

# US Elections 2004

**How did the technology do?**

The dust has begun to settle on November's US Presidential elections. Academics, commentators, politicians and activists are all pawing through the wreckage to find clues to the trillion dollar question. Did Bush win fair? This article will tell you the story of how the USA got to a situation where election results could be so easily questioned. It then looks at some of the problems reported this November along with some potential solutions. Could Open Source have helped? Jason Kitcat investigates

The United States is a huge country with massively decentralised and complex elections. There are hundreds of elections and referenda held simultaneously using punch card, optical scan, touch screen, postal ballot and push-

**Diebold had been foolish enough to**

**leave the source for their core**

**e-voting product on a public FTP server**

button voting systems. It's a legal and technical minefield of overlapping system and legal requirements with no clear national voice on how elections should be run. This makes tracking election issues hugely challenging, particularly given the circus that always surrounds elections. Despite this lack of transparency a raft of irregularities were reported during and after the elections. Many of these reports were collected thanks to activists setting up hotlines and building online issue tracking systems.

Here in the UK election specialists watched the US with huge interest. As there has been little news of e-voting in the UK since the last pilots in 2003 all eyes were on America. No UK pilots were held this year and it isn't clear when the next tests will be held. Across Europe it was clear that if any disasters were reported in the USA then e-voting would likely suffer some serious setbacks.

**THE STORY SO FAR...**

Americans have had machines to vote with for over one hundred years. In fact in 1869 Thomas Edison's first invention, a vote recording system for congress, was rejected as being too quick! Technology plays a major role in US elections even though countries such as France and Canada continue to use pencil and paper. This is because Americans vote on more issues and contests at more regular intervals than virtually any other country in the world. One visit to the polling booth may ask the average American voter to cast twenty votes! Voters will go home having chosen their sheriff, judge, school board, mayor, state congressman, senator, president. They will also have made a decision on, for example, whether gay marriage is allowed or whether creationism can be taught in schools.

If all these votes are packed onto a single

piece of paper counting becomes extremely difficult. The same piece of paper needs to be counted for each race: ten, fifteen, twenty times; a slow and logistically challenging process. Hence the punch card machines, the lever counting contraptions and the

electronic voting systems. All these systems don't just make counting fast, they were intended to make counting viable in high population areas.

As readers may recall punch cards got something of a bad name after officials, lawyers and judges had trouble deciding

who had won in Florida. While the punch cards got most of the attention, they were by no means the only issue. A raft of other problems disenfranchised voters including terrible ballot design, a lack of systems for preventing voters unknowingly casting invalid ballots and, as the BBC and The Guardian reported, the removal of large numbers of people from the electoral register who were likely to vote Democrat.

The uncertainties over the 2000 Florida count resulted in the 'Help America Vote Act' being signed into law by President Bush in 2002. This act, known in e-voting wonk circles as HAVA, pumped \$3.9 billion into elections equipment. The way the act was drafted meant that new voting equipment was rushed into use without the necessary research, oversight or certification bodies being in place. While the act did mandate a new Federal elections commission, the commission had a tiny budget and was only formed after many counties had bought new systems. Deadlines in the legislation meant that counties would not receive their share of the money if old punch card machines weren't replaced before November 2004. So we saw a manic rush of technically unsophisticated electoral administrators running into the arms of vendors just so they could be sure to spend the money. People were begging to spend money quickly, something which doesn't normally happen even in salesman's wildest dreams.

A small band of academics and investigative journalists did try to raise the alarm on the huge potential problems which might arise from rushing the systems into use. Through hard work, good research and some lucky breaks they managed to get electronic voting into the news, making

many more voters, candidates and officials more aware of the risks. This publicity alone is certain to have helped ensure the elections were run more carefully. The publicity surrounding e-voting also resulted in thousands signing a resolution calling for verifiable voting systems, that is systems that could prove that voter intentions were accurately recorded and counted. This resolution had a meaningful impact in several states, especially California where alternatives to voting electronically were made available. Prior to the resolution being started major flaws were found in systems from leading e-voting vendor Diebold and also in the US Military's SERVE Internet voting project. The uncovering of these flaws was key to the resolution for verifiable voting systems gaining a critical mass of support.

Diebold had been foolish enough to leave the source for their core e-voting product on a public FTP server. It was little surprise when security academics led by Avi Rubin of John Hopkins University picked the system apart finding a huge number of basic flaws including hard coded passwords and an extremely questionable architecture. The findings forced the state of Maryland to hire independent consultants to examine the Diebold system that had been purchased. However due to the short amount of time before presidential primaries took place only minimal remedial action could be taken.

Another academic, Bryan Pfaffenberger from the University of Virginia, showed how election officials actually pressured Diebold to ensure that election results could be fiddled. Thanks to a leaked email archive we could see how officials, who often wanted to

these kinds of corrections happen all the time, but why it was necessary to allow such changes to be undetectable in GEMS wasn't made clear.

Another system that came under close scrutiny was the SERVE project. SERVE was set up to help Americans in the armed forces vote when posted overseas. The system was entirely Internet-based and came under increasing scrutiny as the debate over e-voting heated up after the Diebold revelations. Under pressure the Department of Defense asked 10 experts to examine the system. According to the New York Times only four of these experts showed up to both briefings on the system. These four found such fundamental vulnerabilities in the system that they recommended it be shut down. It wasn't long before SERVE was on ice and soldiers were being asked to vote by fax - hardly much of an improvement.

The scene was set for another acrimonious and bitterly fought election. In fact before voting had even begun law suits were already underway in many states, particularly Ohio and California. In several states activists ensured that those unwilling to use an

electronic system could cast a 'provisional' paper ballot. Unfortunately because of poor training few poll workers in those states knew what to do when someone actually wanted to exercise their right not to vote electronically.

As the campaigns wound down lawyers were pressing their courtroom suits, activists were charging their digital cameras, and the voters were hoping someone would actually count their votes.

Well we all know what happened next, Bush won, again. Or did he? Due to the lack of proper audit trails it is virtually impossible to know what really happened. We do have a stack of problem reports collected though. By examining them we can get an idea of how compromised the result might be. We can also learn how Open Source could have avoided some of the issues reported.

**PROBLEM: HAND ME THE ABACUS, THE COMPUTER CAN'T COUNT**

A number of voting machines around the US had trouble counting, which is a little disturbing considering maths is what computers do best. In Franklin County, Ohio

**lawyers were pressing their courtroom**

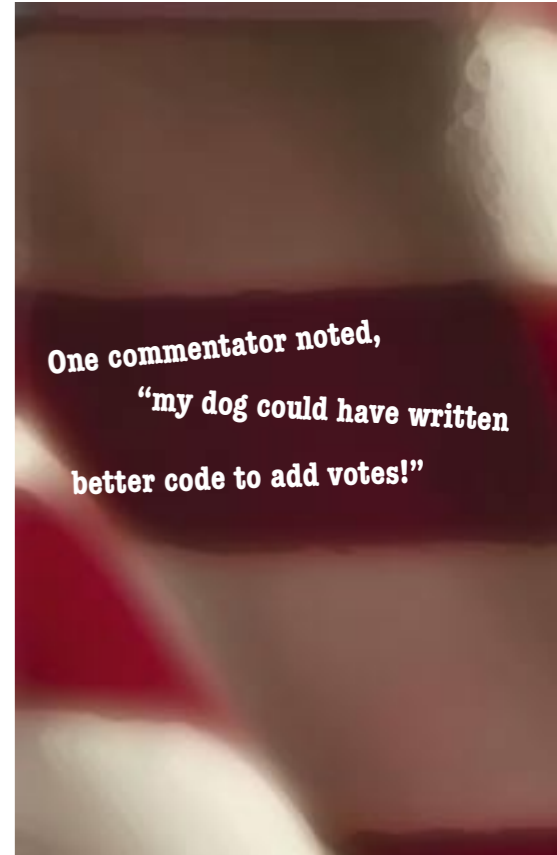
**suits, activists were charging their**

**digital cameras, and the voters were**

**hoping someone would actually**

**count their votes**

correct for 'errors' in precinct results, overruled the concerns of Diebold programmers to ensure that the GEMS counting software would allow manual corrections of counts. Officials claim that



## ■ eVoting in the US elections

the initial result for Gahanna precinct was 4,258 to Bush and 260 to Kerry. This was rather odd considering that only 638 people actually voted in Gahanna precinct, and Bush should have received a grand total of 365 votes. It's not clear what the source of the problem was or if it occurred in other precincts. Reassuringly, zero votes were recorded for another election run at the same time.

Election officials weren't too sharp: It took people spotting the discrepancies on the county's website and calling in before action was taken. Officials claimed the error would

be avoided? Open Source voting software would help verify the validity of the counting logic. Anyone so inclined would be able to read the code and check that it could add right. Classes of school kids could do it as an exercise before each election.

A strong electoral commission to certify and monitor the systems would be vital. Only with a powerful independent authority will vendors respond quickly and professionally to minimum standards and certification requirements. But we need to remember that software is extraordinarily slippery. It's easy to change and hard to

control (as every copy-control scheme ever attempted has shown). Despite being certificated a cracker could slip a malicious slice of code into the e-voting system seconds before voting was to begin. Certification would be of no use then. To really be confident in the result we need an audit trail that is separated from the software. This could be, for example, a paper ballot printed out by the e-voting system. Because voters could check their paper ballot before posting it into the ballot box there's a degree of verification not possible with electronic votes. As they are verified by voters the paper ballots should be counted to provide official, legally binding, results.

for early voting, though they had other units to hand which could have been used if the officials had known the true capacity. The 4,530 votes that are known to be definitely lost are totally unrecoverable. The vendor argued that while they had supplied the wrong information a warning message was ignored as the machine approached being full. Laporte County, Indiana suffered a strange problem where every precinct could not have more than 300 voters. Officials managed to bypass the problem to release correct vote totals, as far as they could tell. However despite a software update turnout figures could still not be accessed as we went to press. We don't know if any votes were lost or misreported as a result of this problem.

These kinds of problems are ones where Open Source can offer little. While more open systems are less likely to have totally absurd flaws, such as limiting to 300 voters per precinct, they cannot in themselves provide solid assurances. Because votes need to be secret, secure and anonymous they are difficult to handle electronically (see 'Furthur down the road... why voting shouldn't be electronic' LinuxUser & Developer 27). Another channel is needed... yes the paper trail. Procedures also need to be robust so that ballot boxes or memory chips are never going to be given the opportunity to overflow.

### PROBLEM: HUMAN ERROR - DOH!

In Gray's Harbor County, Washington some disks were downloaded twice into the system resulting in numbers being inflated. The same double disk trick happened in Sandusky County, Ohio. In Pulaski County, Arkansas the county reported different results to the secretary of state. Results were

**Open Source can't stop bad**

**breath and it certainly can't**

**prevent human error**

supplied to the secretary through a web form into which the figures were typed. The current theory is that someone typed the numbers in wrong. In other counties around the USA ballots were lost, thrown away, mixed with already counted ballots and double counted. Despite the hype Open Source can't stop

bad breath and it certainly can't prevent human error. Well designed software can prevent some basic errors but Murphy's Law will always apply - what can go wrong will go wrong.

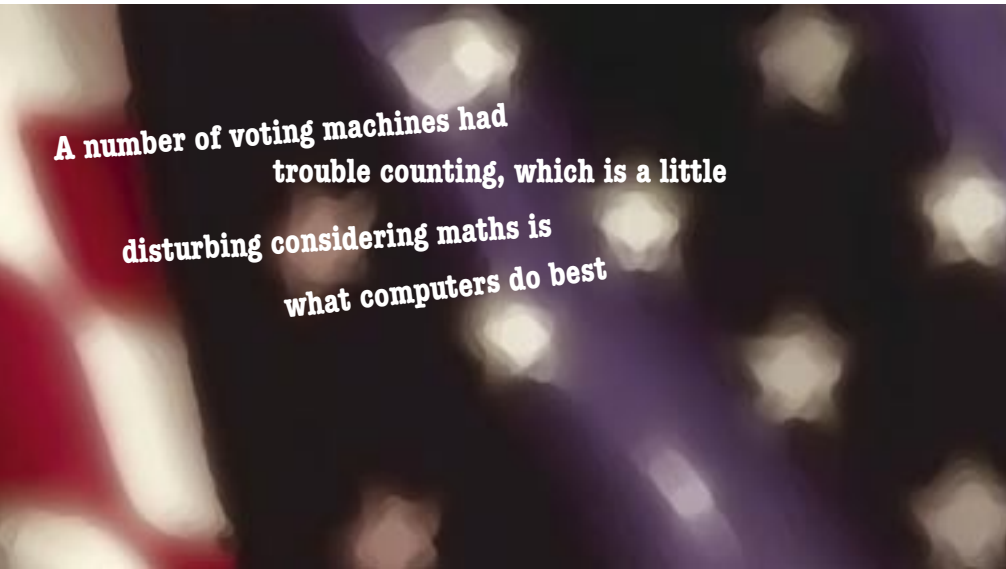
Time and time again reports came through that the people working on the election were poorly trained and had few procedures to follow. Across the world election offices are unloved, they only come into play once a year, at the most. So it's no surprise that during high pressure, one-off events with new virtually untested systems that lots of mistakes will be made. Fortunately there are often easy ways to error check, does the number of votes match the number of voters and so on. Proper trial runs and providing less time pressure for delivering results would help to reduce errors.

## Punched Out

Voting procedures are often subject to accusations of corruption or failure. Few have been as embarrassing as the events in Florida during the 2000 presidential elections, which provided a vivid illustration of the fallibilities of electronic voting systems. Many allegations were made about the Florida elections. The national result was close. Gore had a slight majority of the vote. Bush had a majority of delegates, and the final outcome hinged on the election in Florida. There appear to have been different voting methods in use in different parts of the state, but the controversy centred on the use of Vote-O-Matic punch-card voting systems. The voter punches a hole through the card to register a vote, and the count is performed by computer. Although voting machines were claimed to be more reliable than hand counting, significant errors crept in, caused by slipping card feeds and the notorious "hanging chads", where tiny scraps of punched-out vote holes did not fully detach from the vote card, which meant that the vote was not registered. Once recounts were initiated it was obvious that there were significant errors in the count, and that the majority of lost votes were Democratic votes for Gore.

These machines were not the only source of controversy in the Florida election. BBC journalist Greg Palast broke the story of Governor Jeb Bush and Secretary of State Katherine Harris overseeing a pre-election "purge-and-block" programme to remove more than 50,000 legitimate voters, half of them African Americans and almost all Democrats, from the electoral roll. Palast also reported that in the mostly white counties, machines were set to reject wrongly marked ballots to re-vote; in mostly black counties, the machines ate the bad ballots and did not count them. The recounts were terminated by a court with a Republican majority, and George W Bush became the President of the United States.

Automated counting machines have proved unreliable, yet are used by a third of the US voting population. The vote-counting equipment comes from a variety of private companies using proprietary, closed source software that offers precious few guarantees, despite the fact that organisations such as Computer Professionals for Social Responsibility (CPSR), who have studied such vote counting systems for long periods of time, are on record as saying that the system "has inherent accuracy limitations" and that "careful manual counting of Vote-O-Matic ballots should always be more accurate than machine counts."



A number of voting machines had trouble counting, which is a little disturbing considering maths is what computers do best

have been found during the official count later in the month. Of course it would have been.

Similar problems of more votes being counted than there were voters also occurred in Mecklenburg County and Gastonia, North Carolina; Sarpa County, Omaha saw as many 10,000 too many votes. More reports were still coming in as LinuxUser went to press.

In Broward County, Florida a referendum on gambling held along with the presidential election was thought to be tied. Then it emerged that the counting software used could not handle more than 32,000 votes. Once 32,000 was reached the software started counting backwards. According to officials no other elections were effected.

However the County Mayor Ilene Lieberman was fuming, the supplier ES&S Systems had known about the problem since the same backwards counting happened in a Broward County mayoral election two years ago! As one commentator noted, "my dog could have written better code to add votes!"

How could such counting problems be

What everyone involved in the election process could learn from is the Open Source community's culture of shared problem solving, openness and documented communication

#### PROBLEM: STEALTH ATTACKS

A preliminary study by social scientists from the University of California, Berkeley found that in Florida results in counties using e-voting were skewed towards Bush. This skew is in spite of correcting for demographic differences and past voting patterns. E-voting could have caused a swing in favour of Bush of up to 260,000 voters, however Bush won Florida by 350,000 votes, so the swing wouldn't have changed the final outcome. The reason for the swing is not clear, it could be an unusual growth in support for Bush, fraud or even bad interface design. The problem is that, because no decent audit trails were put in place, attempts to manipulate the results are undetectable.

Exit polls also did not match up with the final results in some areas. Whether this implies fraud or sampling error is impossible to say. Recent counts of optical scan ballots by reporters have shown that some discrepancies were borne out on the actual ballot papers. Areas assumed to be Democrats had, on the day, actually voted for Bush.

#### SO WHAT HAPPENED?

The problem is that we really don't know what happened during the elections. Computer systems were used to manage voter registration, voting, vote counting and

transmission of results to press centres. There was room for undetectable error or fraud at every link in the chain.

Using an Open Source system would certainly reduce the number of bugs, increase debate about design decisions and boost trust in the results. But fundamentally electronic voting is a unique technical challenge. Without well trained officials following tried and tested procedures no voting system will be reliable. No result will be beyond question without a fully verifiable audit trail.

What everyone involved in the election process could learn from is the Open Source community's culture of shared problem solving, openness and documented communication.

There are many challenging problems that election officials face when planning for an unmoveable deadline with a highly limited budget. Yet often separate districts reinvent the wheel. Here in the UK we have recently, thanks to bodies such as the Electoral Commission and the Association of Electoral Administrators, begun to cooperate constructively. Hopefully the US can reach across its state and county lines to help election administrators see their common challenges. If these challenges could be approached in an open and documented way, including when it comes to selecting suppliers, many stakeholders would have significantly more trust in the electoral process than they currently do. Such open approaches would stifle conspiracy

theories before they could even begin.

Paper trails were dismissed as being complex and expensive during the build-up to the November elections. Yet without them every precinct that used all-electronic voting systems cannot disprove any conspiracy theories or claims of malpractice. Not only do candidates and voters lose out, but so does democracy. Voting needs its own Richard Stallman to knock the systems into shape before 2008.

*Jason Kitcat (jason@swingdigital.com) is Managing Director of online community consultancy, Swing Digital.*

### Key Links

**The SERVE report**  
[servesecurityreport.org](http://servesecurityreport.org)

**Summary of e-voting problems in the November 2004 election**  
[www.evoting-experts.com/index.php?p=63](http://www.evoting-experts.com/index.php?p=63)

**The UC Berkeley Florida analysis**  
[ucdata.berkeley.edu/new\\_web/VOTE2004/election04\\_WP.pdf](http://ucdata.berkeley.edu/new_web/VOTE2004/election04_WP.pdf)

**Learn more about e-voting**  
[www.j-dom.org/learn](http://www.j-dom.org/learn)