Who Gets to Count Your Vote?
Computerized and Internet Voting

Barbara Simons

With thanks to David Dill and David Jefferson for some slides
“Those who cast the votes decide nothing. Those who count the votes decide everything.”

Joseph Stalin
Why is e-voting an issue now?

• Florida!
• Help America Vote Act (HAVA)
  – Almost $4B for new voting equipment
  – Must replace punch card and lever machines by 2004 - can get waiver until 2006
  – National Institute of Standards and Technology (NIST) charged with setting standards
    • No money allocated
Outline

• Definitions of computer based voting systems
• Internet voting in the U.S. (SERVE)
• Voter Verified ballots
• US overview
  – Major vendors
  – Testing and Security
• How to steal an election
• Horror stories
• Legislation (HR 2239)
Diebold emails

• Posted on internet
• Cease and desist orders (Swarthmore)
  – Diebold does not acknowledge accuracy of emails
  – Nonetheless, using provisions of DMCA
  – EFF & Stanford Law Clinic request court order to stop Diebold “from issuing specious legal threats”
More headaches for Diebold

- CA Secretary of State halted certification process for “modification” because Diebold may have installed uncertified software in Alameda Co.
  - Nov 3, 2003
Computer based voting machines
Optical Scan

• Advantages
  – Cheaper than touch screen machines
  – Voter verifiable paper ballot
  – If done locally, can check ballot for overvote and undervote

• Disadvantages
  – Multi-lingual ballot can be a problem
  – Disabled people?
Optical Scan for sight impaired

• Vogue Election Systems
  – Touch screen machine marks optical scan ballot
    • Use earphones to assist
  – Ballot can be “verified” by putting it through optical scan machines- also with earphones
  – Also useful for people with literacy problems
  – Avoids overvote and stray marks problems
  – Multiple language capability via touch screen
Direct Recording Electronic (DRE) Advantages

- Touch screen - can have good human factors
- Multilingual
- Can be good for disabled - if done properly
- Instant run-off easy
DRE disadvantages

• Most have no voter verifiable audit trail  
  – Ballots printed at end of election!
• No national standard
• Proprietary software
• Can be difficult to operate and update  
  – Storage security an issue - costly
• expensive
DREs

• Already purchased for over 20% of U.S. voters
• Small number of vendors nationally
• Proprietary software (secret)
  – Independent computer security experts not allowed to view or test software
  – Code held in escrow not sufficient
    • Independent experts not allowed to examine code
Internet Voting
Secure Electronic Registration and Voting Experiment (SERVE)

- $22M DoD project for ‘04 elections and primaries
  - 10 states and subset of counties in those states
  - Military and civilians living out of the country
- System requirement
  - Windows 2000
    - website says Windows 95 and 98 are options
    - MS Explorer 5.5 & above or Netscape Navigator 6.x & above.
    - ActiveX.
SERVE (con’t)

• Users responsible for maintaining the security of their computers, and
  – voting allowed from public computers with internet access (cybercafes)

• Voting for a national election will be conducted using proprietary software, insecure clients, and an insecure network
Some SERVE Security risks

- Denial of service attacks on servers
- Penetration attacks on servers
- Spoofing attacks
- Virus/Trojan horse attacks on clients
- Sysadmin attacks against voters on networks
- Automated vote selling / trading schemes
- Insider attacks
  - phony voter registrations
  - forging, changing, selective destruction of votes
- Bugs in server or client software
Security Example

• Vulnerability in Microsoft Windows Server 2003 software announced July 16, 2003
  – Allow hacker to size control of machine and steal information, delete files, read email
  – Was supposed to be highly reliable and secure
  – Also impacts Windows 2000, NT, and XP
    • Could have been used to compromise some currently used election software
SERVE (con’t)

• What happens if election appears to go smoothly in ‘04?
UK - e-voting 2003

- Phone: texting or voice
- Interactive digital TV
- Kiosks - touch screen machines at libraries, supermarkets, etc.
- Internet
  - Some voters given receipt id so could verify that ballot reached “ballot box”
  - Used voter id and password
- >160,000 voters in 2003
Voter verifiable audit trail

Paper ballots
Definition of voter verification

Any protocol requiring a DRE to write votes onto write-once external media so that they cannot be modified by software, and then allows the voter to independently verify that what is written is an accurate record of his/her choices.

--------------------

The voter also should be able to understand and have confidence in the process.
– Voter must be able to verify the permanent record of his or her vote (i.e., ballot).
– Ballot is deposited in a secure ballot box.
  • Voter can’t keep it because of possible vote selling.
  • Ballot handling and counting must be observable.
– Manual recounts must be performed.
  • When elections are suspect.
  • When candidates challenge.
  • Randomly, to check machines even when elections go smoothly.
Options for VV Audit Trails

- Manual ballots with manual counts
- Optically scanned paper ballots
  - *Precinct-based* scanned ballots have low voter error rates.
- Touch screen machines with printers
  - All major manufacturers have prototypes.
- Other possibilities
- Other media than paper?
  - Cryptographic schemes?
  - All electronic (trustworthy hardware)?
Major vendors for non-internet voting
Election Systems & Software (ES&S)

- Lou Dedier
  - Former CA Deputy Sec’y of State; Director, Voting Systems & Technology Advisor to state Voting Modernization Board
  - Became ES&S VP and general manager of CA operations, Oct. 15, 2002

- Sen. Hagel (Nebraska) major stock holder
  - Machines used to count votes in Hagel’s election
  - No disclosure
Sequoia

• British owned corporate parent is Madison Dearborn, a partner of the Carlyle Group
• Involved with Louisiana corruption case
  – Some Sequoia executives indicted, but escaped trial after giving immunized testimony
• Will be replacing Santa Clara County punch card machines
  – Former Santa Clara County election official now working for Sequoia
Diebold

• “...committed to helping Ohio deliver its electoral votes to the president next year”
  – Walter O’Dell, CEO Diebold

• Diebold has good chance of winning statewide voting machine contract in Ohio

• Ran election for state of Georgia in ‘02
Diebold security issues

• Johns Hopkins U. paper on security issues with Diebold code put Ohio and Maryland decisions on hold
  – Redacted report by SAIC (only about 1/3 made public)
  – Maryland making purchase anyway
  – Maryland Ethics Commission investigation of Gilbert J. Genn - lobbyist for Diebold and SAIC

• Ohio considering Diebold
  – Was going to use SAIC for review
  – Discovered SAIC about to invest $5M in Hart Intercivic
  – Instead using other companies
SAIC Report

• Entire Section 5 “risk assessment findings, including a discussion of the SBE security requirements, threats to the implementation of the AccuVote-TS, likelihood of exploitation of the threat, vulnerabilities, and mitigation strategies and recommendations for improving the security posture” is REDACTED
SAIC Report

• “The voting terminal is an embedded device running Microsoft Windows [REDACTED] as its operating system. The currently used version of the AccuVote-TS software is [REDACTED] written in the C++ language.”
Testing and Security
Weak security measures

• “Security through obscurity” - trying to obtain security by keeping software secret is bad security

• Lack of strong technical national standards
  – Testing
  – Security
Independent Testing Authorities (ITAs)

• Testing and results are secret
• Tests scripts
  – Does not do code review
• Must test for likely bugs
  – Unlikely to detect clever Trojan Horse
  – If malicious code uses randomization, may not be able to determine if bug or intentional
    • May not be repeatable (because of randomization)
Standards
IEEE Standards Committee  
P1583

- Opposition to voter verified ballots
- Current chair works for ES&S
- IEEE is a named member of the (as yet unformed) HAVA technical commission, so this standard may have far-reaching effects.
How to steal a non-internet election
(it’s even easier with the internet)

thanks to David Jefferson
How to steal an election:
Trojan logic undetectable by testing

Add this logic to DRE shutdown procedure.
Hide it.

if ( this was not a test,
    but a real election )
then
    cheat
else
    behave_honestly
This a real election if ...

( ( not test_mode ) and
  ( date = election_day ) and
  ( all votes came in via touchscreen or via accessibility interfaces ) and
  ( 50 < votes_cast < 200 ) )

or

( write_in_candidate = "Micky Mouse" )
This a test if …

( Time between start-up of machine and end of voting is not between 10 and 12 hours ) or

( Votes coming too often or too regularly ) or

( no votes have been changed or missed ) or

( votes coming in through file system or serial port or some other way aside from the touchscreen and/or audio driver )
Example: Probabilistic cheat

change random number up to 3% of Party_A votes to Party_B
change random number up to 1% of Party_B votes to Party_A

Even if noticed during testing, this cheat

• will not be reproducible, and
• will not be distinguishable from a bug
• or from tester error
Ways to hide Trojan logic in DRE code

- Misleading documentation and choice of identifiers
- Bury logic deep in subroutines and data indirection
- Bury in macro expansions, header files, conditional compilations, or obscure, unneeded library routine
- Modify a COTS (Commercial Off The Shelf) component
- Modify compiler, or linker, to insert the logic during compilation
- Put part of the logic as non-functioning code in the first version, and add enabling logic in an “upgrade”.
- Make changes directly to object code, bypassing source.
- Break logic into parts and use different trick on each
Election fraud difficult to detect

- All design documents and code are secret, so no one but ITA can audit the code.
- Election code might be audited only once by the ITA. If passes, may never be audited again.
- COTS code typically not audited at all
- Election code only runs once per year, with no independent check that it is operating correctly
DRE software cannot follow normal industry development practices

- Certification process a disincentive to making code changes, fixes, and upgrades
- Vendors cannot add improvements or fix bugs without recertification.
  - Need multi-state recertification
  - Very slow and expensive
- Else certification system will be very lax
Horror Stories
Broward County, FL Nov 2000

- Precinct 12f
- 713 people voted; machine count 749
- ES&S Ivotronic DREs
- Told by election officials that +-10% a smooth election
- Broward now considering elimination of paperless DREs
Middlesex County, NJ - 2000

- Sequoia DRE taken out of service after 65 votes
- No votes recorded for Dem and Rep candidates for one office, even though their running mates received 27 votes
- Sequoia claimed no votes lost
- Impossible to verify
Comal County, Texas 2002

• 3 winning Republican candidates received 18,181 votes each on optical scan machines
  – No recount performed
  – “Isn’t it the weirdest thing? We noticed it right away, but it is just a big coincidence.”
• County Clerk Joy Treater
Welllington, FL March 2002

- Runoff election between two only candidates
  - Final tally 1263 - 1259
  - 78 ballots had no recorded votes, even though was the only office on ballot
  - Claim made that 78 didn’t vote for anyone
  - Can’t check
Boca Raton Mayor’s race 2002

• Former mayor Emil Danciu came in 3rd
  – 8% undervote
  – Low numbers reported in his home precinct
• Sequoia sold system with trade secret protection
  – 3rd degree felony to reveal specs or software
Boca Raton (con’t)

- Circuit Court Judge John Wessel refused to allow inspection of software, but granted Danciu a walk-inspection of equipment
  - Pre-election testing tested only for first position on ballot
    - Danciu was third
Boca Raton (con’t)

• At end of election, machines placed in mode where testing cannot be performed
  – No post-election test possible
• Voting machines repro programmable
  – How does this impact certification process?
    • “Florida 2002: Sluggish Systems, Vanishing Votes” by Rebecca Mercuri
Nebraska

• Haggle Nebraska Senate races 1996, 2002
  – President and large ownership in company that sold machines used to count elections in Nebraska in ‘96
  – Large stock owner in DRE company (ES&S) that handled ‘02 election
    • Not mentioned in candidate disclosure statements
Georgia

• 2002 Georgia races all on Diebold machines
  – Incumbent Dem. Sen. Max Cleland favored in pre-election polls and exit polls
  – Lost in huge upset
  – No way to verify if count was accurate
Legislation
The Voter Confidence & Increased Accessibility Act (H.R. 2399 - Holt)

• All voting systems must produce voter-verified paper ballot for use in manual audit and recounts
  – Paper ballots the official record for any recount

• Bans use of undisclosed software
  – Software made available by Commission for inspection by any citizen requesting it
H.R. 2239 (con’t)

• Bans wireless communication devices
• Must be implemented by 2004 election
• Requires voting system for persons with disabilities a year earlier than HAVA (Jan 1, 2006)
• Mandatory surprise recount in 0.5% of domestic and overseas jurisdictions
Audit requirements (HAVA)

• “The voting system shall produce a permanent paper record with a manual audit capacity for such systems.

• “The voting system shall provide the voter with an opportunity to change the ballot or correct any error before the permanent paper record is produced.

• “The paper record … shall be available as an official record for any recount…”
What can you do?

- [http://verifiedvoting.org](http://verifiedvoting.org)
  - Petition with signatures of over 1000 computer experts
    - We are also soliciting signatures from organizations and individuals
  - Q/A on DREs
- [http://www.acm.org/usacm/Issues/evoting.htm](http://www.acm.org/usacm/Issues/evoting.htm)