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.

9/07/2004
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
  - ACTIV (0x01)
  - (record vote)
  - SetStat at us CANCELED (0x08)
  - Succeeded

- QueryStatus
  - ACTIV (0x01)

Attack!

- QueryStat at us
  - ACTIV (0x01)
  - (record vote)
  - SetStat at us CANCELED (0x08)
  - Succeeded

- QueryStat at us
  - ACTIV (0x01)
  - (record another vote)

Authenticating election officials

- What kind of card are you?
  - An administrator card

- 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

Will your vote be counted in November?

How can you be sure?

www.ubria.uk/Politics

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

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)

Attempted Trojan Horse in Linux Kernel

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

???
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.

The tallies are $t_1, \ldots, t_n$.

Prover (Elec. Official) → Show me the paper for machine $i.$ (voter-verified paper audit trail)

Verifier (skeptical voter)
• 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