

Security of Electronic Voting

James Walden

Northern Kentucky University

Voting Process Targets

1. Registration
2. Nomination
3. Polling Place Access
4. Voter Manipulation
5. Ballot Manipulation
6. Tabulation

Threats

1. Individual Voters
2. Outside Attackers
3. Poll Workers
4. Election Officials
5. Equipment Vendors
6. Policy Makers

Registration

- Age (lowered to 18, 26th amendment, 1971)
- Race (15th amendment, 1870)
- Gender (20th amendment, 1920)
- Residency
 - DC given presidential vote 23rd amendment, 1961.
- Property Ownership
 - Poll taxes prohibited by 24th amendment, 1964.
- Criminal Record
 - Most states disallow felons to vote in jail.
 - Many states disallowing voting during parole.
 - Only 2 states (KY,VA) permanently disallow.

Voter Purges

Bad Databases

- 2004-05, SSA “resurrected” 23,366 records.

Voters are purged secretly without notice.

- County Election Commissioner Sue Sautermeister purged 10,000 voters before Mississippi March 2008 primary from her home PC.

Bad Matching Criteria.

- 2000, Florida, 60,000 purged based on 80% of surname + DOB. ~5000 appeals afterwards.
- 2008, Muscogee County, GA, purged 700 voters based purely on name. 1/3 appealed.



Voter Purges

HOW BAD MATCHING CRITERIA CAN RESULT IN DISENFRANCHISEMENT

```
Field    >> FN          >> MN          >> LN          >> D.O.B
>> Name 1: >> John         >> Fitzgerald   >> George      >> 11/20/1976
>> Name 2: >> Johnny       >> Fred         >> Georges     >> 11/22/1976

>> Number First Name matching letters = 04 >>
>> Percentage of Last Name = 85.7% >>
>> Result = MATCH >>
```

Source: Gregory Palast, *The Wrong Way to Fix the Vote*, WASH. POST, June 10, 2001, at B01.

Who Will Vote

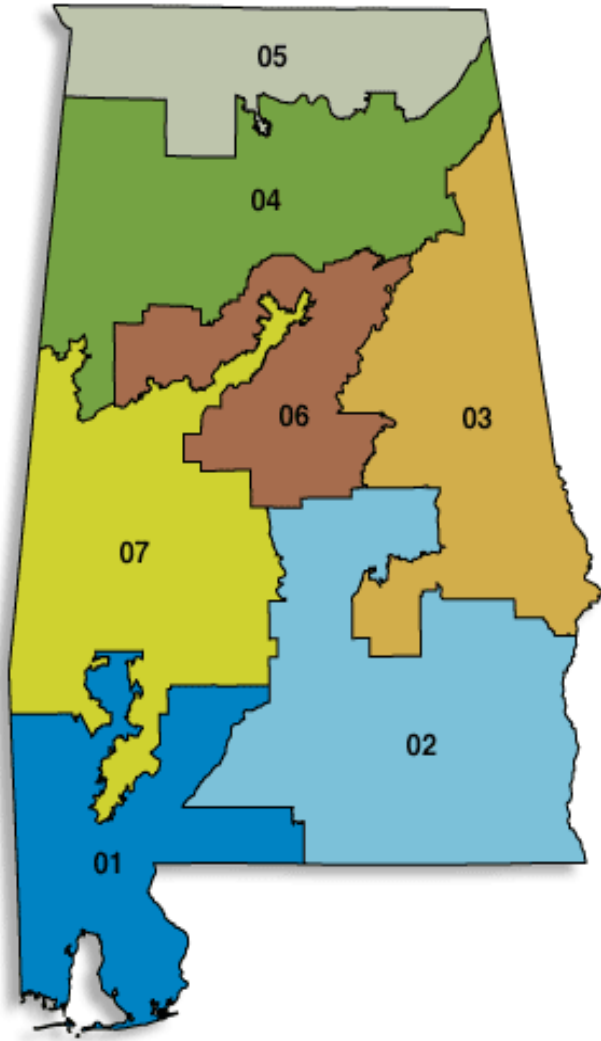
Robo-calls

- Claim that voter can vote by phone.
- Claim that voter is ineligible to vote.
- Incorrect precinct or polling place.
- Incorrect date.
- Annoying calls appear to be from other party.

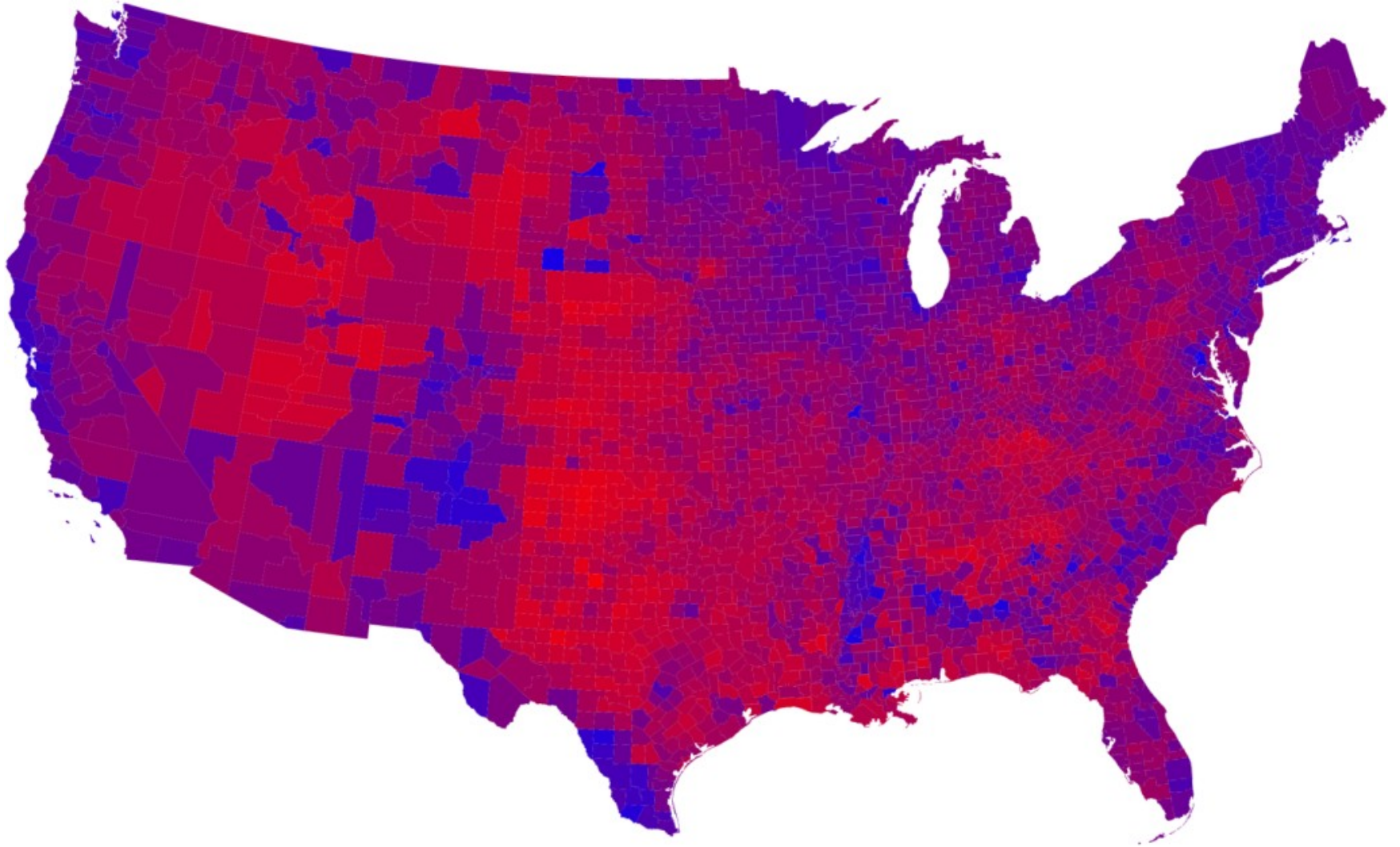
Mandatory voting

- Australia, Brazil, Greece, GA (1777), etc.
- Shifts campaign from motivating base to convincing undecideds.

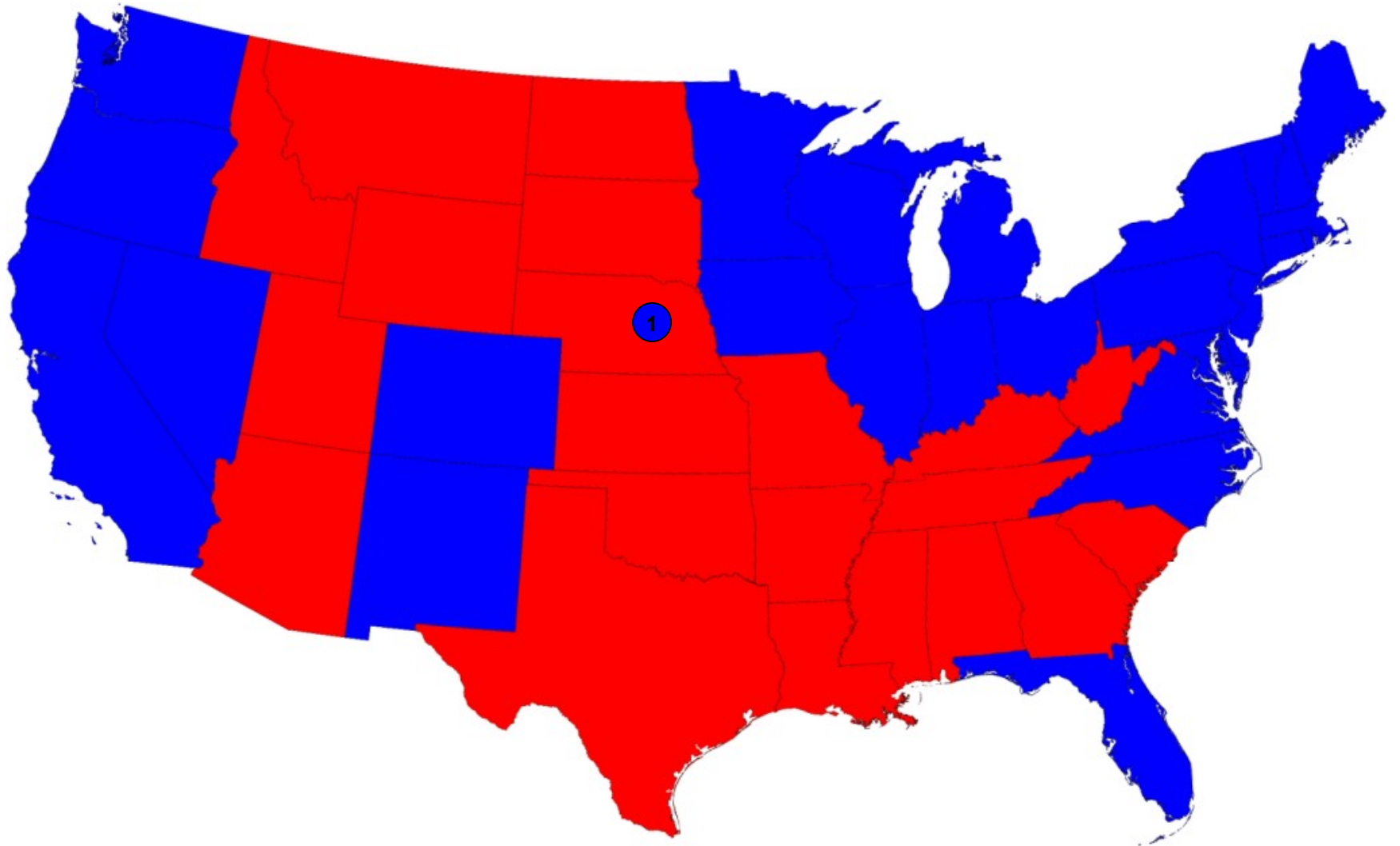
Shortest Splitline Algorithm



Popular Vote (by county)



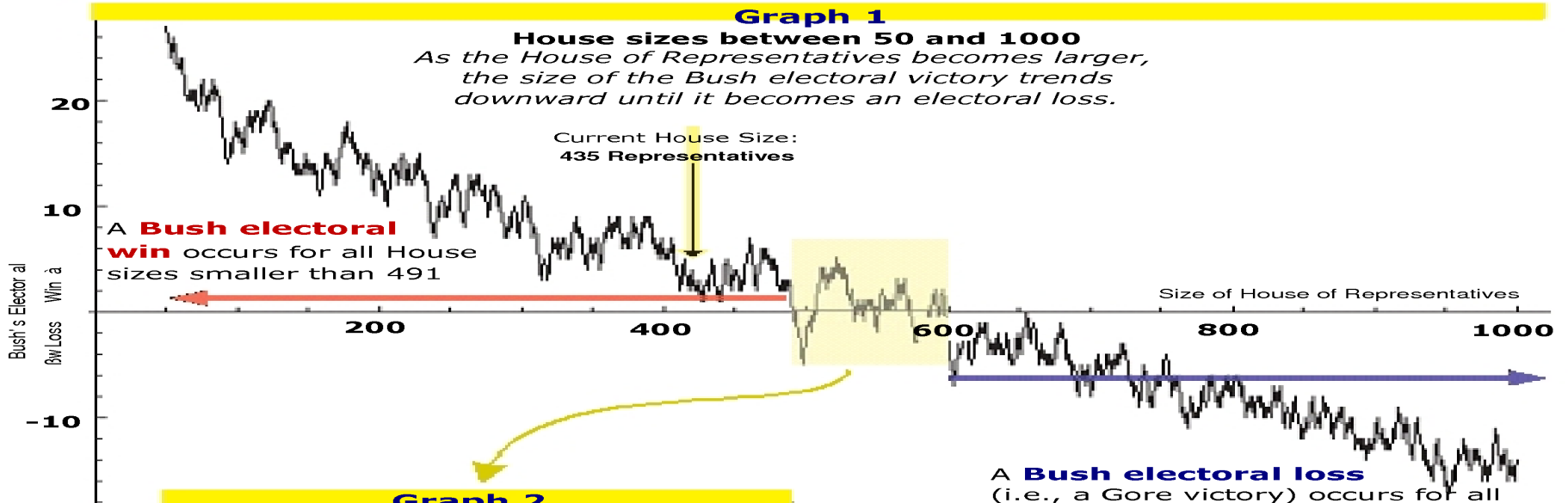
Electoral College Amplifies Fraud



The Neubauer-Zeitlin Analysis
2000 Presidential Election
 Calculation of the Electoral College Results
as a function of the size of the
 House of Representatives

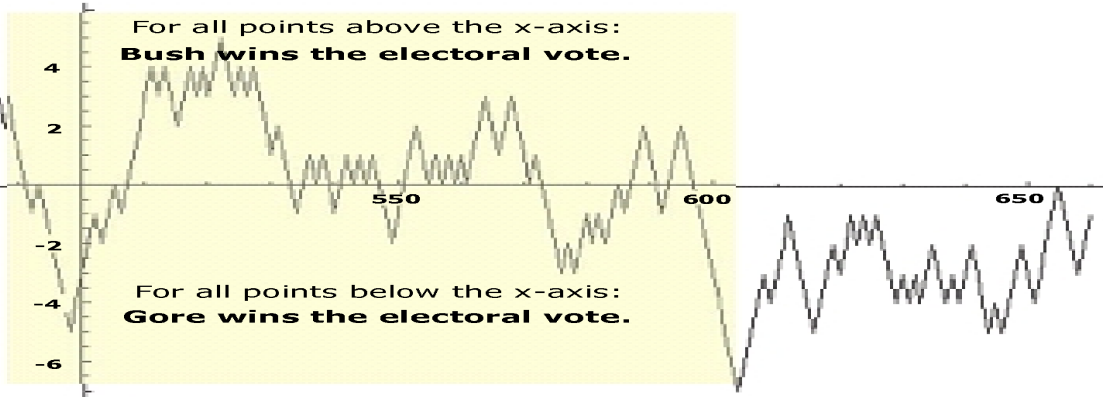
Graph 1

House sizes between 50 and 1000
As the House of Representatives becomes larger, the size of the Bush electoral victory trends downward until it becomes an electoral loss.



Graph 2

House sizes between 480 and 610
The Capricious Outcomes



Paper Ballots

Australian Ballot

- Standard paper ballot.
- Distributed at polls.
- Marked in secret.

Security Issues

- Interpretation of marks.
- Spoiling votes.

GENERAL ELECTION <i>Elección General</i> Sample County <i>Condado de Muestra</i> November 04, 2008 - 04 Noviembre 2008		Precinct <i>Distrito</i> 003
Voter Instructions: Please use a blue or black ink pen to mark your choices on the ballot. To vote for your choice in each contest, completely fill in the box provided to the left of your choice. To vote for a write-in candidate, completely fill in the box provided to the left of the words "Write-In" and write in the name of the candidate on the line provided. Instrucciones para los Votantes: Favor de usar una pluma de tinta negra o azul para marcar su boleta. Para votar por su selección en cada carrera, llene completamente el espacio cuadrado a la izquierda de su selección. Para votar por voto escrito, llene completamente el espacio cuadrado a la izquierda de las palabras "Voto Escrito" y escriba el nombre del candidato en la línea provista.		County Commissioner Precinct 4 <i>Comisionado del Condado Recinto 4</i> Vote for one <i>Vote por uno</i> <input type="checkbox"/> Walt Whitman Historical Party <input type="checkbox"/> Pandora Ancient Party <input checked="" type="checkbox"/> Write-In <i>Voto Escrito</i> John Adams
President <i>Presidente</i> Vote for one <i>Vote por uno</i> <input checked="" type="checkbox"/> Abraham Lincoln Historical Party <input type="checkbox"/> Helen of Troy Ancient Party		City Council <i>Concejo Municipal</i> Vote for two <i>Vote por dos</i> <input checked="" type="checkbox"/> Sojourner Truth <input checked="" type="checkbox"/> Mark Twain <input type="checkbox"/> Harriet Tubman
		Proposition 1 To declare Key Lime Pie the official dessert of Election Day. <i>Vote For or Against</i> Proposición 1 Para declarar el pastel clave de cal el postre oficial del Día Electoral. <i>Vote A Favor o En Contra</i> <input checked="" type="checkbox"/> For <i>A Favor</i> <input type="checkbox"/> Against <i>En Contra</i>

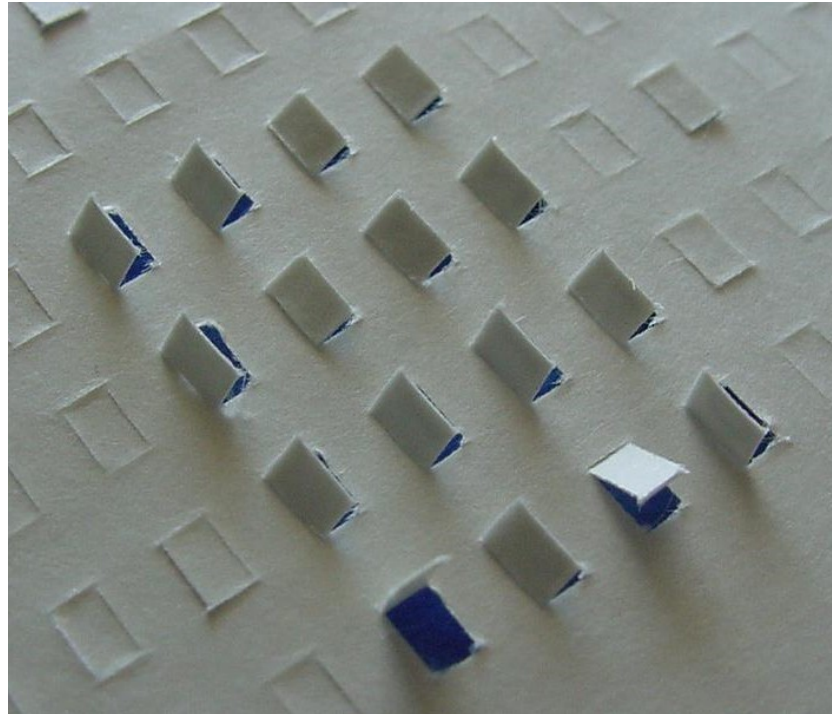
Punched Card Systems

Flaws

- Hanging Chads
- Dimpled Chads
- Chad Jams

HAVA 2002

- Reaction to 2000 Florida.
- \$3.8B to replace punch card + lever machines.
- Accessibility requirements.
- No security requirements.



Electronic Voting (DRE)

Reliability

- History of inaccuracy.
- Hardware failures (10% fail each election).

Security

- Designed like a PC.
- Most use Windows CE.
- Impossible to audit without paper trail.

Usability

- Support for disabilities, multiple ballots, languages.
- Touch screen problems.
- Hart double-selection 'bug'



eSlate made by HartIC

E-Voting Problems in Florida

2000 Volusia County: Diebold voting machine gives Gore -16,022 votes, Bush 2,813 votes in a precinct of 585 voters.

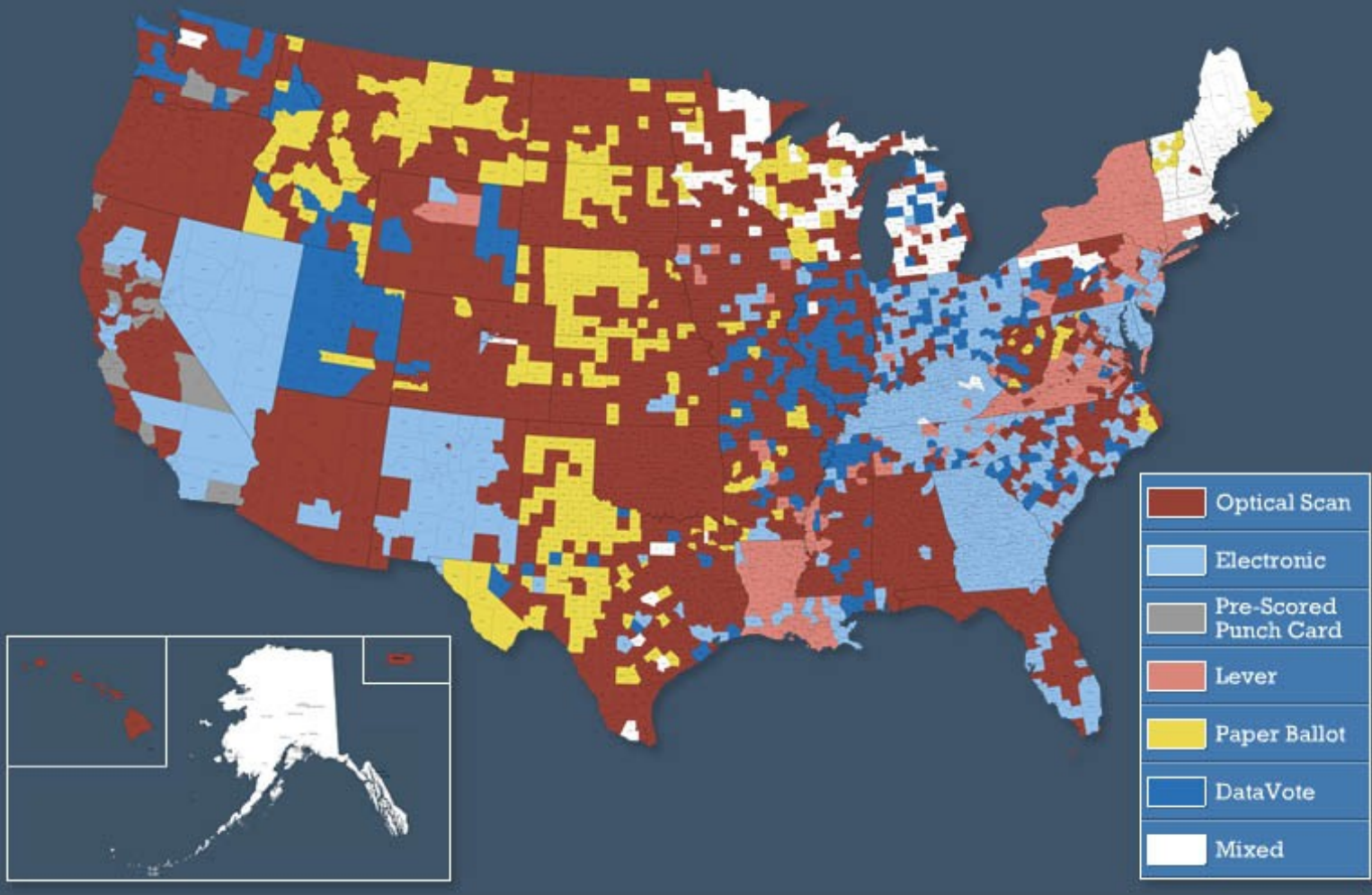
2002 Broward County: With new voting machines, county loses 103,222 votes on election night. Found next day.

2004 Broward County: ."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,"

2006 Sarasota County: 16% undervote in House Race; other counties <1%. Buchanan beat Jennings by 373 votes.

Voting Equipment by County

Type of Voting Equipment by County, 2004



Diebold BallotStation

1. Setup
 - D/L ballot setup
2. Pre-Election
 - L&A testing
3. Election
 - Voting
4. Post-Election
 - Print result tape
 - Transfer votes



The Diebold AccuVote-TS voting machine in our lab

Attack Scenarios

Transferring Votes

- Transfer vote from one candidate to another.
- Leaves total number of votes unchanged.

Denial of Service

- Target precinct that votes for opponent.
- Malware shuts down or wipes machine.
- Forged administrative smartcard attack.

VOTE STEALING CONTROL PANEL

Select the race and candidate to fix:

President of the United States

Candidate Name	Votes So Far
George Washington	9 (90%)
Benedict Arnold	1 (10%)

Set the final outcome: Percent for "Benedict Arnold"

75%

OK Cancel

Injecting Attack Code

Direct installation

- Reboot using smartcard with `fboot.nbo`.
- Reboot using smartcard with `explorer.glb`.
- Replace EPROM.
- Voting machines use standard minibar keys.

Virus

- Infects memory cards.
- Memory cards infect machines on boot.
- Upgrades delivered via memory cards.

Concealing Voting Malware

Timing

- Software only active in Election mode.
- Software only active on certain dates / times.

Knock

- Activates only after secret “knock” given.

Hiding processes and files

- Rootkit techniques
- Virtualization

Obama, McCain Campaigns Hacked

Obama, McCain Campaign Computers Hacked

Tech experts at the Obama headquarters initially believed that the computer systems had been invaded by a computer virus.

By Antone Gonsalves, [InformationWeek](#)

Nov. 5, 2008

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=212000820>

Computer systems used by the Obama and McCain campaigns were reportedly hacked over the summer by an unknown "foreign entity," according to an account of the attacks published Wednesday.

The sophisticated cyberattacks has prompted a federal investigation, [Newsweek reported Wednesday](#). Attacks on both campaigns were similar in that investigators believed a foreign entity or organization sought to steal information on policy positions. Such information could be used in negotiations with the future administration.

Tech experts at the Obama headquarters initially believed that the computer systems had been invaded by a computer virus. The next day, however, they were told by the FBI and Secret Service that the problem was far more serious, the magazine reported.

"You have a problem way bigger than what you understand," an agent told Obama's team, according to [Newsweek](#). "You have been compromised, and a serious amount of files have been loaded off your system."

Federal agents told Obama's aides that the McCain campaign had suffered a similar attack, which a top McCain official later confirmed to [Newsweek](#).

2008 Voting Problems

Kenton County, KY: 108 eSlate machines taken out of service 9am Tuesday due to malfunction. Judge allowed machines to be opened and paper ballots printed so they were counted. Punch machines were available as backups.

Franklin County, OH: One Columbus precinct has 1,066 registered voters but posted 1,138 votes. In suburban Worthington, a precinct has 534 registered voters but counted 633 votes, and another has 951 registered voters but reported 1,095 votes. 35,000 forced to use provisional ballots due to a database 'glitch.'

Election Requirements

- **Privacy**—voters have the right to keep their ballots secret.
- **Incoercibility**—voters cannot prove contents of their ballots.
- **Accuracy**—final tally is sum of all ballots.
- **Availability**—voters should be able to vote when they reach the polling place.
- **Verifiability**—voters can prove to themselves that their ballots were cast as intended and counted and that everyone can prove final tally is accurate.

Alternatives

1. Don't use electronic voting machines.
2. Use voting machines to print ballots only; don't use direct electronic counting.
3. Produce a secure electronic voting machine.

Transparency

Transparency of Process

- Security requirements.
- Reference implementations.
- Public demonstrations.
- Testing guidelines.

Transparency of Elections

- Transparent registration process.
- Publicly viewable logs.

Keep it Simple

Keep it small and verifiable

- Diebold Accuvote over 31,000 lines of C++
- Pvote consists of 460 lines of Python

Prerendered ballots

- Generate ballots as images before election.
- Voting system is a simple finite state machine.

2006 General Election, City of Berkeley, California November 7, 2006

School Board (page 2 of 2)

This contest has 7 boxes on 2 pages. Choose up to TWO boxes.

Touch a box to select or deselect.

John Selawsky

MARIE CURIE

• write in a candidate

Your ballot is **not yet recorded**. Press **NEXT PAGE** to continue or **REVIEW AND FINISH** to review your choices and cast your ballot.

2006 General Election, City of Berkeley, California November 7, 2006

Write-in Candidate for School Board

Q W E R T Y U I O P -
A S D F G H J K L '
Z X C V B N M
SPACE

Use the keyboard above to enter the name of the candidate you wish to write in. Press **ACCEPT** to vote for this candidate or **CANCEL** to not vote for this candidate.

Don't Use Windows

Windows has millions of lines of code.

Security bug rates often over 1/KLOC.

Last Tuesday's updates:

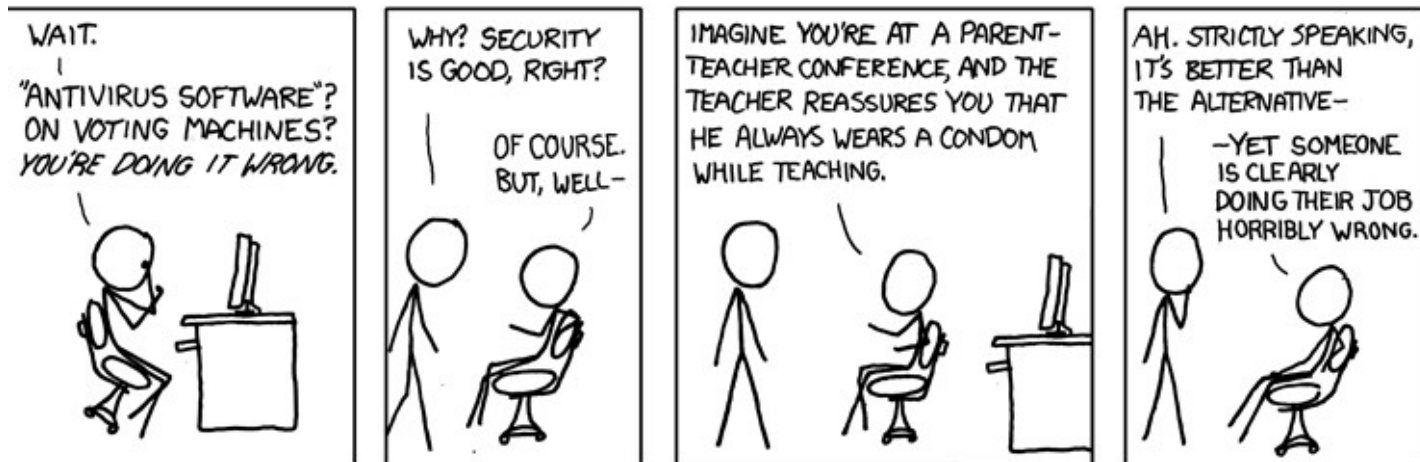
CVE-2008-4037: Remote code execution.

CVE-2008-4029: Remote code execution.

CVE-2007-0099: Race condition.

CVE-2008-4033: Difficult to exploit.

PREMIER ELECTION SOLUTIONS (FORMERLY DIEBOLD)
HAS BLAMED OHIO VOTING MACHINE ERRORS ON PROBLEMS
WITH THE MACHINES' MCAFEE ANTIVIRUS SOFTWARE.



VVPAT

- Humans can't read digital storage, so
- Visually verified paper.

PROBLEMS

- Voters don't verify.
- Cuyahoga 2006: 9.6% of VVPAT destroyed, blank, or compromised.
- Could print extra records if unattended.



Physical Security

Memory cards are easily stolen, modified.



Tamper-evident Tape

- Record serial numbers.
- Check for tampering.

Chain of custody

- Serial numbers for each memory card.
- Track chain of custody like evidence.

