Lecture 35: Electronic Voting

https://cs161.org

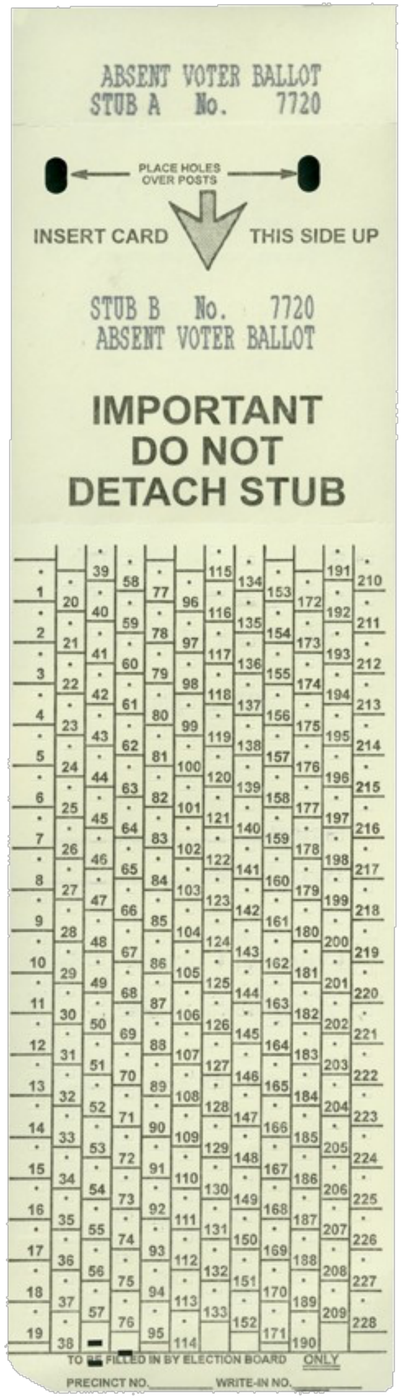
Announcements

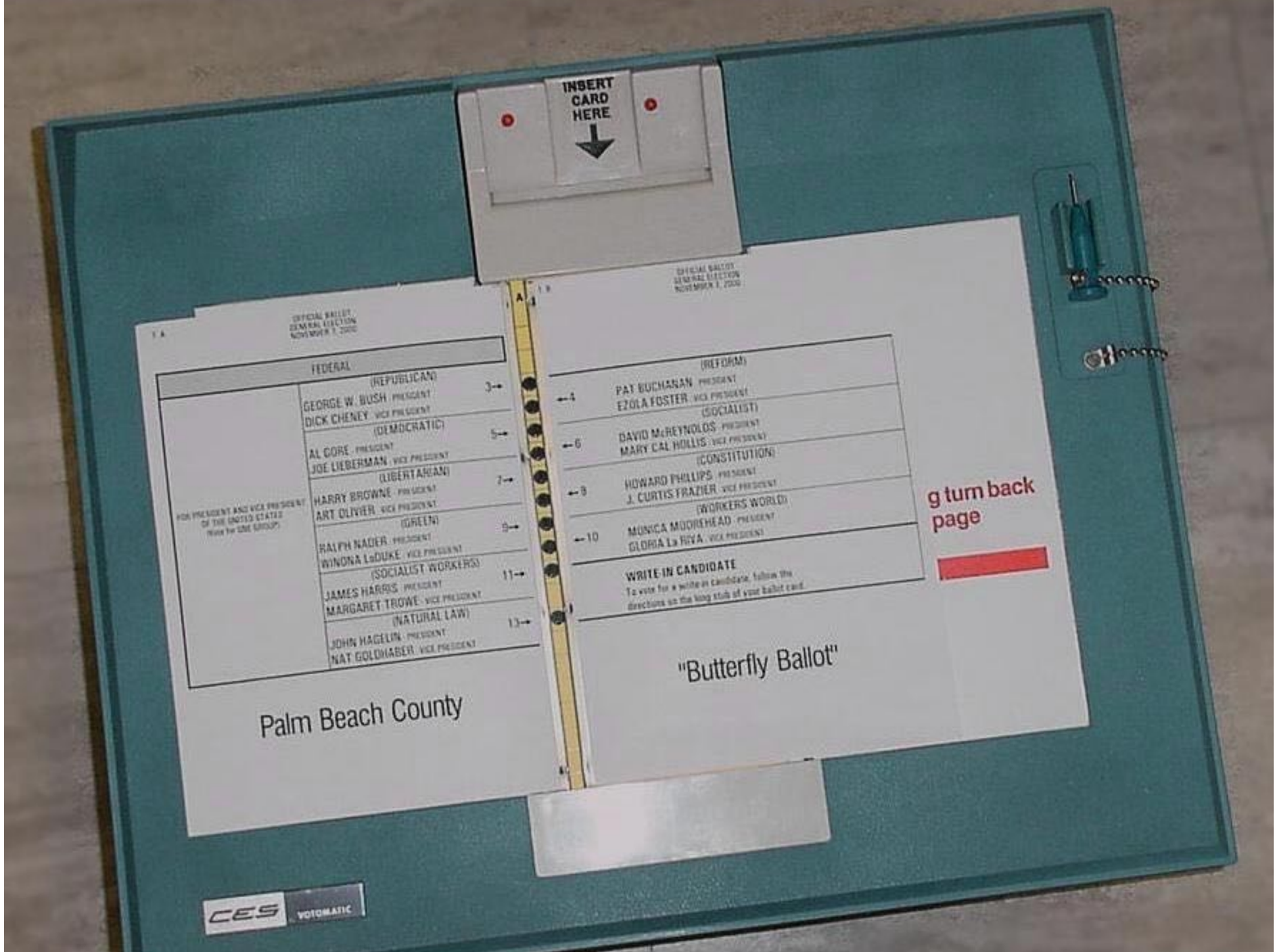
- Homework 3B
- Project 3

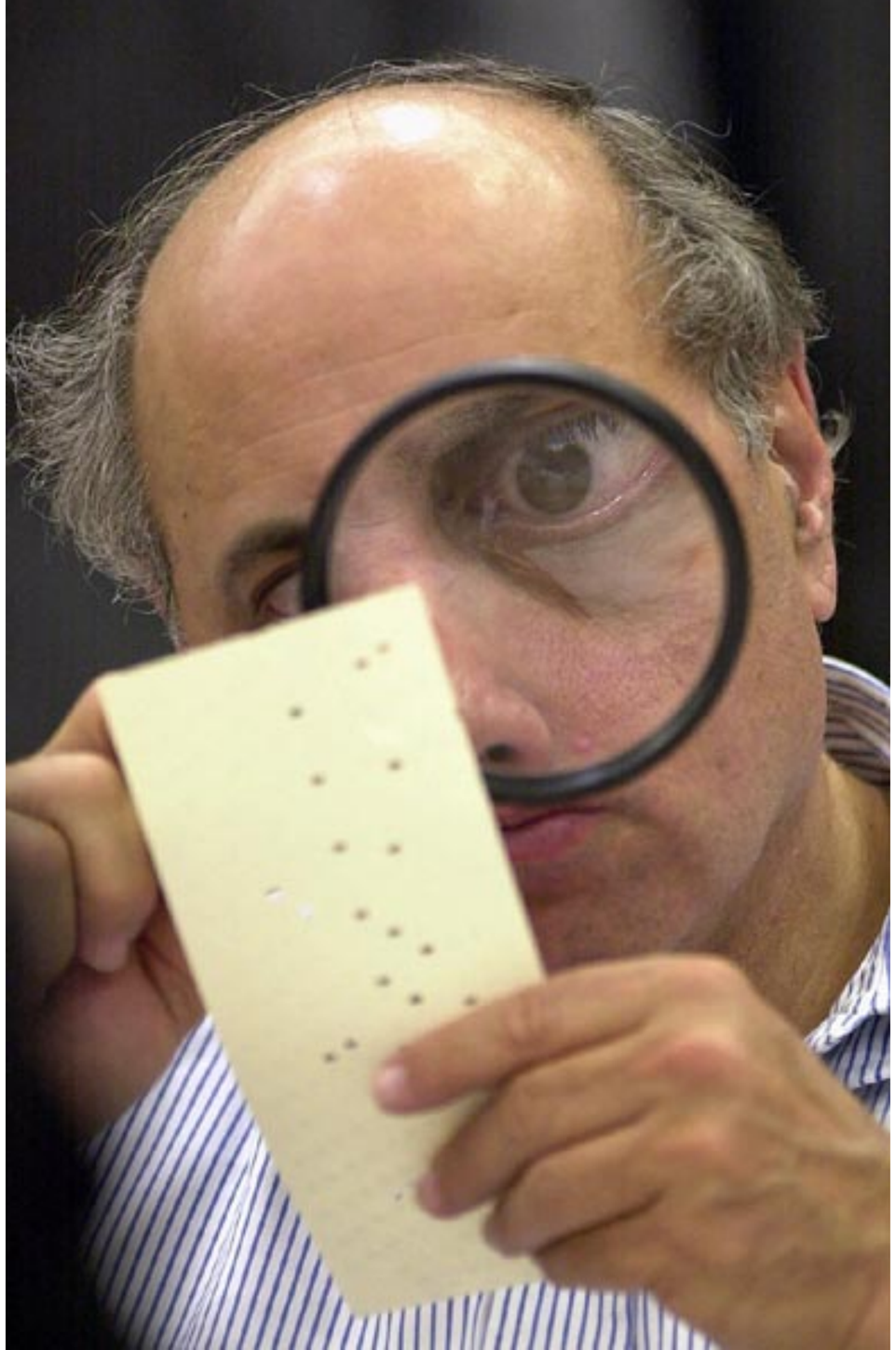
Detection

Security Goals for an Election

- Integrity: no election fraud
- Transparency: Everyone – especially the loser – must be able to verify that the election was conducted appropriately
- Privacy: No one learns how the voter has voted
- Secret ballot: Voter cannot prove how she voted


ABSENT VOTER BALLOT
STUB A No. 7720
PLACE HOLES OVER POSTS
INSERT CARD
THIS SIDE UP
STUB B No. 7720
ABSENT VOTER BALLOT
IMPORTANT
DO NOT
DETACH STUB
TO BE FILLED IN BY ELECTION BOARD ONLY
PRECINCT NO.
WRITE-IN NO.


INSERT CARD HERE
FEDERAL
(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→
Palm Beach County
(REFORM)
←4 PAT BUCHANAN PRESIDENT
EZOLA FOSTER VICE PRESIDENT
(SOCIALIST)
←6 DAVID McREYNOLDS PRESIDENT
MARY CAL HOLLIS VICE PRESIDENT
(CONSTITUTION)
←8 HOWARD PHILLIPS PRESIDENT
J. CURTIS FRAZIER VICE PRESIDENT
(WORKERS WORLD)
←10 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.
g turn back page
"Butterfly Ballot"
CES VOTOMATIC

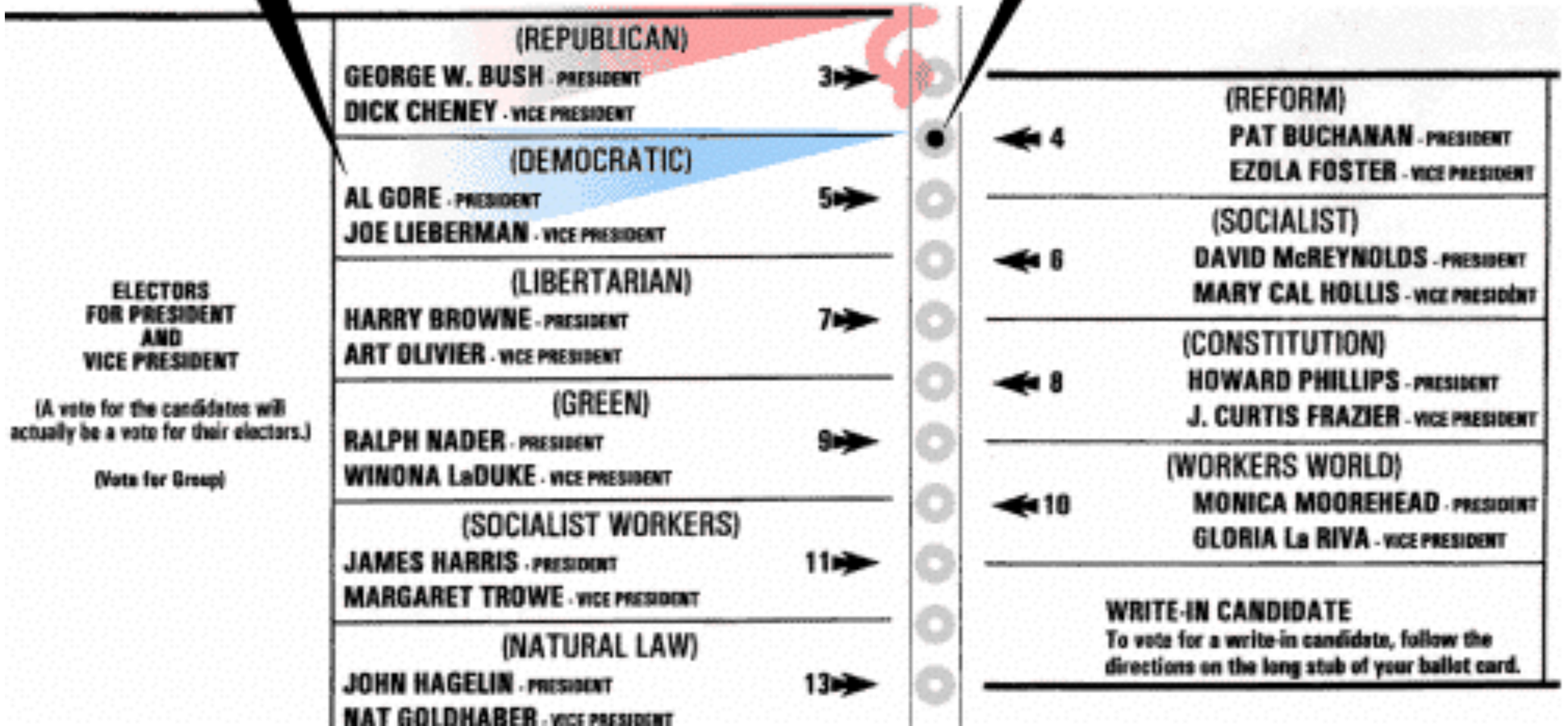


Confusion at Palm Beach County polls

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.



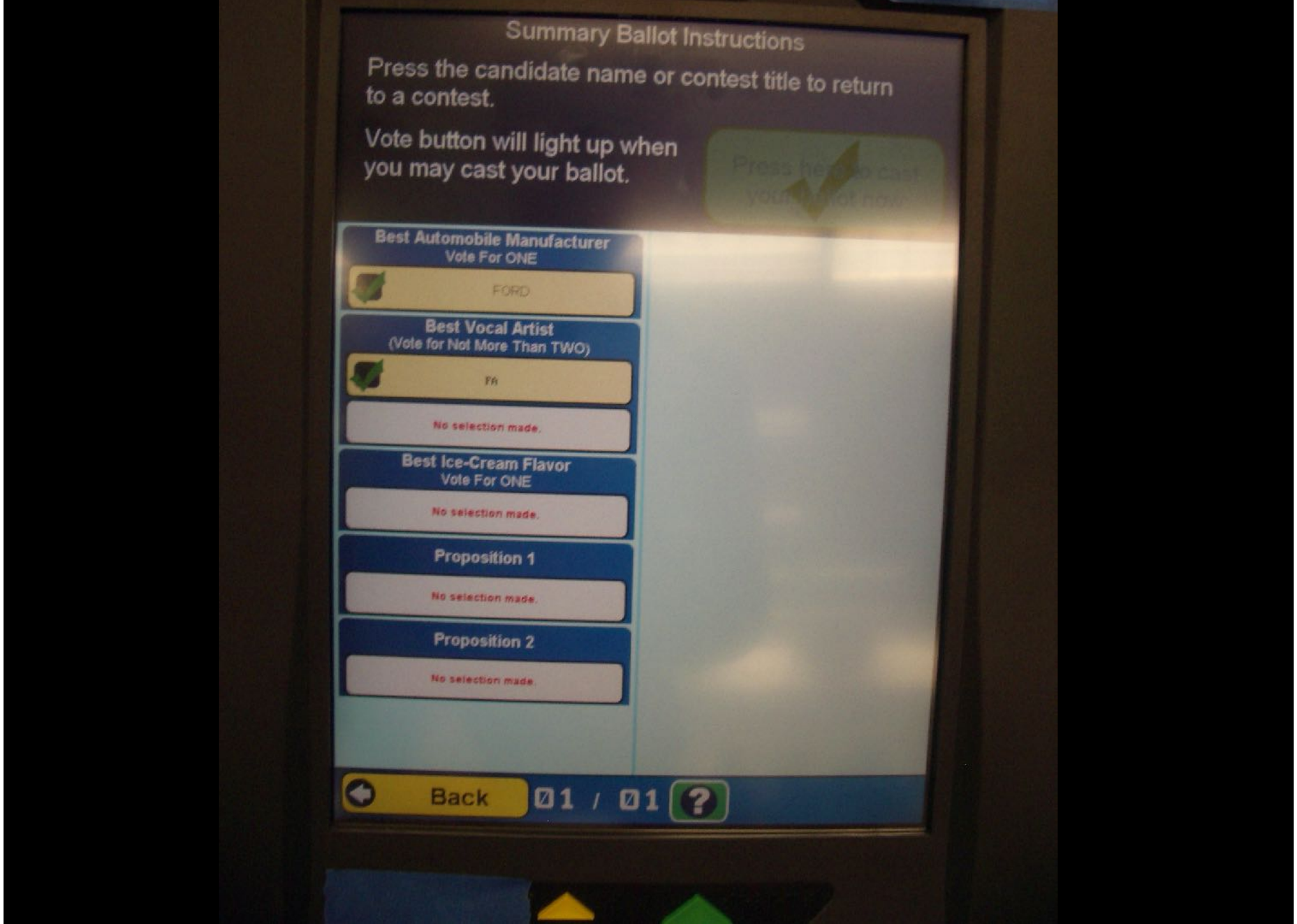
Another Anomaly During the 2000 Election

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".


Please insert
Your Card


Summary Ballot Instructions
Press the candidate name or contest title to return to a contest.
Vote button will light up when you may cast your ballot.
Best Automobile Manufacturer
Vote For ONE
FORD
Best Vocal Artist
(Vote for Not More Than TWO)
FA
No selection made.
Best Ice-Cream Flavor
Vote For ONE
No selection made.
Proposition 1
No selection made.
Proposition 2
No selection made.
Back
01 / 01

Security Requirements for Electronic Voting Machines

- Machine must allow each authorized voter to vote exactly once; must prevent tampering with votes after they are cast.
- Machine should be verifiably trustworthy.
- Machine must randomize the order in which votes were cast.
- Machine must not give voter a “receipt”.

Early use of DREs

- Nov 4, 2002: State of Georgia votes on Diebold DREs.
- March 18, 2003: Diebold source code leaks.
- July 23, 2003: Tadayoshi Kohno, Adam Stubblefield, Avi Rubin, Dan Wallach, “Analysis of an Electronic Voting System”.

Diebold's Voter Authorization Protocol

QueryStatus [Are you a valid card?]

ACTIVE (0x01) [Yup.]

(record vote)

smartcard

[Please cancel yourself.]

SetStatus CANCELED (0x08)

Status = CANCELED

Succeeded [Ok.]

Attack

QueryStatus [Are you a valid card?]

ACTIVE (0x01) [Yup.]

(record vote)

smartcard

[Please cancel yourself.]

SetStatus CANCELED (0x08)

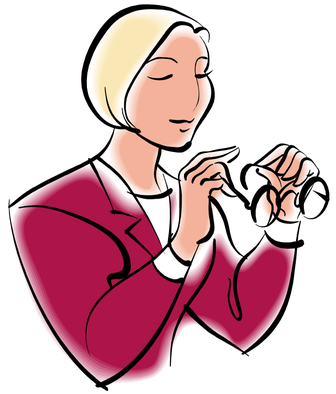
Succeeded [Sure, whatever you say.]

QueryStatus [Are you a valid card?]

ACTIVE (0x01) [Yup. Still valid. Nothing suspicious here.]

(record another vote)

Authenticating Election Officials



What's the secret PIN?

2301

Ok, you have admin access.

What kind of card are you?

An administrator card.

smartcard

What's the secret PIN?

2301


TOUCH
YOU MAY CHANGE
WRITE-IN
CONTINUE
REVIEW
COMPLETE
PAC-MAN

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.

Fall 2003, Ohio

"I am committed to helping Ohio deliver its electoral votes to the president."

-- Wally O'Dell

CEO of Diebold


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
SOFT WARE
SECRET
GOVERNMENT


LIVE FREE
DIE BOLD
VISUALIZE
TRUE
DEMOCRACY
BE THE CHANGE!

California Top-to-Bottom Review

- In 2007, California Secretary of State Debra Bowen commissions a review of California's voting systems.

- 43 experts (led by David Wagner & Matt Bishop) examine voting systems used nationally.

Findings of the TTBR

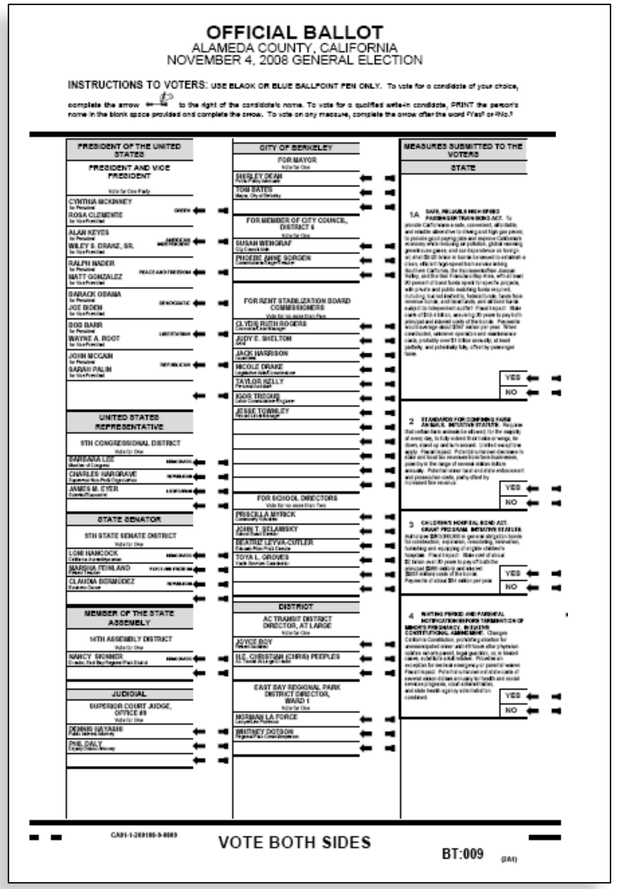
- All voting systems were vulnerable to viral attacks: one outsider could subvert all voting machines countywide

Example Flaw: Diebold/Premier Systems

- Bug: The code that reads data off the memory card has buffer overrun vulnerabilities.
- Attack:
  - Attacker writes malicious code onto a memory card
  - When central PC reads votes off card on election night, it gets infected
  - Infected PC writes malicious code onto all cards used in the next election, infecting entire county

Result of TTBR

- Bowen decertifies most touchscreen e-voting machines and imposes strict new procedural protections.
- Most Californians now vote on paper ballots.



OFFICIAL BALLOT
ALAMEDA COUNTY, CALIFORNIA
NOVEMBER 4, 2008 GENERAL ELECTION

INSTRUCTIONS TO VOTERS: USE BLACK OR BLUE BALLPOINT PEN ONLY. To vote for a candidate of your choice, complete the arrow to the right of the candidate's name. To vote for a qualified write-in candidate, PRINT the person's name in the blank space provided and complete the arrow. To vote on any measure, complete the arrow after the word YES? or NO.?

PRESIDENT OF THE UNITED STATES
PRESIDENT AND VICE PRESIDENT
Vote for One Party
CYNTHIA MCKINNEY / ROSA CLEMENTE — GREEN
ALAN KEYES / MILEY S. DRAKE, SR. — AMERICAN INDEPENDENT
RALPH NADER / MATT GONZALEZ — PEACE AND FREEDOM
BARACK OBAMA / JOE BIDEN — DEMOCRATIC
BOB BARR / WAYNE A. ROOT — LIBERTARIAN
JOHN MCCAIN / SARAH PALIN — REPUBLICAN

UNITED STATES REPRESENTATIVE
9TH CONGRESSIONAL DISTRICT
Vote for One
BARBARA LEE — DEMOCRATIC
CHARLES HARGRAVE — REPUBLICAN
JAMES M. EYER — LIBERTARIAN

STATE SENATOR
9TH STATE SENATE DISTRICT
Vote for One
LONI HANCOCK — DEMOCRATIC
MARSHA FEINLAND — PEACE AND FREEDOM
CLAUDIA BERMUDEZ — REPUBLICAN

MEMBER OF THE STATE ASSEMBLY
14TH ASSEMBLY DISTRICT
Vote for One
NANCY SKINNER — DEMOCRATIC

JUDICIAL
SUPERIOR COURT JUDGE, OFFICE #9
Vote for One
DENNIS HAYBURN
PHIL DALY

CITY OF BERKELEY
FOR MAYOR
Vote for One
BRADLEY DEAN
TOM BATES

FOR MEMBER OF CITY COUNCIL, DISTRICT 6
Vote for One
SUSAN WENGRAF
PRIDGEE JAINE GORDEN

FOR RENT STABILIZATION BOARD COMMISSIONERS
Vote for no more than Five
CLYDE RUTH DOGERS
JUDY E. SHELTON
JACK HARRISON
NICOLE DRAKE
TAYLOR KELLY
KOOS TROOST
JESSE TOWNLEY

FOR SCHOOL DIRECTORS
Vote for no more than Two
PRISCILLA BITTICK
JOHN T. SELAWSKY
BEATRIZ LEYVA-CUTLER
TONYA L. GROVES

DISTRICT
AC TRANSIT DISTRICT DIRECTOR, AT LARGE
Vote for One
JOYCE ROY
H.E. CHRISTOPHER PEEPLES

EAST BAY REGIONAL PARK DISTRICT DIRECTOR, WARD 1
Vote for One
NORMAN LA FORCE
BRITNEY DOTSON

MEASURES SUBMITTED TO THE VOTERS
STATE
1A
YES
NO
2
YES
NO
3
YES
NO
4
YES
NO

VOTE BOTH SIDES
BT:009

Backdoors and the Insider Threat

Ronald Dale Harris

Employee, Gaming Control Board, 1983-1995

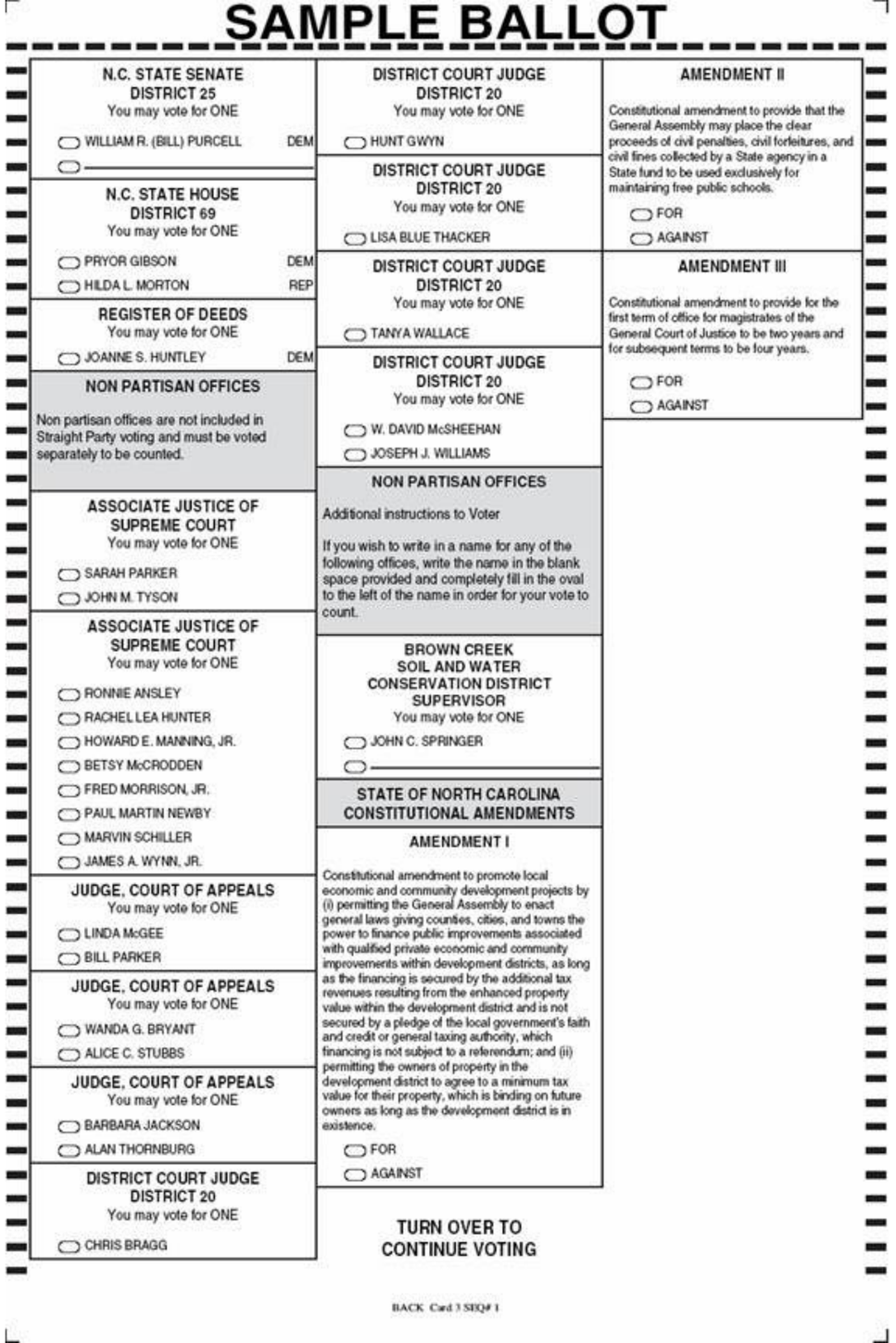
Arrested, Jan 15,1995
Convicted, Sept 23, 1997, for rigging slot machines

Attempted Back Door in Linux Kernel


```
        …
        schedule();
        goto repeat;
}
if ((options == (__WCLONE|__WALL)) && current->uid = 0))
        retval = -EINVAL;
retval = -ECHILD;
end_wait4:
current->state = TASK_RUNNING;
…
```

Defense Against Backdoors in Voting Machines

- Malicious logic hidden by an insider might, e.g., record votes incorrectly to favor one candidate. How would we defend a voting system against this kind of insider threat?
- Potential solutions:
  - Verify that the software is free of Trojans and will work correctly on all future elections. (beyond the state of the art)
  - Assume software might contain Trojans. Verify that software worked correctly in this particular election. (voter-verified paper records + random audits)



SAMPLE BALLOT

N.C. STATE SENATE DISTRICT 25
You may vote for ONE

- WILLIAM R. (BILL) PURCELL — DEM
- _____

N.C. STATE HOUSE DISTRICT 69
You may vote for ONE

- PRYOR GIBSON — DEM
- HILDA L. MORTON — REP

REGISTER OF DEEDS
You may vote for ONE

- JOANNE S. HUNTLEY — DEM

NON PARTISAN OFFICES

Non partisan offices are not included in Straight Party voting and must be voted separately to be counted.

ASSOCIATE JUSTICE OF SUPREME COURT
You may vote for ONE

- SARAH PARKER
- JOHN M. TYSON

ASSOCIATE JUSTICE OF SUPREME COURT
You may vote for ONE

- RONNIE ANSLEY
- RACHEL LEA HUNTER
- HOWARD E. MANNING, JR.
- BETSY McCRODDEN
- FRED MORRISON, JR.
- PAUL MARTIN NEWBY
- MARVIN SCHILLER
- JAMES A. WYNN, JR.

JUDGE, COURT OF APPEALS
You may vote for ONE

- LINDA McGEE
- BILL PARKER

JUDGE, COURT OF APPEALS
You may vote for ONE

- WANDA G. BRYANT
- ALICE C. STUBBS

JUDGE, COURT OF APPEALS
You may vote for ONE

- BARBARA JACKSON
- ALAN THORNBURG

DISTRICT COURT JUDGE DISTRICT 20
You may vote for ONE

- CHRIS BRAGG

DISTRICT COURT JUDGE DISTRICT 20
You may vote for ONE

- HUNT GWYN

DISTRICT COURT JUDGE DISTRICT 20
You may vote for ONE

- LISA BLUE THACKER

DISTRICT COURT JUDGE DISTRICT 20
You may vote for ONE

- TANYA WALLACE

DISTRICT COURT JUDGE DISTRICT 20
You may vote for ONE

- W. DAVID McSHEEHAN
- JOSEPH J. WILLIAMS

NON PARTISAN OFFICES

Additional instructions to Voter

If you wish to write in a name for any of the following offices, write the name in the blank space provided and completely fill in the oval to the left of the name in order for your vote to count.

BROWN CREEK SOIL AND WATER CONSERVATION DISTRICT SUPERVISOR
You may vote for ONE

- JOHN C. SPRINGER
- _____

STATE OF NORTH CAROLINA CONSTITUTIONAL AMENDMENTS

AMENDMENT I

Constitutional amendment to promote local economic and community development projects by (i) permitting the General Assembly to enact general laws giving counties, cities, and towns the power to finance public improvements associated with qualified private economic and community improvements within development districts, as long as the financing is secured by the additional tax revenues resulting from the enhanced property value within the development district and is not secured by a pledge of the local government's faith and credit or general taxing authority, which financing is not subject to a referendum; and (ii) permitting the owners of property in the development district to agree to a minimum tax value for their property, which is binding on future owners as long as the development district is in existence.

- FOR
- AGAINST

AMENDMENT II

Constitutional amendment to provide that the General Assembly may place the clear proceeds of civil penalties, civil forfeitures, and civil fines collected by a State agency in a State fund to be used exclusively for maintaining free public schools.

- FOR
- AGAINST

AMENDMENT III

Constitutional amendment to provide for the first term of office for magistrates of the General Court of Justice to be two years and for subsequent terms to be four years.

- FOR
- AGAINST

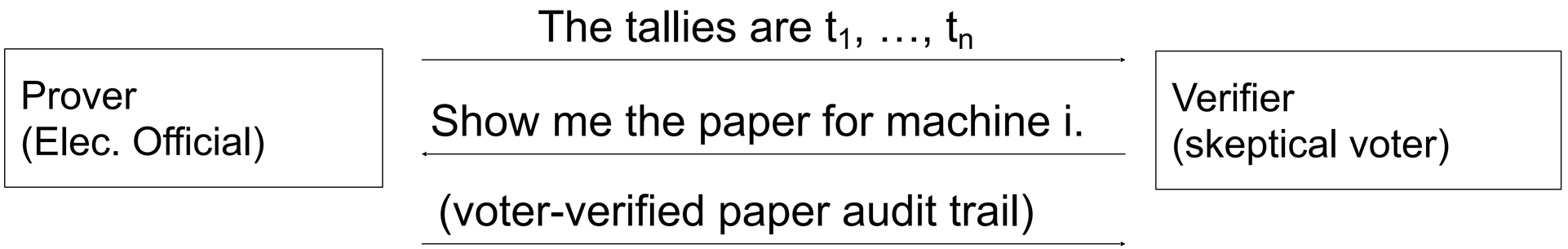
TURN OVER TO CONTINUE VOTING

BACK Card 3 SEQ# 1


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

Statistical Audit

- After election, randomly choose 1% of machines and manually recount the paper records on those machines. If paper count ≠ electronic count, there was fraud.
- If » 100 machines lie, detection is likely. Consequently: If paper count = electronic count, then likely no more than ~100 machines lied.



Conclusions: Electronic voting

- E-voting security is hard, but can be made secure and trustworthy, if it can be audited.

Broader Takeaways

- Sometimes technical threats can be handled through non-technical defenses.
- Seek independent, end-to-end checks that the system is working properly.
- Securing systems against malicious insiders is extremely challenging.
- Business structure determines the technology that is built & deployed. If buyers cannot measure how secure a product is, be prepared for market failures.

Extra Material


THE HAZARDS OF ONLINE VOTING . . .
HORSEY
PRESIDENT OF THE UNITED STATES
VOTE FOR ONE
GEORGE W. BUSH R
JOHN F. KERRY D
RALPH NADER I
LOW-COST HOME MORTGAGE
GENERIC VIAGRA
ENLARGE YOUR THINGY
GREETINGS! I AM NDUGU SCAMU, EX-INTERIOR MINISTER OF NIGERIA, AND I NEED YOUR HELP TO TRANSFER $150,000,000 IN FUNDS TO A BANK