# ELECTRONIC VOTING RISKS & RESEARCH

**DANIEL R. SANDLER**
Department of Computer Science, Rice University

**October 27, 2008 guest lecture for COMP301, "Identity Theft to the iPod"**

# ELECTRONIC VOTING

# RISKS & RESEARCH


**Daniel R. Sandler**

Department of Computer Science, Rice University


**October 27, 2008 guest lecture for COMP301, "Identity Theft to the iPod"**

# electronic voting
# risks & research

**Daniel R. Sandler**
Department of Computer Science, Rice University

**October 27, 2008 guest lecture for COMP301, “Identity Theft to the iPod”**


COMPUTER SECURITY LAB
RICE UNIVERSITY

# why vote?

(please see any number of excellent POLI courses)

# why is public trust in elections important?

“It is enough that the people know there was an election. The people who cast the votes decide nothing. The people who count the votes decide everything.”

—Joe Stalin (?)

# 1. Convince the loser that he lost.


## 2. Convince the electorate.

# why is this so difficult?

1. Failures

2. Fraud

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

(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

(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.

(usability failure)

(equipment failure)

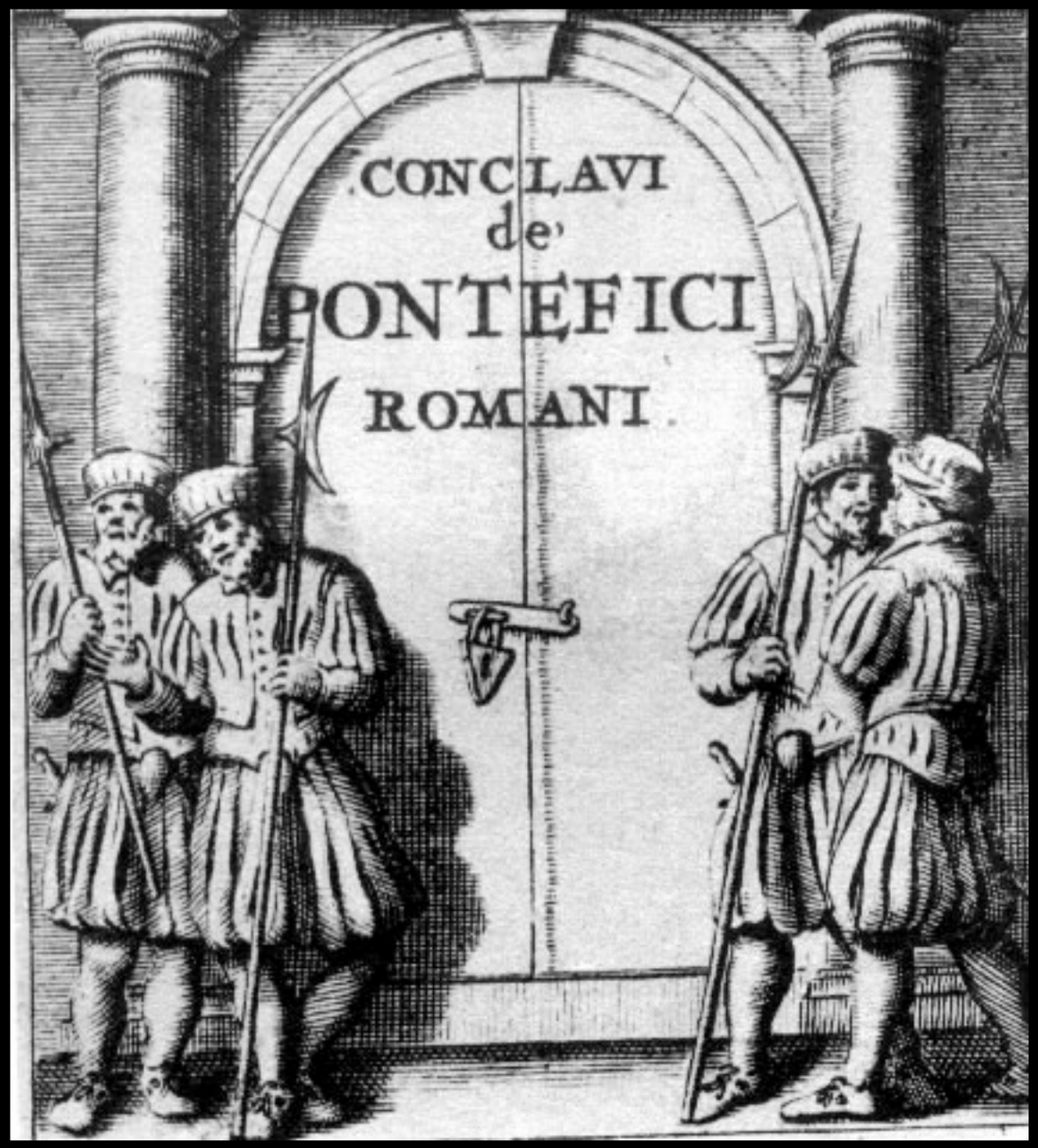
# fraud, e.g.

**Registration frauds**
**Repeat voting**
**Ballot box stuffing**
**Chain ballots**
**Voter assistance**
**Intimidation and Violence**
**Altering Ballots**
**Substitution of Ballots**
**False Count and False Returns**
**Altering Returns**

Joseph P. Harris, *Election Administration in the United States*,
The Brookings Institution, **1934.**

Via D. W. Jones, http://www.cs.uiowa.edu/~jones/voting/nist2005.shtml

it's a lot easier if you can just get everyone together in one room


CONCLAVI
de'
PONTEFICI
ROMANI

# “this doesn’t scale”

# technology

# when did we start using machines to help us vote?

# UNITED STATES PATENT OFFICE.

SYLVANUS E. DAVIS, OF ROCHESTER, NEW YORK, ASSIGNOR OF FIFTY-ONE ONE-HUNDREDTHS TO GEORGE WILSON AND GEORGE B. SELDEN, OF SAME PLACE.

## VOTING-MACHINE.

SPECIFICATION forming part of Letters Patent No. 526,668, dated September 25, 1894.

Application filed June 13, 1894. Serial No. 514,427. (No model.)

*To all whom it may concern:*

Be it known that I, SYLVANUS E. DAVIS, a citizen of the United States, residing at Rochester, in the county of Monroe, in the State of New York, have invented an Improved Voting-Machine, of which the following is a specification, reference being had to the accompanying drawings.

My invention relates to an improved voting-machine,—the construction and operation of which are fully described and illustrated in the following specification and the accompanying drawings,—the novel features thereof being specified in the claims annexed to the said specification.

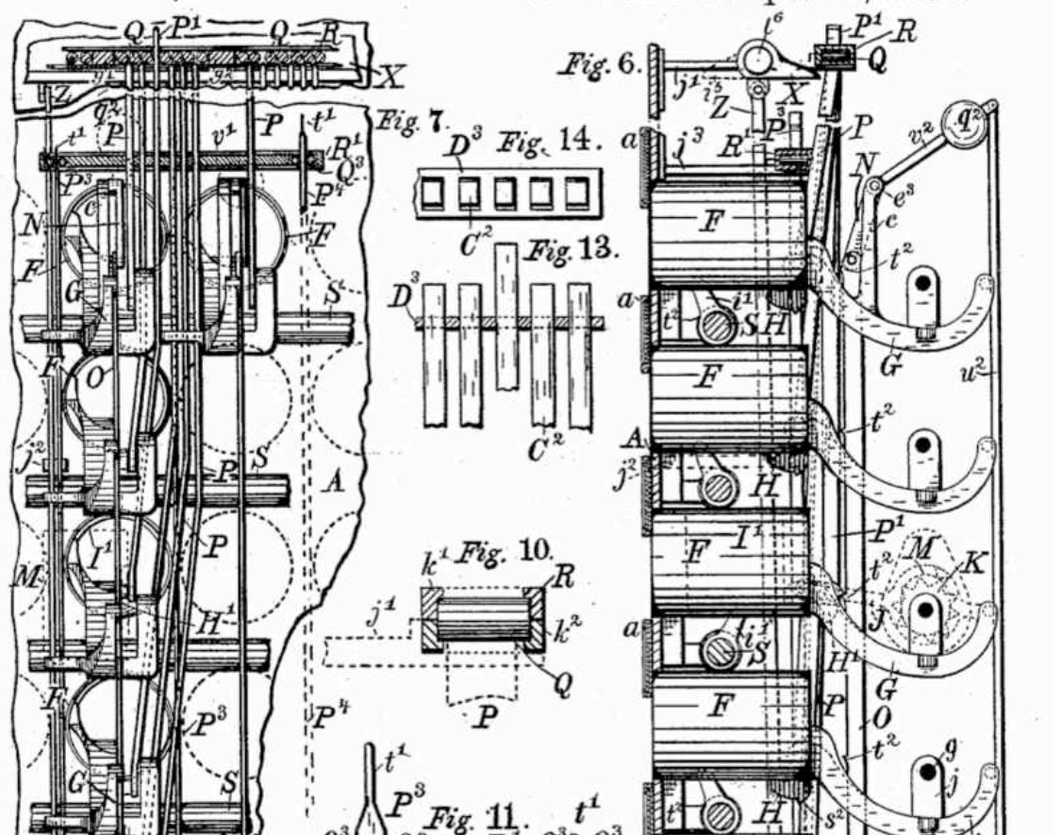
The object of my invention is the production of a voting machine,—a machine for enabling the public to vote at ordinary elections without printed ballots—which shall the interlocking rollers and their supporting frame. Fig. 9 is a longitudinal section of the same on the line 9—9, Fig. 8. Fig. 10 is a transverse section of the same on the line 10—10, Figs. 8 and 9. Fig. 11 is a longitudinal section of the interlocking mechanism of the pushes employed for voting on questions. Fig. 12 represents the block or blocks which may be substituted for one or more of the interlocking-rollers, to render one or more of the voting devices inoperative. Figs. 13 and 14 are respectively a longitudinal section and a plan of the support for the upper ends of the resetting-rods of the group of pushes employed when two or more candidates for the same office are presented by the same party. Fig. 15 is a rear-elevation, partially in section, of the counter,—its casing being partially broken away. Fig. 16 is a side elevation of the

(No Model.) 8 Sheets—Sheet 3.

S. E. DAVIS.

VOTING MACHINE.

No. 526,668. Patented Sept. 25, 1894.



# 2008

# e-voting

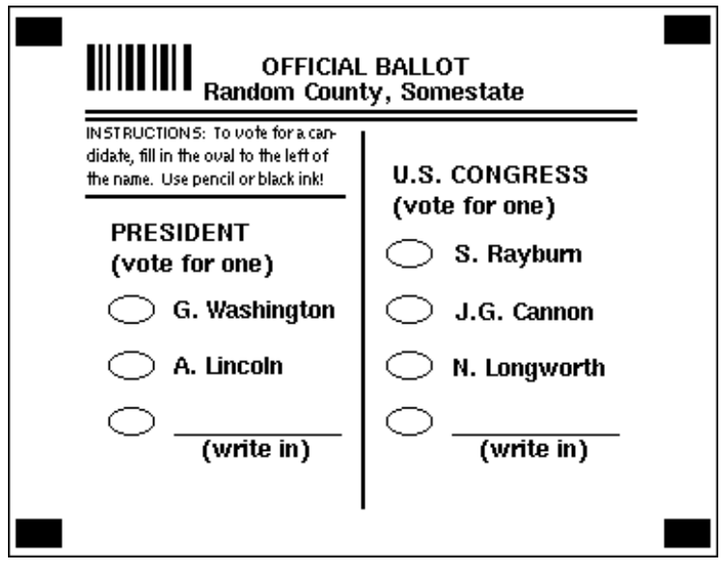
# two flavors of electronic voting

**optical scan (OS)**

**(aka “mark sense”)**

marks made on paper

scanned by a computer




**Source:** http://www.cs.uiowa.edu/~jones/voting/optical/
(plus everything you might ever want to know about mark-sense)

**direct recording electronic (DRE)**

input made on a mechanical or computer interface

recorded directly to electronic/digital media

# benefits of DREs

## human factors

feedback: prevent overvoting / point out undervoting

voter can review & correct mistakes

accessibility (e.g. vision impairment)

administrative: ease of running & canvassing elections

strong voter preference

## technical

fast results

replace failure-prone mechanical systems

replace ambiguous analog systems

can support more sophisticated voting styles

# hazards of DREs

**human factors**

voting user experience may be poor

more things for administrators to mess up, too

(modern) humans are pretty good with paper

**technical**

electromechanical failures

software bugs

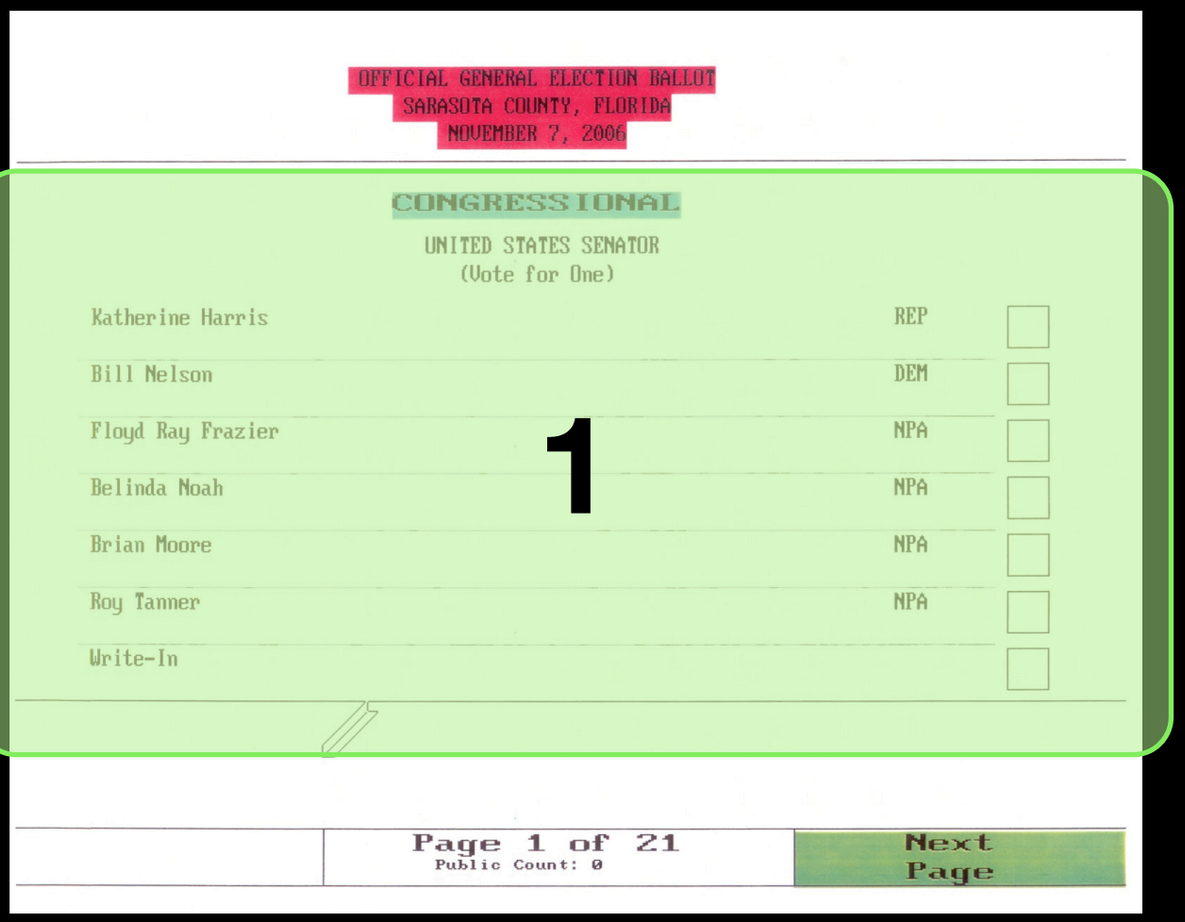
software **malice?**

**fraud:** “retail” → “wholesale”

# human factors issues

**below:** ballot screens from a DRE

**pop quiz:** how many races are shown?




PAGE 1


PAGE 2

ADVERTISING

REDUNDANT INFORMATION





JOHNNY HANSON : CHRONICLE

**A condo so pricey it won't be built**

A Houston tower with limo service, maid suites and residences with 9 1/2 bathrooms? This replica is as close as you'll get. Here's why.

- Outside, inside: How it would've been
- Did Houston need this anyway?
- Already built Houston condos for sale

DJIA 8260.12 +84.35 | NASD 1512.65 +6.75 | OIL 63.53 +0.31

# Lowest consumer confidence

**Index shows consumers most pessimistic since monthly records began** — The outlook signals consumer spending will deteriorate further, deepening the U.S. slump. 9:14 AM

- U.S. stocks, oil higher as global shares jump
- 20-city home price index drops record 16.6% in August
- Our economy: Check stock prices on Houston companies

10 rules to help navigate conflicting campaign data

HPD: Teen in car pretends to choke on seat belt, really dies 10:04 AM

Phone found in Texas death row cell brings wider seizures

A&M to settle last lawsuit stemming from Bonfire collapse

Houston man dies in motorcycle crash on Texas 249

Collision with dump truck, pickup kills Harris County driver 10:22 AM

Houston inspectors examine site of toddler's drowning 10:45 AM

Houston getting rid of law that made criminals of most kids

new topics: Pets | Moms | Belief | Gardening



ADVERTISING/ EXTRANEOUS



## highlights


**Election 2008**

- Learn about candidates, get election news, see Chronicle endorsements
- Voting locations, sample ballots

**Texans chat today**

Talk to McClain at 11:45

- How team got 3 wins
- Can they beat Vikes?

## your stories & photos »

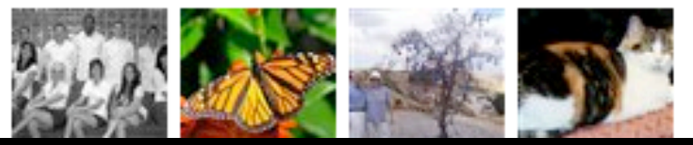
your profile | forums | faq

**Kuff's World**

Politics with Charles Kuffner

Candidate Q&A: Robert Schaffer

**Latest reader photos**



REDUNDANT INFORMATION

# DEWEY DEFEATS TRUMAN

## *G.O.P. Sweep Indicated in State; Boyle Leads in City*

### REPUBLICAN TICKET AHEAD OF 1944 VOTE

**Town Balloting Gives Trend**

*Probable Winners*

### *Tops Coghlan in Hot Race for Attorney*

*Probable Winners*

### RECORD CITY VOTE SEEN IN LATE TALLIES

**Suburbs Ballot Near 375,000**

### BULLETINS ON ELECTIONS

### *Early Count Gives G.O.P. Senate Edge*

### PUTS G.O.P. BACK IN THE WHITE HOUSE

**Sizable Electoral Margin Seen**


# you may have heard about this

## 2006 ballot in Sarasota County, Florida (FL CD 13)

**massive undervote in the congressional race**

massive = **18,000** votes (15%; typical is 1–4%)

margin of victory: **369** (after certified recount)

**possible causes**

“banner blindness”; touchscreen calibration issues;

other undiscovered software problem?

**an official explanation**

voters skipped the race intentionally because of its negative tone

—Vern Buchanan (the winner)

# technical failures

# (faulty hardware & software)

# why?

## only 2 options:

## incompetence

## malice

malice

(no evidence as of yet)

# incompetence

## (evidence abounds!)

# Diebold* AccuVote TS(x)

## the most-studied voting machine

(until 2007's source-code audits—TTBR (CA), EVEREST (OH))

thanks to source code leaked on the internet

**findings by Kohno et al., 2004:**

poor software engineering

incorrect cryptography & crypto protocols

possible for voters to cast multiple votes

vulnerable to malicious software upgrades

***now "Premier Election Systems"**

# e.g. encryption

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

**one key for every voting machine, everywhere**

originally discovered by Doug Jones, 1997

defense: “but the bad guys don’t know what it is”

analogy: anyone else own a Scion?

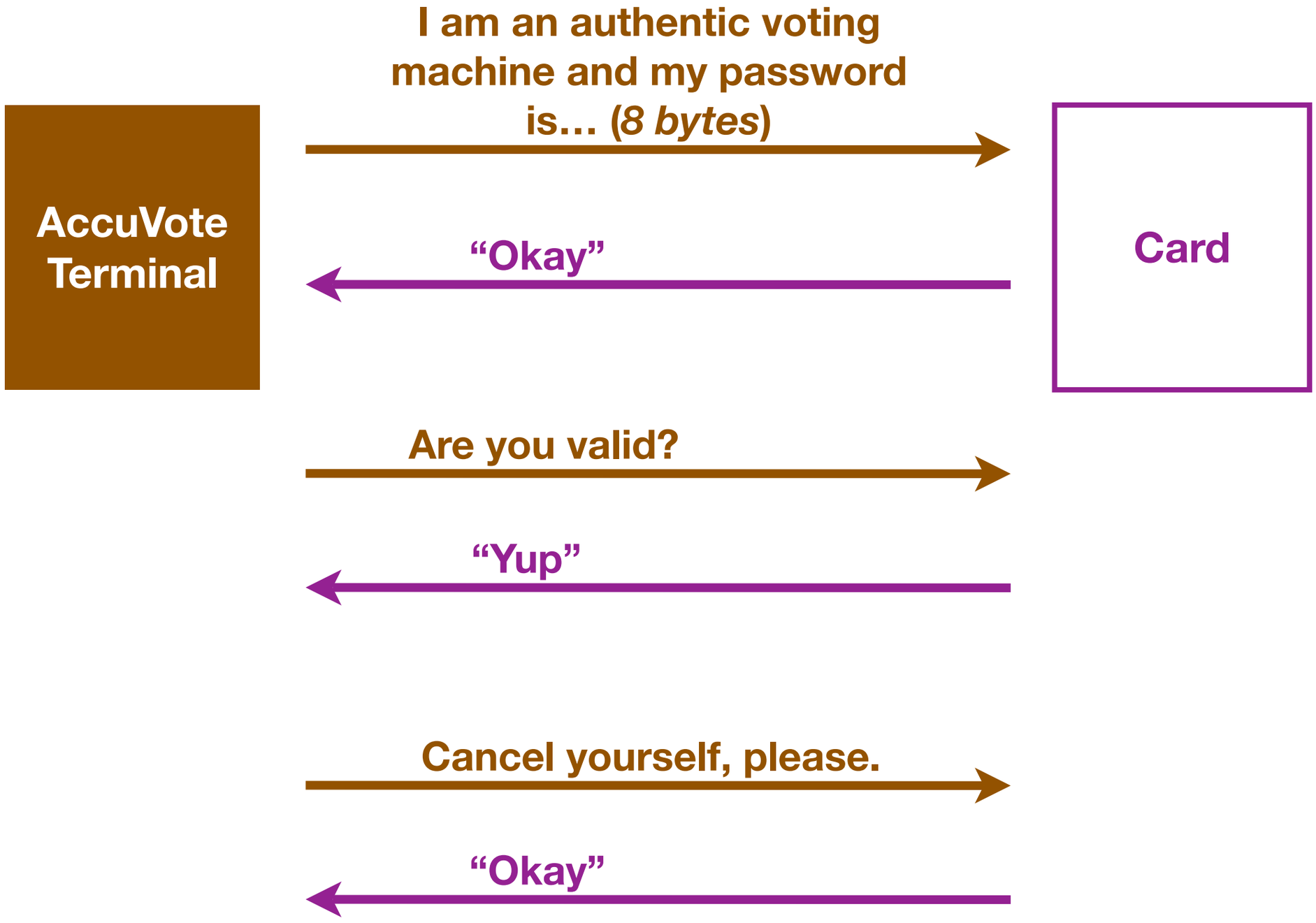
**still the case as of 2007**

although cipher is AES and key may be changed by officials

Source: CA TTBR
http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf

# e.g. voter smartcards

## protocol:



# it gets worse

**Feldman et al., 2006** (citp.princeton.edu/voting)

before the TTBR, so they had to reverse-engineer much of the then-current AccuVote TS

**findings**

malicious (evil) software could steal/alter votes without detection; we have **no way of knowing**

**physical access** (e.g. a voting session) is all that is needed to install malicious software

the software can be designed to:

1. **spread** to other voting machines
2. **alter** the tally
3. **remove** all traces

**ZOMG VOTING MACHINE VIRUS!!1!!!one!**

# on the topic of viruses—

## 2007: Diebold/Premier machines used in OH found to have problems

thanks to e-voting researchers' "EVEREST study"
http://www.nytimes.com/2007/12/15/us/15ohio.html
http://siis.cse.psu.edu/everest.html

hundreds of votes found to have been lost in 2004

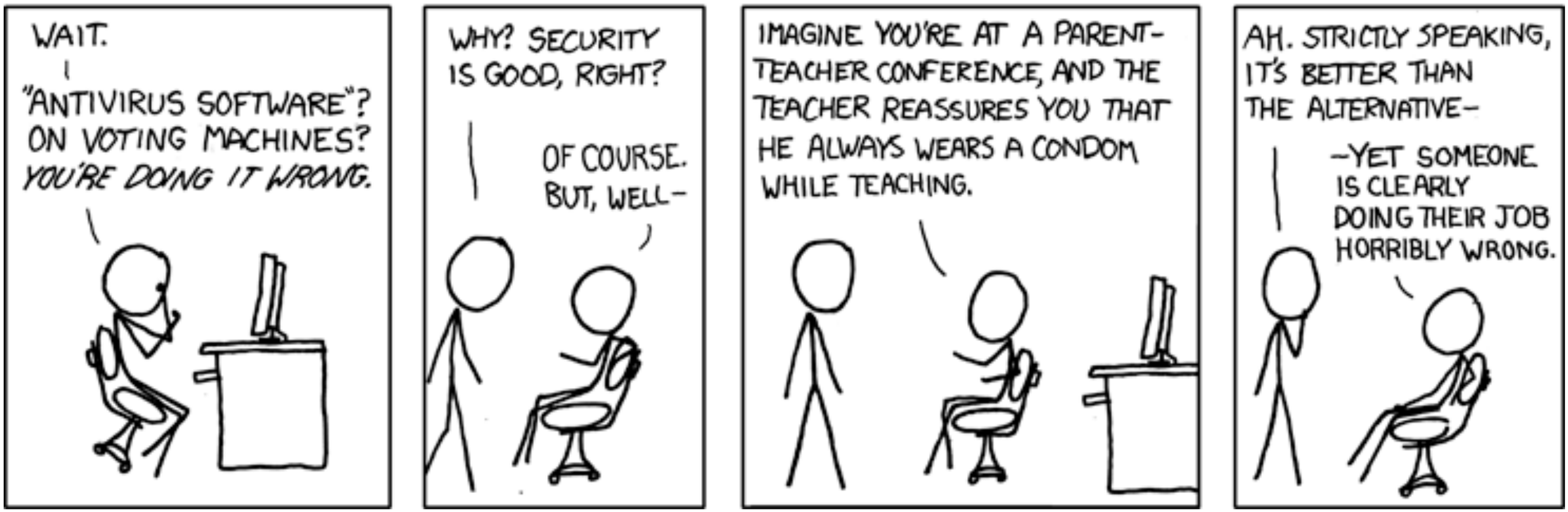
Diebold's original explanation:

**McAfee anti-virus software installed on the tabulation machines**

they are, after all, everyday Windows PCs

think about this for a second—how ridiculous is that?

PREMIER ELECTION SOLUTIONS (FORMERLY DIEBOLD) HAS BLAMED OHIO VOTING MACHINE ERRORS ON PROBLEMS WITH THE MACHINES' MCAFEE ANTIVIRUS SOFTWARE.




http://www.**xkcd**.com/463/

# can’t we do this job horribly right?

# ACCURATE

**A CENTER FOR CORRECT, USABLE, RELIABLE, AUDITABLE, AND TRANSPARENT ELECTIONS**

accurate-voting.org

## NSF-funded multi-institution research center

Dan S. Wallach, Rice University, associate director

**goals**

technology research

policy research

education

**explicit non-goal**

build a voting machine

**and yet…**

# VoteBOX

## a tamper-evident, verifiable voting system

**DANIEL R. SANDLER,** KYLE DERR, DAN S. WALLACH
RICE UNIVERSITY

EXCERPTED FROM SLIDES DELIVERED AT
**USENIX SECURITY '08**
AUGUST 1, 2008

skip it?

**why?**
lots of research on
**individual pieces**
of the e-voting problem

# VoteBox

integrates these techniques
in a **single system**

**trustworthy**
**reliable**
**tamper-evident**
**verifiable**

# goals

**minimized software stack**

less code to audit → more practical software audits

**resistance to failure & tampering**

prevent or minimize data loss

**tamper-evidence**

if resistance is futile

**verifiability**

cast-as-intended; counted-as-cast

# techniques
## used in VoteBox

**1. PRUI: pre-rendered user interfaces**

DRE user experience; minimized software stack

**2. AUDITORIUM: network layer**

resistance to failure; tamper-evidence

**3. immediate ballot challenge**

verifiability

# PRUI pre-rendered user interfaces

## very restricted graphics API

`blit(bitmap, x, y)`

`next_event()` → *keyboard or (x, y) input*

## what's not here?

windowing system; widgets; fonts & text rendering

## inspiration: Pvote

pioneering work on PRUI in e-voting

*(Yee, EVT '06 & '07)*

STEP 1
Read Instructions

**You are now on**
**STEP 2**
**Make your choices**

STEP 3
Review your choices

STEP 4
Record your vote

# President and Vice President of the United States

*Race 1 of 27*

To make your choice, click on the candidate's name or on the box next to his/her name. A green checkmark will appear next to your choice. If you want to change your choice, just click on a different candidate or box.

| President and Vice President of the United States<br>*(You may vote for one)* | |
|---|---|
| ☐ Gordon Bearce<br>Nathan Maclean | REP |
| ☐ Vernon Stanley Albury<br>Richard Rigby | DEM |
| ☑ Janette Froman<br>Chris Aponte | LIB |

Click to go back to instructions

←Previous Page

Click to go foward to next race

Next Page→

LABEL **ID=L51**

LABEL **ID=L52**

STEP 1
Read Instructions

LABEL **ID=L10**

To make your choice, click on the candidate's name or on the box next to his/her name. A green checkmark will appear next to your choice. If you want to change your choice, click on a different candidate or box.

LABEL **ID=L2**

**You are now on STEP 2**

LABEL **ID=L13**

**President and Vice President of the United States**

*(You may vote for one)*

LABEL **ID=L50**

☐ Gordon Bearce REP

GROUP TOGGLE BUTTON **ID=B100**

☐ Vernon Stanley Albury DEM

GROUP TOGGLE BUTTON **ID=B101**

☑ Janette Froman LIB

GROUP TOGGLE BUTTON **ID=B102**

STEP 3

LABEL **ID=L14**

STEP 4

LABEL **ID=L16**

BACKGROUND
LABEL **ID=L1**

LABEL **ID=L1002**

Click to go back to instructions

←PREV PG **ID=L1000**

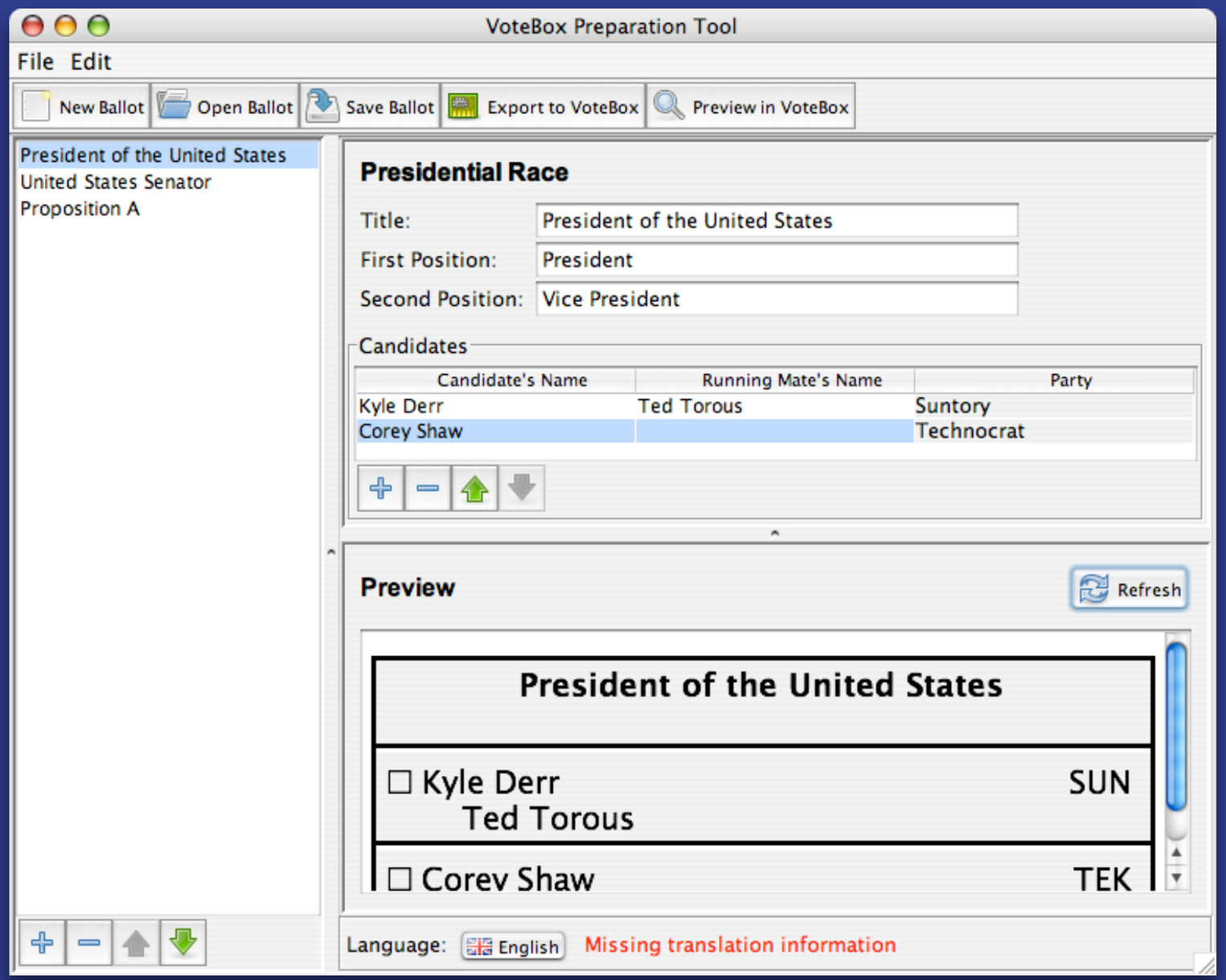
LABEL **ID=L1003**

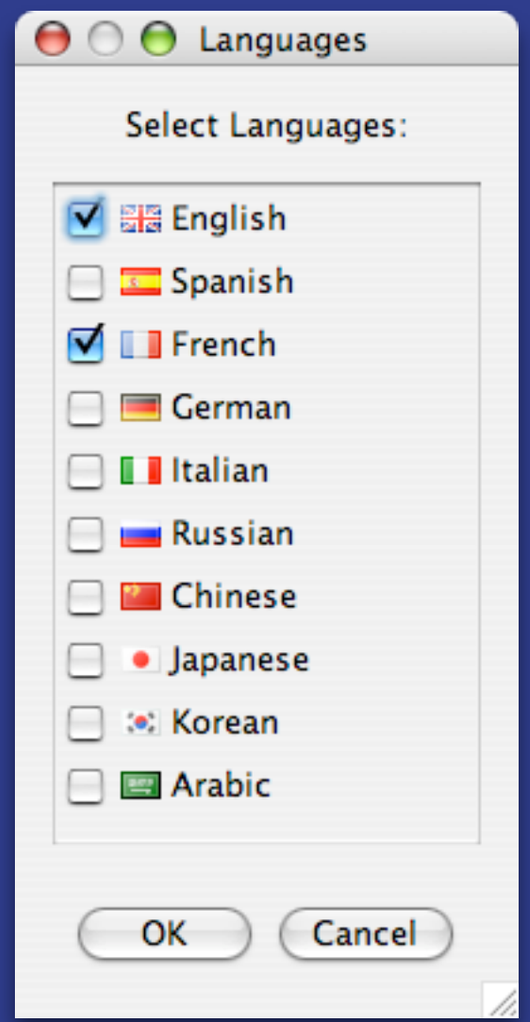
Click to go foward to next race

**ID=L1001** NEXT PG→

# VoteBox ballot creator

…where the pre-rendering happens



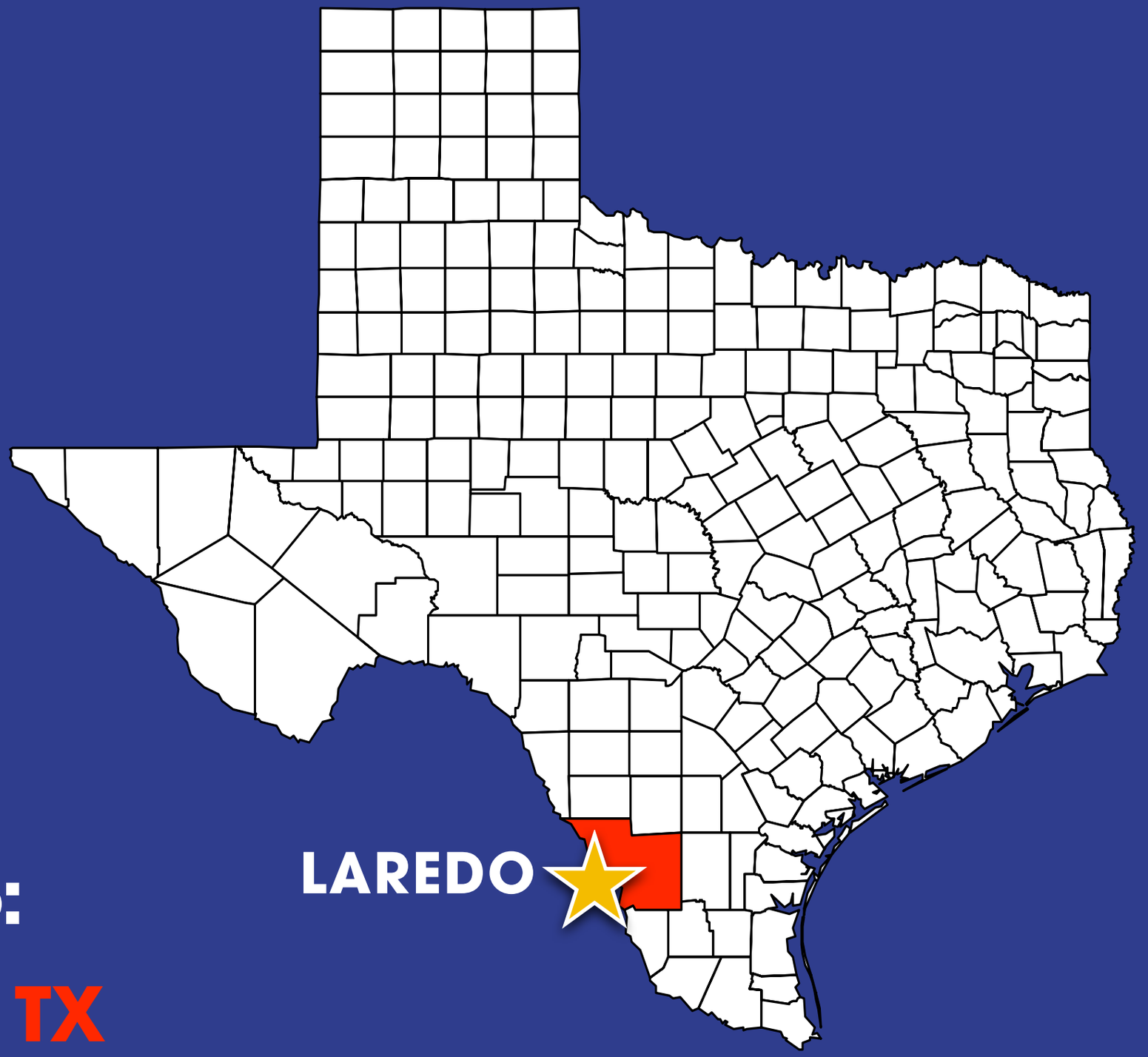



# AUDITORIUM

## even honest voting machines fail!

we can't trust voting machines with critical election data

at least, not without redundancy




# March 7, 2006:

# Webb County, TX

2006 Democratic primary election

(County's first use of DREs)

# example event log

| Votronic | PEB# | Type | Date | Time | Event |
|---|---|---|---|---|---|
| 5140052 | 161061 | SUP | 03/07/2006 | 15:29:03 | 01 Terminal clear and test |
| | 160980 | SUP | 03/07/2006 | 15:31:15 | 09 Terminal open |
| | | | 03/07/2006 | 15:34:47 | 13 Print zero tape |
| | | | 03/07/2006 | 15:36:36 | 13 Print zero tape |
| | 160999 | SUP | 03/07/2006 | 15:56:50 | 20 Normal ballot cast |
| | | | 03/07/2006 | 16:47:12 | 20 Normal ballot cast |
| | | | 03/07/2006 | 18:07:29 | 20 Normal ballot cast |
| | | | 03/07/2006 | 18:17:03 | 20 Normal ballot cast |
| | | | 03/07/2006 | 18:37:24 | 22 Super ballot cancel |
| | | | 03/07/2006 | 18:41:18 | 20 Normal ballot cast |
| | | | 03/07/2006 | 18:46:23 | 20 Normal ballot cast |
| | 160980 | SUP | 03/07/2006 | 19:07:14 | 10 Terminal close |

# problem #1 :
# logs starting mid-day

```
03/07/2006 15:29:03  Terminal clear and test
03/07/2006 15:31:15  Terminal open
```

## Polls opened around 7 AM across Webb Co.

What happened to this machine between 7 and 3:30?
**Were votes cast and then lost?**

(10 total machines)

# problem #2
# election events on wrong day

| Votronic | PEB# | Type | Date | Time | Event |
|---|---|---|---|---|---|
| 5142523 | 161061 | SUP | 02/26/2006 | 19:07:05 | 01 Terminal clear and test |
| | 161115 | SUP | 03/06/2006 | 06:57:23 | 09 Terminal open |
| | | | 03/06/2006 | 07:01:47 | 13 Print zero tape |
| | | | 03/06/2006 | 07:03:41 | 13 Print zero tape |
| | 161109 | SUP | 03/06/2006 | 10:08:26 | 20 Normal ballot cast |
| | | | | | [... 9 more ballots cast ...] |
| | 161115 | SUP | 03/06/2006 | 19:29:00 | 27 Override |
| | | | 03/06/2006 | 19:29:00 | 10 Terminal close |

**The election was held on 03/07!**

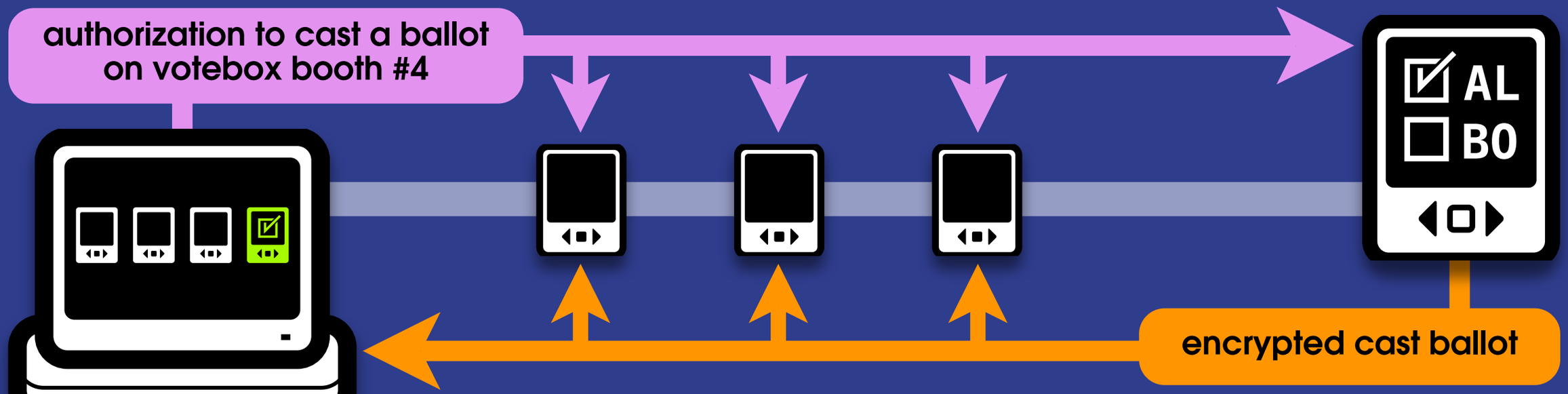
otherwise, a pretty normal voting pattern

(4 machines / 41 votes)

☀ 103°F

# AUDITORIUM

Sandler and Wallach. **Casting votes in the Auditorium.** EVT'07.




**the AUDITORIUM polling place network**

joins all voting machines together

all election events are signed and broadcast

each broadcast is logged by every machine

# hash chains


**key ingredient in AUDITORIUM**

every signed broadcast includes SHA(earlier events)

events “entangled” between machines

**we can now reason about our audit logs**

provable ordering & completeness of the record

*…crucial in the voting context*

**query the log at runtime or offline**

Sandler et al. **Finding the evidence in tamper-evident logs.** SADFE ’08.

# “cast as intended”

**the biggest challenge for DREs**

how can the voter be sure the computer:

*captured the voter’s choices faithfully,*

*encrypted the ballot correctly,*

*and broadcast it in the Auditorium?*

unlike “counted as cast,” no amount of procedure or *post facto* auditing can correct this

# ballot challenge

**voter makes selections**

**voting machine commits publicly to voter's choices**

voter's choice

**cast the ballot**

**challenge**

- reveal commitment
- spoil ballot

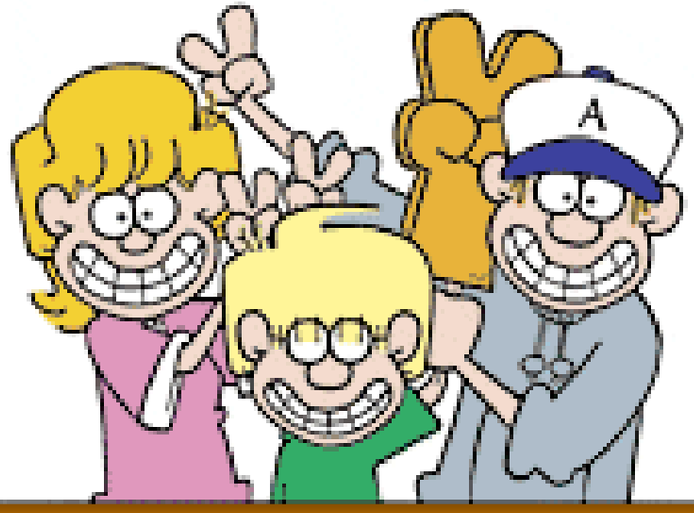
# big finish

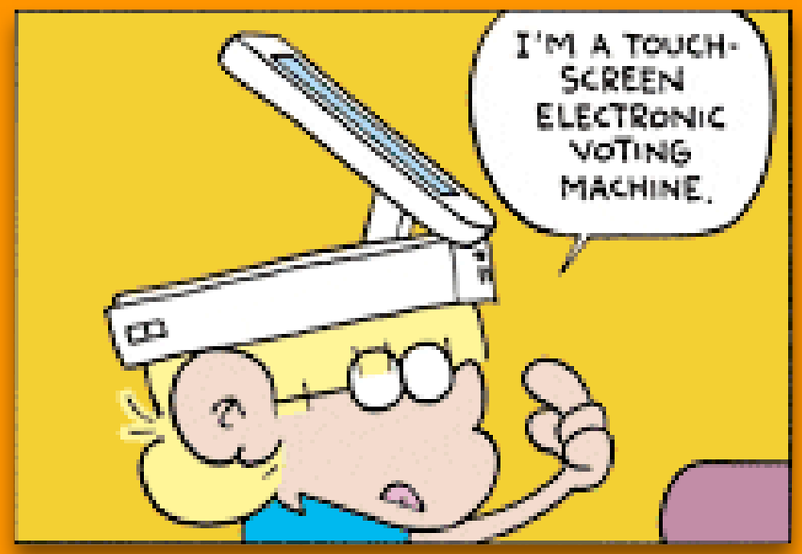
# will next week's election be hacked?

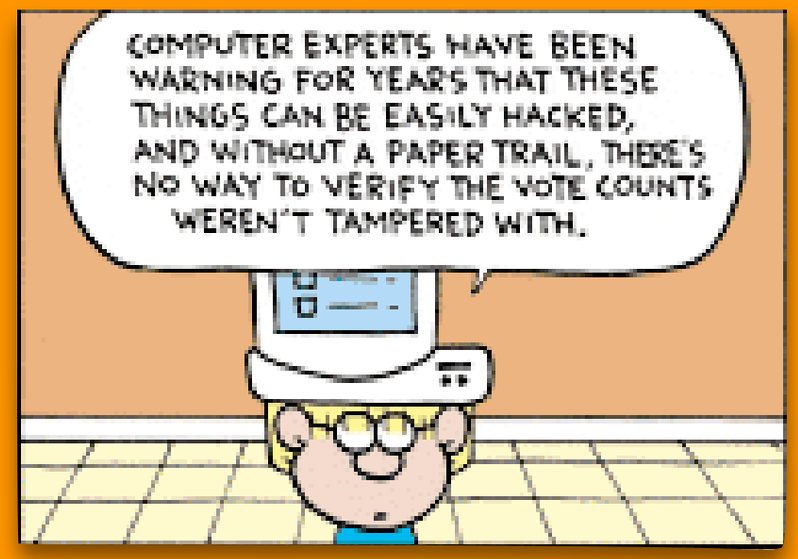
# will next week's election results be trustworthy?

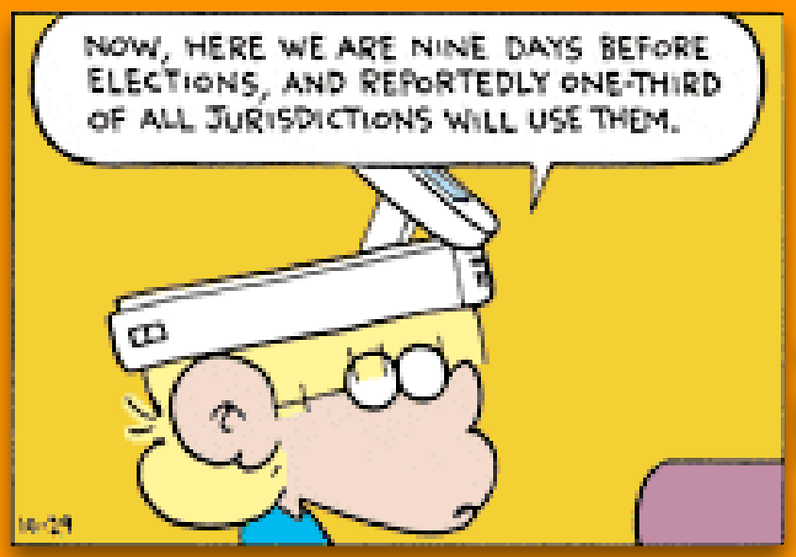
# FoxTrot

by Bill Amend

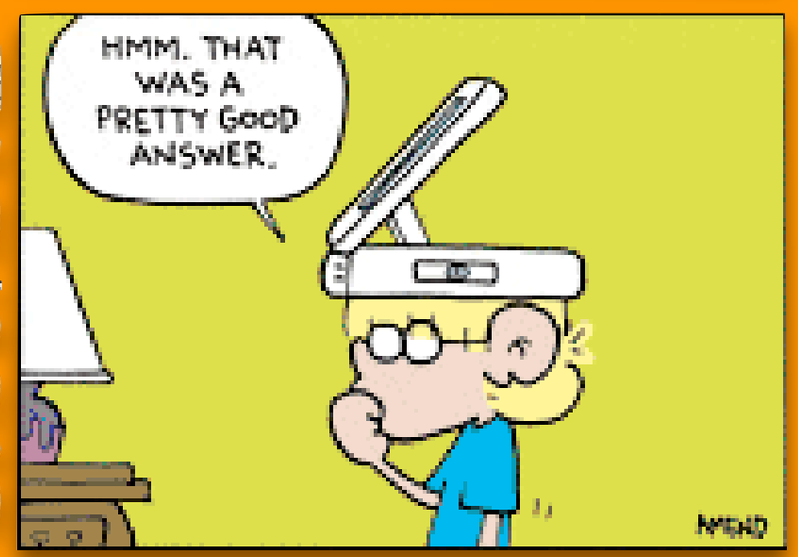


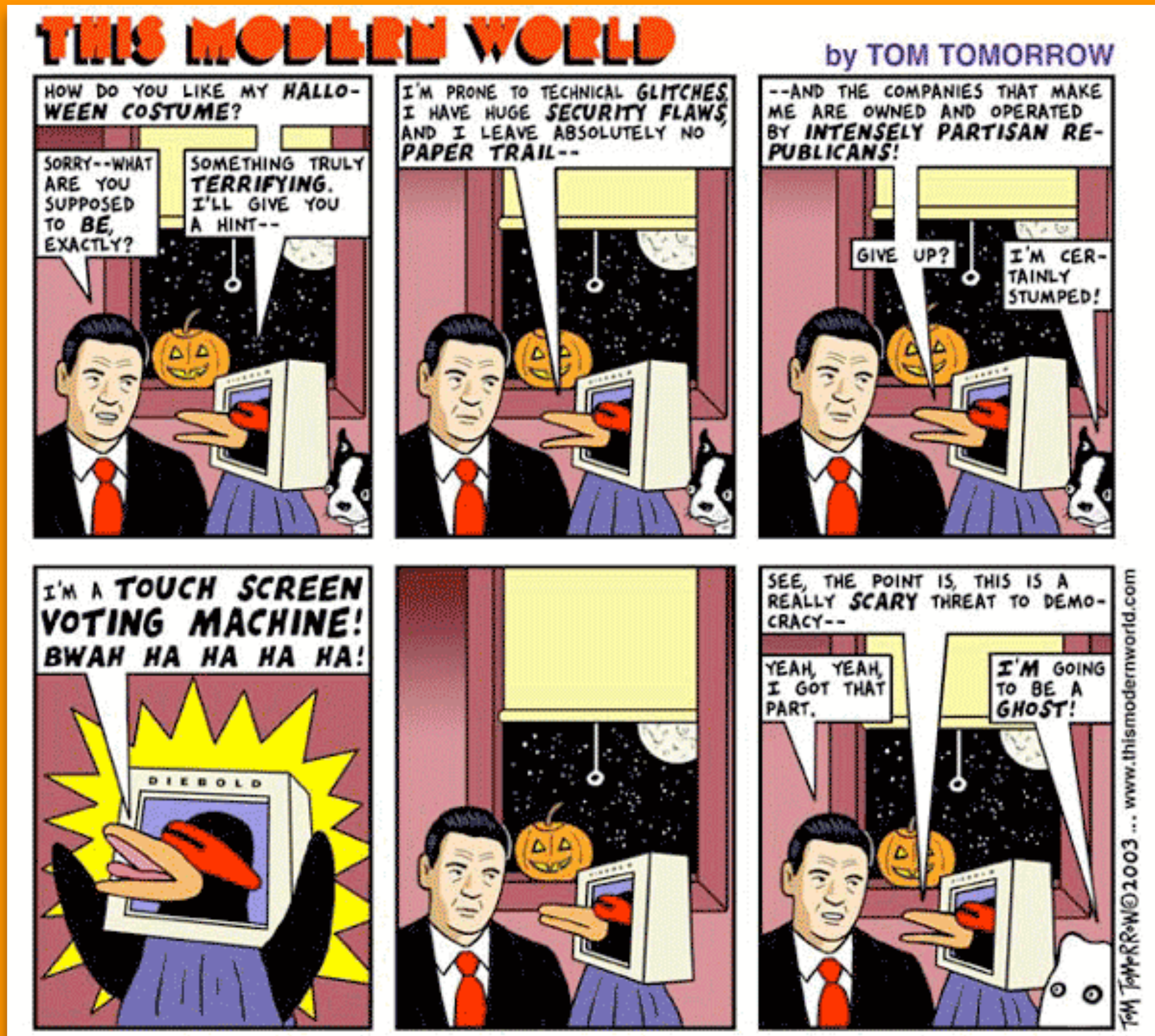








**FoxTrot,** October 29, 2006




**This Modern World,** October 28, 2003