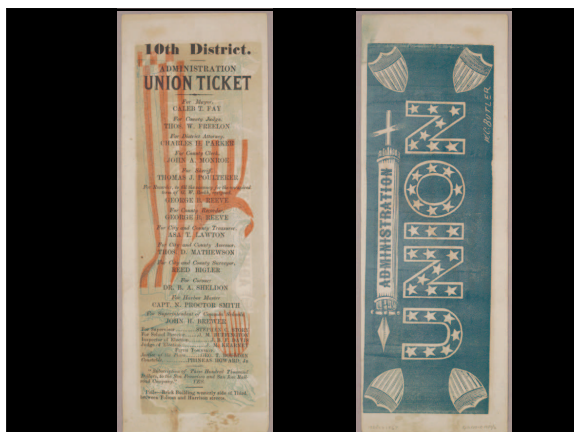
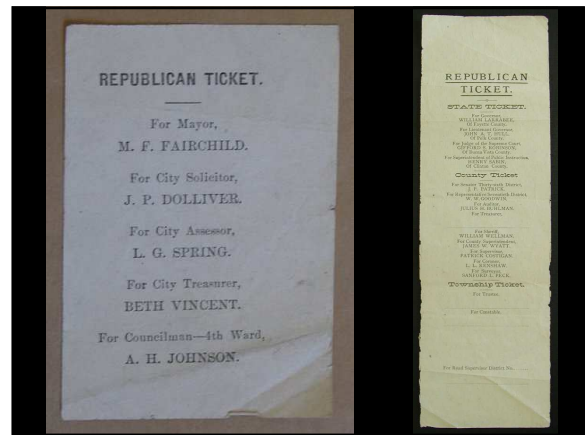
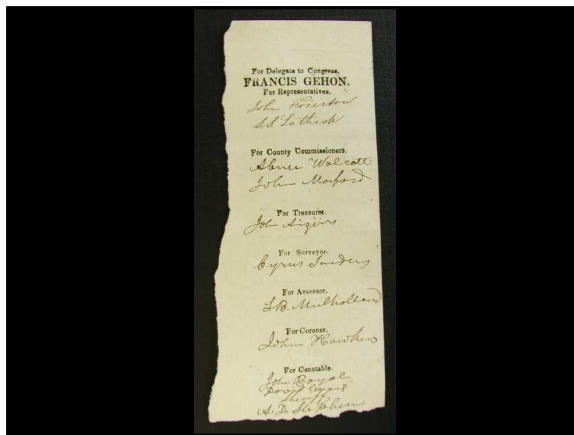


# Elections, Computer Security, and Electronic Voting

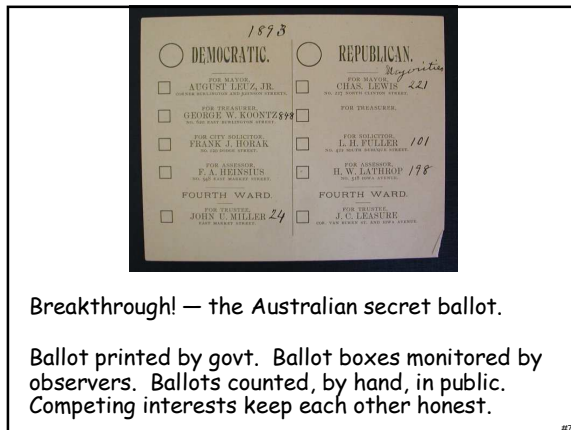
CS161 12/7/2005  
David Wagner



## Security Goals for an Election

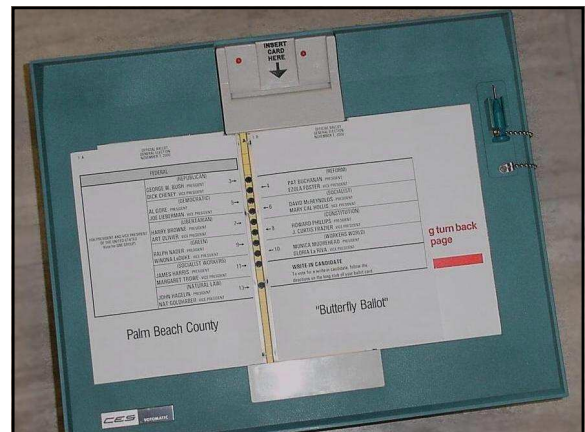
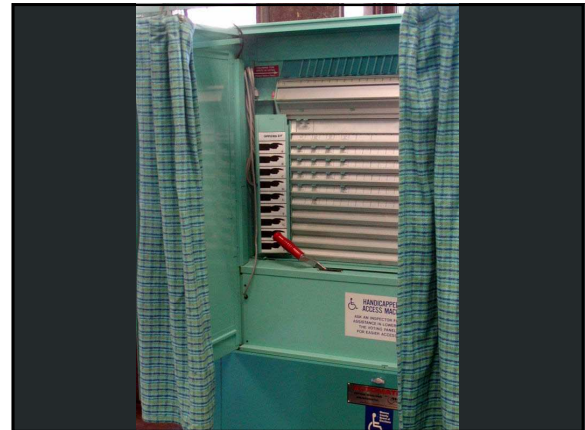
- Integrity: No election fraud
- Transparency: Everyone must be able to verify that the election was conducted appropriately
- Privacy: No one learns how the voter has voted
- Secret ballot: Voter cannot prove how she voted





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.

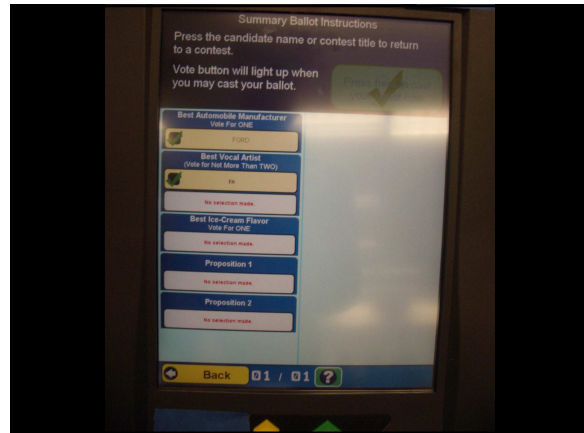
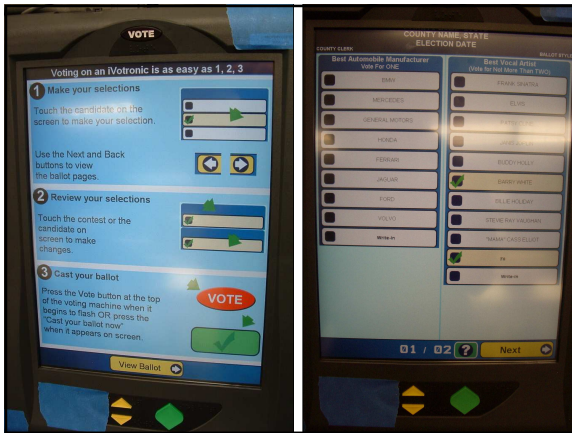
Punching the second hole casts a vote for the Reform party.

ELECTORS FOR PRESIDENT AND VICE PRESIDENT	(REPUBLICAN)	(DEMOCRATIC)	(LIBERTARIAN)	(GREEN)	(SOCIALIST WORKERS)	(NATURAL LAW)	(REFORM)	(SOCIALIST)	(CONSTITUTION)	(WORKERS WORLD)
1	GEORGE W. BUSH - PRESIDENT	AL GORE - PRESIDENT	HARRY BROWNE - PRESIDENT	RALPH NADER - PRESIDENT	JAMES HARRIS - PRESIDENT	JOHN HAGELIN - PRESIDENT	PAT BUCHANAN - PRESIDENT	DAVID MURKIN - PRESIDENT	HOWARD PHILLIPS - PRESIDENT	MONICA MOOREHEAD - PRESIDENT
2	DICK CHENEY - VICE PRESIDENT	JOE LIEBERMAN - VICE PRESIDENT	ART OLIVER - VICE PRESIDENT	WINDA LADUNE - VICE PRESIDENT	MARGARET TROWE - VICE PRESIDENT		SEOLA POSTER - VICE PRESIDENT	MARY CAL HOLLS - VICE PRESIDENT	J. CURTIS FRAZER - VICE PRESIDENT	GLORIA LA RIVA - VICE PRESIDENT
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										

WRITE-IN CANDIDATE

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





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

#19

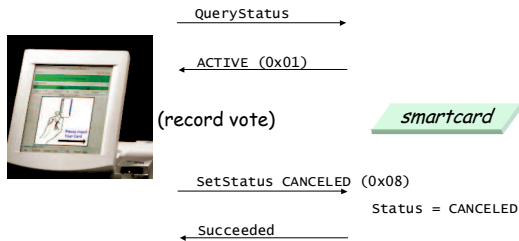
Nov 4, 2002:  
State of Georgia votes on Diebold DREs.

March 18, 2003:  
Diebold source code leaks.

July 23, 2003:  
Tadayoshi Kohno, Adam Stubblefield, Avi Rubin, Dan Wallach, "Analysis of an Electronic Voting System".

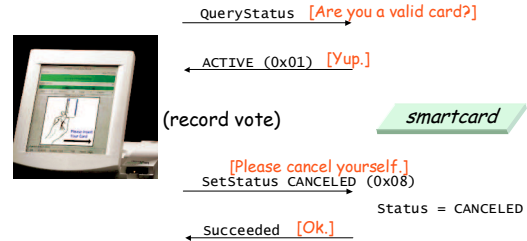
#20

### The voter authorization protocol



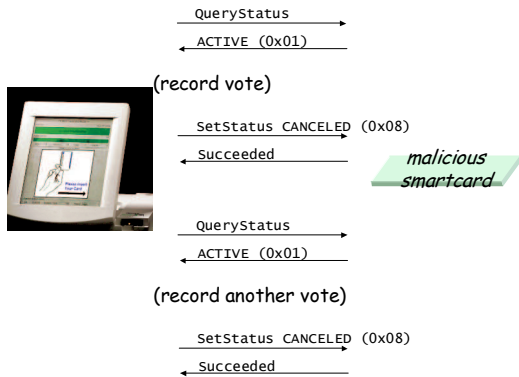
#21

### The voter authorization protocol



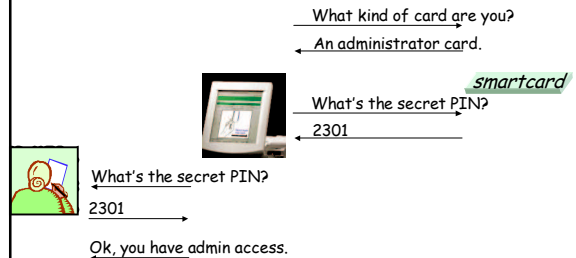
#22

### Attack!



#23

### Authenticating election officials



#24

### Source code excerpts

```

#define DESKEY ((des_key*)"F2654hd4")

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

#25

### Source code excerpts

```

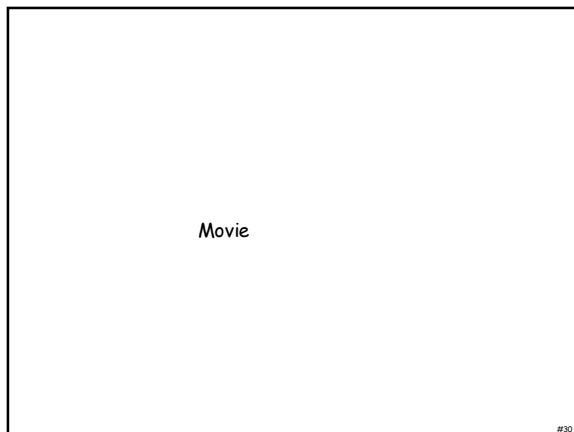
// LCG - Linear Congruential Generator -
// used to generate ballot serial numbers
// A pseudo-random-sequence generator
// (per Applied Cryptography, Bruce Schneier)

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

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

#26





### 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;
...

```



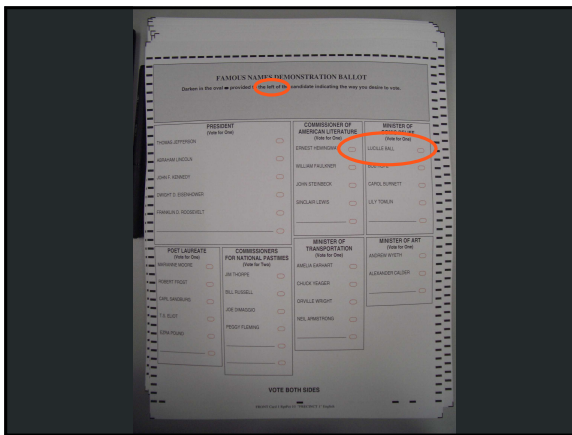
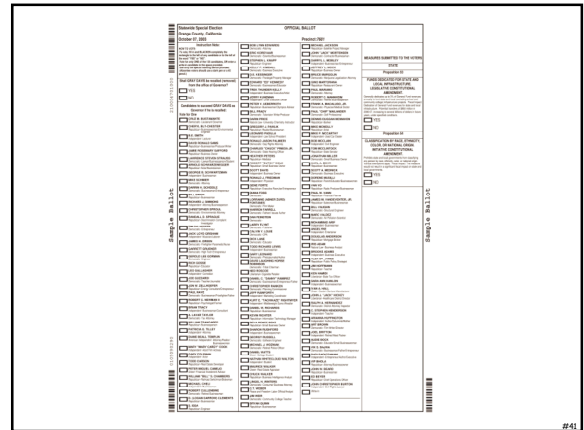
### Trojan Horses and Voting Machines

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)

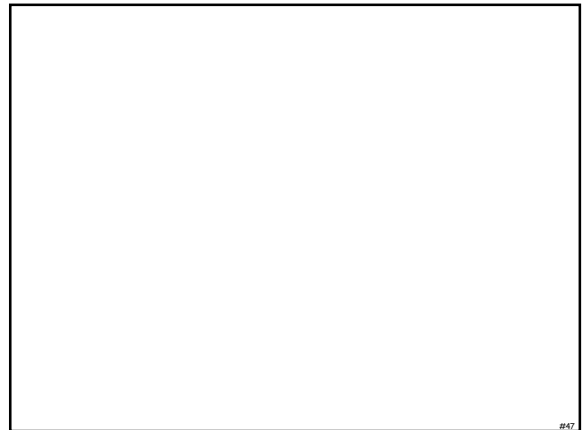
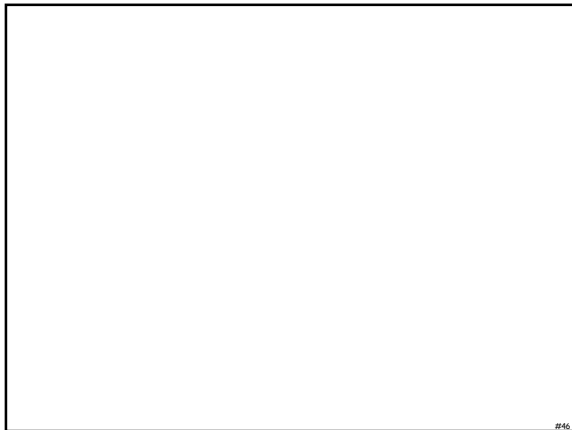




### Conclusions

- 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





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

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

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

### Machine error gives Bush 3,893 extra votes in Ohio

By John McCarthy, Associated Press

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

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

### Broward Vote-Counting Blunder Changes Amendment Result

POSTED: 1:34 pm EST November 4, 2004

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

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

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

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



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



