The California Top-to-Bottom Review of Voting Systems

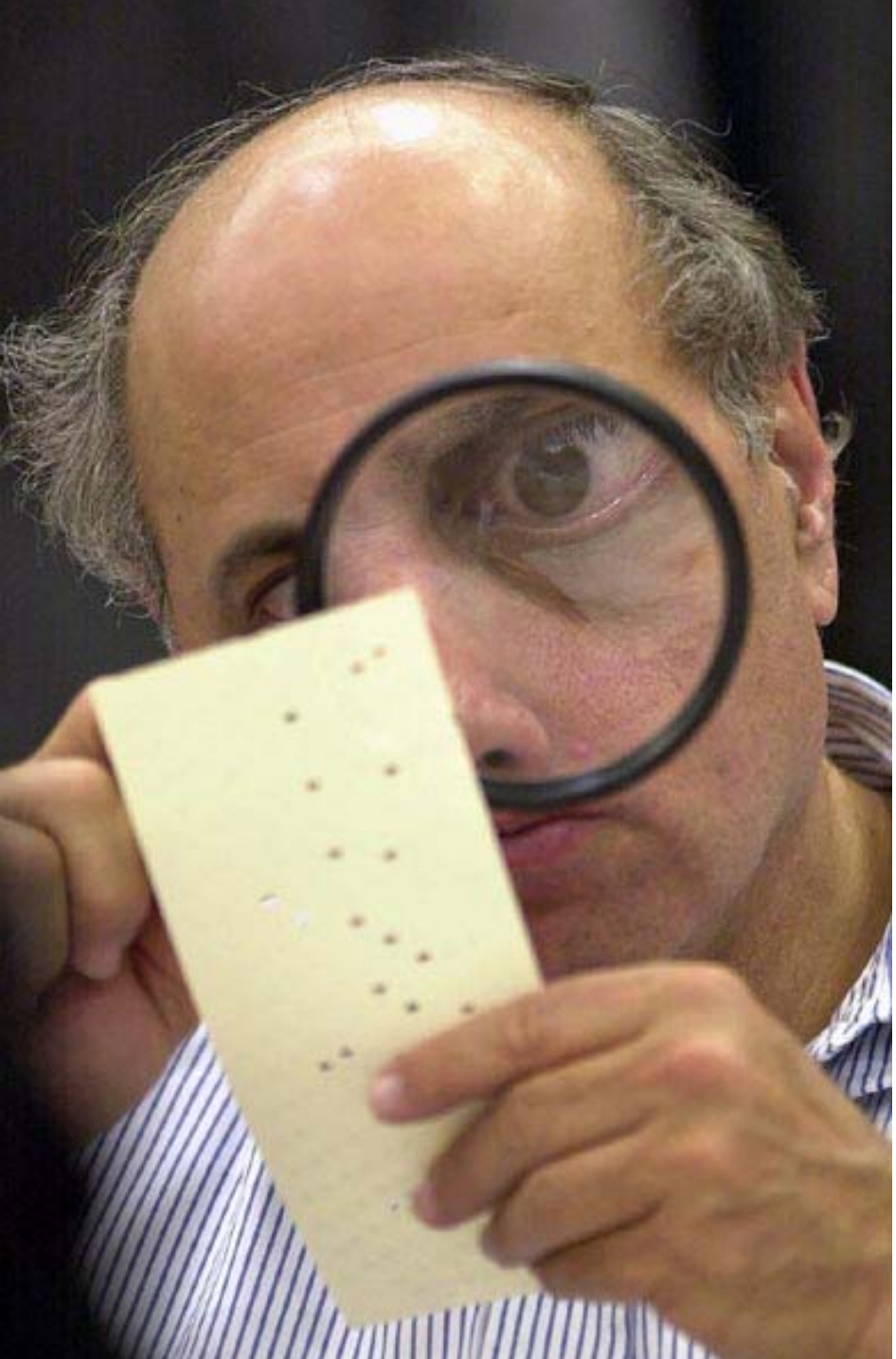
David Wagner
UC Berkeley

ACCURATE

A CENTER FOR
CORRECT, USABLE,
RELIABLE, AUDITABLE,
AND TRANSPARENT ELECTIONS

An Abbreviated History of E-Voting

David Wagner, UC Berkeley

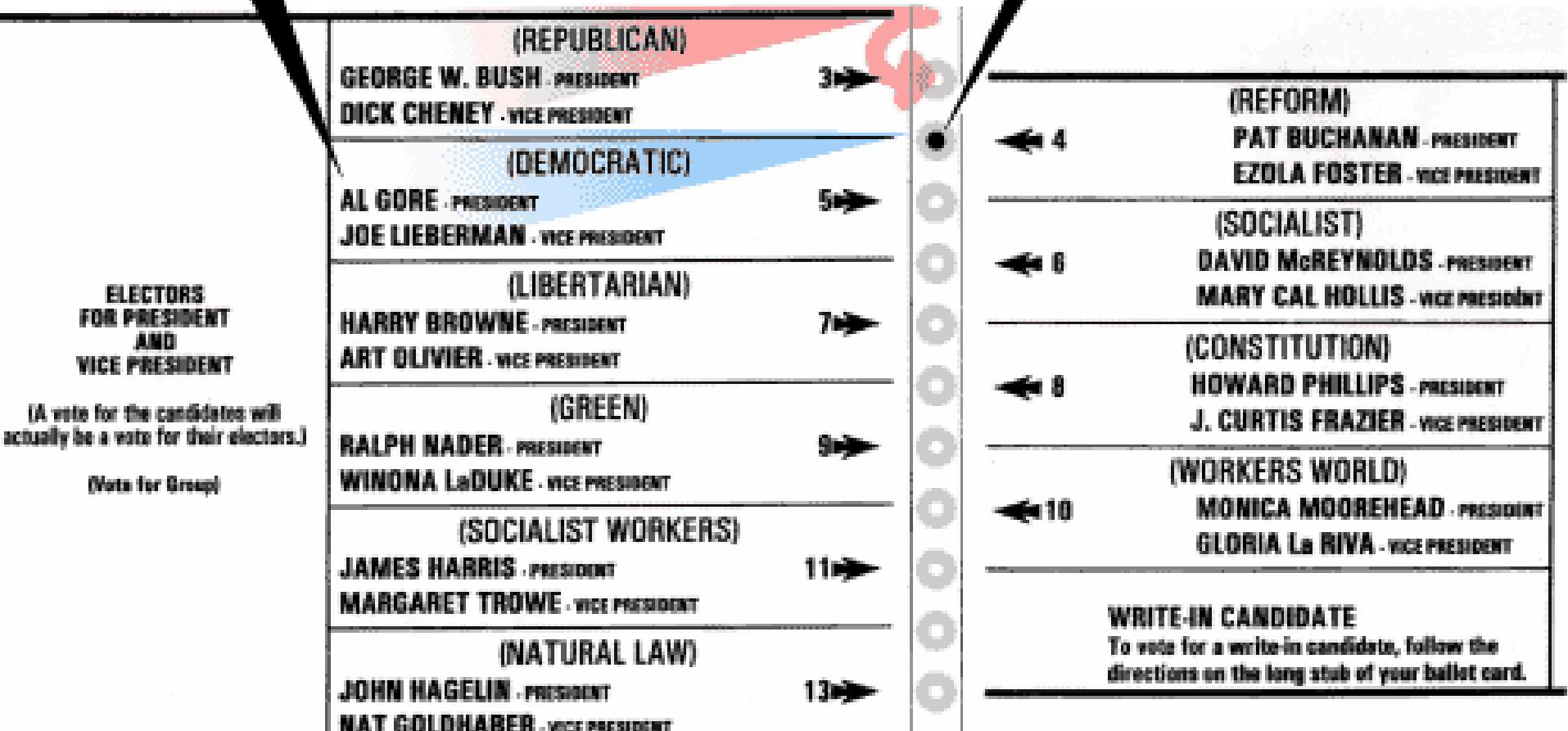


Confusion at Palm Beach County polls

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.



From: Lana Hires
Subject: 2000 November Election

I need some answers! Our department is being audited by the County.

I have been waiting for someone to give me an explanation as to why Precinct 216 gave Al Gore a minus 16022 when it was uploaded. Will someone please explain this so that I have the information to give the auditor instead of standing here "looking dumb".

2000 Election Spurs Electoral Reform

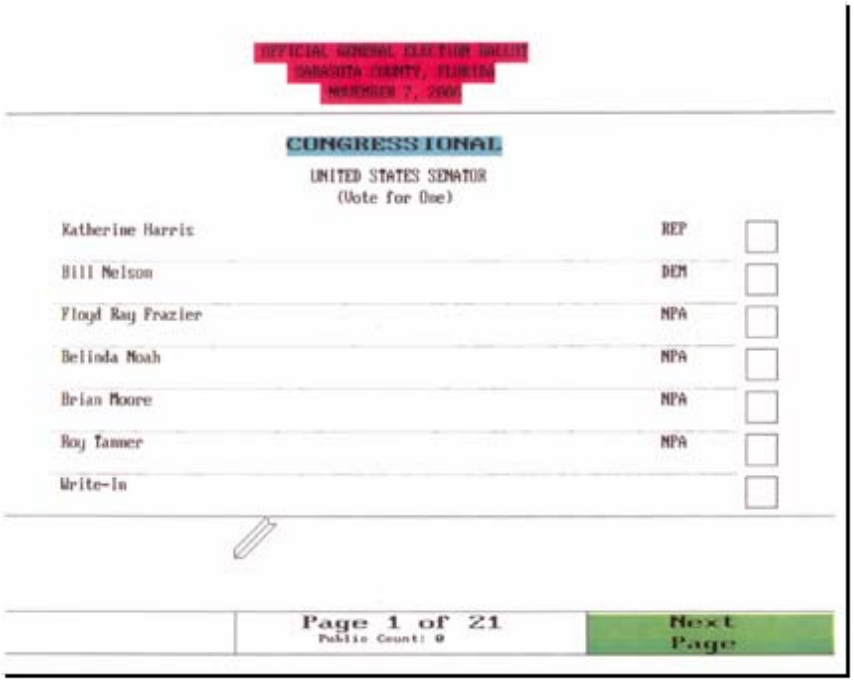
ct 2002: Congress passes Help America Vote Act (HAVA): states must upgrade voting systems by 2006; provides $3.6 billion in federal funding.

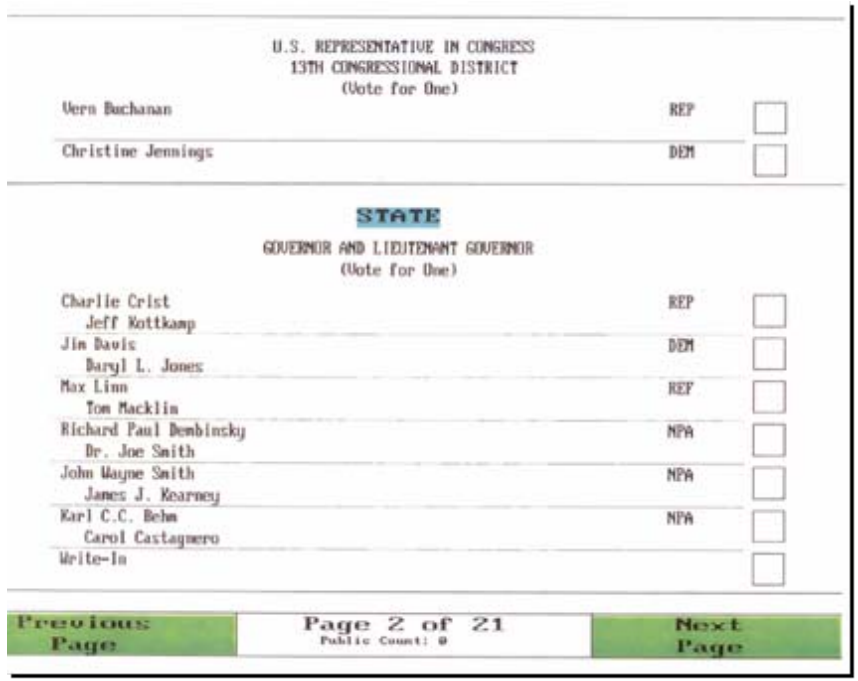
AVA accelerates adoption of e-voting.

KEYS TO THE KINGDOM

Photo taken from Diebold's online store. The keys that open every Diebold touch-screen voting machine. Working copies have been made from the photo.

U.S. Congress Rep., Sarasota FL, Nov 2006





Margin of victory: 369 votes (0.15% of voters)
No vote recorded: 18,412 votes (14% of e-voters)

David Wagner, UC Berkeley

California Top-to-Bottom Review

Jun 2007: Secretary Bowen hires 43 experts to evaluate voting systems used in CA.

Diebold


Accu-Vote
PLACE BALLOT INSIDE TO KEEP VOTING SECRET
After Voting is Completed
INSTRUCTIONS TO VOTERS
When inserting ballot into Accu-Vote Machine,
GRIP BELOW
DOTTED LINE

Hart InterCivic

Sequoia Voting Systems

Teams

Matt Bishop, PI:

- Accessibility
- Red teams

David Wagner, PI:

- Document review
- Source code review

Teams

Matt Bishop, PI:

- Accessibility
- Red teams

David Wagner, PI:

- Document review
- Source code review

Team members

- Diebold, Hart: *Bob Abbott,* Mark Davis, Joseph Edmonds, Luke Florer, Elliot Proebstel, Brian Porter, Sujeet Shenoi, Jacob Stauffer
- Sequoia: *Dick Kemmerer, Giovanni Vigna,* Davide Balzarotti, Greg Banks, Marco Cova, Viktoria Felmetsger, William Robertson, Fredik Valeur
- Diebold: *David Wagner, Alex Halderman,* Joe Calandrino, Ari Feldman, Harlan Yu, Bill Zeller
- Hart: *Eric Rescorla*, Sreenu Inguva, Hovav Shacham, Dan Wallach
- Sequoia: *Matt Blaze,* Arel Cordero, Sophie Engle, Chris Karlof, Naveen Sastry, Micah Sherr, Till Stegers, Ping Yee

Team members (more)

Document review:

- Diebold: Candice Hoke, Dave Kettyle, Tom Ryan
- Hart: Joe Hall, Laura Quilter
- Sequoia: Aaron Burstein, Nathan Good, Deirdre Mulligan

Accessibility:

- Diebold, Hart, Sequoia: Noel Runyan, Jim Tobias

We found…

We found… significant security problems in all 3 systems.

Crypto was often severely flawed, or missing entirely.

Sequoia

Sequoia invented their own password encryption algorithm.

Sequoia

Sequoia invented their own password encryption algorithm. With the Sequoia algorithm, the password "**`sekret`**" encrypts to "**`sekretXYZ`**"*.

Sequoia

Sequoia invented their own password encryption algorithm. With the Sequoia algorithm, the password "**`sekret`**" encrypts to "**`sekretXYZ`**"*.

* Obfuscated for 'security'; "XYZ" are not the real letters.

Sequoia

"We could not find a single instance of correctly used cryptography that successfully accomplished the security purposes for which it was apparently intended."

— Sequoia source team

Diebold

One of Diebold's passwords was

Diebold

One of Diebold's passwords was "**`diebold`**".

Hart

In some places, Hart avoided trivially broken crypto by…

Hart

In some places, Hart avoided trivially broken crypto by… omitting it entirely.

Hart

In some places, Hart avoided trivially broken crypto by… omitting it entirely.

When you connect a polling-place machine to the county's central PC, it trusts the PC implicitly.
The county PC can instruct the machine to overwrite its software, and it will blindly comply. (No authentication!)

Diebold and Hart's systems fail to adequately protect the secrecy of the ballot.

Diebold

The Diebold touchscreen stores vote records in the order they were cast.

Diebold

The Diebold touchscreen stores vote records in the order they were cast.

A crypto PRNG is used to generate unique IDs, stored with each vote record…

Diebold

The Diebold touchscreen stores vote records in the order they were cast.

A crypto PRNG is used to generate unique IDs, stored with each vote record… but the seed is known to officials, enabling them to recover the order votes were cast in.

Diebold

The Diebold touchscreen stores vote records in the order they were cast.

A crypto PRNG is used to generate unique IDs, stored with each vote record… but the seed is known to officials, enabling them to recover the order votes were cast in.

Each electronic vote record is time stamped.

Hart

The Hart e-voting machine stores vote records in a pseudorandom order.

Hart

The Hart e-voting machine stores vote records in a pseudorandom order.

But it stores the CRC of each vote record in the audit log…

Hart

The Hart e-voting machine stores vote records in a pseudorandom order.

But it stores the CRC of each vote record in the audit log… and audit log entries are stored in the order they're logged.

The code fails to follow sound engineering principles expected of security-critical systems.

Diebold

```
void GlibPutPixel(UINT xx, UINT yy, Pixel_t Color) {
  // Check for library not initialized or (x,y) out of range
  if(FrameBuffer != FALSE || (xx < USER_X) || (yy < USER_Y)) {
    // Compute the frame buffer offset and write the pixel
    FrameBuffer[FB_OFFSET(xx,yy)] = Color;
  }
}
```

Diebold

```
TCHAR name;
_stprintf(&name, _T("\\Storage Card\\%s"),
   findData.cFileName);
Install(&name, hInstance);
```

All 3 systems allow malicious code to propagate virally.

Diebold

The Diebold code that reads data off the memory card has buffer overruns and other vulnerabilities.

Diebold

1. Attacker writes malicious data onto a memory card.
2. Uploading results at county HQ on election night infects county machines.
3. Infected county machines write malicious data and code onto memory cards that will infect all polling-place machines in the county in the next election.

Hart

After the election, each polling-place machine is connected by Ethernet to a county PC. The PC can install new software onto the voting machine.

Hart

After the election, each polling-place machine is connected by Ethernet to a county PC. The PC can install new software onto the voting machine.

The voting machine can exploit buffer overruns in the code on the PC to take control of the PC.

Hart

1. Attacker installs malicious code onto a voting machine.
2. When connected to the county PC, it hacks the PC.
3. The county PC then installs malicious code onto every voting machine subsequently connected to it.

A single individual, with no special access, could introduce a virus onto a single voting machine,

A single individual, with no special access, could introduce a virus onto a single voting machine, and this virus could infect every machine in the county.

Quotes from the reports

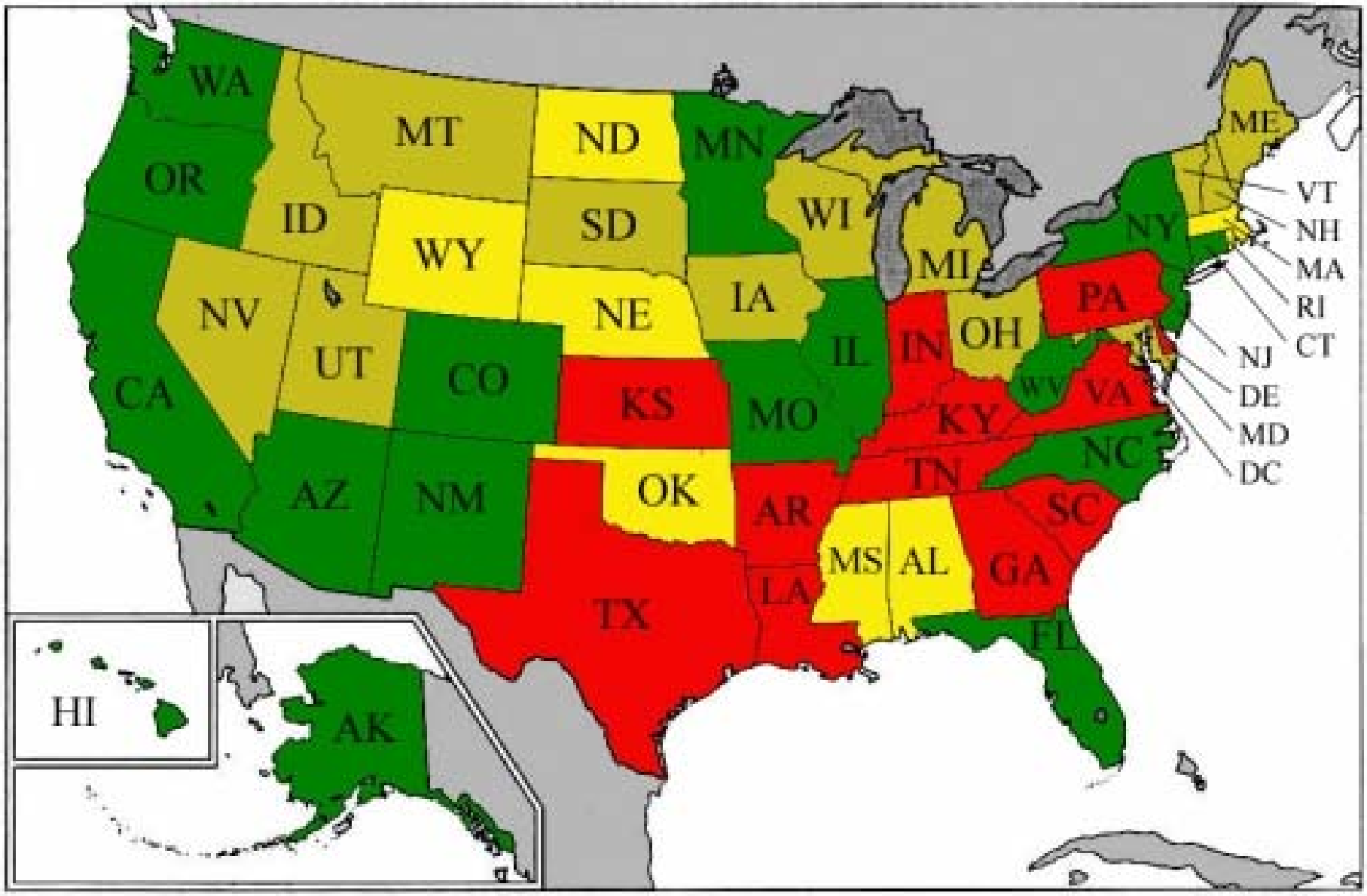
- “We found pervasive security weaknesses throughout the Sequoia software. Virtually every important software security mechanism is vulnerable to circumvention.”
- “Our study of the Diebold source code found that the system does not meet the requirements for a security-critical system. It is built upon an inherently fragile design and suffers from implementation flaws that can expose the entire voting system to attacks.”
- “The Hart software and devices appear to be susceptible to a variety of attacks which would allow an attacker to gain control of some or all of the systems in a county. [..] Many of these attacks can be mounted in a manner that makes them extremely hard to detect and correct. We expect that many of them could be carried out in the field by a single individual, without extensive effort, and without long-term access to the equipment.”

David Wagner, UC Berkeley

Results

On August 6th, California Secretary of State Debra Bowen imposed new conditions on the use of these 3 voting systems.

National relevance



Concluding thoughts

- E-voting is a paradigmatic trustworthiness problem, and one where researchers from many fields can have a big impact

- Voting systems must be auditable if they are to be worthy of our trust

Backup slides / extras

The Importance of Verification

- Transparency is essential. We must be able to convince the loser, and his/her supporters, that he/she lost the election.

- Requirement: Voters must be able to verify that their votes are recorded correctly. Observers must be able to verify that votes are counted correctly.

The Technical Challenge

- Determining whether software will work correctly on Election Day is beyond the state of the art in computer science. How to provide verification?

- Analogy: Running an election on Satan's computers. How do we do that securely, when the computers might misbehave in arbitrarily pernicious ways?

A Solution Framework

Verify votes are recorded correctly:

- Voter-verified paper records

Verify votes are counted correctly:

- Routine post-election audits (statistical recounts)

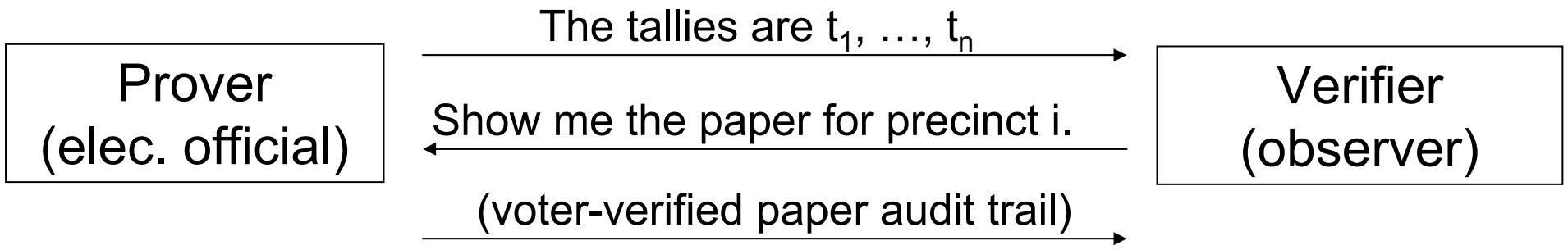
- Goal of an audit: Provide evidence that a 100% manual recount would not change the election outcome.

1% Statistical Audit

- After election, publish vote totals in each precinct. Randomly choose 1% of precincts and manually recount the paper records in those precincts. If paper count $\neq$ electronic count, there was fraud or error.

- If $\geq$ 300 precincts are erroneous, detection is likely. Consequently: If paper count $=$ electronic count, then no more than $\approx$300 precincts are erroneous.

The Protocol



Election Staff Convicted in Recount Rig

By M.R. KROPKO
The Associated Press
Wednesday, January 24, 2007; 6:09 PM

CLEVELAND -- Two election workers were convicted Wednesday of rigging a recount of the 2004 presidential election to avoid a more thorough review in Ohio's most populous county.

Prosecutors accused Maiden and Dreamer of secretly reviewing preselected ballots before a public recount on Dec. 16, 2004. They worked behind closed doors for three days to pick ballots they knew would not cause discrepancies when checked by hand, prosecutors said.

Verifiable Randomness

Need verifiably random sample selection.

It must be:

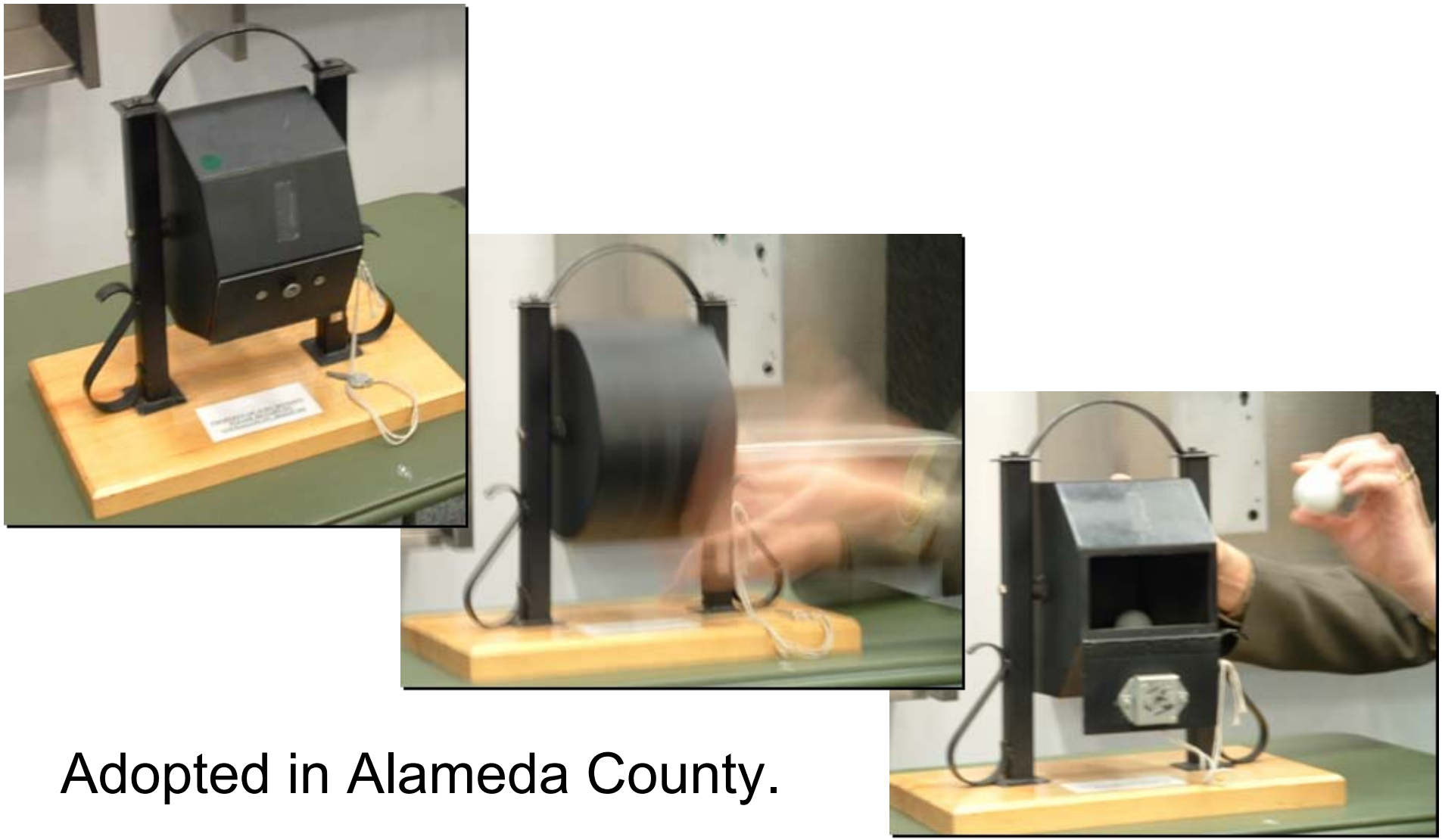
- transparent (no computers);
- understandable (no fancy math);
- designed so observers can verify that it is free of manipulation;
- efficient (choose large samples quickly).

Solution #1: 10-sided Dice

- Number the precincts 0,1,2,3,...
- Throw three 10-sided dice to get a random number in the range 0,...,999.
- If the number is a valid precinct, add it to the sample. Repeat until sample is large enough.

- Adopted in several California counties.

Solution #2: Lottery-style Drawings



Adopted in Alameda County.

David Wagner, UC Berkeley


PHEBOLD

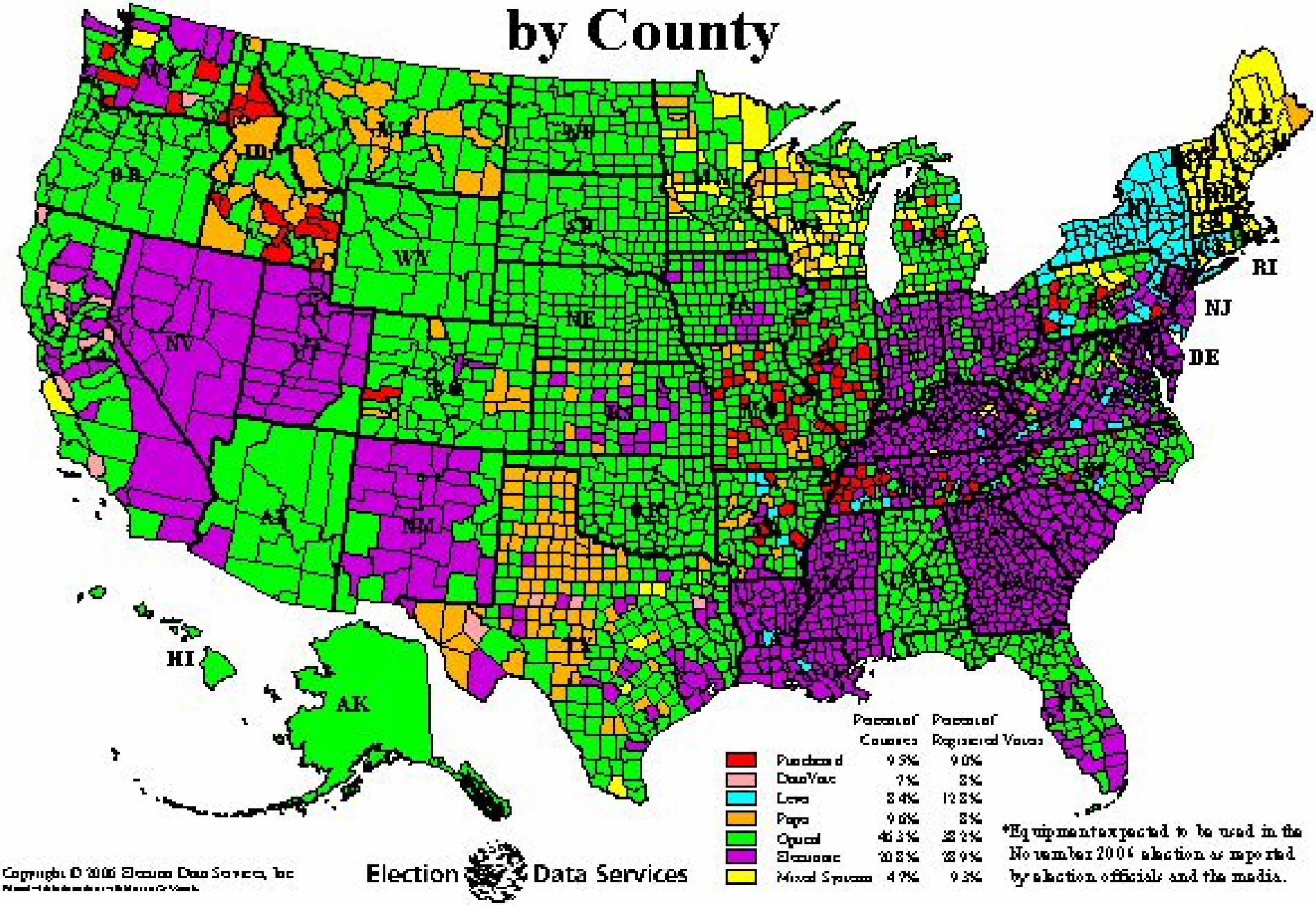

** TEST COUNTING MODE **
Please Insert
Your Card


09/07/2004


VOTE
You have already checked the maximum selections in this contest.
If you wish to select a different selection in this contest, you must first de-select a previous selection.
Return to ballot


Accu-Vote
PLACE BALLOT INSIDE TO KEEP VOTING SECRET
INSTRUCTIONS TO VOTERS
After Voting is Completed:
1. Cloister ballot inside this secrecy folder.
2. Take ballot and secrecy folder to Accu-Vote machine.
3. Feed ballot straight into machine while holding onto the area below dotted line.
When inserting ballot into Accu-Vote Machine,
GRIP BELOW
DOTTED LINE

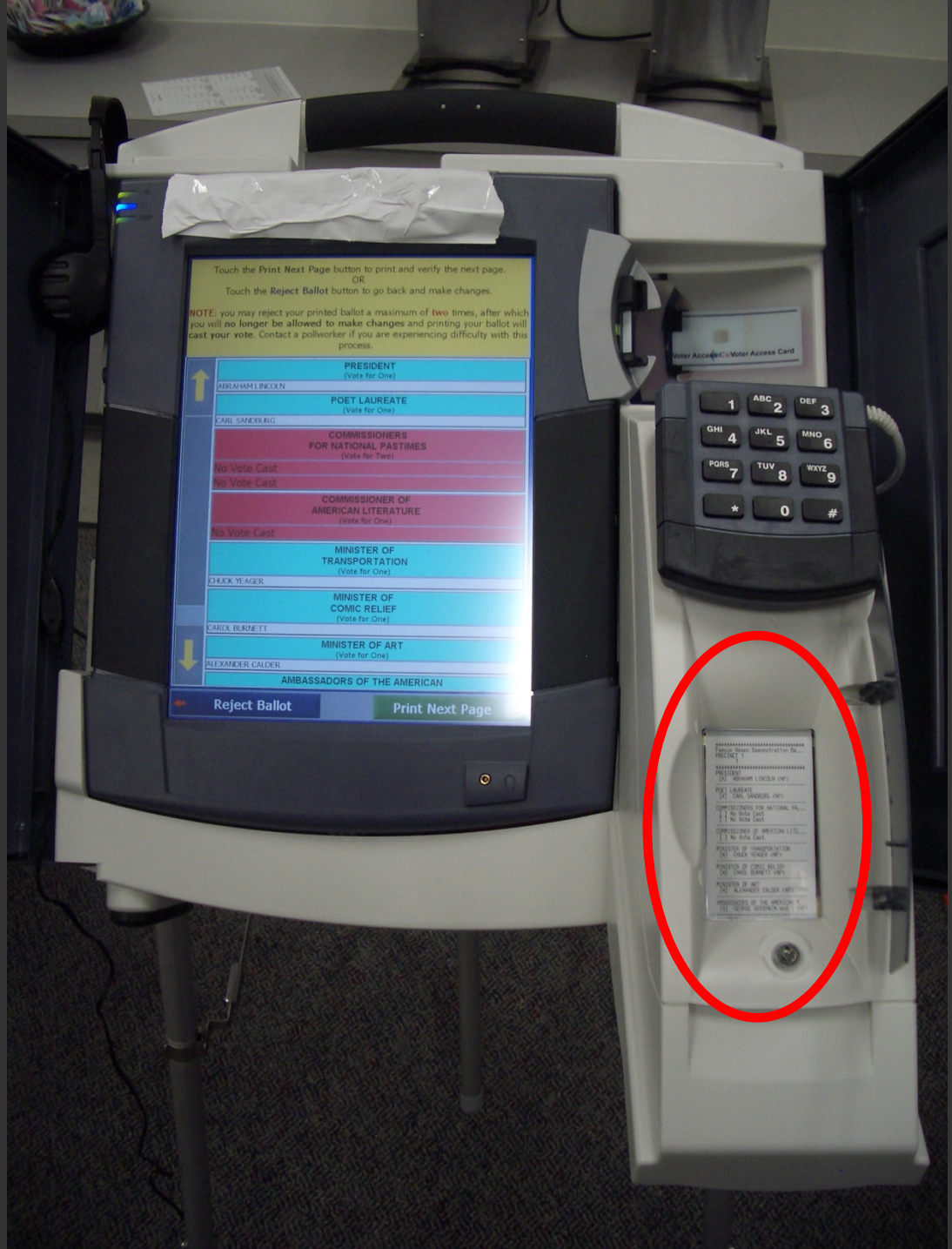
Anticipated 2006 Voting Equipment Usage by County



California Rebukes Vendor, Apr 2004

Citing concerns about the security and reliability of new computerized voting machines, California Secretary of State Kevin Shelley announces Friday during a Sacramento news conference that he is banning the use of touch-screen voting machines in the state in the November election

Problem Statement


Touch the Print Next Page button to print and verify the next page.
OR
Touch the Reject Ballot button to go back and make changes.
NOTE: you may reject your printed ballot a maximum of two times, after which you will no longer be allowed to make changes and printing your ballot will cast your vote. Contact a pollworker if you are experiencing difficulty with this process.
PRESIDENT
(Vote for One)
ABRAHAM LINCOLN
POET LAUREATE
(Vote for One)
CARL SANDBURG
COMMISSIONERS FOR NATIONAL PASTIMES
(Vote for Two)
No Vote Cast
No Vote Cast
COMMISSIONER OF AMERICAN LITERATURE
(Vote for One)
No Vote Cast
MINISTER OF TRANSPORTATION
(Vote for One)
CHUCK YEAGER
MINISTER OF COMIC RELIEF
(Vote for One)
CAROL BURNETT
MINISTER OF ART
(Vote for One)
ALEXANDER CALDER
AMBASSADORS OF THE AMERICAN
Reject Ballot
Print Next Page
Voter Access Card
1
ABC 2
DEF 3
GHI 4
JKL 5
MNO 6
PQRS 7
TUV 8
WXYZ 9
*
0
#

Two Fundamental Audit Problems

1. After an audit is performed, compute the level of confidence that it provides (assuming worst-case errors).

2. Design an audit strategy that provides a desired level of confidence at minimum cost, or maximum confidence at fixed cost.

Challenges for Statistical Audit Analysis

- Sample stratified by counties.
- Contest boundaries may cross county lines.
- Precinct selection not equiprobable across counties.
- Precinct sizes vary.
- Base rate of occasionally miscounted votes. (So, you can't cry foul after seeing just one miscounted vote.)
- Is calculation of confidence level NP-hard?

Credits: Philip Stark

Challenges for Statistical Audit Design

- All of the above, plus…
- Margin of victory differs in each contest.
- Can't wait until you have vote totals from all counties before beginning audit in some counties.
- Need an escalation strategy if audit cannot rule out possibility of error in election outcome. (Sequential hypothesis testing?)
- Cost of audit should be predictable and fair.
- Is statistical audit design NP-hard?

Improving Audits? (speculative)

- Can we reduce cost of audits by reducing unit size?
  - Ballot-based audits. e.g., print a serial number on ballot as it is scanned, and pick a random sample of ballots.

- Can we use demographic or historical voting data to reduce cost of audits?

Conclusions

- E-voting security is hard, because computers aren't transparent.
- Auditing can help. Statistics can make up for the failings of computer science.

To Learn More…

- "Evaluation of Audit Sampling Models and Options for Strengthening California's Manual Count." Report of the California Post-Election Audit Standards Working Group. July, 2007.

- "Post-Election Audits: Restoring Trust in Elections." Brennan Center and Samuelson Cyberlaw Clinic. August, 2007.

- Talk to Philip Stark.

Extras, leftovers

More than 4,500 North Carolina votes lost because of mistake in voting machine capacity

JACKSONVILLE, N.C. (AP) — More than 4,500 votes have been lost in one North Carolina county because officials believed a computer that stored ballots electronically could hold more data than it did. Scattered other problems may change results in races around the state.

Officials said UniLect Corp., the maker of the county's electronic voting system, told them that each storage unit could handle 10,500 votes, but the limit was actually 3,005 votes.

Machine error gives Bush 3,893 extra votes in Ohio

By John McCarthy, Associated Press

COLUMBUS, Ohio — An error with an electronic voting system gave President Bush 3,893 extra votes in suburban Columbus, elections officials said.

Franklin County's unofficial results had Bush receiving 4,258 votes to Democrat John Kerry's 260 votes in a precinct in Gahanna. Records show only 638 voters cast ballots in that precinct. Bush's total should have been recorded as 365.

Broward Vote-Counting Blunder Changes Amendment Result

POSTED: 1:34 pm EST November 4, 2004

BROWARD COUNTY, Fla. -- The Broward County Elections Department has egg on its face today after a computer glitch misreported a key amendment race, according to WPLG-TV in Miami.

Amendment 4, which would allow Miami-Dade and Broward counties to hold a future election to decide if slot machines should be allowed at racetracks, was thought to be tied. But now that a computer glitch for machines counting absentee ballots has been exposed, it turns out the amendment passed.

"The software is not geared to count more than 32,000 votes in a precinct. So what happens when it gets to 32,000 is the software starts counting backward," said Broward County Mayor Ilene Lieberman.

Broward County Mayor Ilene Lieberman says voting counting error is an "embarrassing mistake."

That means that Amendment 4 passed in Broward County by more than 240,000 votes rather than the 166,000-vote margin reported Wednesday night. That increase changes the overall statewide results in what had been a neck-and-neck race, one for which recounts had been going on today. But with news of Broward's error, it's clear amendment 4 passed.

November 8, 2004

George Gilbert
Director of Elections
Guilford County Board of Elections
Greensboro, NC

Dear George,

As you know, Tuesday's election drew an unprecedented number of voters to the polls. This unanticipated level of voter participation was a challenge that we believe was managed very well in Guilford County.

On behalf of the team at Election Systems & Software, I would like to congratulate you and your staff on running a very successful election. And, all of us at ES&S want to thank you for the opportunity to partner with you to carry out our important roles in the democratic process. The success of this election was the result of a tremendous amount of hard work from everyone involved. Where challenges did arise, we worked together to address them quickly and effectively so the election process continued uninterrupted. The countless hours of preparation paid off, and all in all, it was a very good day.

One challenge we did face was the incorrect information contained in preliminary and unofficial returns for certain contests in the Guilford County "One Stop" precinct used to collect totals for early voting. As you know, this occurred because exceptional voter participation generated a number of ballots and votes cast that exceeded the capacity of single precinct vote counters accepting this amount of data in the Election Reporting Manager results reporting software.

This limitation in the results reporting software was previously documented and known to ES&S. To clarify further, the limitation has nothing to do with the Votronic tabulation systems. No votes were lost. All ballot data and vote counts were correctly captured and reported by the Votronic touch screen tabulation systems.

We regret any confusion the discrepancy in early vote totals has caused.

We would like to explain in further technical detail what caused this issue, should you or others at the county have questions. The 32,767 capacity limitation at a single precinct level is a function of the design and definition of the results database used by ERM. The data storage element used to record votes at the precinct level is a two byte binary field. 32,767 is 2 to the 15th power, which is the maximum number held by a two byte word (16 bits) in memory, where the most significant bit is reserved as the sign bit (a plus or minus indicator). Additionally, ERM precinct

11208 John Galt Boulevard, Omaha, Nebraska 68137-2364 USA
PHONE: (402) 593-0101 ■ Toll Free: 1 (800) 247-8683 ■ FAX: (402) 593-8107
Equal Opportunity Employer/Affirmative Action Employer
www.essvote.com

count level data is stored in a binary computer format known as two's complement. Data on ERM results reports are printed as the absolute value of the two's complement of the associated data in the ERM database. This means that once the 32,767 limitation is reached, additional incremental tallies of vote results would not be printed correctly (32,768 through 65, 536 would actually be represented as 65,536 to 32,768).

While this value, 32,767 is certainly higher than any practical value that could be tabulated in a single election day precinct, the consideration of reporting all absentee ballots or early voting into a single absentee or "One Stop" precinct does hold the possibility of yielding much higher totals than what may be possible in single election day precincts.

While the discrepancy in preliminary vote totals did cause some early confusion, it is very important to note that the final results reported to the state were accurate and complete. Final counts based on the Votronic systems and paper tapes were fully accurate and correct.

To avoid this limitation in elections where the One Stop early voting totals may exceed the 32,767 limitation, ES&S would recommend one of the following:

1. Using the Unity EDM software, code multiple precincts to support the larger counts. Create a split for each ballot style for each precinct. Configure early voting terminals and follow vote collection procedures that would ensure no individual precinct totals would approach the 32,767 limitation.

2. Collect early voting "One Stop" and other absentee votes into Election Day precincts.

3. Upgrade systems and software to the Unity 2.5 or Unity 3.0 versions, when available in North Carolina. The ERM database has been expanded in these versions to accommodate vote totals in excess of millions of votes in any individual precinct.

Heretofore, in previous elections, Guilford County had configured, collected and distributed the early voting results into multiple separately defined precincts (as suggested above, avoiding this limitation). ES&S was not aware that this practice had changed. Had we been aware of this change, we would have advised Guilford County of this limitation and suggested one of the other configuration options.

ES&S shares Guilford County's commitment to making sure every vote cast is counted accurately. We are absolutely confident in the accuracy of the final results that were reported. If you have additional questions on this issue, please do not hesitate to contact me.

Sincerely,

Ken Carbullido
Senior Vice President, Product and Software Development
Election Systems & Software Inc.

Maintaining Voter Confidence. Enhancing the Voting Experience

11208 John Galt Boulevard, Omaha, Nebraska 68137-2364 USA
PHONE: (402) 593-0101 ■ Toll Free: 1 (800) 247-8683 ■ FAX: (402) 593-8107
Equal Opportunity Employer/Affirmative Action Employer
www.essvote.com

We would like to explain in further technical detail what caused this issue, should you or others at the county have questions. The 32,767 capacity limitation at a single precinct level is a function of the design and definition of the results database used by ERM. The data storage element used to record votes at the precinct level is a two byte binary field. 32,767 is 2 to the 15th power, which is the maximum number held by a two byte word (16 bits) in memory, where the most significant bit is reserved as the sign bit (a plus or minus indicator). Additionally, ERM precinct count level data is stored in a binary computer format known as two's complement. Data on ERM results reports are printed as the absolute value of the two's complement of the associated data in the ERM database. This means that once the 32,767 limitation is reached, additional incremental tallies of vote results would not be printed correctly (32,768 through 65, 536 would actually be represented as 65,536 to 32,768).


http://denvervoice.org


LIVE FREE
ELECTRONIC VOTING IS UNRELIABLE
PAPER BALLOTS
THE COMPUTER ATE MY VOTE!


HOW LONG WILL IT TAKE TO GET IT RIGHT


ELECTION FRAUD
MEDIA BLACKOUT


VOTE
but
VERIFY!


VOTING WITHOUT AUDITING ARE WE INSANE?


SECRET SOFTWARE SECRET GOVERNMENT


LIVE FREE or DIE BOLD
VISUALIZE TRUE DEMOCRACY
BE THE CHANGE!
Paper Ballots Hand Counted
SECURE ELECTIONS