Secure & Fair Elections

Ben Adida
ben@mit.edu
http://ben.adida.net
Cryptography and Information Security Group
MIT Computer Science and Artificial Intelligence Lab

November 2nd, 2004

Attribution-ShareAlike Creative Commons License
(except where marked otherwise)
Expert Opinion

http://avirubin.com/vote/dailyshow.mov
Is Voting Really That Difficult?

Actually, YES.

- The stakes are high
- Problems are not easily detected
- The Requirements seem contradictory
- Experts vs. Electorate
Today’s Discussion

- Paper Trail?
- Voting System Requirements
- A Complex Threat Model
- Components of Voting
- Future Solutions
The Paper Trail

- Yes, paper is actually expensive (multi-language, logistic costs)
- Yes, all machines are vulnerable
- No, not as simple as ATM
- No, Paper is not the only way

- BUT...
  Paper is the quickest fix today
Voting Requirements

- Registration & Check-in
  - not too onerous (disenfranchisement)
  - not too easy (fraud)
- Vote Verification
  - voter is confident of his vote
  - voter cannot sell his vote
The Voter Is An Adversary!
Cast as Intended
Confusion at Palm Beach County polls
Some Al Gore supporters may have mistakenly voted for Pat Buchanan because of the ballot’s design.

Although the Democrats are listed second in the column on the left, they are the third hole on the ballot.

Punching the second hole casts a vote for the Reform party.

http://www.mit.edu/~jtidwell/ballot_design.html
(this slide content is NOT under a CC License)
Confusion at Palm Beach County polls
Some Al Gore supporters may have mistakenly voted for Pat Buchanan because of the ballot's design.

Confusion could have been avoided with a simple redesign.

http://www.mit.edu/~jtidwell/ballot_design.html
(this slide content is NOT under a CC License)
Verify Before Casting

Alert Dialog
You have chosen Pat Buchanan
Are you sure?

No
Yes
Recorded as Cast
Voting Machine
Hard Drive

Vote Recorded:
YES
Counted as Recorded
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.

Scavenged ballot box lids haunt S.F. elections

Erin McCormick, Chronicle Staff Writer

Monday, January 7, 2002
A Bright Future: Cryptography and Universal Verifiability
Crypto “Bag of Tricks”

- Public-Key Encryption
- Secret Sharing
- ZK Proofs
Do you need to be a cryptographer to trust the voting system?
Summary

- Paper is a quick (but necessary?) fix
- Voting is Hard to do right
- The Voter is an Adversary
- Complex Schemes offer hope?
Questions?
Backup Slides
Public-Key Encryption

"John Kerry"

Public Key

f4ec163dab6

Private Key
Secret Sharing

ACLU
NRA
Democrats
Republicans
The French
Threshold Decryption
Zero-Knowledge Proofs

Proof of Mixing:
(1) no duplication
(2) no deletion
(3) no addition