

# Electronic Voting Systems

Professor Daniel Lopresti

dal9@lehigh.edu

Computer Science and Engineering

*Engineering 005 Project*

*Fall 2006*

# Project Summary 1

## Motivation:

- Fair and accurate elections are vital for a healthy democracy.
- Any voting system carries with it some risk. Past experience with paper ballots, lever machines, etc., has let us understand that risk.
- Electronic voting systems introduce whole new classes of risks.

## Questions we want to answer:

- What are the risks associated with e-voting technologies?
- How can these risks best be mitigated?
- Can the current certification process identify bad e-voting systems?
- If not, what would be an effective certification procedure?

# Project Summary 2

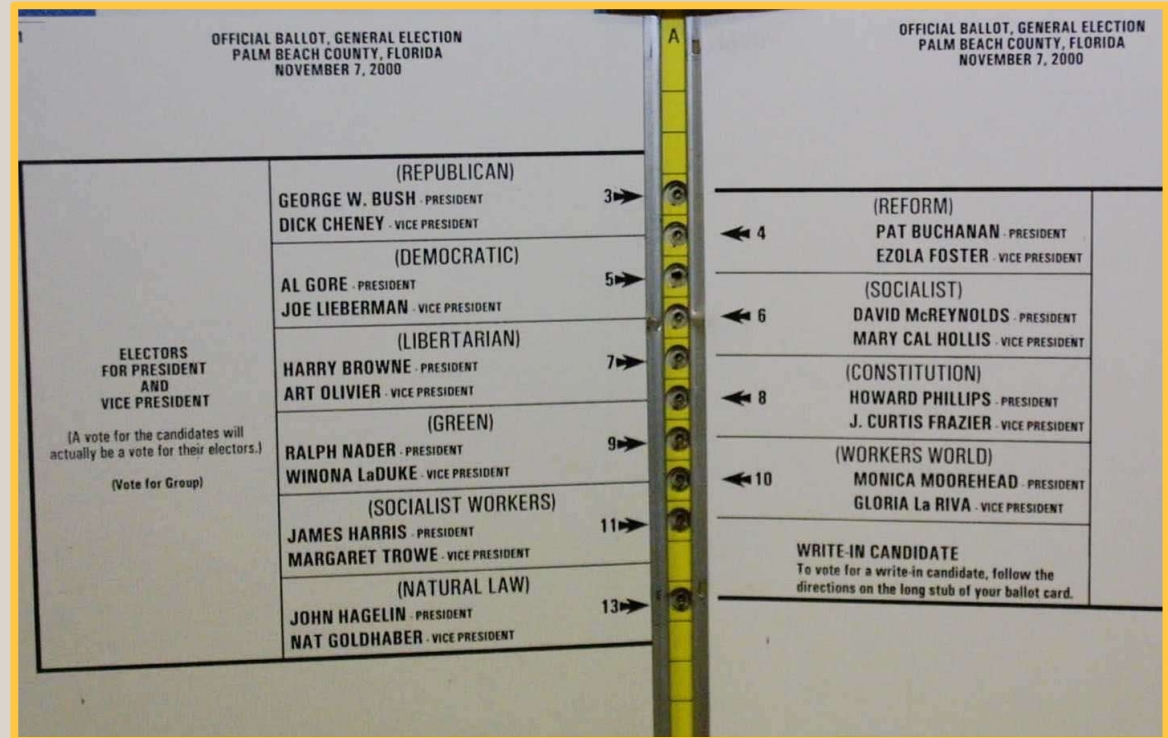
## Project plan:

- Teams of 4-5 students with complementary interests and expertise.
- Bi-weekly meetings to study current e-voting systems, certification processes, official government records, publicized vulnerabilities, best-practices for software and systems engineering.
- Support from Professor Lopresti and two students actively studying e-voting systems, Emily Cohen '08 and Dave Heefner '08.

***You don't need to be a “hacker” to elect this project!  
You just need to care about fair and accurate elections.***

# Background Leading to HAVA

The infamous butterfly ballot from the 2000 Presidential election:



The Florida ballot is a classic example of bad user interface design. Computer software can suffer from such problems just as easily.

[http://www2.indystar.com/library/factfiles/gov/politics/election2000/img/prezrace/butterfly\\_large.jpg](http://www2.indystar.com/library/factfiles/gov/politics/election2000/img/prezrace/butterfly_large.jpg)

# Election Technology & HAVA

The Help America Vote Act (HAVA) provides funds for states to replace punched card and lever voting systems. It does not mandate the use of any particular e-voting technology.

Some general goals to keep in mind as we weigh alternatives:

- secure and transparent elections,
- accurate determination of voter intent,
- voter anonymity,
- accessibility for disabled voters and non-native English voters,
- if possible, prevent overvoting (invalidates voter's ballot),
- if possible, prevent unintentional undervoting (voter confusion?).

[http://www.fec.gov/hava/law\\_ext.txt](http://www.fec.gov/hava/law_ext.txt)

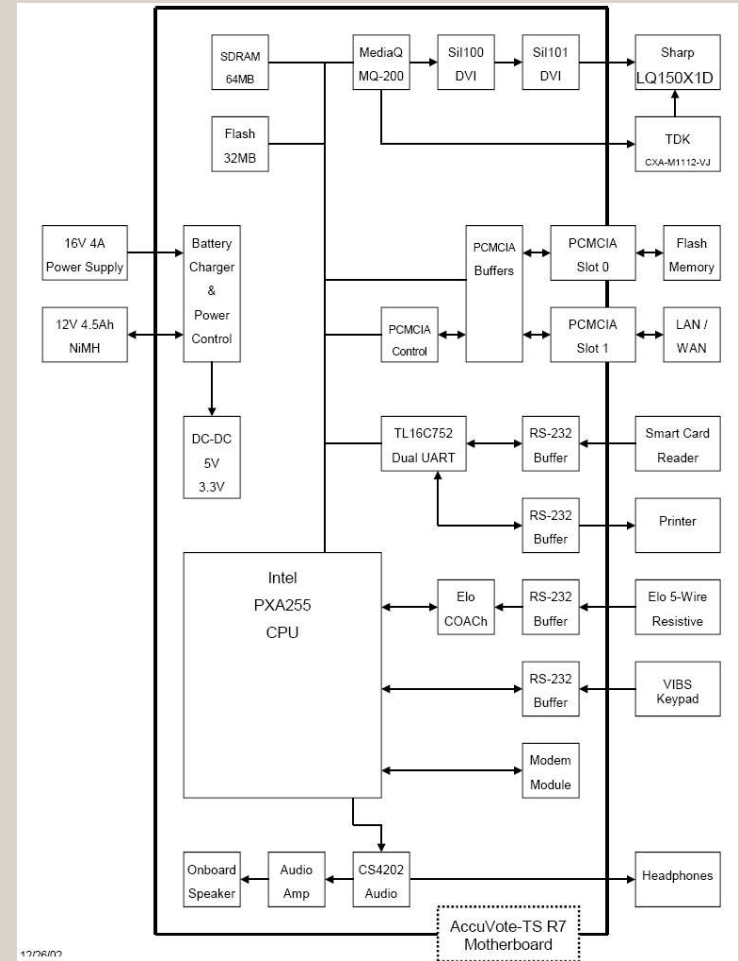
# Diebold AccuVote System

Recent demo in Allentown:



Diebold AccuVote-TSx  
block diagram:

*These systems are nothing more than specialized computers!*



<http://www.wfmz.com/cgi-bin/tt.cgi?action=viewstory&storyid=13711>

[http://www.bbvforums.org/forums/messages/1954/AccuVote-TSx\\_2\\_02\\_System\\_Overview-23267.pdf](http://www.bbvforums.org/forums/messages/1954/AccuVote-TSx_2_02_System_Overview-23267.pdf)

# More Photos from Diebold Demo



*Paper tape  
(used for end-of-day tally)*



*Built-in  
printer*



*PCMCIA slot*



*PCMCIA card*

# Short Video Clip

From the official video record of the Pennsylvania certification examination for Diebold AccuVote and OptiScan systems conducted by the Office of the Secretary of the Commonwealth in Harrisburg on November 22, 2005.



# E-voting Risks

While there are several e-voting vendors, one truth holds: all computer hardware/software systems of this complexity have bugs.

Bugs can manifest themselves in different ways:

- cause system to be unreliable (crash, lose votes),
- create openings that allow an outsider to compromise election,
- create openings that allow an inside to compromise election.

***Such attacks can be impossible to detect after-the-fact!***

# Risk Analysis of E-voting Software

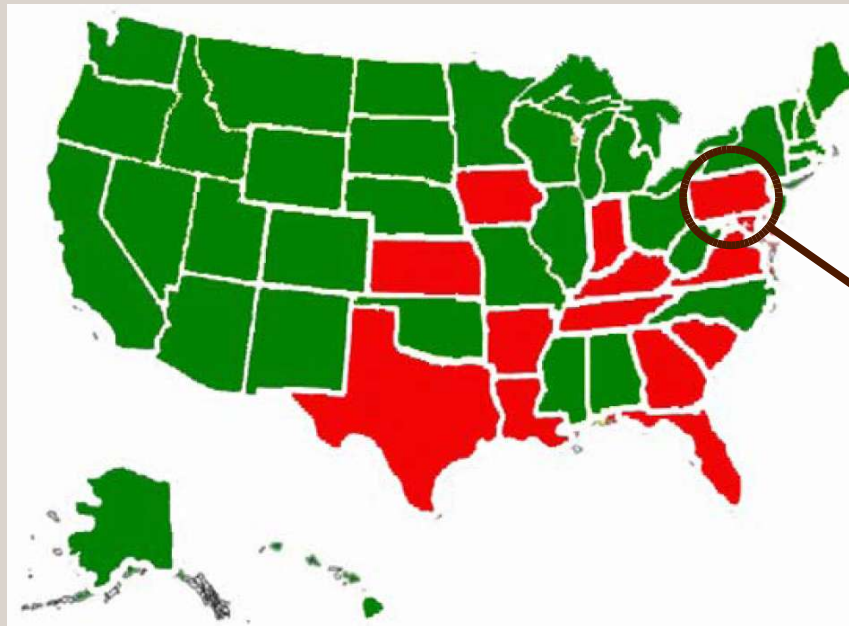
- Avi Rubin and colleagues at Johns Hopkins and Rice obtained copy of Diebold e-voting software which appeared on Internet.\*
- Studied it carefully – made results public in 2003.
- Findings include:
  - “... far below even the most minimal security standards ...”
  - “... unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, ...”
  - “... voters ... can cast unlimited votes without being detected ...”



*\* E-voting vendors often assert they must be allowed to keep their software secret to protect it. This proves the futility of that idea.*

"Analysis of an Electronic Voting System," Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *IEEE Symposium on Security and Privacy*, 2004.

# Voter-Verified Paper Audit Trail

- A key recommendation from many security experts is the establishment of a Voter-Verified Paper Audit Trail (VVPAT).
- As of today, this is only way to guarantee an independent recount.



 = VVPAT  
 = No VVPAT

Pennsylvania

From [CoalitionforVotingIntegrity.org](http://CoalitionforVotingIntegrity.org), 8/19/06

# Current Events and a Challenge

"I'm not sure what it takes to have a paper backup," Stoffa said. "There's no way it can be in place by November."

Stoffa said he spoke to the local residents and told them to take two of the county's electronic voting machines and try to compromise the voting results.

"No one has proven how it can be done," Stoffa said.

## **Voting machine suit filed**

**Plaintiffs ask for new machines' decertification. They claim lack of paper record could mask a fraud.**

Wednesday, August 16, 2006

**By Sarah Cassi**  
**The Express-Times**

Voter advocates filed a lawsuit Tuesday in Philadelphia seeking to stop most Pennsylvania counties from using "paperless" electronic voting machines, saying that such systems leave no paper record that could be used in the event of a recount, audit or other problem.

The suit asks the state's Commonwealth Court to decertify machines used in 59 of Pennsylvania's 67 counties, including Lehigh and Northampton. The

"It's awfully late to be doing this, with an election in November," Northampton County Executive John Stoffa said.

Stoffa said the county will follow what the law tells it to do, but electronic voting machines will be used this November.

"I'm not sure what it takes to have a paper backup," Stoffa said. "There's no way it can be in place by November."

Stoffa said he spoke to the local residents and told them to take two of the county's electronic voting machines and try to compromise the voting results.

"No one has proven how it can be done," Stoffa said.

<http://www.pennlive.com/search/index.ssf?/base/news-7/1155701208319930.xml?expresstimes?npa&coll=2&thispage=1>

# Final Details

- First meeting on Sept. 6 at 1:10 pm in PL 122.
- Totally non-partisan – a question of democracy, not politics.
- You don't need to be a hacker to elect this project!
- For more details on e-voting in general, see:  
<http://www.cse.lehigh.edu/~lopresti/other.html#e-voting>