, 2006 4:49 am ET

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

California E-Voting Machine Allows Multiple Votes

Allen Martin
Reporting

OCTOBER 31, 2006

Hugo Chavez in the Voting Machine
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

Hugo Chavez in the Voting Machine

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

By Paul DeGregorio
McCLATCHY-TRIBUNE
Rogers precinct, with more than 100 percent voter turnout, alarmed both of them.
Rogers precinct, with more than 100 percent voter turnout, alarmed both of them.
Rogers precinct, with more than 100 percent voter turnout, alarmed both of them.

**Thief grabs voting machine from election official's car**
By ROGER H. AYLWORTH - Staff Writer
Article Launched:11/07/2006 12:00:00 AM PST

**Voter smashes touch-screen machine in Allentown**

Last Updated: November 7, 2006 - 2:19 PM EST
Rogers precinct, with more than 100 percent voter turnout, alarmed both of them.

Voter smashes touch-screen machine in Allentown
Wooten got the news from his wife, Roxanne, who went to City Hall on Wednesday to see the election results.

"She saw my name with zero votes by it. She came home and asked me if I had voted for myself or not. I told her I did," said Wooten, owner of a local bar.
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

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

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

http://www.cs.uiowa.edu/~jones/voting/pictures/
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: open-audit elections

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

Let’s talk about it.
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

Voting System

convince

Alice

Carl the Coercer
1892 - Australian Ballot

DEMOCRATIC:

FOR MAYOR,
AUGUST LEUZ, JR.
CORNER BURLINGTON AND JOHNSON STREETS.

FOR TREASURER,
GEORGE W. KOONTZ
NO. 620 EAST BURLINGTON STREET.

FOR CITY SOLICITOR,
FRANK J. HORAK
NO. 120 DODGE STREET.

FOR ASSESSOR,
F. A. HEINSIUS
NO. 948 EAST MARKET STREET.

FIFTH WARD.

FOR TRUSTEE,
JOHN U. MILLER
EAST MARKET STREET.

REPUBLICAN:

FOR MAYOR,
CHAS. LEWIS
NO. 227 NORTH CLINTON STREET.

FOR TREASURER,

FOR SOLICITOR,
L. H. FULLER
NO. 422 SOUTH DUBUQUE STREET.

FOR ASSESSOR,
H. W. LATHROP
NO. 318 IOWA AVENUE.

MAYORITIES:

1893

848

101

198

24

221

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

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

The Ballot Handoff

Alice the Voter

Clinton
The Ballot Handoff

Alice the Voter

Clinton

- [Diagram showing a mail envelope labeled Clinton being handed over to a voter represented by a stick figure.]
The Ballot Handoff

Alice the Voter

Clinton

Rice
The Ballot Handoff

Alice the Voter

Black Box

Clinton

Rice
Chain of Custody
Chain of Custody

Vendor

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

Voting Machine

Vendor

/*
 * source
 * code
 */

if (...)
Chain of Custody

Polling Location

Voting Machine

Vendor

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

1. Vendor
2. Voting Machine
3. Polling Location
4. Alice

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

1. Vendor
2. Voting Machine
3. Polling Location
4. Alice
Chain of Custody

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

Polling Location

Alice

Ballot Box Collection

Results
Chain of Custody

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

2. Voting Machine

3. Polling Location

4. Alice

5. Ballot Box Collection

6. Results
   ......

Polling Location --> Voting Machine --> Paper Trail Bypass --> Ballot Box Collection --> Results
Chain of Custody

Polling Location → Voting Machine → Paper Trail Bypass → Black Box → Results

Vendor

/*
 * source
 * code
 */

if (...)
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 McCt

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

Erin McCt
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 voters, who had requested them more than two weeks ago, election officials said.
The Cost of Secrecy

Scavenged ballot box lids haunt S.F. elections

Erin McCrory

Helicopter Crash Delays Afghan Vote Count

Helicopter 1 province crash

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
The Cost of Secrecy

Scavenged ballot box lids haunt S.F. elections

Erin McC
e
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 Count
election officials said.

Mexico Presidential Election Ballots Found in Dump

SARASOTA
18,000 votes in U.S. House race may be lost

Thousands of votes were either not counted or not cast in Sarasota's nationally watched congressional race.
Is Secrecy Important? 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]
Open-Audit Voting

[Chaum81], [Benaloh85], [PIK93], [BenalohTuinstra92], [SK94], [Neff2001], [FS2001], [Chaum2004], [Neff2004], [Ryan2004], [Chaum2005]
Properties of OAV

(1) Alice verifies her vote.

(2) Everyone verifies tallying.

(3) Alice cannot be coerced by Eve.
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

Tally

Rice........2
Clinton...1

Alice: Rice
Bridget: Clinton
Carol: Rice
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
Verification
Ballot Data Flow

Encrypted
Votes

Alice
Bridget
encryption

Encrypted
Votes

Verification
Ballot Data Flow
Ballot Data Flow

Verifi

Encryption

Alice

Bridget

Encrypted Votes

anonymization

Verification

Ballot Data Flow
Ballot Data Flow

Verification

Ballot Data Flow

Decryption
Results

Tally

Verification

Ballot Data Flow

decryption

anonymization

 decryption

Encrypted Votes

encryption

Alice

Bridget
Results

Tally

Registration

Database

Verification

Ballot Data Flow

decryption

anonymization

Encryption Votes

Alice

Bridget

encrypted

encrypted

encrypted

Results
Zero-Knowledge Proof
Zero-Knowledge Proof

Vote For: Clinton
Zero-Knowledge Proof

Vote For: Clinton

President: Mickey Mouse

Vote For: Clinton
Zero-Knowledge Proof

This last envelope likely contains “Clinton”
Zero-Knowledge Proof

Open envelopes don’t prove anything after the fact.
Scratch-and-Vote
Scratch 'N Win Ballots To Debut In November
July 19, 2006 | Issue 42•29

WASHINGTON, DC—In an effort to increase voter participation while generating additional revenue, several state election boards announced plans Monday to introduce new Scratch 'N Win ballots in November, giving citizens the chance to win the right to vote in the 2006 elections.
1. Receive two ballots.
2. Choose one randomly for auditing by scratch-off.
2. Choose one randomly for auditing by scratch-off.

Can be done by a political organization of voter's choice.
In Private

3. Vote.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinton</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rice</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

Clinton
None
Rice
4. Tear & Discard left half of ballot.
In Private

4. Tear & Discard left half of ballot.
5. Tear & Discard scratch-off.
Public Ballot Box

Alice  Bridget  Carol

☐  ☑  ☑
PARAMETERS
#1 - Rice
#2 - Clinton
#3 - None

M=10, Public Key = $pk$

Clinton
None
Rice

$E_{pk}(2^{10}; r_1)$
$E_{pk}(2^{20}; r_2)$
$E_{pk}(2^0; r_3)$
Homomorphic Tallying

- 0001 0000 0000  Vote for Clinton
- 0000 0001 0000  Vote for Rice
- 0000 0000 0001  Vote for None
- 0004 0001 0008  Sample Tally

[B+2001, P1999]
Scratch & Vote is one system. There are many others.
In Summary
In Summary

• End-to-End verification
In Summary

- End-to-End verification
- Secrecy and Verifiability are reconcilable
In Summary

• End-to-End verification
• Secrecy and Verifiability *are* reconcilable
• Simplicity & Practicality are well on their way...
In Summary

• End-to-End verification
• Secrecy and Verifiability *are* reconcilable
• Simplicity & Practicality are well on their way...
• The Paper Trail is not enough. Hand-Counted Ballots are not enough.
In Summary

- End-to-End verification
- Secrecy and Verifiability *are* reconcilable
- Simplicity & Practicality are well on their way...
- The Paper Trail is not enough. Hand-Counted Ballots are not enough.
- **Open-Audit Voting**: let *anyone* verify.
Questions?
Practical Considerations

5 questions, 5 options per question.

- **Ballot Verification**: less than a second.
- **Barcode Encoding**: PDF417 open standard.
- **Barcode Size**: 10 square inches of barcode for a full sheet visual ballot.
- **Proof Time**: ~3 seconds per ballot.