CS 155 June 1, 2004

Electronic Voting

Dan Boneh John Mitchell

Issues

- Voting system security requirements
  - Secret ballot, reliable counting, voter anonymity, ...
- Voting technology
  - History: Paper ballots, lever machines, ...
  - Direct Recording Electronic (DRE) systems
- Case studies
  - Diebold case study
  - Internet voting (retracted by gov't)
- Cryptographic approaches
- Politics
  - Voting Rights Act bills H.R. 3295 and S. 565
  - California Secretary of State Kevin Shelley
  - IEEE Standards committee

Voting Principles

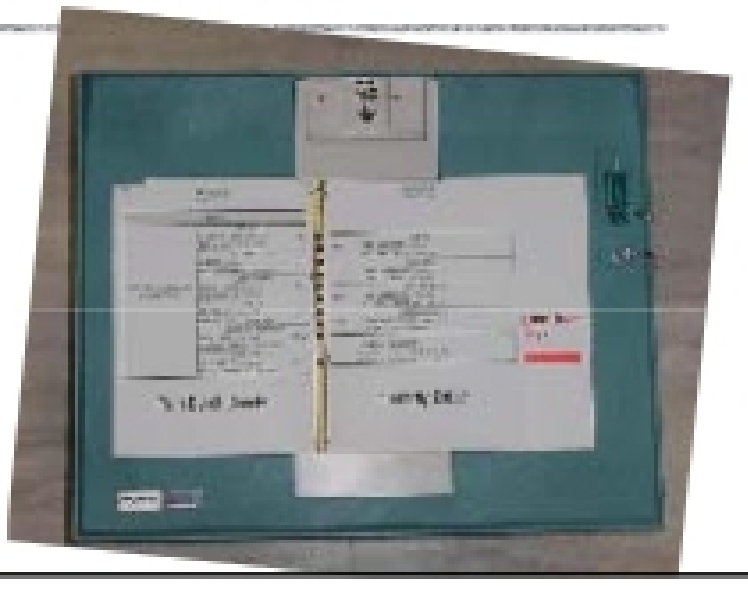
- Voter eligibility
  - No voter should have more than one vote
- Secret Ballot
  - Votes cast in secret
  - Voter should be confident that vote cast correctly
- Reliable counting
  - Public system, typically with officials from all parties
  - Ability to recount

    Some election officials may prefer not to do this
- Anonymity
  - Voter should not leave voting booth with any proof of the way he/she voted

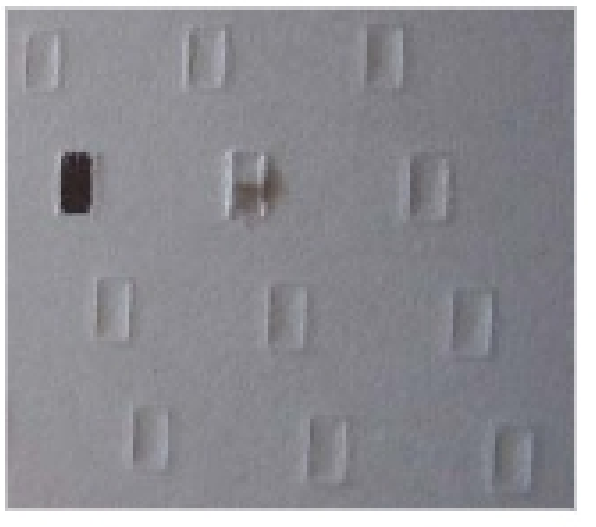
Recent History

- 2000 Presidential Election
  - Hanging chad, contested absentee votes
- Help America Vote Act (HAVA, HR 3295, Oct 02)
  - Mandates voting process reform in all states
  - Voters must be able to verify ballots before they are cast
  - "permanent paper record with a manual audit capacity"
  - voter must have "opportunity to change the ballot or correct any error before the permanent paper is produced"
- Electronic voting
  - Touchscreen, Direct Recording Electronic (DRE) systems
  - Proponents argue HAVA requirements are met if the voter verifies a screen version of the ballot, and if a paper report can be printed later for audit purposes

Punch card device



Punched card



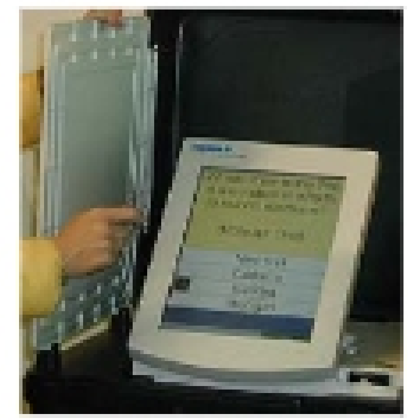
Other alternatives

- Mechanical lever machines
  - Voter flips mechanical levers
  - Machine reports votes
  - Tamper-proof counter similar to car odometer
- Optical scan of paper ballots
  - Like our teaching evaluations …
  - Fairly reliable counting method
  - Requires pencil and paper ballots

Lever machine

Touch-screen voting

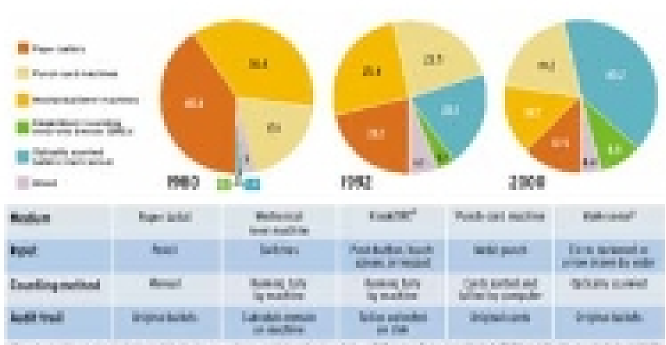
- Usability
  - Customized ballot
  - Easy to read, vote
  - Accessible to blind
    wear headphones
- Vote counting
  - DRE system provides quick count
- Voter "authentication"
  - smartcard reader (lower-right corner)



Diebold AccuVote-TS

http://www.sos.state.ga.us/

How votes are cast



IEEE Spectrum
Oct 2002

Problems with electronic voting

- Washington Post 11/6/2003
  - Software glitch in November's election in Virginia
  - Advanced Voting Solutions touchscreen machines
  - "Voters in three precincts reported that when they attempted to vote for [Thompson], the machines initially displayed an 'x' next to her name but then, after a few seconds, the 'x' disappeared. In response to Thompson's complaints, county officials tested one of the machines in question yesterday and discovered that it seemed to subtract a vote for Thompson in about 'one out of a hundred tries,' said Margaret K. Luca, secretary of the county Board of Elections. "

    http://www.washingtonpost.com/wp-dyn/articles/A6291-2003Nov5.html
- Indianapolis Star 11/9
  - Software glitch in November's election
    - 19,000 registered voters
    - 144,000 votes tallied
    - actual number of votes cast was 5,352
  - MicroVote touchscreen machines

    http://www.indystar.com/articles/6/091021-1008-009.html

Voter Verified Audit Trail

IEEE Spectrum
Oct 2002

Case Study: Diebold machine

T. Kohno, A. Stubblefield, A. Rubin,
D. Wallach

Basis for study

- Proprietary system
  - Certification mandated by election laws
    - Without public review: Security through obscurity
- Diebold system leaked
  - AccuVote-TS DRE voting system, Oct 2000 - April 2002
  - Available on open ftp server
  - Identified by activist Bev Harris
  - Some zip files, cvs repository
    - DMCA concern over zip "encryption"
    - Available on New Zealand site
- No access to Diebold's back-end election management system

Some problems

- Encrypted votes and audit logs
  - 56-bit DES in CBC mode with static IVs
  - #define DESKEY ((des_key*)"F2654hD4")
  - Unkeyed public function (CRC) for integrity
- No authentication of smartcard to voting terminal
- Insufficient code review

Sample comment in code

```
//  LCG - Linear Conguential Generator
//  used to generate ballot seriel numbers
//  A psuedo-random-sequence generator
//  (per Applied Cryptography,
//  by Bruce Schneier, Wiley, 1996)
```

Unfortunately, linear congruential generators cannot be used for cryptography"

Page 369

Applied Cryptography, by Bruce Schneier

- BallotResults.cpp
Diebold Election Systems

Other examples

"this is a bit of a hack for now."

AudioPlayer.cpp

"the BOOL beeped flag is a hack so we don't beep twice. This is really a result of the key handling being gorped."

WriteIn.cpp

"the way we deal with audio here is a gross hack."

BallotSelDlg.cpp

"need to work on exception "caused by audio". I think they will currently result in double-fault."

BallotDlg.cpp