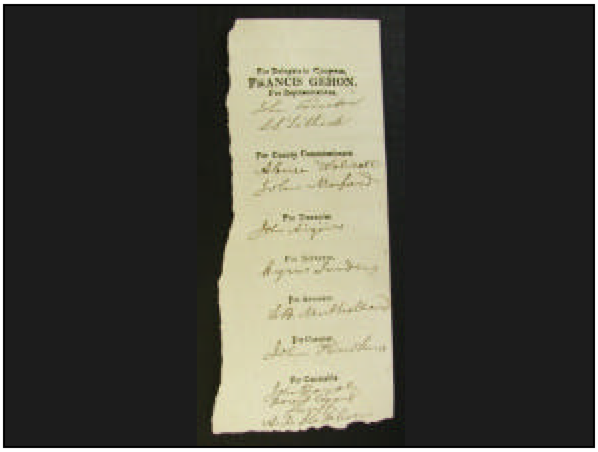
CS 194-1 (CS 161) Computer Security

Lecture 24

Elections, Computer Security, and Electronic Voting

November 29, 2006
Prof. Anthony D. Joseph
http://cs161.org/

(Slides courtesy of Prof. David Wagner)



For Delegate to Congress,
FRANCIS GEHON.
For Representatives

For County Commissioners

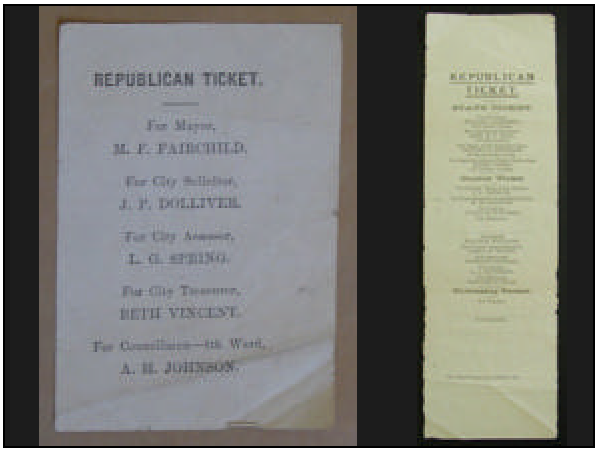
For Treasurer

For Sheriff

For Assessor

For Coroner

For Constable



REPUBLICAN TICKET.

For Mayor,
M. F. FAIRCHILD.

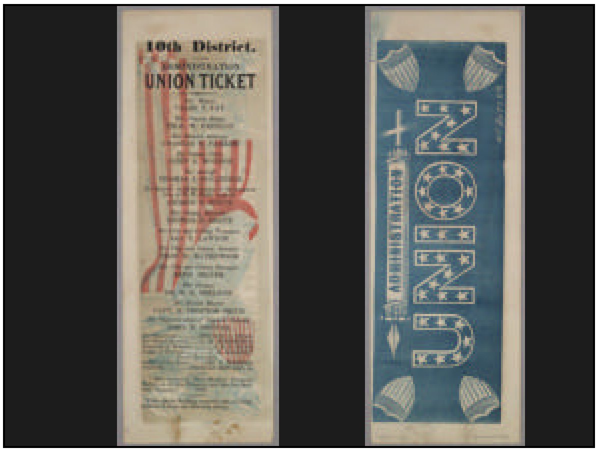
For City Solicitor,
J. P. DOLLIVER.

For City Assessor,
L. G. SPRING.

For City Treasurer,
SETH VINCENT.

For Councilmen—4th Ward,
A. H. JOHNSON.

REPUBLICAN
TICKET.
STATE TICKET



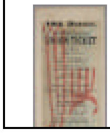
10th District.
ADMINISTRATION
UNION TICKET

UNION
ADMINISTRATION

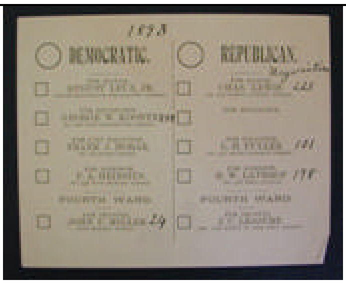
Security Goals for an Election

- Integrity: No election fraud
- Transparency: Everyone must be able to verify that the election was conducted appropriately

- Privacy: No one learns how the voter has voted

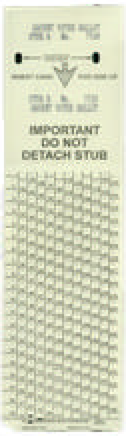


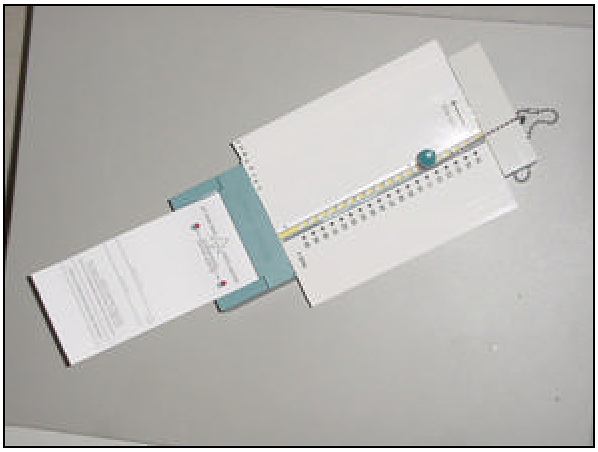
- Secret ballot: Voter cannot prove how she voted

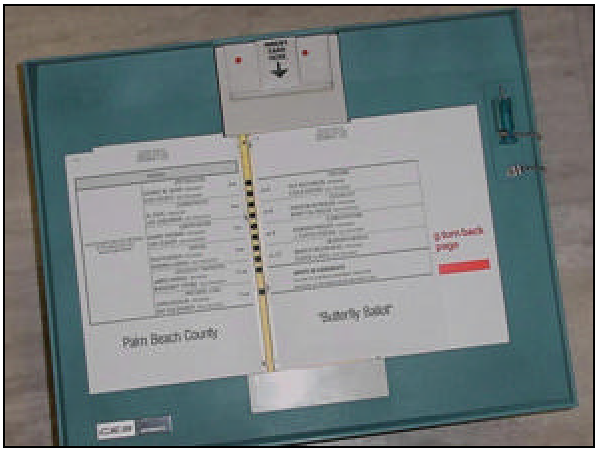


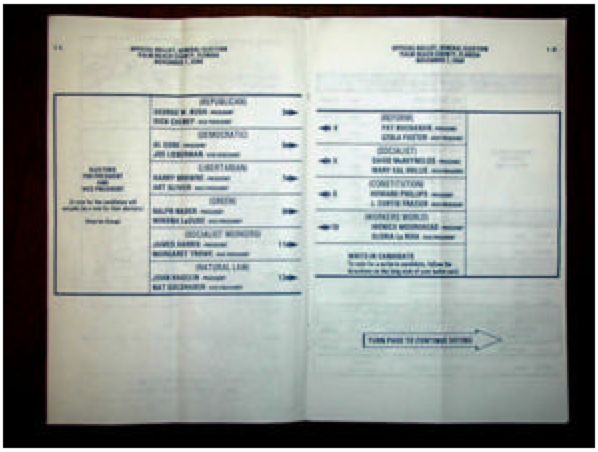
Breakthrough! — the Australian secret ballot.

Ballot printed by govt. Ballot boxes monitored by observers. Ballots counted, by hand, in public. Competing interests keep each other honest.



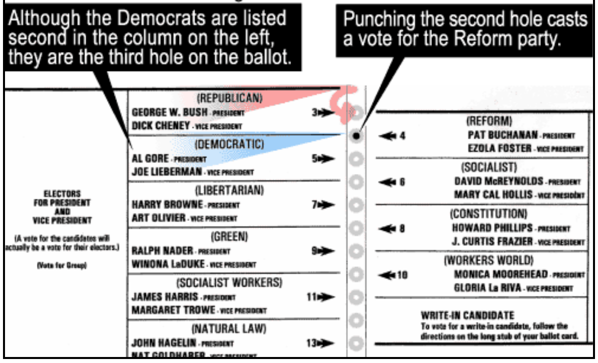






Confusion at Palm Beach County polls

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.

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 ➤

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

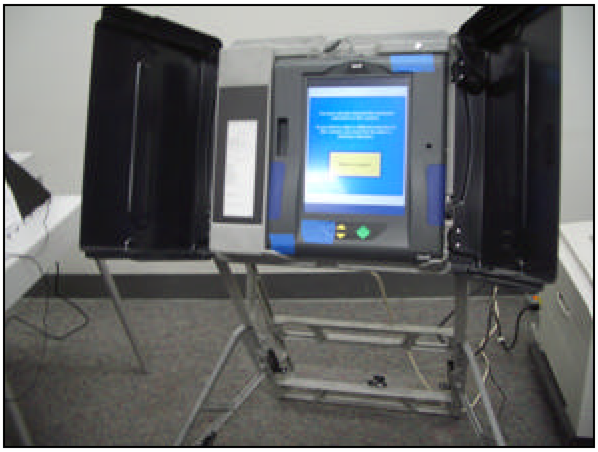
(SOCIALIST)
◄ 6
DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT

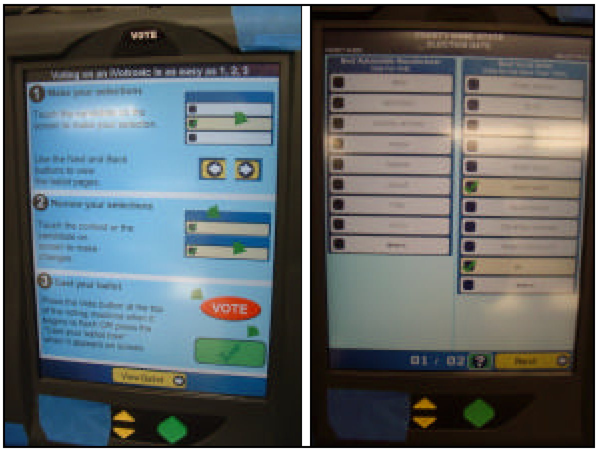
(CONSTITUTION)
◄ 8
HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT

(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.

09/07/2004



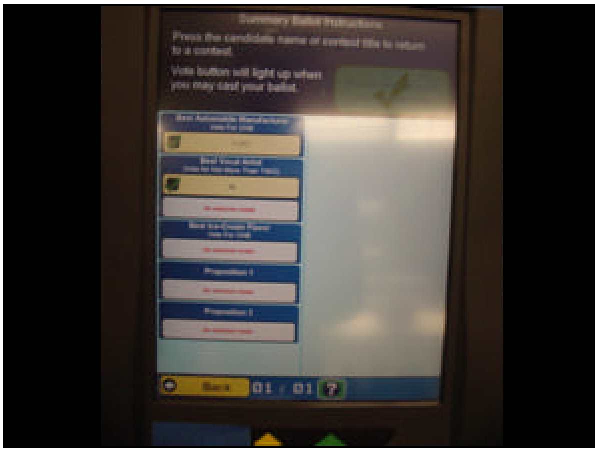


Voting on an iVotronic is as easy as 1, 2, 3

1 Make your selections

2 Review your selections

3 Cast your ballot



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.

Question: How do election security goals apply to touchscreen (DRE) electronic voting machines?

1. Machine must allow each authorized voter to vote exactly once; must prevent tampering with votes after they are cast.

2. Machine should be verifiably trustworthy.

3. Machine must randomize the order in which votes were cast.

4. Machine must not give voter a “receipt”.

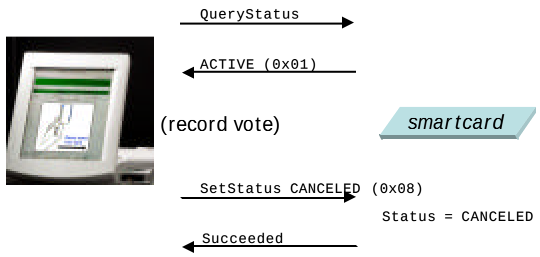
☞ Security Goals for an Election:
Integrity, Transparency, Privacy, Secret ballot

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”.

The voter authorization protocol



QueryStatus →

← ACTIVE (0x01)

(record vote)

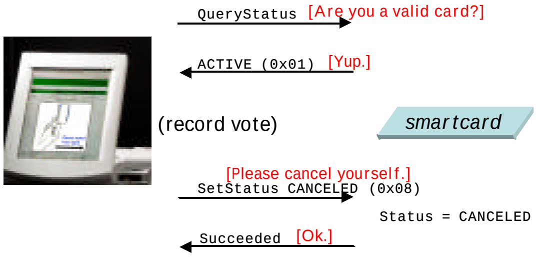
smartcard

SetStatus CANCELED (0x08) →

Status = CANCELED

← Succeeded

The voter authorization protocol



QueryStatus [Are you a valid card?] →

← ACTIVE (0x01) [Yup.]

(record vote)

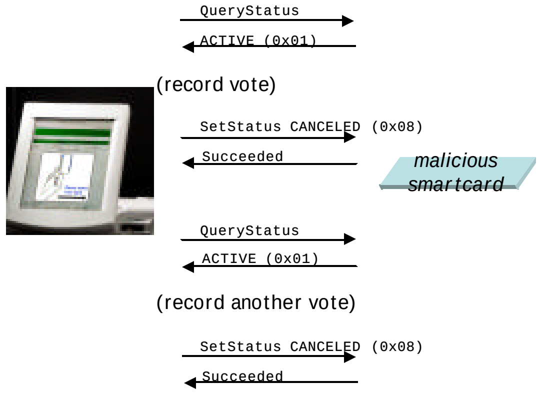
smartcard

[Please cancel yourself.]
SetStatus CANCELED (0x08) →

Status = CANCELED

← Succeeded [Ok.]

Attack!



QueryStatus →

← ACTIVE (0x01)

(record vote)

SetStatus CANCELED (0x08) →

← Succeeded

malicious smartcard

QueryStatus →

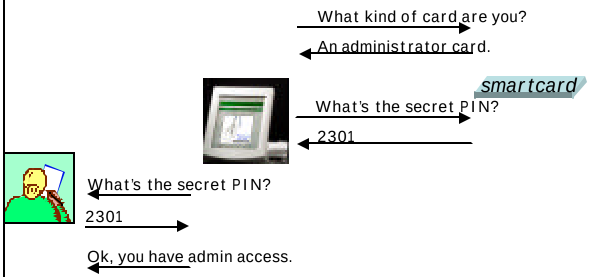
← ACTIVE (0x01)

(record another vote)

SetStatus CANCELED (0x08) →

← Succeeded

Authenticating election officials



What kind of card are you? →

← An administrator card.

smartcard

What’s the secret PIN? →

← 2301

← What’s the secret PIN?

2301 →

← Ok, you have admin access.

Source code excerpts

```
#define DESKEY ((des_key*)”F2654hD4”)



DESCBCEncrypt((des_c_block*)tmp,
(des_c_block*)record.m_Data, totalSize,
DESKEY, NULL, DES_ENCRYPT);
```

Source code excerpts

```
// LCG - Linear Congruential Generator -
// used to generate ballot serial numbers
// A psuedo-random-sequence generator
// (per Applied Cryptography, Bruce Schneier)

int lcgGenerator(int lastSN) {
  return ((lastSN*1366) + 150889)%714025;
}
```

“Unfortunately, linear congruential generators cannot be used for cryptography.”
— Applied Cryptography, p.369

Reactions from voters

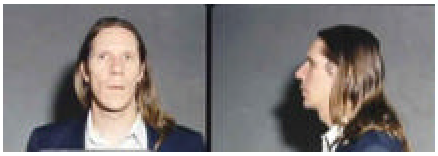
"It's not who votes that counts.
It's who counts the votes."
Diebold. Because democracy is too important to leave to chance.
DIEBOLD

Will your vote be
counted in November?
HACK
THE
VOTE
How can you be sure?
www.ubidubium.net/Politics

ELECTRONIC VOTING IS UNRELIABLE
PAPER BALLOTS
THE COMPUTER ATE MY VOTE!
VOTING WITHOUT AUDITING ARE WE INSANE?
SECRET SOFTWARE SECRET GOVERNMENT
HOW LONG WILL IT TAKE TO GET IT RIGHT
ELECTION FRAUD
MEDIA BLACKOUT
VOTE

Movie

Trojan Horses and the Insider Threat



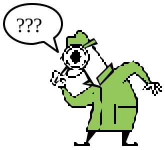
Ronald Dale Harris

Employee, Gaming Control Board, 1983-1995

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

Attempted Trojan Horse in Linux Kernel

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



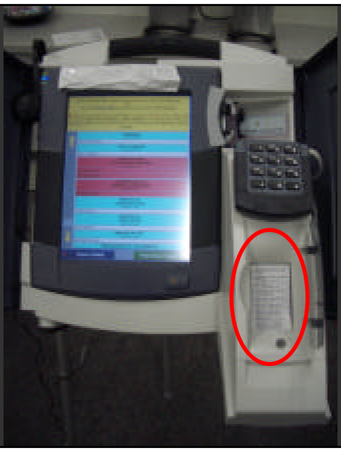
Trojan Horses and Voting Machines

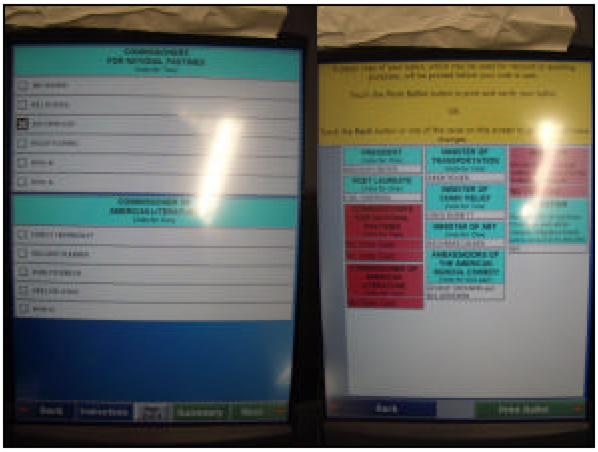
Malicious logic hidden by an insider might, e.g., record votes incorrectly to favor one candidate. Extremely difficult to prevent or detect.

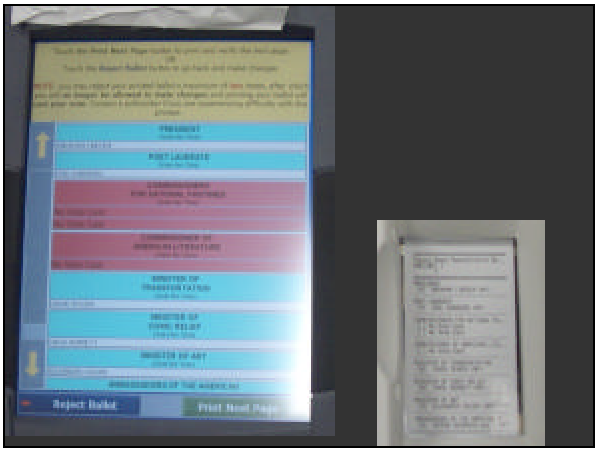
Potential solutions:

- Verify that the software is free of Trojans. (beyond the state of the art)

- Verify that output of the sw is correct.
  - Voter-verified paper audit trail, 1% audits
  - Optical scan (paper ballots)
  - Ballot marking devices (paper ballots)

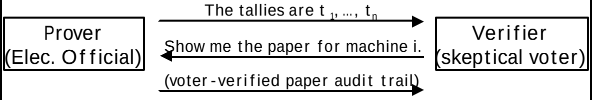






Statistical audit

- 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 cheat, detection is likely. Consequently: If paper count = electronic count, then no more than ~100 machines cheated.

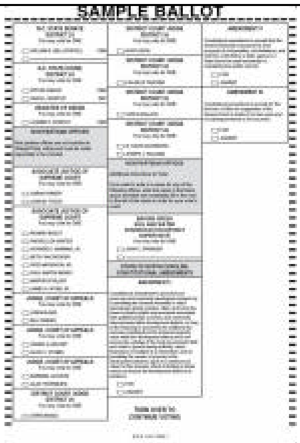

Prover (Elec. Official)

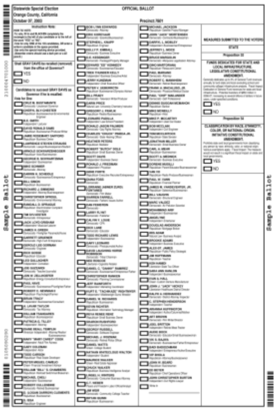
Verifier (skeptical voter)

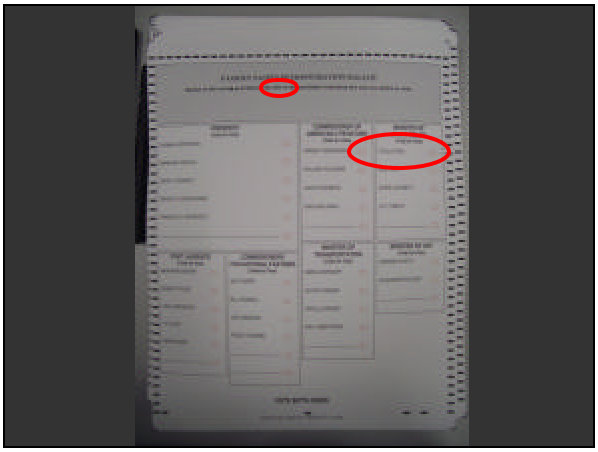
The tallies are $t_1, \ldots, t_n$

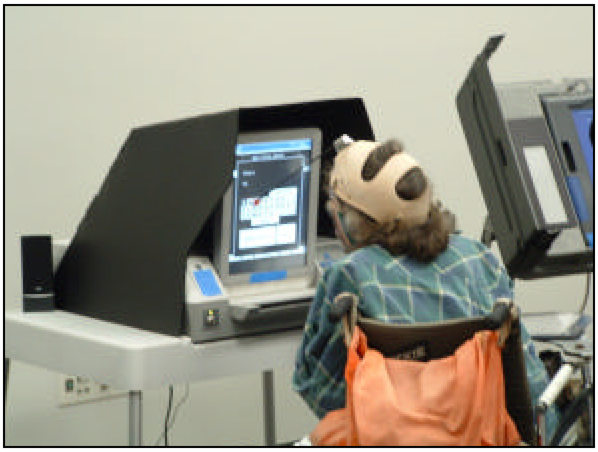
Show me the paper for machine i.

(voter-verified paper audit trail)


SAMPLE BALLOT


Sample Ballot

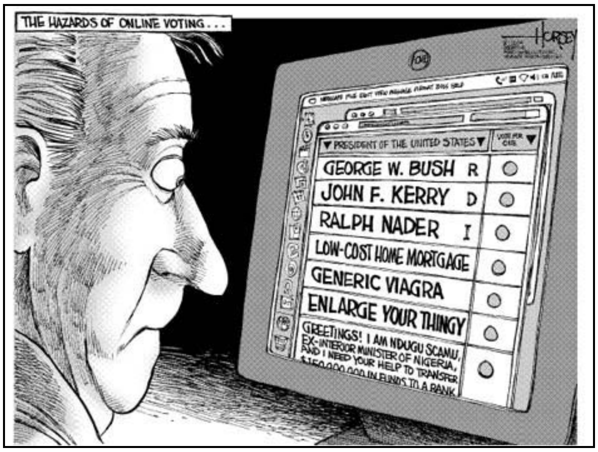




Conclusions

- E-voting security is hard, because computers aren't transparent.
- All known solutions use paper. Secure paperless voting is an open research problem.
- Computer science is deeply relevant to democracy.

- Technical principles:
  - Two-person control, separation of duties
  - Statistical audit
  - Security against malicious insiders


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