Making Every E-Vote Count

Friends of the Lehigh Libraries
October 2008

Daniel P. Lopresti

Department of Computer Science & Engineering

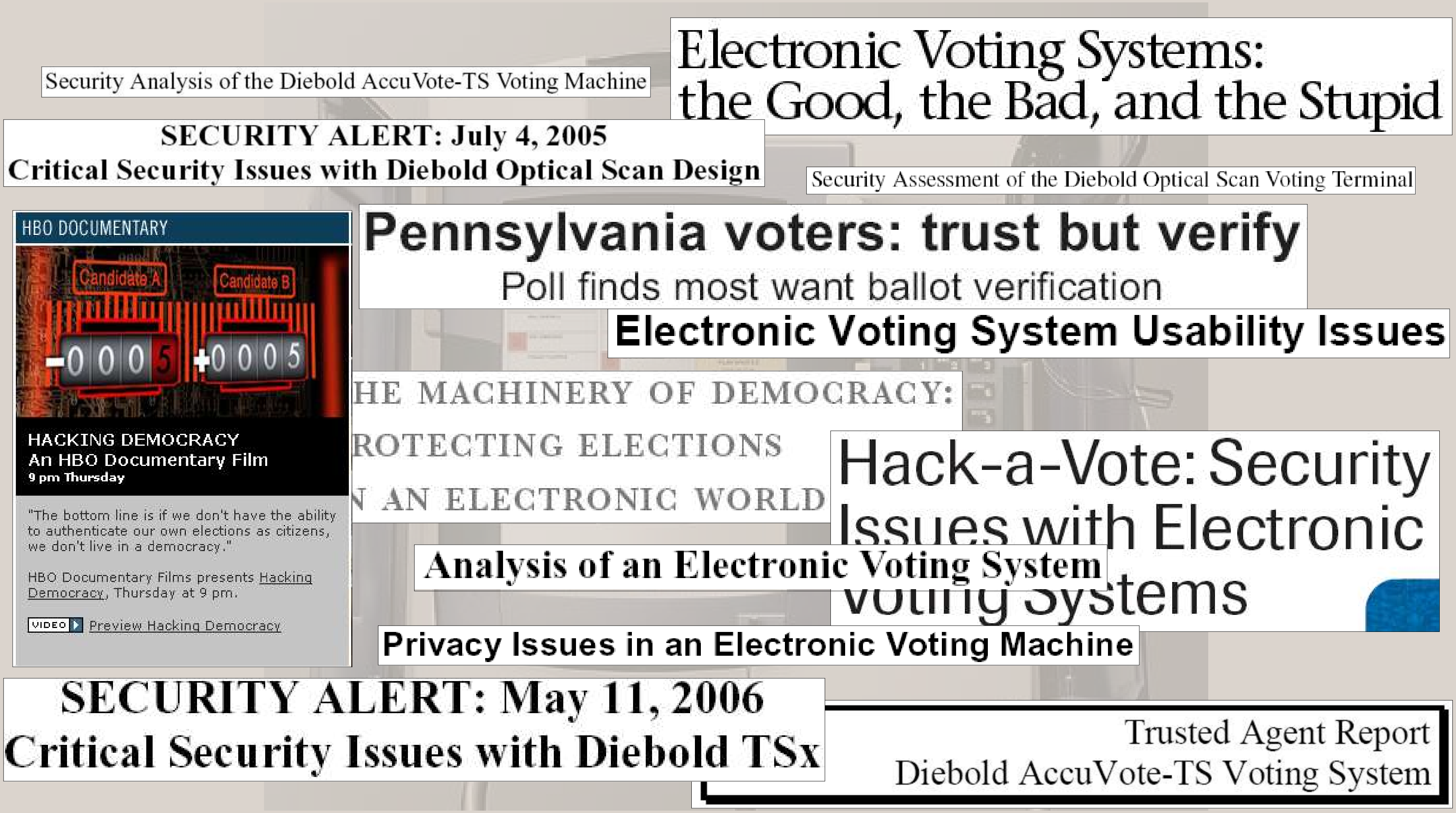
dal9@lehigh.edu

http://www.cse.lehigh.edu/~lopresti

First word

VOTE
VOTE!
VOTE
LEAVE YOUR MARK
VOTE
Let Your Voice Be Heard
Get Out And
VOTE!!
VOTE
VOTE
VOTE
Vote
ROCK THE VOTE
VOTE
VOTE
vote!
VOTE
GET OUT THE
VOTE!
VOTE
VOTE
Vote
2008
VOTE

E-voting in the news



Security Analysis of the Diebold AccuVote-TS Voting Machine

Electronic Voting Systems: the Good, the Bad, and the Stupid

SECURITY ALERT: July 4, 2005
Critical Security Issues with Diebold Optical Scan Design

Security Assessment of the Diebold Optical Scan Voting Terminal

HBO DOCUMENTARY

Candidate A
Candidate B
-0005
+0005

HACKING DEMOCRACY
An HBO Documentary Film
9 pm Thursday

"The bottom line is if we don't have the ability to authenticate our own elections as citizens, we don't live in a democracy."

HBO Documentary Films presents Hacking Democracy, Thursday at 9 pm.

VIDEO Preview Hacking Democracy

Pennsylvania voters: trust but verify
Poll finds most want ballot verification

Electronic Voting System Usability Issues

HE MACHINERY OF DEMOCRACY:
ROTECTING ELECTIONS
N AN ELECTRONIC WORLD

Hack-a-Vote: Security Issues with Electronic Voting Systems

Analysis of an Electronic Voting System

Privacy Issues in an Electronic Voting Machine

SECURITY ALERT: May 11, 2006
Critical Security Issues with Diebold TSx

Trusted Agent Report
Diebold AccuVote-TS Voting System

Why are we interested?

Motivation:

- Fair and accurate elections are vital for a healthy democracy.
- Any voting system carries with it some risk. Past experience with paper ballots, lever machines, etc., has let us understand that risk.
- Electronic voting systems introduce whole new classes of risks.

Some questions we attempt to answer in our work:

- What are the risks associated with e-voting technologies?
- How can these risks best be mitigated?
- Can the current certification process identify bad e-voting systems?
- If not, what would be an effective certification procedure?

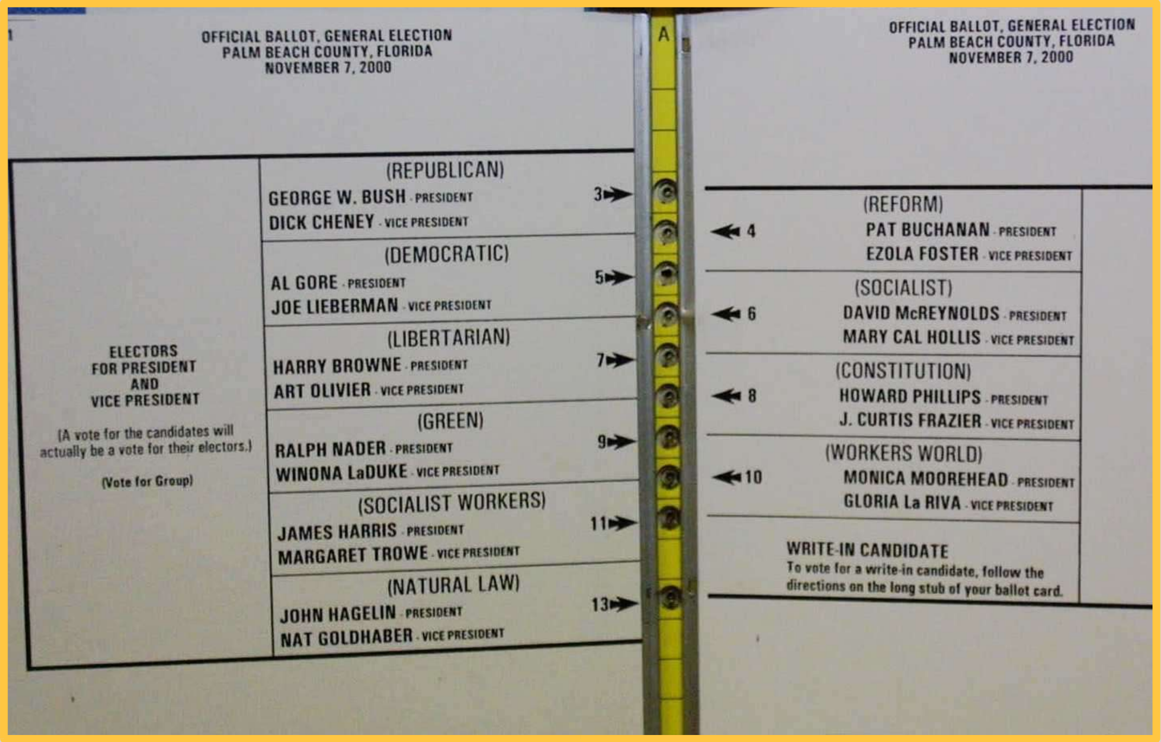
Main take-away points

- E-voting systems are nothing more than general-purpose computers running specialized voting software.
- Same concerns arise as in any complex software/hardware system.
- Current certification process provides little or no assurance: it is incapable of identifying many critical vulnerabilities.
- Other states have banned e-voting systems still in use in PA.
- We can – and should – do better.

Despite these concerns (or perhaps because of them) everyone should still actively participate in the democratic process. Vote!

How did we get here?

The infamous butterfly ballot from the 2000 Presidential election:



OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

ELECTORS
FOR PRESIDENT
AND
VICE PRESIDENT

(A vote for the candidates will actually be a vote for their electors.)

(Vote for Group)

(REPUBLICAN)
GEORGE W. BUSH - PRESIDENT
DICK CHENEY - VICE PRESIDENT
3→

(DEMOCRATIC)
AL GORE - PRESIDENT
JOE LIEBERMAN - VICE PRESIDENT
5→

(LIBERTARIAN)
HARRY BROWNE - PRESIDENT
ART OLIVIER - VICE PRESIDENT
7→

(GREEN)
RALPH NADER - PRESIDENT
WINONA LaDUKE - VICE PRESIDENT
9→

(SOCIALIST WORKERS)
JAMES HARRIS - PRESIDENT
MARGARET TROWE - VICE PRESIDENT
11→

(NATURAL LAW)
JOHN HAGELIN - PRESIDENT
NAT GOLDHABER - VICE PRESIDENT
13→

A

OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

←4
(REFORM)
PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT

←6
(SOCIALIST)
DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT

←8
(CONSTITUTION)
HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT

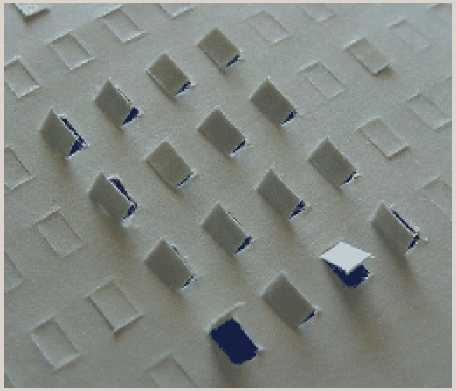
←10
(WORKERS WORLD)
MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT

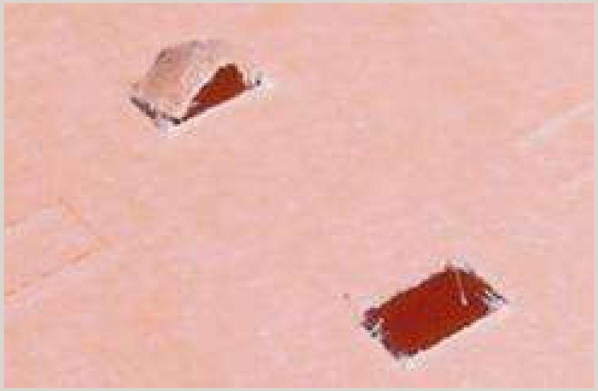
WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.

The Florida ballot is a classic example of bad user interface design. Computer software can suffer from such problems just as easily.

http://www2.indystar.com/library/factfiles/gov/politics/election2000/img/prezrace/butterfly_large.jpg

Hanging chads & voter intent





Votomatic technology used in Florida was prone to paper jams. This led to hanging and dimpled chads, making it hard to determine voter intent.

http://www.cs.uiowa.edu/~jones/cards/chad.html
http://www.pushback.com/justice/votefraud/DimpledChadPictures.html

Election technology & HAVA

The Help America Vote Act (HAVA) provides funds for states to replace punched card and lever voting systems. It does not mandate the use of direct recording electronic (DRE) systems.

Some general goals to keep in mind as we weigh alternatives:

- secure and transparent elections,
- accurate determination of voter intent,
- voter anonymity,
- accessibility for disabled voters and non-native English voters,
- if possible, prevent overvoting (invalidates voter's ballot),
- if possible, prevent unintentional undervoting (voter confusion?).

http://www.fec.gov/hava/law_ext.txt

E-voting Risks

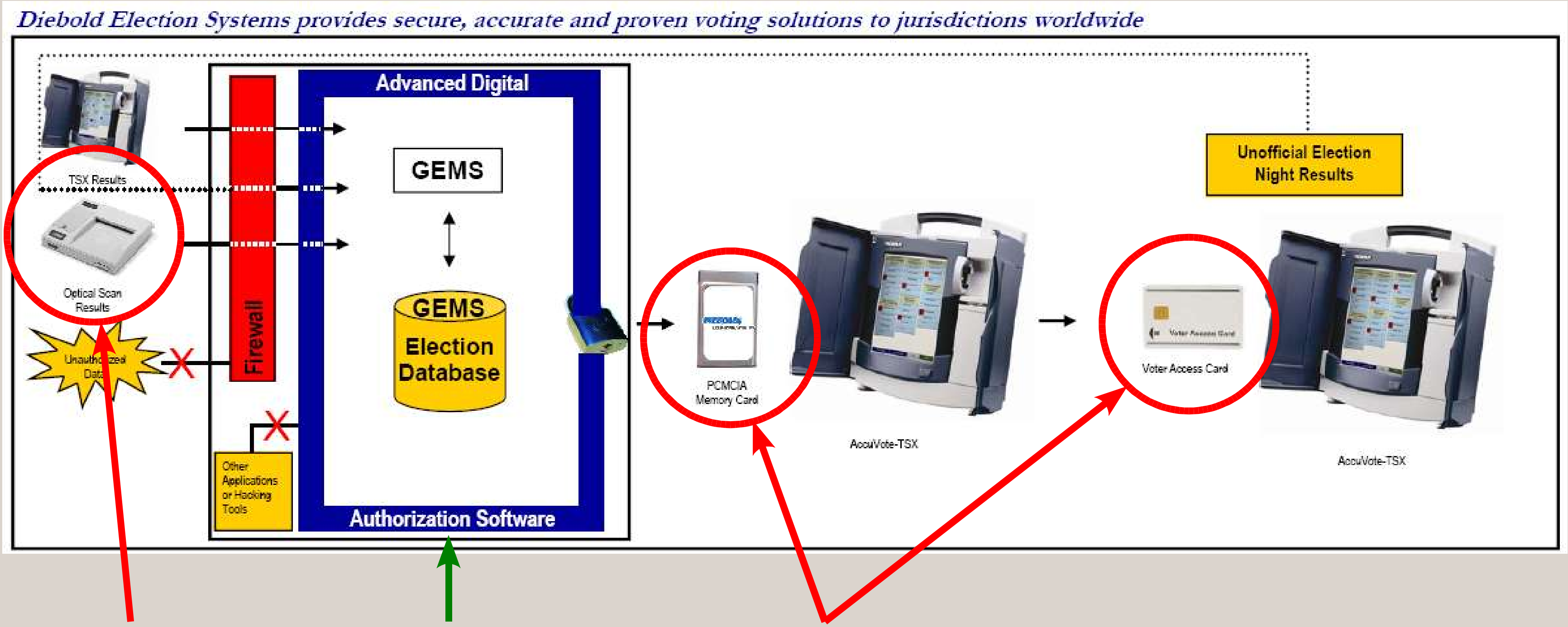
While there are a number of DRE vendors, one truth holds: all computer hardware/software systems of this complexity have bugs.

Bugs can manifest themselves in different ways:

- cause system to be unreliable (crash, lose votes),
- create openings that allow an outsider to compromise election,
- create openings that allow an inside to compromise election.

Such attacks can be impossible to detect after-the-fact.

Diebold security



What we mostly worry about

May or may not be safe

What we mostly worry about

(But insider attacks can arise anywhere.)

http://www.diebold.com/dieboldes/pdf/industrysecurity.pdf

Risk analysis of e-voting software

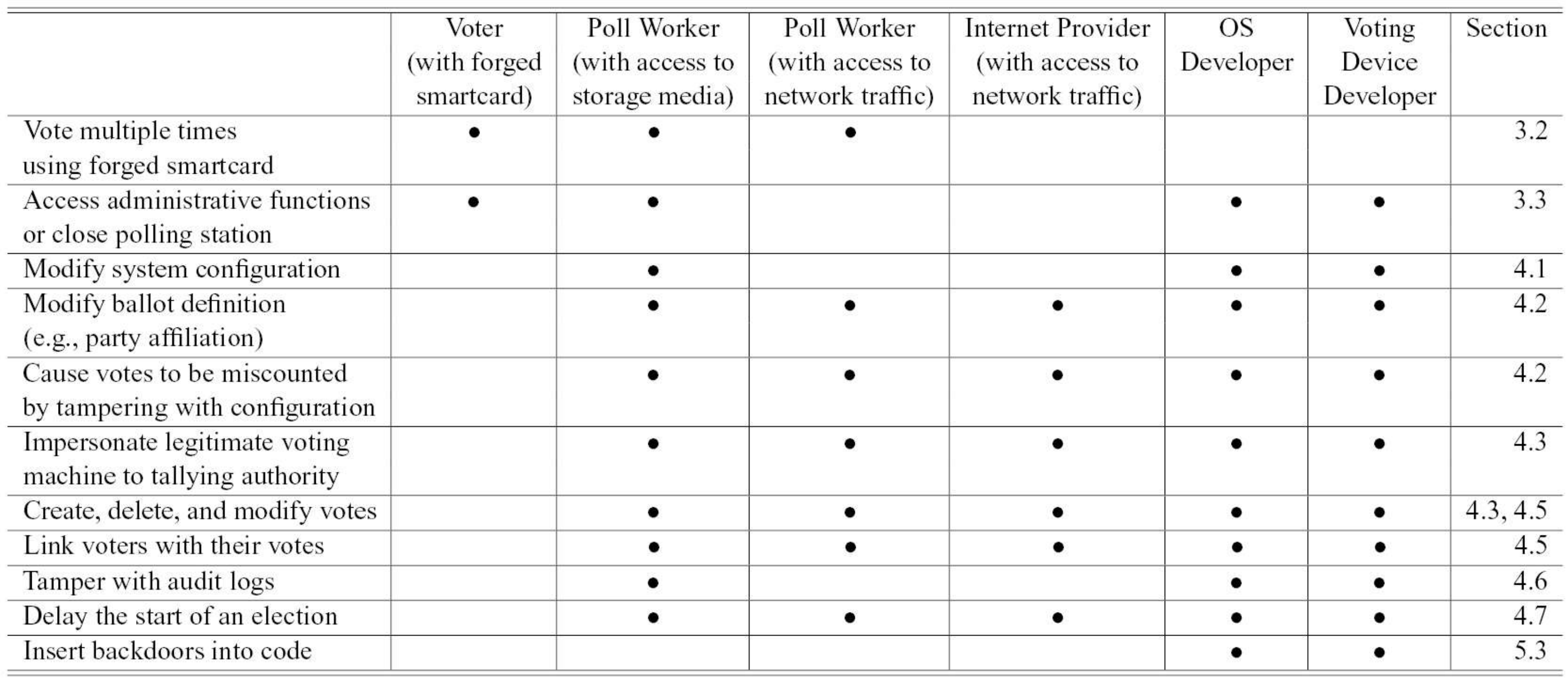
- Avi Rubin and colleagues at Johns Hopkins obtained copy of Diebold e-voting software which appeared on the Internet.*
- Studied it carefully – made results public in 2003.
- Findings include:
    - "... far below even the most minimal security standards ..."
    - "... unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, ..."
    - "... voters ... can cast unlimited votes without being detected ..."

* E-voting vendors often assert they must be allowed to keep their software secret to protect it. This proves the futility of that idea.

"Analysis of an Electronic Voting System," Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *IEEE Symposium on Security and Privacy*, 2004.

Risk analysis of e-voting software

Summary of potential vulnerabilities identified by Rubin, et al.



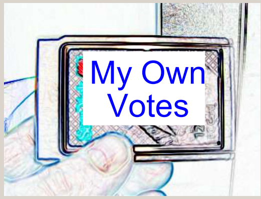
	Voter (with forged smartcard)	Poll Worker (with access to storage media)	Poll Worker (with access to network traffic)	Internet Provider (with access to network traffic)	OS Developer	Voting Device Developer	Section
Vote multiple times using forged smartcard	●	●	●				3.2
Access administrative functions or close polling station	●	●			●	●	3.3
Modify system configuration		●			●	●	4.1
Modify ballot definition (e.g., party affiliation)		●	●	●	●	●	4.2
Cause votes to be miscounted by tampering with configuration		●	●	●	●	●	4.2
Impersonate legitimate voting machine to tallying authority		●	●	●	●	●	4.3
Create, delete, and modify votes		●	●	●	●	●	4.3, 4.5
Link voters with their votes		●	●	●	●	●	4.5
Tamper with audit logs		●			●	●	4.6
Delay the start of an election		●	●	●	●	●	4.7
Insert backdoors into code					●	●	5.3

"Analysis of an Electronic Voting System," Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *IEEE Symposium on Security and Privacy*, 2004.

One potential exploit

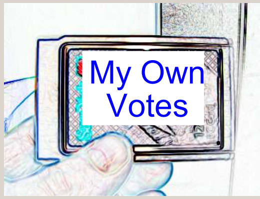
Attempt is made to protect integrity of voting records by encrypting them before storage on PCMCIA memory card ...

Okay!



No way!

... unfortunately, the key is hardwired in the code and now widely known across Internet (it's “F2654hD4”).



Okay!

"Analysis of an Electronic Voting System," Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *IEEE Symposium on Security and Privacy*, 2004.

Some lessons never learned

Another paper, several years later, notes:

"There is a serious flaw in the key management of the crypto code that otherwise should protect the AV-TSx from memory card attacks. Unless election officials avail themselves of the option to create new cryptographic keys, the AV-TSx uses a default key. This key is hard coded into the source code for the AV-TSx, which is poor security practice because, among other things, it means the same key is used in every such machine in the U.S. Worse, the particular default key in question was openly published two and a half years ago in a famous research paper, and is now known by anyone who follows election security, and can be found through Google."

"Security Analysis of the Diebold AccuBasic Interpreter" by David Wagner, David Jefferson, Matt Bishop, Chris Karlof, and Naveen Sastry, February 14, 2006.

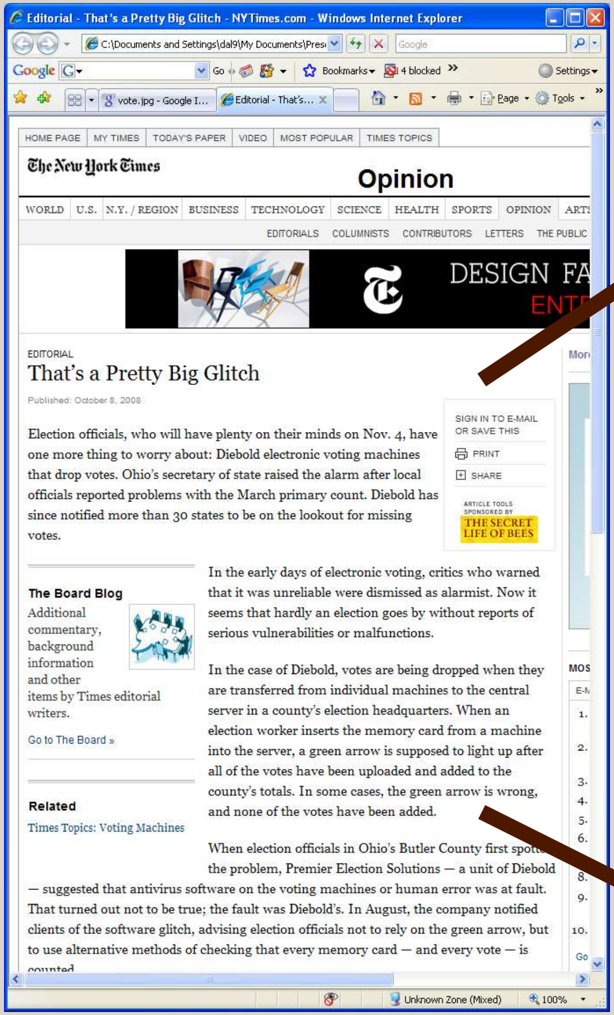
Later risk analyses

- In May 2006, Finnish security expert Harri Hursti exposed a serious flaw in the Diebold AccuVote TSx touchscreen system.
- This flaw allows system to be permanently reprogrammed in a matter of a few minutes. No special hardware is required.
- Later, a team of Princeton researchers announced they had implemented Hursti's attack and proved that it works. They used an older Diebold system given by an anonymous donor.
- The Princeton team also implemented a virus form of the attack that spreads from one infected machine to others via memory card.
- Case opened using several methods, including picking the lock.

"Diebold TSx Evaluation: Critical Security Issues with Diebold TSx," by Harri Hursti, May 11, 2006.

"Security Analysis of the Diebold AccuVote-TS Voting Machine" by Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, September 13, 2006.

Our problems are far from over



EDITORIAL

That's a Pretty Big Glitch

Published: October 8, 2008

Election officials, who will have plenty on their minds on Nov. 4, have one more thing to worry about: Diebold electronic voting machines that drop votes. Ohio's secretary of state raised the alarm after local officials reported problems with the March primary count. Diebold has since notified more than 30 states to be on the lookout for missing votes.

In the early days of electronic voting, critics who warned that it was unreliable were dismissed as alarmist. Now it seems that hardly an election goes by without reports of serious vulnerabilities or malfunctions.

In the case of Diebold, votes are being dropped when they are transferred from individual machines to the central server in a county's election headquarters. When an election worker inserts the memory card from a machine into the server, a green arrow is supposed to light up after all of the votes have been uploaded and added to the county's totals. In some cases, the green arrow is wrong, and none of the votes have been added.

When election officials in Ohio's Butler County first spott the problem, Premier Election Solutions — a unit of Diebold — suggested that antivirus software on the voting machines or human error was at fault. That turned out not to be true; the fault was Diebold's. In August, the company notified clients of the software glitch, advising election officials not to rely on the green arrow, but to use alternative methods of checking that every memory card — and every vote — is counted

The Board Blog

Additional commentary, background information and other items by Times editorial writers.

Go to The Board »

Related

Times Topics: Voting Machines

New York Times, October 8, 2008

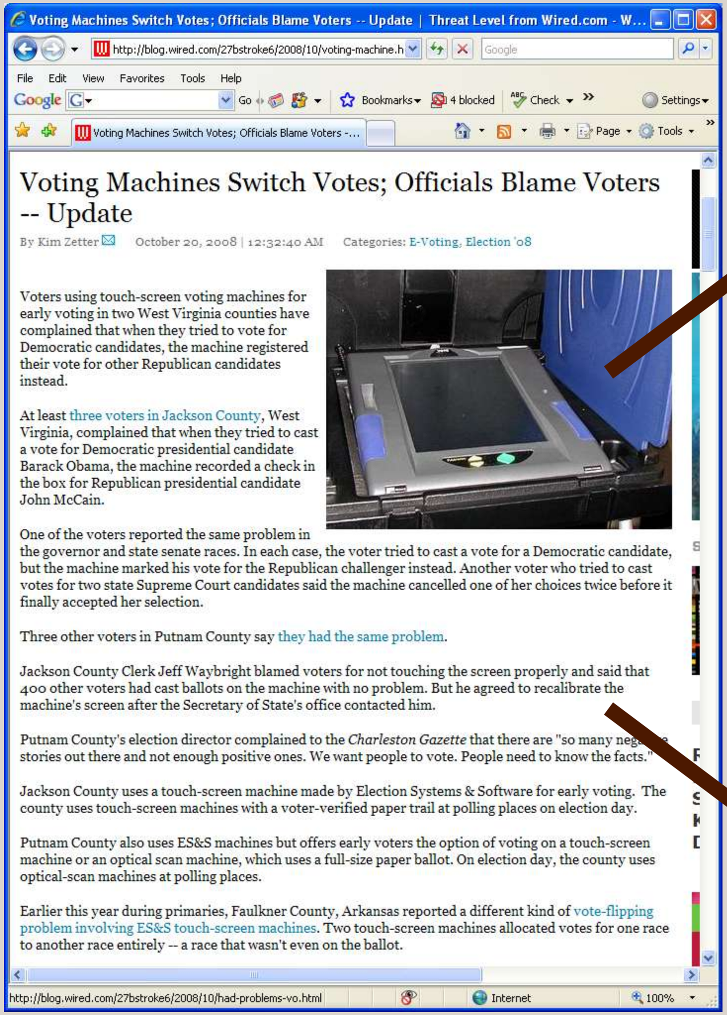
"Election officials, who will have plenty on their minds on Nov. 4, have one more thing to worry about: Diebold electronic voting machines that drop votes.

…

In the case of Diebold, votes are being dropped when they are transferred from individual machines to the central server in a county's election headquarters. When an election worker inserts the memory card from a machine into the server, a green arrow is supposed to light up after all of the votes have been uploaded and added to the county's totals. In some cases, the green arrow is wrong, and none of the votes have been added."

LEHIGH UNIVERSITY

And a couple days ago …


Voting Machines Switch Votes; Officials Blame Voters -- Update | Threat Level from Wired.com - W...
http://blog.wired.com/27bstroke6/2008/10/voting-machine.h
Google
File Edit View Favorites Tools Help
Google G Go Bookmarks 4 blocked Check Settings
Voting Machines Switch Votes; Officials Blame Voters -...
Page Tools
http://blog.wired.com/27bstroke6/2008/10/had-problems-vo.html
Internet
100%

Voting Machines Switch Votes; Officials Blame Voters -- Update

By Kim Zetter   October 20, 2008 | 12:32:40 AM   Categories: E-Voting, Election '08

Voters using touch-screen voting machines for early voting in two West Virginia counties have complained that when they tried to vote for Democratic candidates, the machine registered their vote for other Republican candidates instead.

At least three voters in Jackson County, West Virginia, complained that when they tried to cast a vote for Democratic presidential candidate Barack Obama, the machine recorded a check in the box for Republican presidential candidate John McCain.

One of the voters reported the same problem in the governor and state senate races. In each case, the voter tried to cast a vote for a Democratic candidate, but the machine marked his vote for the Republican challenger instead. Another voter who tried to cast votes for two state Supreme Court candidates said the machine cancelled one of her choices twice before it finally accepted her selection.

Three other voters in Putnam County say they had the same problem.

Jackson County Clerk Jeff Waybright blamed voters for not touching the screen properly and said that 400 other voters had cast ballots on the machine with no problem. But he agreed to recalibrate the machine's screen after the Secretary of State's office contacted him.

Putnam County's election director complained to the *Charleston Gazette* that there are "so many negative stories out there and not enough positive ones. We want people to vote. People need to know the facts."

Jackson County uses a touch-screen machine made by Election Systems & Software for early voting. The county uses touch-screen machines with a voter-verified paper trail at polling places on election day.

Putnam County also uses ES&S machines but offers early voters the option of voting on a touch-screen machine or an optical scan machine, which uses a full-size paper ballot. On election day, the county uses optical-scan machines at polling places.

Earlier this year during primaries, Faulkner County, Arkansas reported a different kind of vote-flipping problem involving ES&S touch-screen machines. Two touch-screen machines allocated votes for one race to another race entirely -- a race that wasn't even on the ballot.

Wired Blog, October 20, 2008

"Voters using touch-screen voting machines for early voting in two West Virginia counties have complained that when they tried to vote for Democratic candidates, the machine registered their vote for other Republican candidates instead.

…

Jackson County Clerk Jeff Waybright blamed voters for not touching the screen properly and said that 400 other voters had cast ballots on the machine with no problem. But he agreed to recalibrate the machine's screen after the Secretary of State's office contacted him."

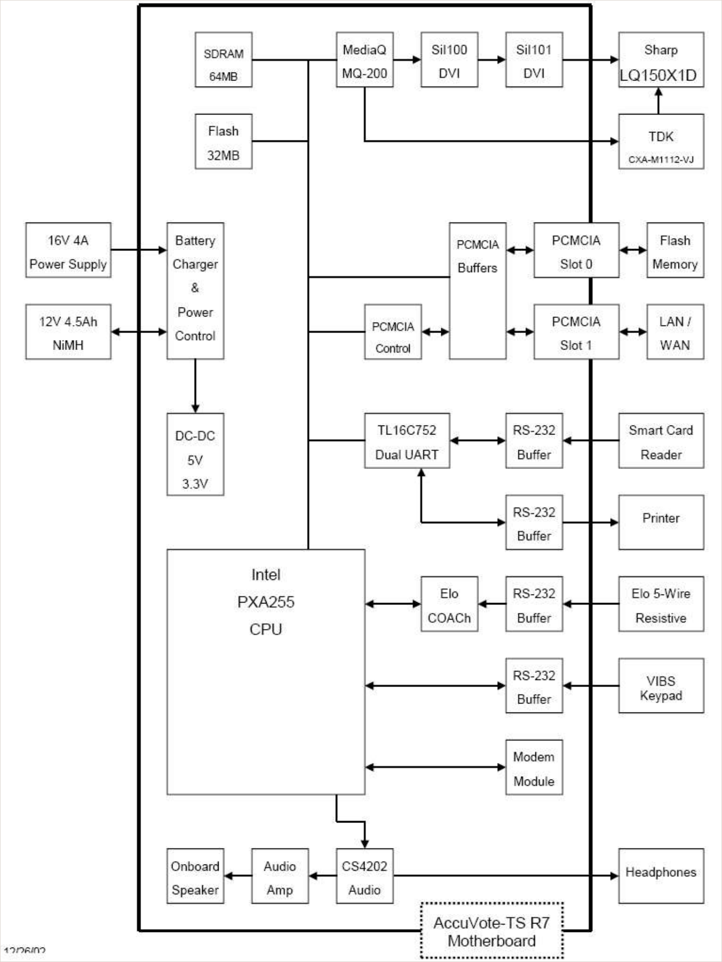
Misrepresentation #1

"E-voting machines are not computers."

Diebold AccuVote System

Demo in Allentown:

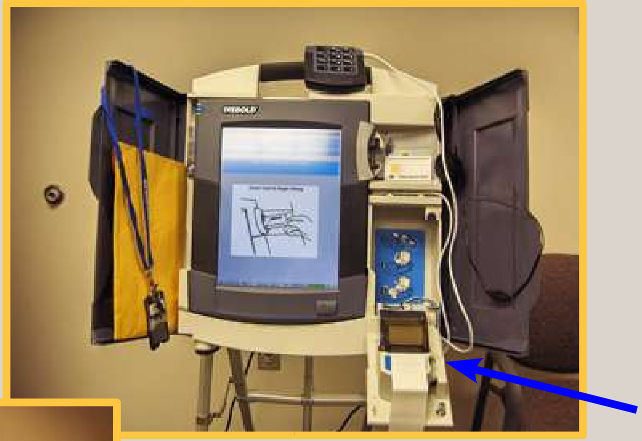
Diebold AccuVote-TSx block diagram:



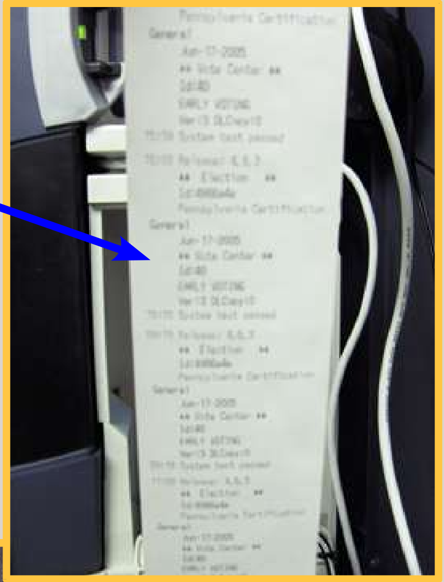
> DRE systems are nothing more than specialized computers.

http://www.wfmz.com/cgi-bin/tt.cgi?action=viewstory&storyid=13711
http://www.bbvforums.org/forums/messages/1954/AccuVote-TSx_2_02_System_Overview-23267.pdf

More photos from Diebold demo



Built-in printer



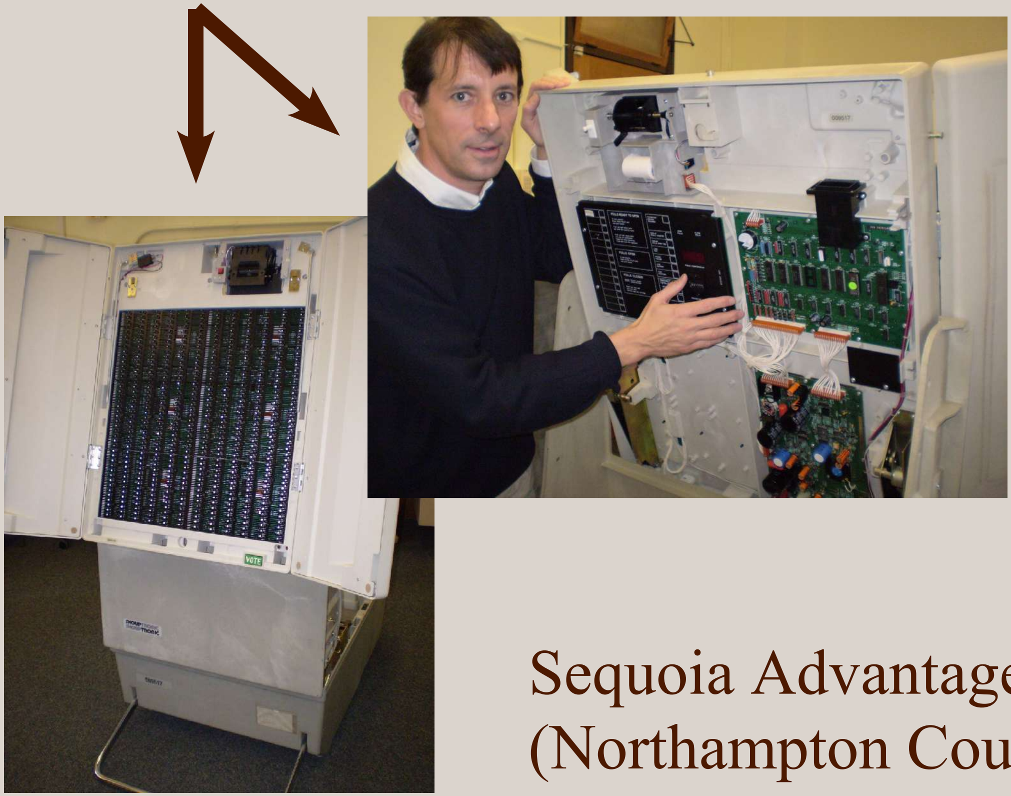
Paper tape (used for end-of-day tally)

PCMCIA slot

PCMCIA card

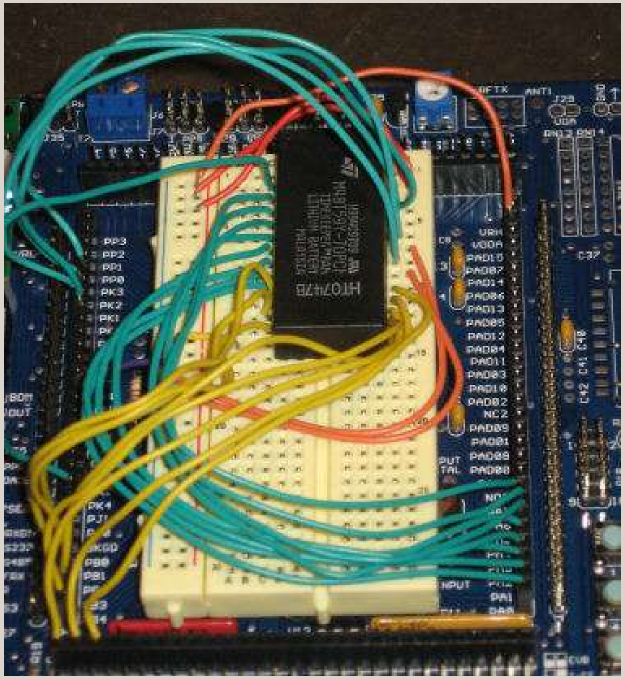
E-voting Machines We Own

Danaher / Shouptronic 1242
(Bucks County)

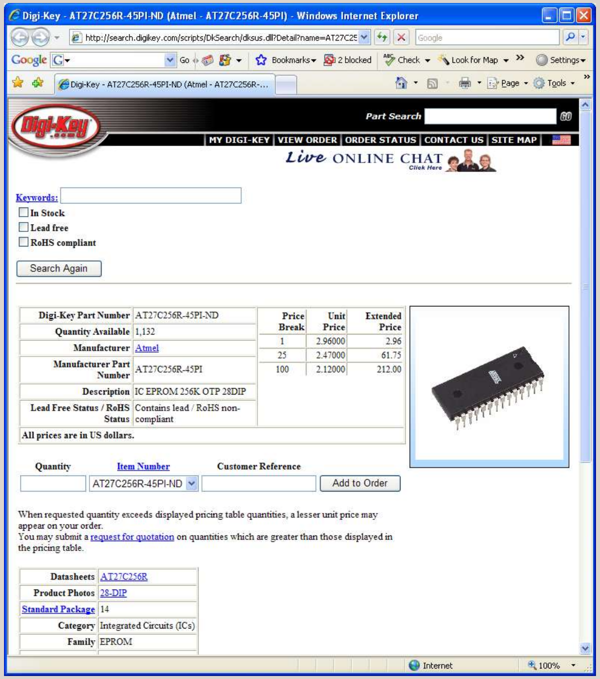


Sequoia Advantage
(Northampton County)

E-voting Machines We Own



Circuit built by Lehigh undergrad to read EPROM (Danaher firmware)


Digi-Key - AT27C256R-45PI-ND (Atmel - AT27C256R-45PI) - Windows Internet Explorer
http://search.digikey.com/scripts/DkSearch/dksus.dll?Detail?name=AT27C25
Google
Go
Bookmarks
2 blocked
Check
Look for Map
Settings
Digi-Key - AT27C256R-45PI-ND (Atmel - AT27C256R-...
Page
Tools
Digi-Key
Part Search
GO
MY DIGI-KEY
VIEW ORDER
ORDER STATUS
CONTACT US
SITE MAP
Live ONLINE CHAT
Click Here
Internet
100%

Keywords:

□ In Stock
□ Lead free
□ RoHS compliant

Search Again

Digi-Key Part Number	AT27C256R-45PI-ND
Quantity Available	1,132
Manufacturer	Atmel
Manufacturer Part Number	AT27C256R-45PI
Description	IC EPROM 256K OTP 28DIP
Lead Free Status / RoHS Status	Contains lead / RoHS non-compliant

Price Break	Unit Price	Extended Price
1	2.96000	2.96
25	2.47000	61.75
100	2.12000	212.00

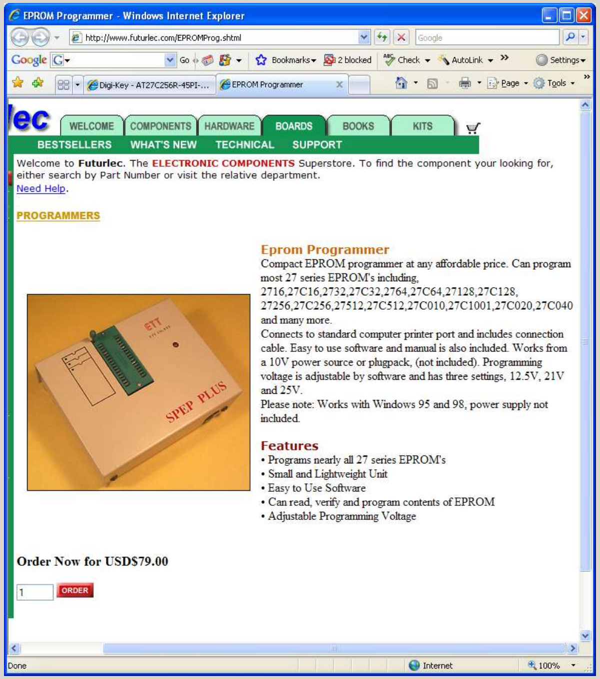
All prices are in US dollars.

Quantity	Item Number	Customer Reference	
	AT27C256R-45PI-ND		Add to Order

When requested quantity exceeds displayed pricing table quantities, a lesser unit price may appear on your order.
You may submit a request for quotation on quantities which are greater than those displayed in the pricing table.

Datasheets	AT27C256R
Product Photos	28-DIP
Standard Package	14
Category	Integrated Circuits (ICs)
Family	EPROM

Replacement EPROM cost is less than $3.00



Welcome to **Futurlec**. The **ELECTRONIC COMPONENTS** Superstore. To find the component your looking for, either search by Part Number or visit the relative department.
Need Help.

PROGRAMMERS

Eprom Programmer

Compact EPROM programmer at any affordable price. Can program most 27 series EPROM's including, 2716,27C16,2732,27C32,2764,27C64,27128,27C128, 27256,27C256,27512,27C512,27C010,27C1001,27C020,27C040 and many more.
Connects to standard computer printer port and includes connection cable. Easy to use software and manual is also included. Works from a 10V power source or plugpack, (not included). Programming voltage is adjustable by software and has three settings, 12.5V, 21V and 25V.
Please note: Works with Windows 95 and 98, power supply not included.

Features

- Programs nearly all 27 series EPROM's
- Small and Lightweight Unit
- Easy to Use Software
- Can read, verify and program contents of EPROM
- Adjustable Programming Voltage

Order Now for USD$79.00

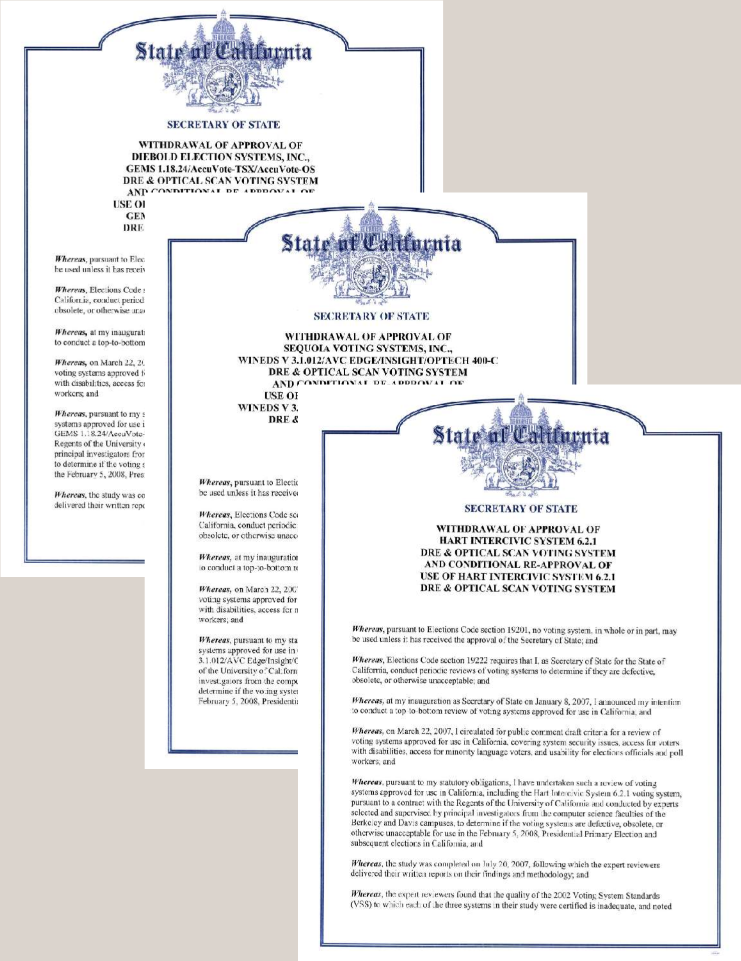
1 ORDER

EPROM programmer is $79.00

Misrepresentation #2

"E-voting machines have been tested by federal and state authorities, so they must be safe."

CA and OH Toss Out DRE's



State of California

SECRETARY OF STATE

WITHDRAWAL OF APPROVAL OF
DIEBOLD ELECTION SYSTEMS, INC.,
GEMS 1.18.24/AccuVote-TSX/AccuVote-OS
DRE & OPTICAL SCAN VOTING SYSTEM
AND CONDITIONAL RE-APPROVAL OF
USE OI
GEM
DRE

Whereas, pursuant to Elec
be used unless it has receiv

Whereas, Elections Code s
California, conduct period
obsolete, or otherwise una

Whereas, at my inaugurat
to conduct a top-to-bottom

Whereas, on March 22, 20
voting systems approved f
with disabilities, access fo
workers; and

Whereas, pursuant to my s
systems approved for use i
GEMS 1.18.24/AccuVote-
Regents of the University
principal investigators fro
to determine if the voting s
the February 5, 2008, Pres

Whereas, the study was co
delivered their written repo

State of California

SECRETARY OF STATE

WITHDRAWAL OF APPROVAL OF
SEQUOIA VOTING SYSTEMS, INC.,
WINEDS V 3.1.012/AVC EDGE/INSIGHT/OPTECH 400-C
DRE & OPTICAL SCAN VOTING SYSTEM
AND CONDITIONAL RE-APPROVAL OF
USE OF
WINEDS V 3.
DRE &

Whereas, pursuant to Electio
be used unless it has received

Whereas, Elections Code sec
California, conduct periodic
obsolete, or otherwise unacc

Whereas, at my inauguration
to conduct a top-to-bottom re

Whereas, on March 22, 2007
voting systems approved for
with disabilities, access for m
workers; and

Whereas, pursuant to my sta
systems approved for use in
3.1.012/AVC Edge/Insight/C
of the University of Californ
investigators from the compu
determine if the voting syste
February 5, 2008, Presidentia

State of California

SECRETARY OF STATE

WITHDRAWAL OF APPROVAL OF
HART INTERCIVIC SYSTEM 6.2.1
DRE & OPTICAL SCAN VOTING SYSTEM
AND CONDITIONAL RE-APPROVAL OF
USE OF HART INTERCIVIC SYSTEM 6.2.1
DRE & OPTICAL SCAN VOTING SYSTEM

Whereas, pursuant to Elections Code section 19201, no voting system, in whole or in part, may be used unless it has received the approval of the Secretary of State; and

Whereas, Elections Code section 19222 requires that I, as Secretary of State for the State of California, conduct periodic reviews of voting systems to determine if they are defective, obsolete, or otherwise unacceptable; and

Whereas, at my inauguration as Secretary of State on January 8, 2007, I announced my intention to conduct a top-to-bottom review of voting systems approved for use in California; and

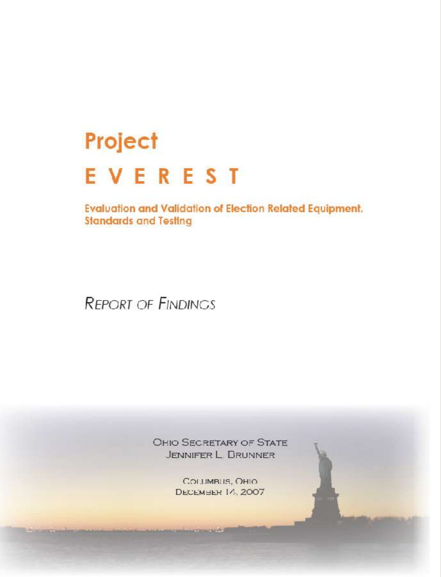
Whereas, on March 22, 2007, I circulated for public comment draft criteria for a review of voting systems approved for use in California, covering system security issues, access for voters with disabilities, access for minority language voters, and usability for elections officials and poll workers; and

Whereas, pursuant to my statutory obligations, I have undertaken such a review of voting systems approved for use in California, including the Hart Intercivic System 6.2.1 voting system, pursuant to a contract with the Regents of the University of California and conducted by experts selected and supervised by principal investigators from the computer science faculties of the Berkeley and Davis campuses, to determine if the voting systems are defective, obsolete, or otherwise unacceptable for use in the February 5, 2008, Presidential Primary Election and subsequent elections in California; and

Whereas, the study was completed on July 20, 2007, following which the expert reviewers delivered their written reports on their findings and methodology; and

Whereas, the expert reviewers found that the quality of the 2002 Voting System Standards (VSS) to which each of the three systems in their study were certified is inadequate, and noted

http://www.sos.state.oh.us/sos/info/everest.aspx



Project
EVEREST

Evaluation and Validation of Election Related Equipment, Standards and Testing

REPORT OF FINDINGS

OHIO SECRETARY OF STATE
JENNIFER L. BRUNNER

COLUMBUS, OHIO
DECEMBER 14, 2007

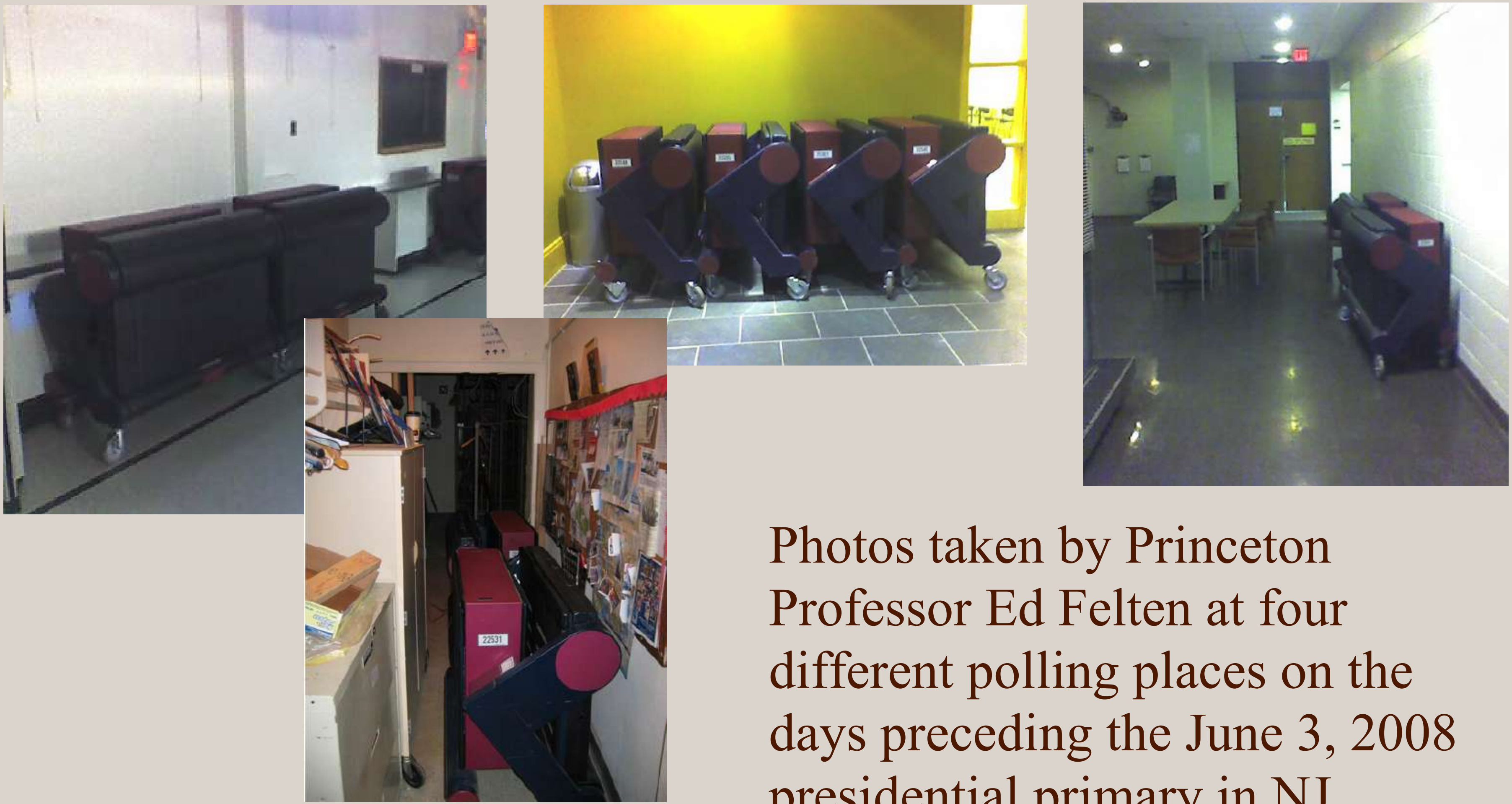
http://www.sos.state.oh.us/sos/info/everest.aspx

All of these machines were previously certified at the federal and state level. Some are still in use in PA counties.

Misrepresentation #3

"Computer security researchers are alarmists. They ignore the physical security designed to protect these systems."

Physical security is questionable



Photos taken by Princeton Professor Ed Felten at four different polling places on the days preceding the June 3, 2008 presidential primary in NJ.

http://citp.princeton.edu/voting/advantage/

Misrepresentation #4

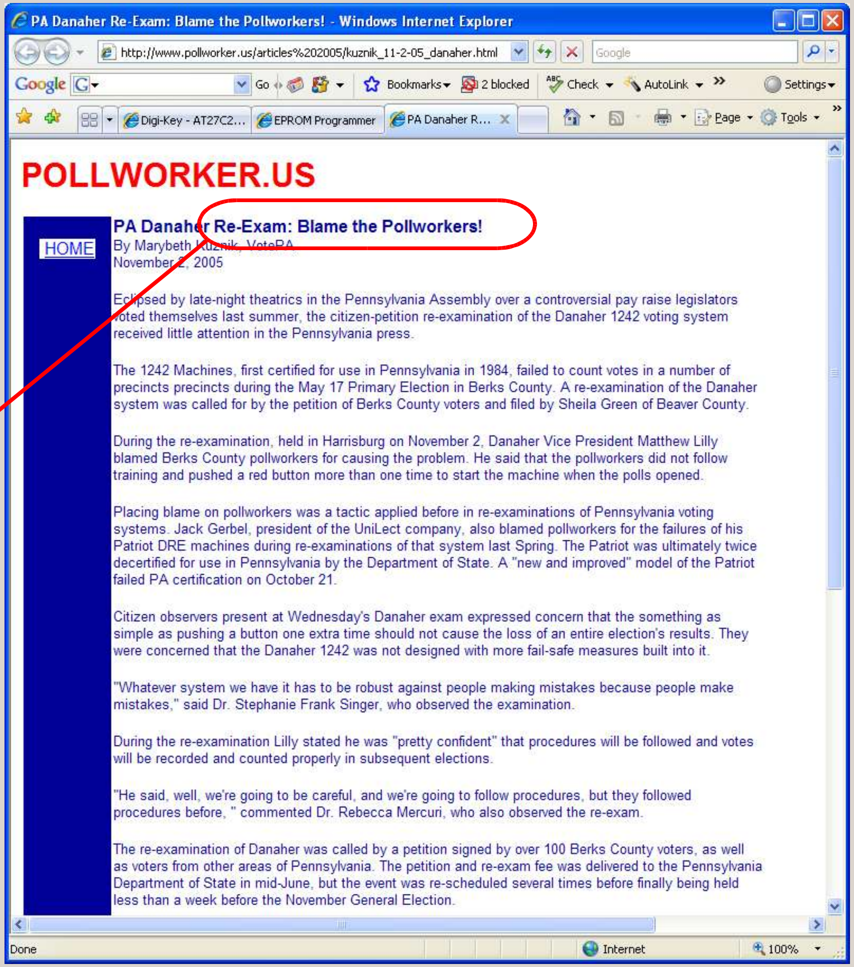
"E-voting machines have never malfunctioned or lost votes in a real election."

Case of the Danaher 1242

Nearly 200 votes are lost through a combination of vendor and pollworker mistakes in May 2005 primary in Berks County.

Blame the pollworkers???

In reality, it was a combination of two errors: the main error was made by Danaher (the vendor). Pollworkers' mistake was secondary.


PA Danaher Re-Exam: Blame the Pollworkers! - Windows Internet Explorer
http://www.pollworker.us/articles%202005/kuznik_11-2-05_danaher.html
Google
Google
Go
Bookmarks
2 blocked
Check
AutoLink
Settings
Digi-Key - AT27C2...
EPROM Programmer
PA Danaher R...
Page
Tools
HOME
Done
Internet
100%

POLLWORKER.US

PA Danaher Re-Exam: Blame the Pollworkers!
By Marybeth Kuznik, VotePA
November 2, 2005

Eclipsed by late-night theatrics in the Pennsylvania Assembly over a controversial pay raise legislators voted themselves last summer, the citizen-petition re-examination of the Danaher 1242 voting system received little attention in the Pennsylvania press.

The 1242 Machines, first certified for use in Pennsylvania in 1984, failed to count votes in a number of precincts precincts during the May 17 Primary Election in Berks County. A re-examination of the Danaher system was called for by the petition of Berks County voters and filed by Sheila Green of Beaver County.

During the re-examination, held in Harrisburg on November 2, Danaher Vice President Matthew Lilly blamed Berks County pollworkers for causing the problem. He said that the pollworkers did not follow training and pushed a red button more than one time to start the machine when the polls opened.

Placing blame on pollworkers was a tactic applied before in re-examinations of Pennsylvania voting systems. Jack Gerbel, president of the UniLect company, also blamed pollworkers for the failures of his Patriot DRE machines during re-examinations of that system last Spring. The Patriot was ultimately twice decertified for use in Pennsylvania by the Department of State. A "new and improved" model of the Patriot failed PA certification on October 21.

Citizen observers present at Wednesday's Danaher exam expressed concern that the something as simple as pushing a button one extra time should not cause the loss of an entire election's results. They were concerned that the Danaher 1242 was not designed with more fail-safe measures built into it.

"Whatever system we have it has to be robust against people making mistakes because people make mistakes," said Dr. Stephanie Frank Singer, who observed the examination.

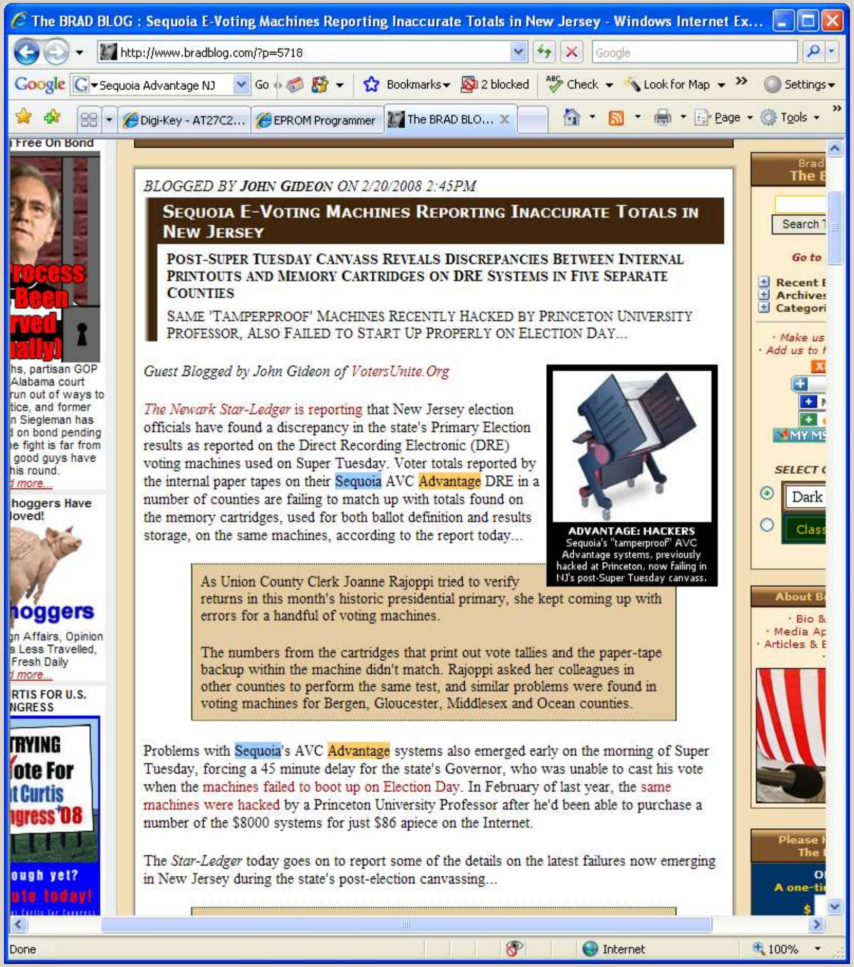
During the re-examination Lilly stated he was "pretty confident" that procedures will be followed and votes will be recorded and counted properly in subsequent elections.

"He said, well, we're going to be careful, and we're going to follow procedures, but they followed procedures before, " commented Dr. Rebecca Mercuri, who also observed the re-exam.

The re-examination of Danaher was called by a petition signed by over 100 Berks County voters, as well as voters from other areas of Pennsylvania. The petition and re-exam fee was delivered to the Pennsylvania Department of State in mid-June, but the event was re-scheduled several times before finally being held less than a week before the November General Election.

http://www.pollworker.us/articles%202005/kuznik_11-2-05_danaher.html

Case of the Sequoia Advantage



The BRAD BLOG : Sequoia E-Voting Machines Reporting Inaccurate Totals in New Jersey - Windows Internet Ex...

http://www.bradblog.com/?p=5718

BLOGGED BY ***JOHN GIDEON*** *ON 2/20/2008 2:45PM*

SEQUOIA E-VOTING MACHINES REPORTING INACCURATE TOTALS IN NEW JERSEY

POST-SUPER TUESDAY CANVASS REVEALS DISCREPANCIES BETWEEN INTERNAL PRINTOUTS AND MEMORY CARTRIDGES ON DRE SYSTEMS IN FIVE SEPARATE COUNTIES

SAME 'TAMPERPROOF' MACHINES RECENTLY HACKED BY PRINCETON UNIVERSITY PROFESSOR, ALSO FAILED TO START UP PROPERLY ON ELECTION DAY...

Guest Blogged by John Gideon of VotersUnite.Org

The Newark Star-Ledger is reporting that New Jersey election officials have found a discrepancy in the state's Primary Election results as reported on the Direct Recording Electronic (DRE) voting machines used on Super Tuesday. Voter totals reported by the internal paper tapes on their Sequoia AVC Advantage DRE in a number of counties are failing to match up with totals found on the memory cartridges, used for both ballot definition and results storage, on the same machines, according to the report today...

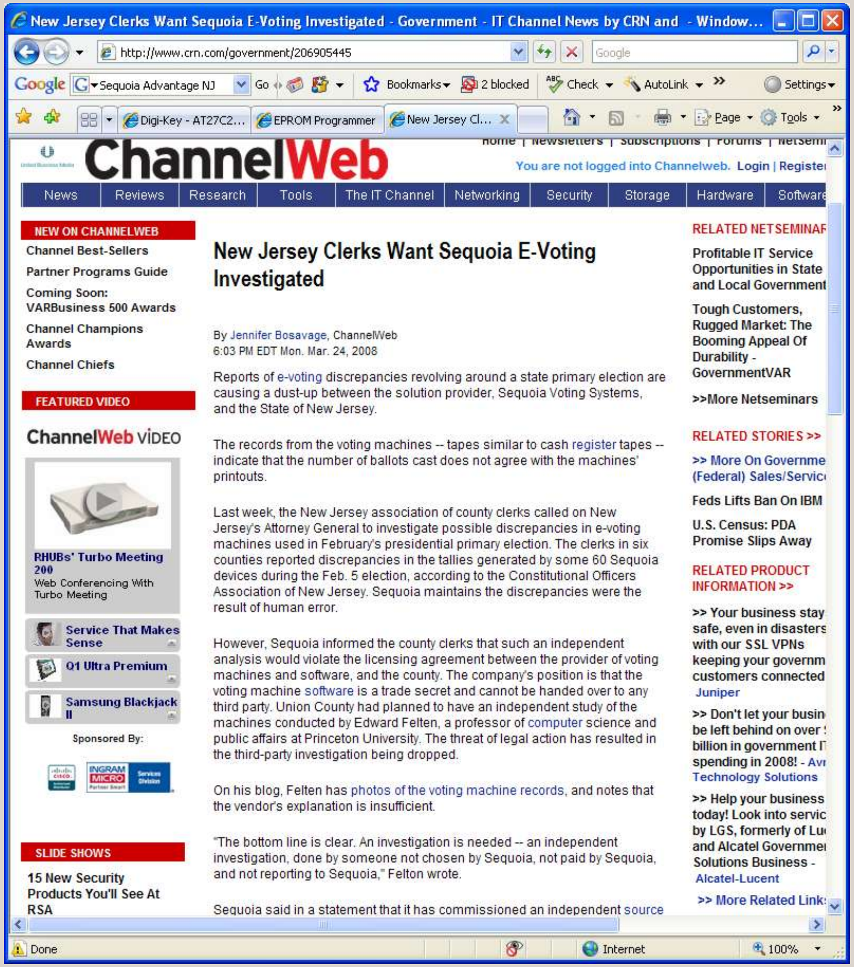
ADVANTAGE: HACKERS
Sequoia's "tamperproof" AVC Advantage systems, previously hacked at Princeton, now failing in NJ's post-Super Tuesday canvass.

> As Union County Clerk Joanne Rajoppi tried to verify returns in this month's historic presidential primary, she kept coming up with errors for a handful of voting machines.
>
> The numbers from the cartridges that print out vote tallies and the paper-tape backup within the machine didn't match. Rajoppi asked her colleagues in other counties to perform the same test, and similar problems were found in voting machines for Bergen, Gloucester, Middlesex and Ocean counties.

Problems with Sequoia's AVC Advantage systems also emerged early on the morning of Super Tuesday, forcing a 45 minute delay for the state's Governor, who was unable to cast his vote when the machines failed to boot up on Election Day. In February of last year, the same machines were hacked by a Princeton University Professor after he'd been able to purchase a number of the $8000 systems for just $86 apiece on the Internet.

The *Star-Ledger* today goes on to report some of the details on the latest failures now emerging in New Jersey during the state's post-election canvassing...

http://www.pollworker.us/articles%202005/kuznik_11-2-05_danaher.html



New Jersey Clerks Want Sequoia E-Voting Investigated - Government - IT Channel News by CRN and - Window...

http://www.crn.com/government/206905445

New Jersey Clerks Want Sequoia E-Voting Investigated

By Jennifer Bosavage, ChannelWeb
6:03 PM EDT Mon. Mar. 24, 2008

Reports of e-voting discrepancies revolving around a state primary election are causing a dust-up between the solution provider, Sequoia Voting Systems, and the State of New Jersey.

The records from the voting machines -- tapes similar to cash register tapes -- indicate that the number of ballots cast does not agree with the machines' printouts.

Last week, the New Jersey association of county clerks called on New Jersey's Attorney General to investigate possible discrepancies in e-voting machines used in February's presidential primary election. The clerks in six counties reported discrepancies in the tallies generated by some 60 Sequoia devices during the Feb. 5 election, according to the Constitutional Officers Association of New Jersey. Sequoia maintains the discrepancies were the result of human error.

However, Sequoia informed the county clerks that such an independent analysis would violate the licensing agreement between the provider of voting machines and software, and the county. The company's position is that the voting machine software is a trade secret and cannot be handed over to any third party. Union County had planned to have an independent study of the machines conducted by Edward Felten, a professor of computer science and public affairs at Princeton University. The threat of legal action has resulted in the third-party investigation being dropped.

On his blog, Felten has photos of the voting machine records, and notes that the vendor's explanation is insufficient.

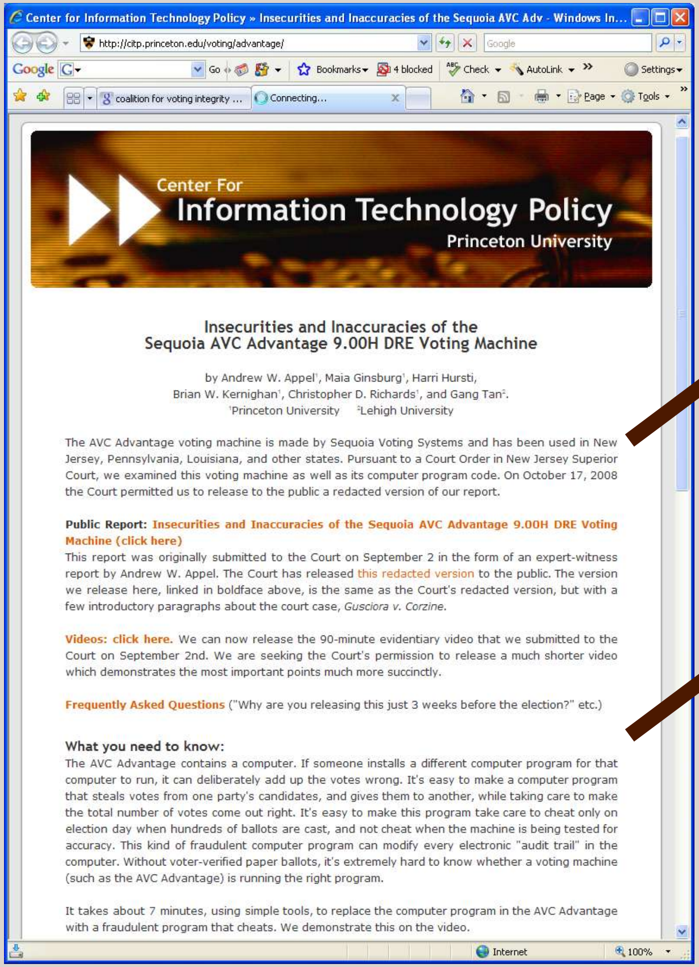
"The bottom line is clear. An investigation is needed -- an independent investigation, done by someone not chosen by Sequoia, not paid by Sequoia, and not reporting to Sequoia," Felton wrote.

Sequoia said in a statement that it has commissioned an independent source

Google
Sequoia Advantage NJ
Go
Bookmarks
2 blocked
Check
AutoLink
Settings
Digi-Key - AT27C2...
EPROM Programmer
New Jersey Cl...
Page
Tools
ChannelWeb
Home | Newsletters | Subscriptions | Forums | NetSemi
You are not logged into Channelweb. Login | Register
News
Reviews
Research
Tools
The IT Channel
Networking
Security
Storage
Hardware
Software
NEW ON CHANNELWEB
Channel Best-Sellers
Partner Programs Guide
Coming Soon: VARBusiness 500 Awards
Channel Champions Awards
Channel Chiefs
FEATURED VIDEO
ChannelWeb VIDEO
RHUBs' Turbo Meeting 200
Web Conferencing With Turbo Meeting
Service That Makes Sense
Q1 Ultra Premium
Samsung Blackjack II
Sponsored By:
SLIDE SHOWS
15 New Security Products You'll See At RSA
RELATED NETSEMINAR
Profitable IT Service Opportunities in State and Local Government
Tough Customers, Rugged Market: The Booming Appeal Of Durability - GovernmentVAR
>>More Netseminars
RELATED STORIES >>
>> More On Governme (Federal) Sales/Servic
Feds Lifts Ban On IBM
U.S. Census: PDA Promise Slips Away
RELATED PRODUCT INFORMATION >>
>> Your business stay safe, even in disasters with our SSL VPNs keeping your governm customers connected
Juniper
>> Don't let your busin be left behind on over billion in government I spending in 2008! - Av Technology Solutions
>> Help your business today! Look into servic by LGS, formerly of Lu and Alcatel Governme Solutions Business -
Alcatel-Lucent
>> More Related Link
Done
Internet
100%

http://www.crn.com/government/206905445

Case of the Sequoia Advantage


Center for Information Technology Policy » Insecurities and Inaccuracies of the Sequoia AVC Adv - Windows In...
http://citp.princeton.edu/voting/advantage/
Google
Google
Go
Bookmarks
4 blocked
Check
AutoLink
Settings
coalition for voting integrity ...
Connecting...
Page
Tools
Center For
Information Technology Policy
Princeton University
Internet
100%

Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine

by Andrew W. Appel[1], Maia Ginsburg[1], Harri Hursti,
Brian W. Kernighan[1], Christopher D. Richards[1], and Gang Tan[2].
[1]Princeton University [2]Lehigh University

The AVC Advantage voting machine is made by Sequoia Voting Systems and has been used in New Jersey, Pennsylvania, Louisiana, and other states. Pursuant to a Court Order in New Jersey Superior Court, we examined this voting machine as well as its computer program code. On October 17, 2008 the Court permitted us to release to the public a redacted version of our report.

Public Report: Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine (click here)
This report was originally submitted to the Court on September 2 in the form of an expert-witness report by Andrew W. Appel. The Court has released this redacted version to the public. The version we release here, linked in boldface above, is the same as the Court's redacted version, but with a few introductory paragraphs about the court case, *Gusciora v. Corzine*.

Videos: click here. We can now release the 90-minute evidentiary video that we submitted to the Court on September 2nd. We are seeking the Court's permission to release a much shorter video which demonstrates the most important points much more succinctly.

Frequently Asked Questions ("Why are you releasing this just 3 weeks before the election?" etc.)

What you need to know:
The AVC Advantage contains a computer. If someone installs a different computer program for that computer to run, it can deliberately add up the votes wrong. It's easy to make a computer program that steals votes from one party's candidates, and gives them to another, while taking care to make the total number of votes come out right. It's easy to make this program take care to cheat only on election day when hundreds of ballots are cast, and not cheat when the machine is being tested for accuracy. This kind of fraudulent computer program can modify every electronic "audit trail" in the computer. Without voter-verified paper ballots, it's extremely hard to know whether a voting machine (such as the AVC Advantage) is running the right program.

It takes about 7 minutes, using simple tools, to replace the computer program in the AVC Advantage with a fraudulent program that cheats. We demonstrate this on the video.

http://citp.princeton.edu/voting/advantage/

Extensive analysis performed by team of researchers from Princeton.

"What Sequoia leaves out is that this programming error disenfranchised voters, by denying them the ability to vote in their own party's primary."

Gang Tan, a professor who recently joined our department, participated in the study last summer.

Who supports the use of DRE's?

Michael Shamos, Ph.D., J.D., is a Professor at Carnegie Mellon. He has extensive experience with electronic voting and is the primary independent expert responsible for certifying voting machines in Pennsylvania and other states.

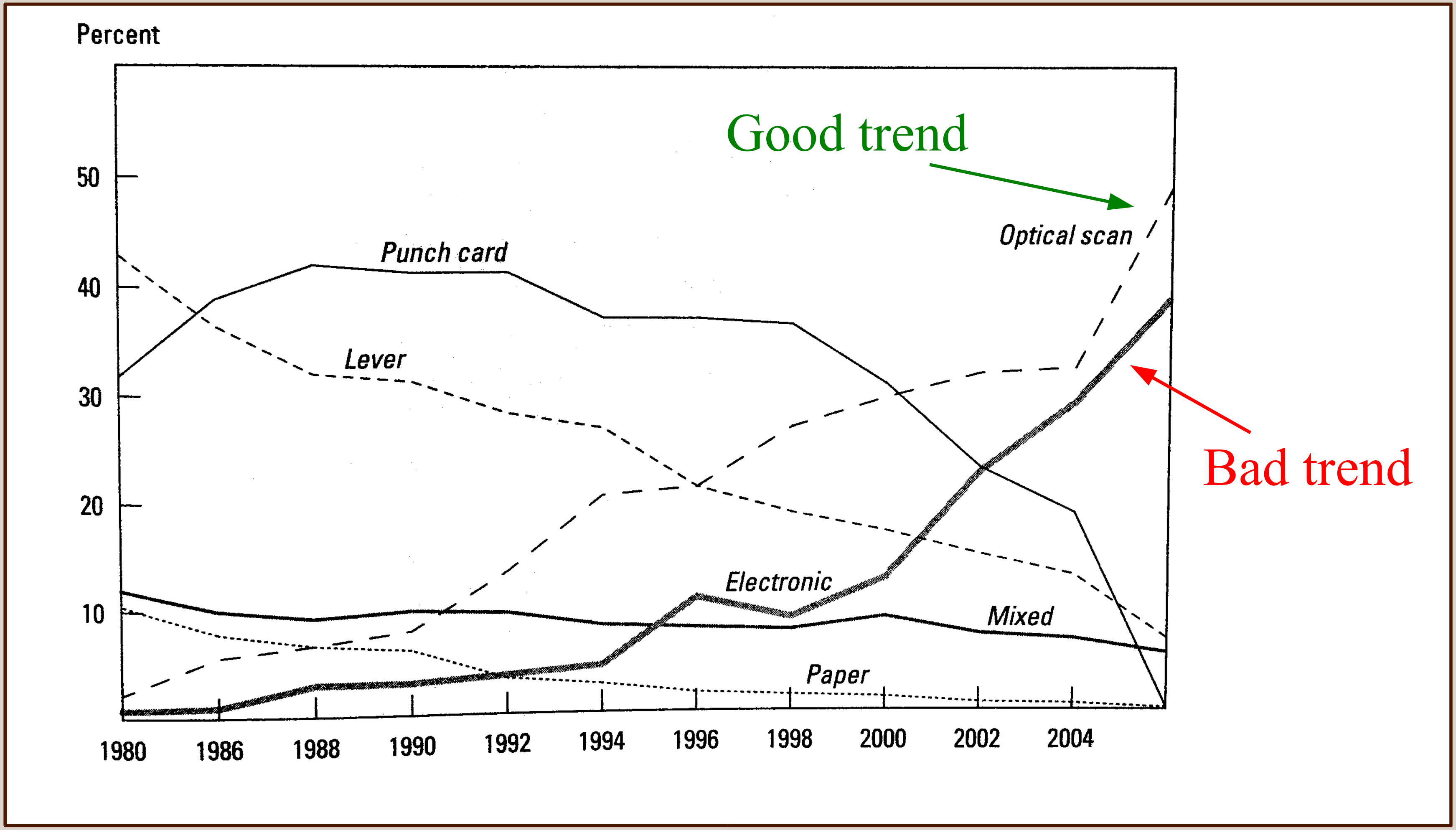
In a 2007 article for the National Academy of Engineering, he writes:

> “Voting machines are among the least reliable devices on this planet.”

???

"Voting as an Engineering Problem," Michael Shamos, The Bridge (National Academy of Engineering), vol. 37, no. 2, 2007.
http://www.nae.edu/nae/bridgecom.nsf/weblinks/MKEZ-744MD8

Voting system use in the U.S.

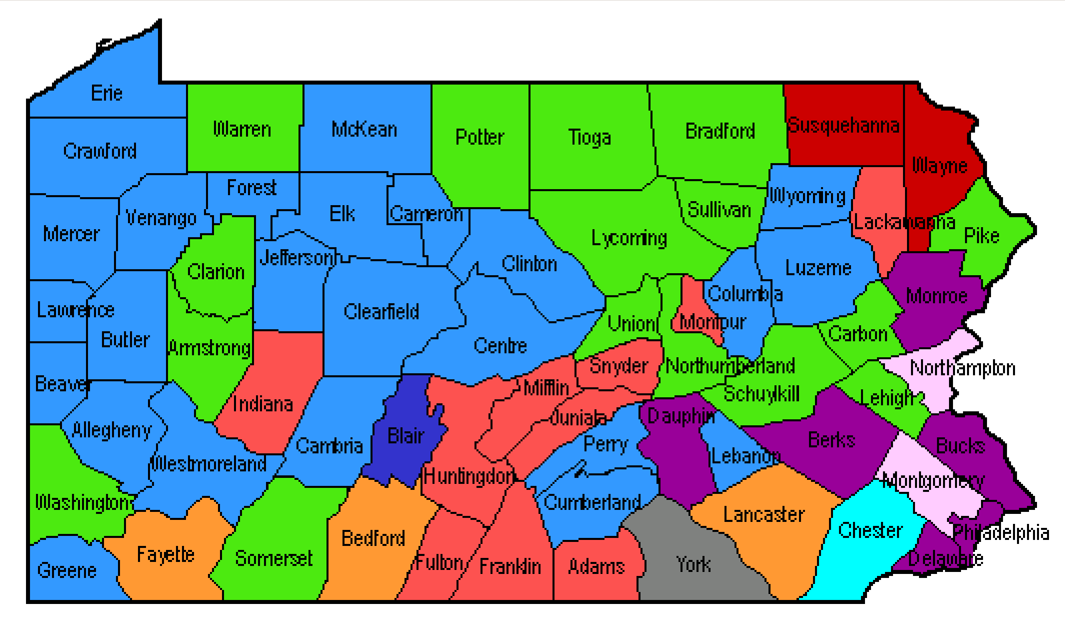


Good trend

Bad trend

From *Voting Technology: The Not-So-Simple Act of Casting a Ballot*, by Paul S. Herrnson, et al, Brookings Institution Press, 2008.

E-Voting in Pennsylvania



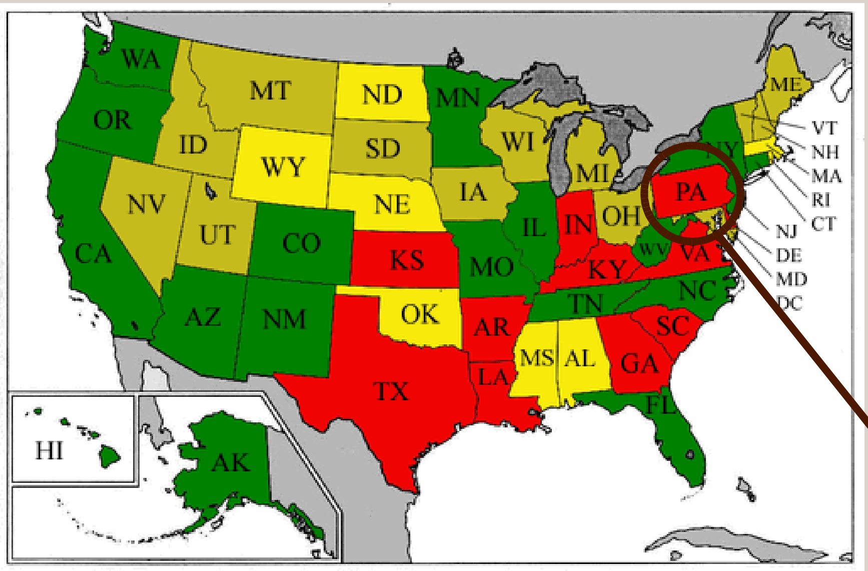
AVS, once used in Northampton County, was decertified

🟦	ES&S iVotronic	🟨	~~Advanced WINvote~~	🟪	Danaher 1242	🟦	Hart InterCivic eSlate2
🟦	ES&S Model 100/iVotronic	🟥	ES&S Model 650/AutoMark	⬛	Sequoia Edge	⬜	Sequoia Advantage
🟥	ES&S Model 100/AutoMark	🟩	Premier (Diebold) TSX	🟧	Hart InterCivic eScan / Hart InterCivic eSlate		

http://www.dos.state.pa.us/voting/cwp/view.asp?a=1218&Q=446365

Voter-Verified Paper Records

- A key recommendation from many security experts is the use of Voter-Verified Paper Records (VVPR).
- As of today, this is only way to guarantee an independent recount.



🟩 VVPR + manual audits required (13)

🟨 VVPR required; No audit requirement (14)

🟨 VVPR not required but in use statewide; No audit requirement (8)

🟥 No VVPR requirement; No audit requirement (15)

Pennsylvania

From http://www.verifiedvoting.org/ 10/23/08

Attempts to fix this in the courts

Banfield v. Cortes, 922 A.2d 36 (Pa. Commw. Ct., 2007), filed August 2006. At issue: whether Pennsylvania Secretary of State properly certified electronic voting equipment used in state.

There are two points of contention in particular.

Pennsylvania Election Code, 25 P.S. § 3031 states:

"Electronic voting system" means a system in which one or more voting devices are used to permit the registering or recording of votes and in which such votes are computed and tabulated by automatic tabulating equipment. The system shall provide for a permanent physical record of each vote cast."

What constitutes a “physical record”?

As an expert witness in this case, I argue that:

> “... none of the DREs certified in Pennsylvania is capable of retaining a “permanent physical record of each vote cast” as required by the Pennsylvania Election Code.
>
> ... these systems maintain what is best described as an “electronic record” of the activity that occurs on the machine. The accuracy or permanence of data stored electronically cannot be guaranteed due to the inherent characteristics of electronic computer memory.”

Note: Michael Shamos is the lead technical expert for the state. Banfield v. Cortes is currently on hold in the PA Supreme Court.

Another point of contention

> 25 P. S. § 3031.17. Statistical sample
>
> The county board of elections, as part of the computation and canvass of returns, shall conduct a statistical recount of a random sample of ballots after each election using manual, mechanical or electronic devices of a type different than those used for the specific election. The sample shall include at least two (2) per centum of the votes cast or two thousand (2,000) votes whichever is the lesser.

Does simply printing out the contents of computer memory onto paper constitute a recount "of a type different" than the original tally produced by the same machine electronically?

PERFECT Project

NSF-funded research project centered here at Lehigh:

- Lehigh: Ziad Munson (Sociology) and Dan Lopresti (Computer Science & Engineering).
- Muhlenberg: Chris Borick (Political Science)
- RPI: George Nagy (Electrical, Computer & Systems Engineering)
- Boise State: Elisa Barney Smith (Electrical & Computer Engineering)

PERFECT stands for “Paper and Electronic Records for Elections: Cultivating Trust”

Research questions

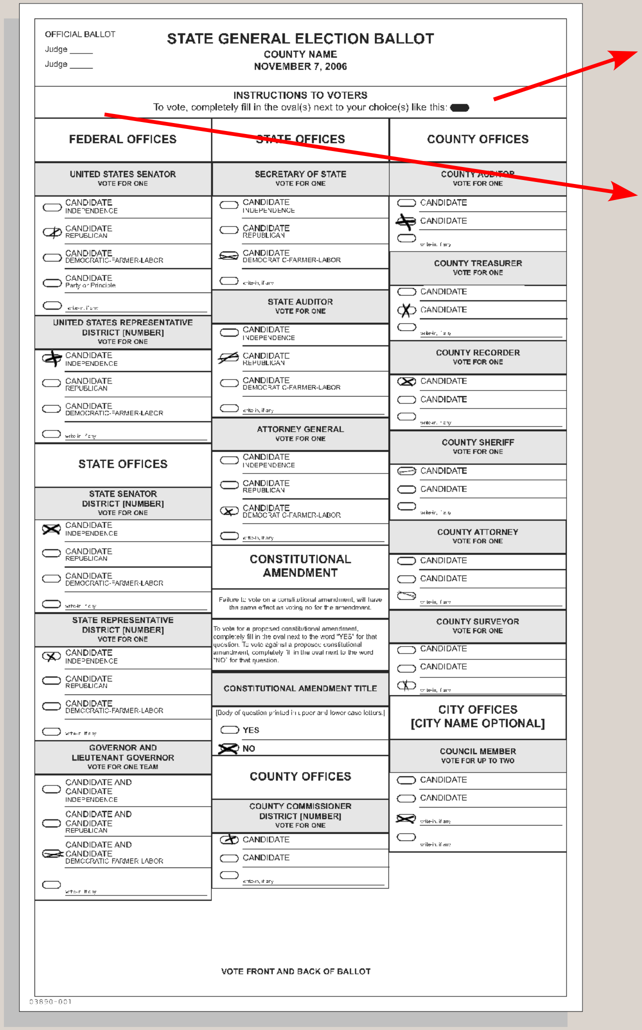
Issues that arise from using paper ballots in elections:

- Accurate interpretation of marginal markings.
- Human cost, error rate, and bias in performing manual recounts.
- Failure modes in ballot imaging (e.g., paper jams).
- Systematic errors due to ballot layout (one candidate may be disadvantaged over another based on physical location on page).

Also keep in mind:

- U.S. Elections can be complex (10's to 100's of choices).
- Impact of "voter error" (e.g., improper markings, erasures).
- Potential for traditional ballot-box stuffing.
- Computer hackers attempting to manipulate the vote.

Counting votes is not so easy



OFFICIAL BALLOT
Judge _____
Judge _____

STATE GENERAL ELECTION BALLOT
COUNTY NAME
NOVEMBER 7, 2006

INSTRUCTIONS TO VOTERS
To vote, completely fill in the oval(s) next to your choice(s) like this: ●

FEDERAL OFFICES

UNITED STATES SENATOR
VOTE FOR ONE

○ CANDIDATE INDEPENDENCE
☒ CANDIDATE REPUBLICAN
○ CANDIDATE DEMOCRATIC-FARMER-LABOR
○ CANDIDATE Party or Principle
○ write-in, if any

UNITED STATES REPRESENTATIVE
DISTRICT [NUMBER]
VOTE FOR ONE

☒ CANDIDATE INDEPENDENCE
○ CANDIDATE REPUBLICAN
○ CANDIDATE DEMOCRATIC-FARMER-LABOR
○ write-in, if any

STATE OFFICES

STATE SENATOR
DISTRICT [NUMBER]
VOTE FOR ONE

☒ CANDIDATE INDEPENDENCE
○ CANDIDATE REPUBLICAN
○ CANDIDATE DEMOCRATIC-FARMER-LABOR
○ write-in, if any

STATE REPRESENTATIVE
DISTRICT [NUMBER]
VOTE FOR ONE

☒ CANDIDATE INDEPENDENCE
○ CANDIDATE REPUBLICAN
○ CANDIDATE DEMOCRATIC-FARMER-LABOR
○ write-in, if any

GOVERNOR AND
LIEUTENANT GOVERNOR
VOTE FOR ONE TEAM

○ CANDIDATE AND CANDIDATE INDEPENDENCE
○ CANDIDATE AND CANDIDATE REPUBLICAN
☒ CANDIDATE AND CANDIDATE DEMOCRATIC-FARMER-LABOR
○ write-in, if any

STATE OFFICES

SECRETARY OF STATE
VOTE FOR ONE

○ CANDIDATE INDEPENDENCE
○ CANDIDATE REPUBLICAN
☒ CANDIDATE DEMOCRATIC-FARMER-LABOR
○ write-in, if any

STATE AUDITOR
VOTE FOR ONE

○ CANDIDATE INDEPENDENCE
☒ CANDIDATE REPUBLICAN
○ CANDIDATE DEMOCRATIC-FARMER-LABOR
○ write-in, if any

ATTORNEY GENERAL
VOTE FOR ONE

○ CANDIDATE INDEPENDENCE
○ CANDIDATE REPUBLICAN
☒ CANDIDATE DEMOCRATIC-FARMER-LABOR
○ write-in, if any

CONSTITUTIONAL AMENDMENT

Failure to vote on a constitutional amendment, will have the same effect as voting no for the amendment.

To vote for a proposed constitutional amendment, completely fill in the oval next to the word "YES" for that question. To vote against a proposed constitutional amendment, completely fill in the oval next to the word "NO" for that question.

CONSTITUTIONAL AMENDMENT TITLE

[Body of question printed in upper and lower case letters.]

○ YES
☒ NO

COUNTY OFFICES

COUNTY COMMISSIONER
DISTRICT [NUMBER]
VOTE FOR ONE

☒ CANDIDATE
○ CANDIDATE
○ write-in, if any

COUNTY OFFICES

COUNTY AUDITOR
VOTE FOR ONE

○ CANDIDATE
☒ CANDIDATE
○ write-in, if any

COUNTY TREASURER
VOTE FOR ONE

○ CANDIDATE
☒ CANDIDATE
○ write-in, if any

COUNTY RECORDER
VOTE FOR ONE

☒ CANDIDATE
○ CANDIDATE
○ write-in, if any

COUNTY SHERIFF
VOTE FOR ONE

☒ CANDIDATE
○ CANDIDATE
○ write-in, if any

COUNTY ATTORNEY
VOTE FOR ONE

○ CANDIDATE
○ CANDIDATE
☒ write-in, if any

COUNTY SURVEYOR
VOTE FOR ONE

○ CANDIDATE
○ CANDIDATE
☒ write-in, if any

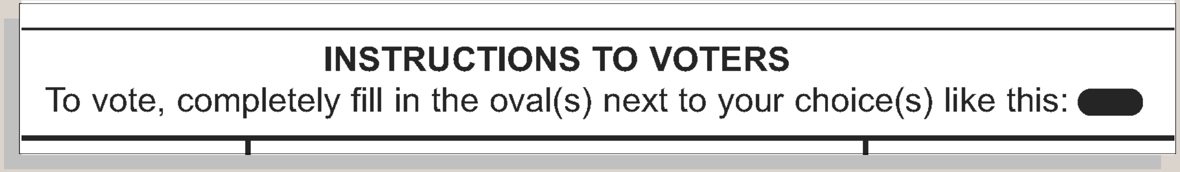
CITY OFFICES
[CITY NAME OPTIONAL]

COUNCIL MEMBER
VOTE FOR UP TO TWO

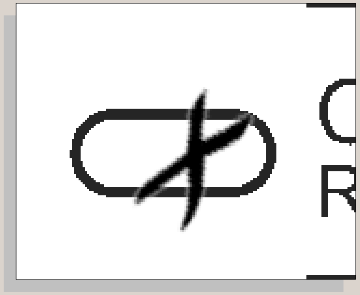
○ CANDIDATE
○ CANDIDATE
☒ write-in, if any
○ write-in, if any

VOTE FRONT AND BACK OF BALLOT

03890-001



INSTRUCTIONS TO VOTERS
To vote, completely fill in the oval(s) next to your choice(s) like this: ●



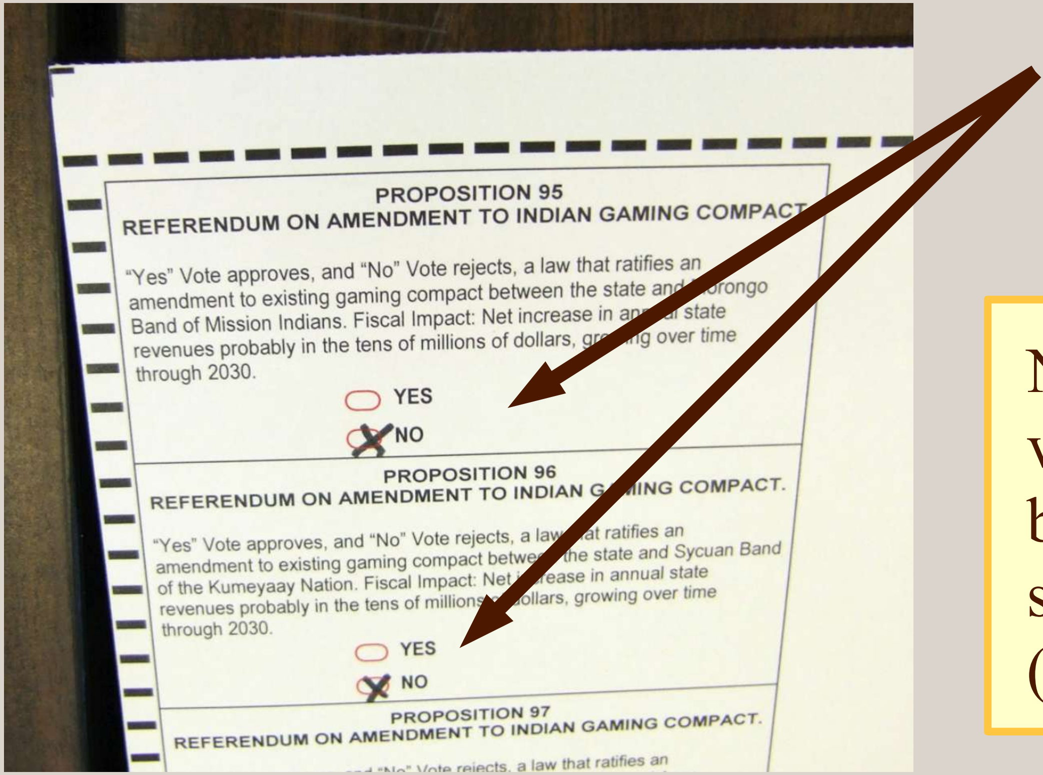
Is this a legal vote?

- Courts would probably say so ...
- ... but op-scan readers might not count it.

Increasing demands that machine's interpretation match a human's.

Counting votes is not so easy

Real ballot from an election in CA:



PROPOSITION 95

REFERENDUM ON AMENDMENT TO INDIAN GAMING COMPACT

"Yes" Vote approves, and "No" Vote rejects, a law that ratifies an amendment to existing gaming compact between the state and Morongo Band of Mission Indians. Fiscal Impact: Net increase in annual state revenues probably in the tens of millions of dollars, growing over time through 2030.

○ YES

☒ NO

PROPOSITION 96

REFERENDUM ON AMENDMENT TO INDIAN GAMING COMPACT.

"Yes" Vote approves, and "No" Vote rejects, a law that ratifies an amendment to existing gaming compact between the state and Sycuan Band of the Kumeyaay Nation. Fiscal Impact: Net increase in annual state revenues probably in the tens of millions of dollars, growing over time through 2030.

○ YES

☒ NO

PROPOSITION 97

REFERENDUM ON AMENDMENT TO INDIAN GAMING COMPACT.

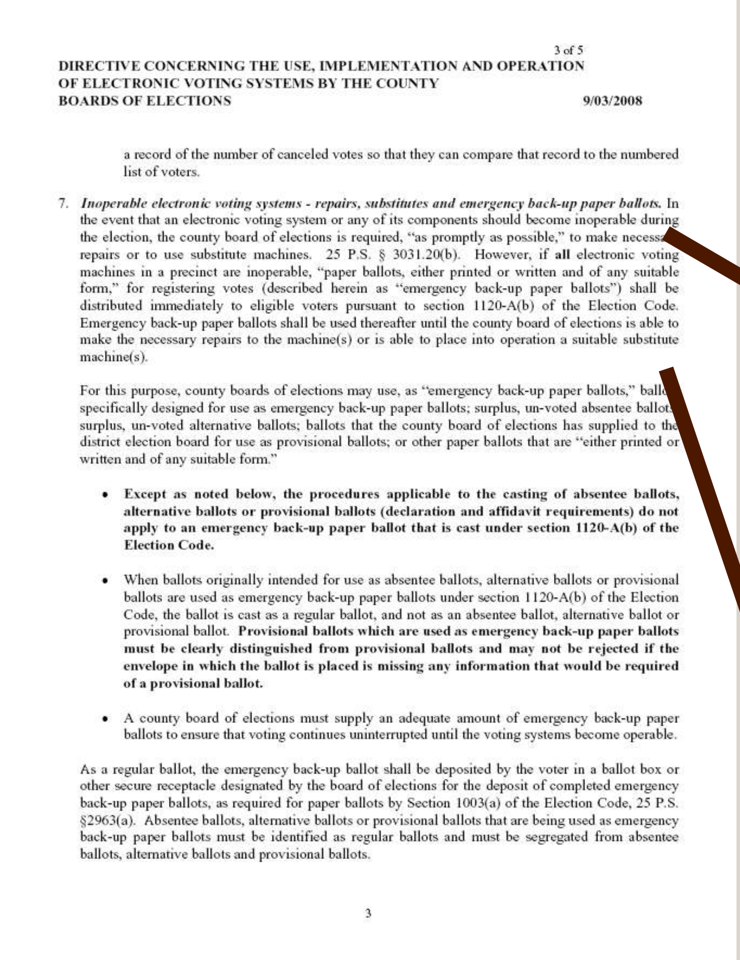
and "No" Vote rejects, a law that ratifies an

One of these votes was counted correctly by the op-scan equipment, the other wasn't.

Note: this does not mean voting on paper ballots is bad, just (1) manual audits should be mandatory, and (2) more research is needed.

"Improving California's 1% Manual Tally Procedure," Joseph Lorenzo Hall, UC Berkeley School of Information, EVT Workshop 2008.

Another lawsuit filed just this week



3 of 5

DIRECTIVE CONCERNING THE USE, IMPLEMENTATION AND OPERATION OF ELECTRONIC VOTING SYSTEMS BY THE COUNTY BOARDS OF ELECTIONS **9/03/2008**

a record of the number of canceled votes so that they can compare that record to the numbered list of voters.

7. ***Inoperable electronic voting systems - repairs, substitutes and emergency back-up paper ballots.*** In the event that an electronic voting system or any of its components should become inoperable during the election, the county board of elections is required, "as promptly as possible," to make necessa repairs or to use substitute machines. 25 P.S. § 3031.20(b). However, if **all** electronic voting machines in a precinct are inoperable, "paper ballots, either printed or written and of any suitable form," for registering votes (described herein as "emergency back-up paper ballots") shall be distributed immediately to eligible voters pursuant to section 1120-A(b) of the Election Code. Emergency back-up paper ballots shall be used thereafter until the county board of elections is able to make the necessary repairs to the machine(s) or is able to place into operation a suitable substitute machine(s).

   For this purpose, county boards of elections may use, as "emergency back-up paper ballots," ballo specifically designed for use as emergency back-up paper ballots; surplus, un-voted absentee ballots surplus, un-voted alternative ballots; ballots that the county board of elections has supplied to the district election board for use as provisional ballots; or other paper ballots that are "either printed or written and of any suitable form."

   - **Except as noted below, the procedures applicable to the casting of absentee ballots, alternative ballots or provisional ballots (declaration and affidavit requirements) do not apply to an emergency back-up paper ballot that is cast under section 1120-A(b) of the Election Code.**
   - When ballots originally intended for use as absentee ballots, alternative ballots or provisional ballots are used as emergency back-up paper ballots under section 1120-A(b) of the Election Code, the ballot is cast as a regular ballot, and not as an absentee ballot, alternative ballot or provisional ballot. **Provisional ballots which are used as emergency back-up paper ballots must be clearly distinguished from provisional ballots and may not be rejected if the envelope in which the ballot is placed is missing any information that would be required of a provisional ballot.**
   - A county board of elections must supply an adequate amount of emergency back-up paper ballots to ensure that voting continues uninterrupted until the voting systems become operable.

   As a regular ballot, the emergency back-up ballot shall be deposited by the voter in a ballot box or other secure receptacle designated by the board of elections for the deposit of completed emergency back-up paper ballots, as required for paper ballots by Section 1003(a) of the Election Code, 25 P.S. §2963(a). Absentee ballots, alternative ballots or provisional ballots that are being used as emergency back-up paper ballots must be identified as regular ballots and must be segregated from absentee ballots, alternative ballots and provisional ballots.

3

Directive issued by the Secretary of State on September 3, 2008:

"… if all electronic voting machines in a precinct are inoperable, "paper ballots, either printed or written and of any suitable form," for registering votes (described herein as "emergency back-up paper ballots") shall be distributed immediately to eligible voters …"

http://www.dos.state.pa.us/elections/lib/elections/090_election_administration_tools/evs_directive.pdf

Emergency paper ballot measure

"... if all electronic voting machines in a precinct are inoperable ..."

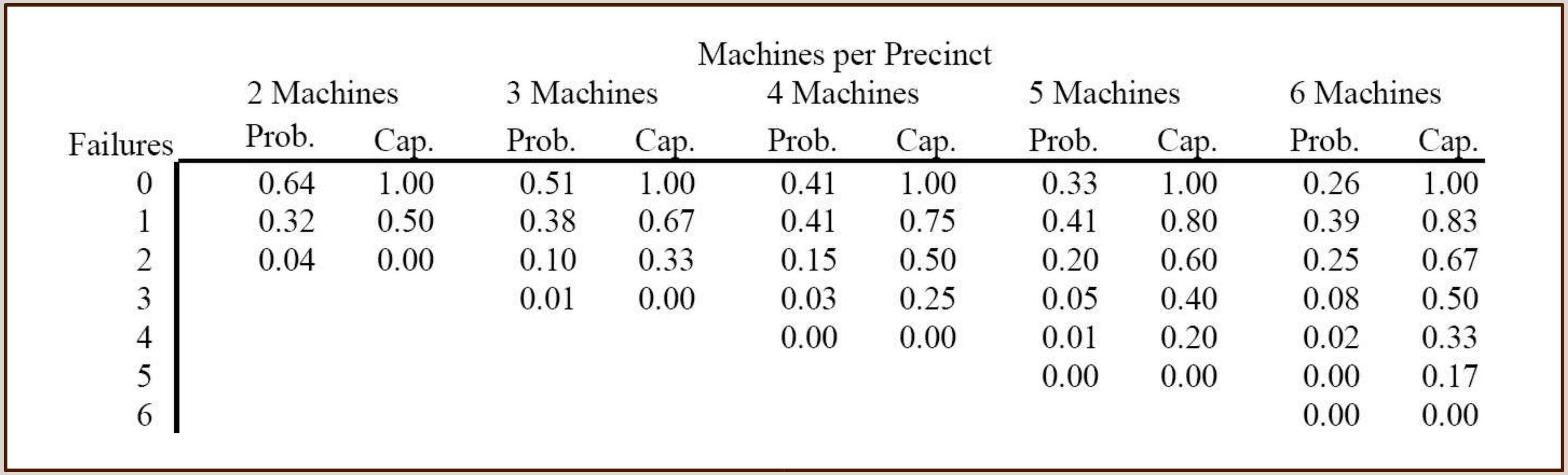
What happens of all but one of the machines are inoperable?

Long lines, impatient (and angry) voters, some of whom can't afford to wait and thus are disenfranchised.

http://www.dos.state.pa.us/elections/lib/elections/090_election_administration_tools/evs_directive.pdf

Emergency paper ballot measure

Our lawsuit seeks to lower Secretary of State's “100% rule” to a more reasonable failure rate before paper ballots are used, say 50%.



	Machines per Precinct									
	2 Machines		3 Machines		4 Machines		5 Machines		6 Machines	
Failures	Prob.	Cap.	Prob.	Cap.	Prob.	Cap.	Prob.	Cap.	Prob.	Cap.
0	0.64	1.00	0.51	1.00	0.41	1.00	0.33	1.00	0.26	1.00
1	0.32	0.50	0.38	0.67	0.41	0.75	0.41	0.80	0.39	0.83
2	0.04	0.00	0.10	0.33	0.15	0.50	0.20	0.60	0.25	0.67
3			0.01	0.00	0.03	0.25	0.05	0.40	0.08	0.50
4					0.00	0.00	0.01	0.20	0.02	0.33
5							0.00	0.00	0.00	0.17
6									0.00	0.00

DRE failure rates of up to 20% have been observed. Our statistical analysis shows that this implies a precinct with 2 machines has a 32% chance of operating at 50% of capacity.

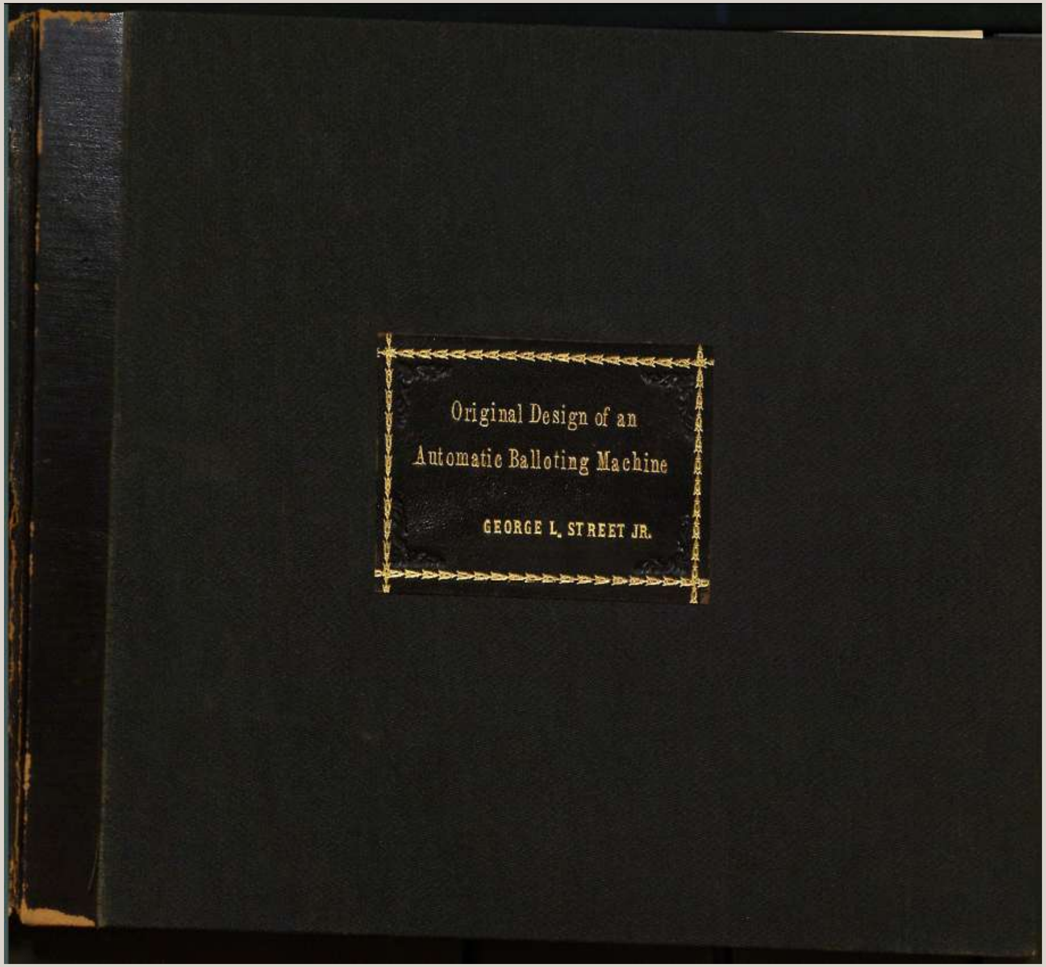
“Analysis of Volume Testing of the AccuVote Tsx / AccuView,” Matt Bishop, Loretta Guarino, David Jefferson, and David Wagner, October 2005.

Interesting historical connection

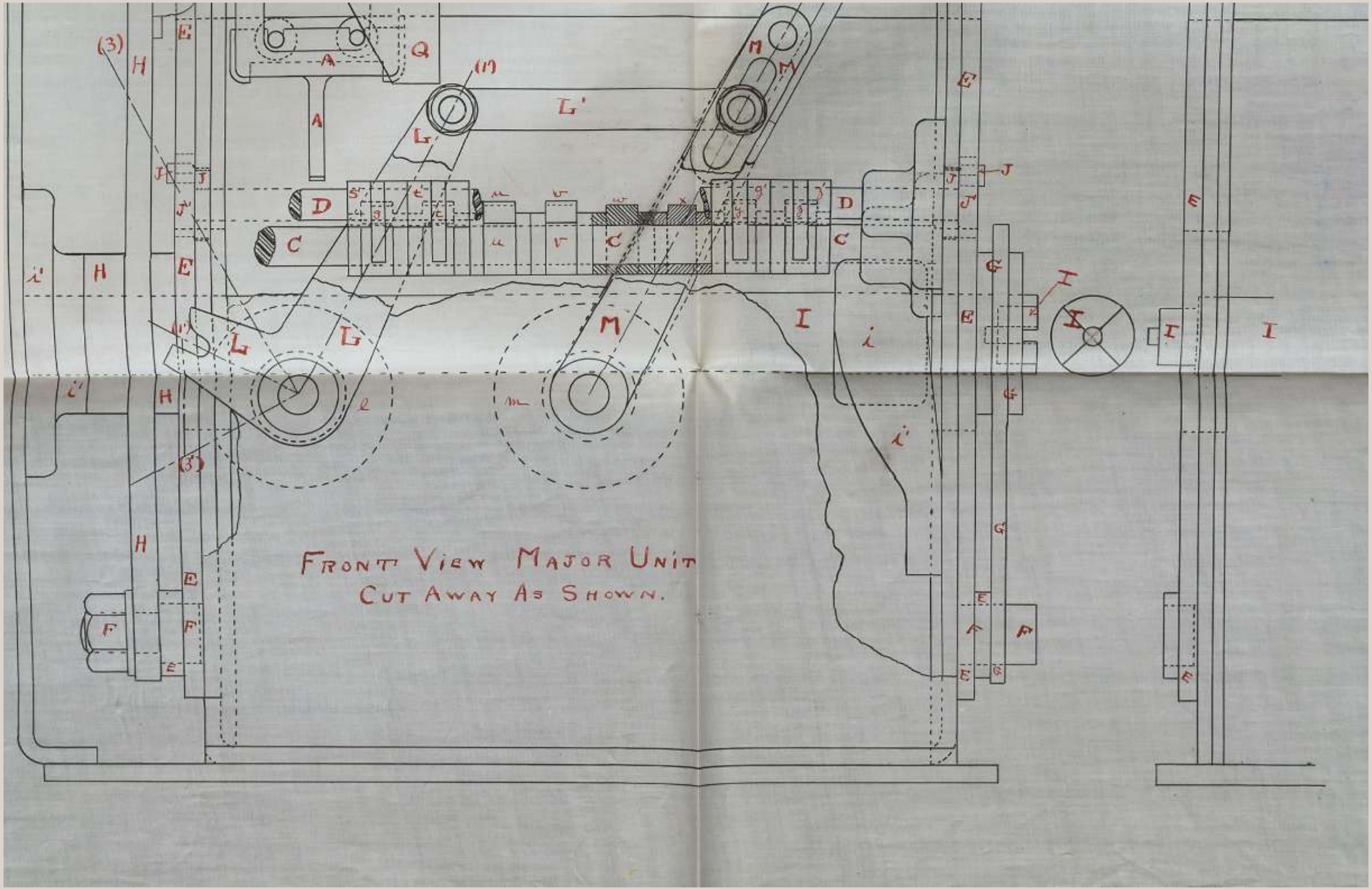
Undergraduate thesis "Original Design of an Automatic Balloting Machine" by George L. Street Jr.

Street was a member of the Lehigh Class of '06 (1906, that is).

Thanks to Ilhan Citak for finding and scanning this.



George L. Street Jr.'s 1906 thesis



FRONT VIEW MAJOR UNIT
CUT AWAY AS SHOWN.

Common retorts

- 🟩 “These attack scenarios are unlikely.”
- 🟩 “Our e-voting systems are certified, so they must be safe.”
- 🟩 “Poll workers are trained to recognize potential problems.”
- 🟥 “Multiple copies of the data are stored in the system, so we're okay.”
- 🟥 “Re-printing the end-of-day tally is just as good as a recount.”
- 🟪 “There's no evidence of anyone having success in an attack like this.”

My assessment: 🟩 = optimistic 🟥 = wrong 🟪 = plain silly

There is no doubt we need good policies and procedures in addition to good, safe technology. (I believe almost everyone involved would like to do the right thing.)

My recommendations

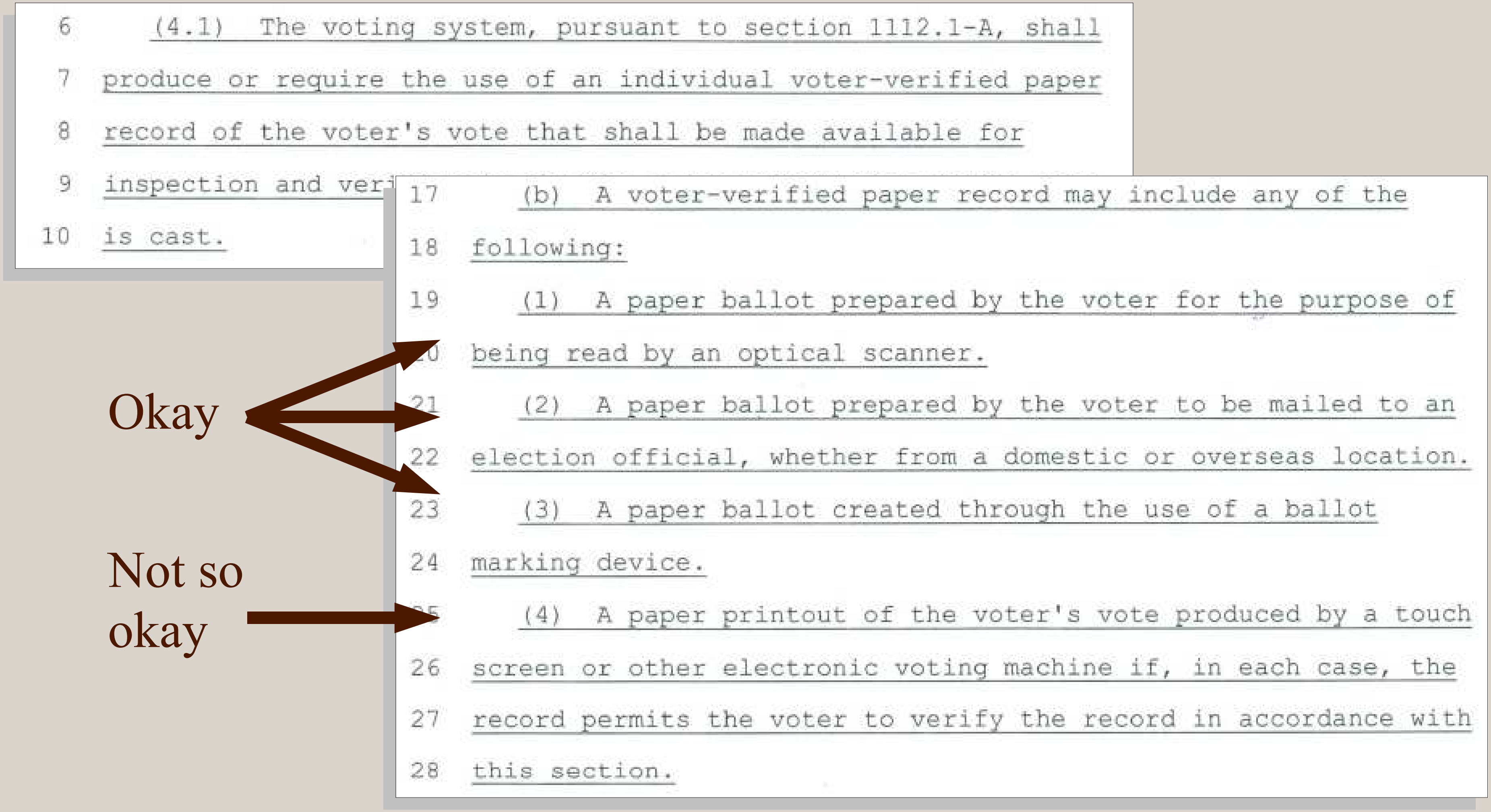
For secure and transparent elections, we should insist on:

- Giving independent experts unfettered access to e-voting software and hardware for verification purposes.
- Use of Voter Verified Paper Records (VVPR).
- Mandatory audits (hand-count a random sampling of all ballots).

And tell our lawmakers to pass pending legislation:

- H.R. 550 (The Voter Confidence and Increased Accessibility Act).
- Pennsylvania H.B. 53.

Pennsylvania H.B. 53



(4.1) The voting system, pursuant to section 1112.1-A, shall produce or require the use of an individual voter-verified paper record of the voter's vote that shall be made available for inspection and veri

is cast.

(b) A voter-verified paper record may include any of the following:

(1) A paper ballot prepared by the voter for the purpose of being read by an optical scanner.

(2) A paper ballot prepared by the voter to be mailed to an election official, whether from a domestic or overseas location.

(3) A paper ballot created through the use of a ballot marking device.

(4) A paper printout of the voter's vote produced by a touch screen or other electronic voting machine if, in each case, the record permits the voter to verify the record in accordance with this section.

Okay

Not so okay

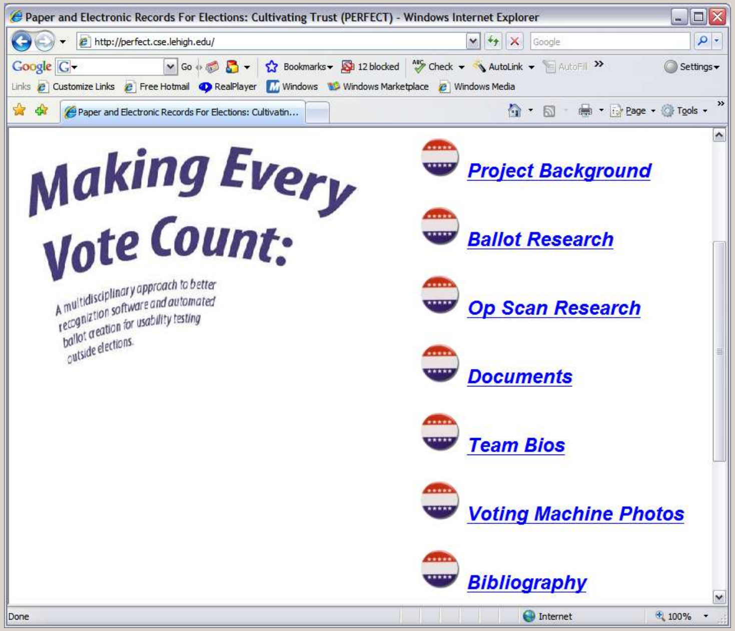
Last Word

VOTE
VOTE!
VOTE
LEAVE YOUR MARK
VOTE
Let Your Voice Be Heard
Get Out And
VOTE!!
VOTE
VOTE
VOTE
Vote
ROCK THE VOTE
VOTE
VOTE
vote!
VOTE
GET OUT THE
VOTE!
VOTE
VOTE
Vote 2008
VOTE

http://perfect.cse.lehigh.edu/

Paper and Electronic Records for Elections: Cultivating Trust

Thank you!



Paper and Electronic Records For Elections: Cultivating Trust (PERFECT) - Windows Internet Explorer

http://perfect.cse.lehigh.edu/

Making Every Vote Count:

A multidisciplinary approach to better recognizton software and automated ballot creation for usability testing outside elections.

- Project Background
- Ballot Research
- Op Scan Research
- Documents
- Team Bios
- Voting Machine Photos
- Bibliography

This work was supported in part by the National Science Foundation under award numbers NSF-0716368, NSF-0716393, NSF-0716647, and NSF-0716543. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect those of the National Science Foundation.