Beyond the Paper Trail

Ben Adida
Harvard

February 27th, 2007
IEEE Social Implications of Technology
Goals of this Talk

➡ Current voting technology has serious flaws.
➡ Voting is hard.
➡ Commonly proposed solutions fall short.
➡ Open-Audit voting has the potential to revolutionize how we audit elections.
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

Originally published October 26, 2006
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.

Last Updated: November 7, 2006 - 2:19 PM EST

Voter smashes touch-screen machine in Allentown
We can do better

**open-audit elections (using cryptography)**

Direct, end-to-end verification.
No need to trust equipment.
Anyone can audit.

We should be talking about it.
How We Got Here
The 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...
Why is Voting so Hard?
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
Hand Vote
1892 - Australian Ballot

Democrat:

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.

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.

FOR TRUSTEE,
J. C. LEASURE
COR. VAN BUREN ST. AND IOWA AVENUE.

Majorities:

Democrat: 848

Republican: 221

198
The Breakfast Election

Salty

Sweet

http://www.flickr.com/photos/35034346243@N01/91524057/
The Ballot Handoff

Alice the Voter

Black Box

Salty
Sweet
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 -> Ballot Box Collection
The Cost of Secrecy

Scavenged ballot box lids haunt S.F. elections

Erin McCr
Monday, 1

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

RAW STORY
Published: Thursday July 6, 2006
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]
Aviation and Banking?

- Little defense against insiders
- Failures are obvious
- Complete audit logs
- Transferability of claims

These are poor analogies.

http://commons.wikimedia.org/wiki/Image:738100.jpg
http://www.sxc.hu/photo/206579
The Paper Trail

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

Vendor

Polling Location

Paper Trail Bypass

Alice

Black Box

Results

.....
Open-Source

* **Idea**: see the source, see the bugs
  - disclosed source is really what’s needed
  - open-source also removes vendor lock-in, but this is a business issue, not a security issue.

* **Issues**
  - inspected code same as running code?
  - is the whole stack open-source? COTS exemption?
  - what about integrity of the ballot box?
Threat Model

* Who is the attacker?
  ➡ administration officials, candidates, poll workers, even voters

* What is the Benefit?
  ➡ election of the leader of the free world

* How will the attacks be carried out?
  ➡ corruption of input, ballot box, transport, tallying
  ➡ coercion of voters

* Where will the attacks be hidden?
  ➡ honest mistakes: randomly distributed in the process
  ➡ malicious intent: hiding where you least defend
Open-Audit Elections
Open-Audit Voting achieves verifiability and secrecy without depending on equipment correctness.

Anyone can audit.
Anyone. Really.
Public Ballots

Alice: Sweet
Bridget: Sweet
Carol: Salty

Tally
Sweet.......2
Salty.........1
Encrypted Public Ballots

Alice: Rice
Bridget: Clinton
Carol: Rice

Tally: Sweet......2
Salty........1

Alice verifies her vote
Everyone verifies the tally
Cryptographic Techniques

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

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

![Diagram showing encryption process with examples of messages and their encrypted forms.](image-url)
Threshold Decryption

Secret key is shared amongst multiple parties: all (or at least a quorum) need to cooperate to decrypt.
How do I get an encrypted ballot?
Zero-Knowledge Proof

Vote For: Sweet

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

Open envelopes don’t prove anything after the fact.
Benaloh Casting Protocol

Alice

"Vote for Sweet"

Encrypted Ballot

Alice

"AUDIT"

"CAST"

Decrypted Ballot

Signed Encrypted Ballot

VERIFICATION

Each mix server shuffles the encrypted votes.
Mixnet

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

\[ c = \text{Enc}_{p_{k_1}}(\text{Enc}_{p_{k_2}}(\text{Enc}_{p_{k_3}}(m))) \]
Verifying a Mixnet

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

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002
Homomorphic Tabulation

$\text{Enc}(m_1) \times \text{Enc}(m_2) = \text{Enc}(m_1 + m_2)$

Yes = Enc(1)
No = Enc(0)

EncryptedTally = $\text{Enc}(m_a) \times \text{Enc}(m_b) \times \text{Enc}(m_c)$

= $\text{Enc}(m_a + m_b + m_c)$
Putting It Together

Voting Equipment & Ballot Flow
Verification

Polling Location
Voting Machine
Vendor
/*
 * source
 * code
 */
if (...

Public Ballot Box

Receipt

Alice

Results

1

2

Voting Equipment & Ballot Flow
 Verification
Open-Audit Elections

- **Alice** verifies **her vote**.
- **Everyone** verifies **the tally**.
- **Incoercibility** is enforced.
Goals of this Talk

➡️ Current voting technology has serious flaws.
➡️ Voting is hard.
➡️ Commonly proposed solutions fall short.
➡️ Open-Audit voting has the potential to revolutionize how we audit elections.
Questions?