Black Box Voting

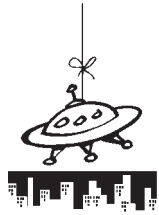
Ballot Tampering in the 21st Century

by Bev Harris

with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar



Plan Nine Publishing
1237 Elon Place
High Point NC 27263
888.454.0098
www.plan9.org

Black Box Voting: BallotTampering in the 21st Century is an original publication of Bev Harris and is published by Plan Nine Publishing.

ISBN 1-929462-45-X
First Printing October 2003

 For information on this book and the investigation into the voting machine industry, please go to www.blackboxvoting.com.

Printed in the USA

Dedication

First of all, thank you Lord.

I dedicate this work to my husband Sonny, my rock and my mentor, who has tolerated being ignored and bored and galled by this thing every day for a year, and without fail, stood fast with affection and support and encouragement. He must be nuts.

And to my father, who fought and took a hit in Germany, who lived through Hitler and saw first hand what can happen when a country gets suckered out of democracy. And to my sweet mother, whose ancestors hosted a stop on the Underground Railroad, who gets that disapproving look on her face when people don't do the proper thing.

And to the kids, Megan and CJ and David IV and of course, Casey, who supplied me with constant encouragement and located some hackers to provide a point of view. And Erika, the nosiest child on earth who grew up to become a successful reporter for a major news outlet, for telling me sternly, "Mom, that is not a story. You have to prove it." And when I did prove it, for saying "Mom, that is B section. Get some more if you want it on A-1."

Introduction

When we started digging around on this story, we expected to find the odd body part or two. Little did we know — we were digging in a graveyard. Suddenly, the dead bodies were piling up so fast that activists everywhere were screaming "Enough, enough we can't take any more!"

The first six chapters were written B.D.,"before Diebold." The rest were written afterwards, making for a somewhat schizophrenic book, a handy little activism tool that begins with history, archive searches and interviews about theoretical vote-rigging, but suddenly becomes a little too real even for us. So hurry, c'mon over with your own merry little band. We have a democracy to defend.

Bev Harris
David Allen

Why is verifying the accuracy of electronic voting machines forbidden?

Do you want your government to be subject to the "consent of the governed?" Well, we are all in danger of losing our say and if you have any doubt about that, pick up a highlighter, dive into this book, and find out as much as you can about the machines upon which the sanctity of your vote depends. Putting the integrity back into our voting system is going to require a fight, and we don't have much time. That's what this book is all about: Prepare to engage!

In an effort to avoid a rerun of the Florida 2000 fiasco, well-meaning but uninformed legislators enacted a sweeping election reform bill. Unfortunately, the bill turned out to be a danger, instead of a safeguard to our democracy.

The bill, called the Help America Vote Act (HAVA), rushes us into subtle changes in the way our electoral system works, undermining the very fabric of our voting system.

The HAVA bill was intended to modernize our election process, moving us from the world of subjectively interpreted ballots with their hanging chads to the precision world of digital computers. However, rather than solving the problem, our legislators made it worse.

Why is it *illegal* to verify the accuracy of electronic voting machines?

To accommodate computerized vote-counting, many states passed legislation designed to streamline elections, laws which specify how our votes are counted. These laws focus on ballot-handling procedures, and they appear benign — until they are used! Try this:

"I would like to find out whether the machine counted accurately, by comparing the actual ballots to the computer count."

Take two blank stares and a copy of the rulebook, please. That is called a "hand recount," and it is not allowed except in very special circumstances and, in many states, only in an exceptionally close race and with a court order.

Or try asking this:

"Who *does* compare the actual ballots to the computer tally in my precinct?"

Counting at the precinct? We don' need no steenkin' *precinct* counts! Nowadays we like to merge 'em, consolidate 'em, and have *big* counting going on in the fewest possible places. How can we take time for a little thing like comparing the ballots with the computer? We've got bigger, better things to do — and did you see the new modems? Heck, these machines are even hooked up for wireless!

"But do they *count* accurately?"

(Doublespeak alert! Know the talking points or go down in flames!) Oh-these-machines-are-tested-and-tested-and-we-do-a-logic-and-accuracy-test-and-they-have-internal-redundant-systems-and-are-specially-certified-and-we-hold-the-code-in-escrow-and-the-federal-government-has-officially-endorsed-them-and-these-are-state-of-the-art-and-hearings-were-held-on-this-and-we've-never-had-any-problems-and—

"But do they count accurately?"

Sometimes you just have to trust. Okay?

"Well...can they be rigged?"

That is asking to us prove a negative. I think we have gone about as far as we can go with this.

Satisfied?

I wasn't.

But it gets better: Of course, it is very modern not to look at the actual ballots, but now we've decided not to *have* any ballots. Now we've got the Black Box!

Black Box Voting. All I want to know is this:

Does it COUNT accurately?

1
Why Vote?

Does anyone really care about voting anymore? Only about half of the eligible U.S. voters even bother to vote in federal elections. The percentage ranges from around 49 percent (1996) to 63 percent (1960). In the 2000 U.S. national election, only 51.3 percent of eligible voters chose to go to the polls.[1]

Now, if you live in a country like Australia, where the law requires that you vote, you might find our lackadaisical voting behavior here in the U.S. to be shocking. Perhaps we should be taken to the woodshed for our frequent failure to vote, but — although it's certainly true that we are a bit cavalier about exercising our voting rights — have you ever heard of anyone who doesn't want the *right* to vote?

I've been told that voting machines are a "non-issue" and the issue is a "sure loser," not because the machines have been proven to count properly, but because supposedly no one cares. Well, explain that to my e-mail server, which has become so jammed with incoming messages from concerned citizens that I had to get help to deal with it! Explain that to my telephone, because suddenly my voicemail fills up every two hours. Citizens are upset. They want to know what's going to be done about this issue. People everywhere are talking, writing, mailing, meeting, agitating, complaining and volunteering about the voting machine problem.

Voting machine accuracy is only a "non-issue" when you don't know very much about it. As a publicist, I've pitched hundreds of issues, but I've never seen one that upsets people like this one. We may not always choose to exercise our vote, but we absolutely insist on being *able* to vote, and we demand a voting system that can be trusted!

"I like to see the people awake and alert. The good sense of the people will soon lead them back if they have erred in a moment of surprise."

— Thomas Jefferson to John Adams, 1786

Which do you think we are (which do you want to be?)

Correct answer may depend on your point of view

Communism — Political system under which the economy, including capital, property, major industries and public services, is controlled and directed by the state and in that sense is "communal."

Democracy — Government by the people, directly or through elected representatives. There is no precise definition of democracy on which all agree, but in a true democracy: Citizens have a say in decisions that shape their lives; the government is run by majority rule, with recognition of minority rights; citizens are guaranteed freedom of speech, press and assembly, can run for office and form opposition political parties and are entitled to privacy, individual dignity and equal opportunities.

Dictatorship — Government whose final authority rests in the hands of one supreme head. Dictatorships are rarely benevolent and often have scant regard for human rights. Also called an autocracy.

Feudalism — A medieval form of social, economic and political organization featuring a pyramidal structure. The lowest part of the pyramid is occupied by an underclass which is obliged to work for the property owners. Traditional feudalism had no middle class; however, in modern versions, a middle class manages the underclass and functions to fuel consumerism for the owner.

Kleptocracy — Representatives of the people, through their appointment of unelected government employees and ties to favored business entities, gradually transfer the public commons to cronies through privatization for the purpose of increasing personal wealth and power.

Fascism — The main elements of fascism are pride in the nation, emphasis on the military, strong government and loyalty to a strong leader. **Nazism**, modeled on fascism, adds specific targeting of various minority groups, and an intense focus on "protecting" citizens from perceived threats. Benito Mussolini, the founder of fascism said that fascism might also be described as "**corporatism**," as it merges state and corporate power. **Corporate Fascism** is not the same thing as **capitalism**. Capitalism emphasizes entrepreneurship and small to medium-sized businesses, rejects monopoly, does not marry corporations into government, and regulates businesses that provide water, power and communications infrastructure. Some describe corporate fascism as "socialized costs, privatized profits."

Monarchy — Government by a single sovereign, whereby a queen or king, empress or emperor holds absolute or limited power, usually inherited. In this century most European monarchies have become constitutional or limited, meaning political power is vested in elected officials and the monarch's duties are largely ceremonial.

Oligarchy — Government that is controlled by a small group of individuals, who

What the founders had in mind

When the United States was formed, our founders had a clear idea what government should and should not be. The purpose of the government was to provide for the common good. As Benjamin Franklin wrote, "In free governments the rulers are the servants and the people their superiors and sovereigns."

Our founders intended that the ultimate power in our society should rest in the people themselves. They set it up so that we should exercise those powers either directly or through representatives.

"Government is instituted for the common good; for the protection, safety, prosperity, and happiness of the people; and not for profit, honor, or private interest of any one man, family, or class of men; therefore, the people alone have an incontestable, unalienable, and indefeasible right to institute government; and to reform, alter, or totally change the same, when their protection, safety, prosperity, and happiness require it."

— John Adams, Article VII, Massachusetts Constitution

"There is only one force in the nation that can be depended upon to keep the government pure and the governors honest, and that is the people themselves. They alone, if well informed, are capable of preventing the corruption of power, and of restoring the nation to its rightful course if it should go astray. They alone are the safest depository of the ultimate powers of government."

— Thomas Jefferson

govern in their own interests.

Plutocracy — Government by the wealthy. A plutocracy can also describe a government on which a group of wealthy people control or influence the government.

Republic — Government by representatives of an established electorate who rule in behalf of the electors. A republic is founded on the idea that every citizen has a right to participate, directly or indirectly, in affairs of state, and the general will of the people should be sovereign.

Theocracy — Government run by priests or clergy.

Why voting is so important

"Governments are instituted among men, deriving their just powers from the consent of the governed."

Declaration of Independence

If our government is set up so that our rulers are our servants and we are their sovereigns, the method devised for us to exercise our sovereignty is through the vote.

If we, collectively, are the source of authority for our government, we must have a way to communicate our instructions. We must be able to select the representatives we think can best implement our will; we need to be able to change them, reorganize them if need be, and decide how they will conduct our business.

Most importantly, we must reach some approximate agreement about what we want, and that is done by placing people, initiatives and referenda on the ballot and casting our votes on them. In some situations, a vote is literally a voice ("aye" or "nay"). When it is impractical to shout out our vote, we cast votes by ballot, and the loudest "voice" wins.

We are a nation of laws, but if our laws conflict with our collective will, there will be little incentive to follow them. It is only because our representatives were chosen by our own voice that we agree to abide by the laws they vote upon, on our behalf.

Because our representatives must return to us from time to time, asking for permission to represent us again, we have a way to encourage them to behave the way we want them to.

"Nothing so strongly impels a man to regard the interest of his constituents, as the certainty of returning to the general mass of the people, from whence he was taken, where he must participate in their burdens."

— George Mason, speech, Virginia Ratifying Convention, June 17, 1788

Why trust in our voting system is so important

Trust is the element that keeps us from taking to the streets every time we disagree with something our government does. As long as we feel our repre-

sentatives are deciding most things, and the very important things, the way we would ask them to, we are content. If we elected them in an election that all agreed was fair, but they make an egregious choice, one that many of us feel we cannot live with, our governmental system sanctions our protest. We reserve such behavior for unusual circumstances, knowing that when the next election rolls around, we can always vote them out.

Perceived lack of integrity in the voting system is guaranteed to produce shouts of indignation, but because *most* elections are perceived to be fair, we can still show some patience with the situation.

If, however, we come to perceive that most elections cannot be trusted, we've got a huge problem. Suddenly, these people don't have our permission to do anything. Why follow laws that they passed, if we don't believe they were fairly elected? Why should we accept anything they do? Why should we follow the law if *they* didn't? Why should we cooperate with our government at all?

"That love of order and obedience to the laws, which so remarkably characterize the citizens of the United States, are sure pledges of internal tranquility; and the elective franchise, if guarded as the ark of our safety, will peaceably dissipate all combinations to subvert a Constitution, dictated by the wisdom, and resting on the will of the people."

— Thomas Jefferson to Benjamin Waring, 1801

As you can see, Thomas Jefferson understood what really makes the system tick. But take away trust in the voting system, and all bets are off. This is what the architects of the new unauditable voting systems have never understood: The vote is the underpinning for our authorization of every law, every government expenditure, every tax, every elected person. But if we don't *trust* the voting system, we will never accept that those votes represent our voice, and that kind of thing can cause a whole society to quit cooperating!

Not Everyone Has Your Best Interest At Heart

Americans prefer to feel good. They want to believe that elections are fair and machines count right, and that people don't cheat.

And yet, there are scholars even within our own country who might advocate, if not subverting the system, at least lying to the voters.

Democracy is for suckers?

According the late University of Chicago professor Leo Strauss, all city states are based on fraud. He believed that ordinary people can't handle this truth.[2] "[Strauss] argued that Platonic truth is too hard for people to bear," writes political columnist William Pfaff..."Hence it has become necessary to tell lies to people about the nature of political reality. An elite recognizes the truth, however, and keeps it to itself...The ostensibly hidden truth is that expediency works."[3]

Such a philosophy, when applied by radicals, might lead to considerable dissarray in our society. In fact, when writers like Pfaff and Seymour Hersh exposed the Straussian studies of Deputy Defense Secretary Paul Wolfowitz, Abram Shulsky of the Pentagon's Office of Special Plans, and writer William Kristol, a great hue and cry arose. Some of the writings of Strauss appear sinister indeed. Have his followers put our democracy at risk?

Strauss is complex, and to select only those writings that can form a rationale for evildoing and then apply them to anyone who studied under him is a bit disengenuous. Besides, many other philosophers provide fodder for those who will do wrong.

But I bring up Strauss, and the powerful men in public office who studied under Strauss and his protegés, to show you that simply wanting to feel good about our political systems, wanting to trust and have faith, is not always wise. While you are feeling comfortably safe, someone may very well be out there rationalizing the elitism and greed that can eliminate your freedom. Whatever your opinions on current political figures, our founding fathers would tell you to expect and prepare for a usurpation of power by people who care not a fig about your comfort. It is not inconceivable that at some point, someone in power will believe that his agenda is more important than your vote.

It's just a matter of time, our founders said, before you'll need to rein in your leaders. Thomas Jefferson, especially, foresaw many of the dangers we face today and exhorted us toward constant vigilance. I give you his words:

"Unless the mass retains sufficient control over those entrusted with the powers of their government, these will be perverted to their own oppression, and to the

perpetuation of wealth and power in the individuals and their families selected for the trust."

—Thomas Jefferson to M. van der Kemp, 1812

"No other depositories of power [but the people themselves] have ever yet been found, which did not end in converting to their own profit the earnings of those committed to their charge."

— Thomas Jefferson to Samuel Kercheval, 1816

"If once [the people] become inattentive to the public affairs, you and I, and Congress and Assemblies, Judges and Governors, shall all become wolves. It seems to be the law of our general nature, in spite of individual exceptions."

— Thomas Jefferson to Edward Carrington, 1787

"[We] should look forward to a time, and that not a distant one, when corruption in this as in the country from which we derive our origin will have seized the heads of government and be spread by them through the body of the people; when they will purchase the voices of the people and make them pay the price. Human nature is the same on every side of the Atlantic and will be alike influenced by the same causes."

— Thomas Jefferson: Notes on Virginia Q.XIII, 1782

"How long we can hold our ground, I do not know. We are not incorruptible; on the contrary, corruption is making sensible though silent progress."

— Thomas Jefferson, 1799

And for a current take on our situation:

"We basically now have intellectuals who have justified imperialism, who have legitimated wealth inequality, and they are intellectuals ...who are using their gifts on behalf of power rather than truth...But I really believe we're about to lose our democracy, if we don't speak out."

— Cornell West

When things go wrong

Through your right to vote, you exercise your power over those who govern you. Maybe you have never written a letter to your legislator. Perhaps you think that no matter what you do, they'll just do what they want anyway. The last chapter in this book focuses on practical activism; this section is about your responsibility to

engage.

Our founders did not promise to be the caretakers for their gift of democracy to us. They told us that if we don't feed it, our democracy will die. They warned us that it would get sick sometimes and explained that it was up to us to administer the right medicine.

If things are not going right, let your elected officials know. If you have to, remind them that they'll soon need to return to you for a vote! What good is your voice if you don't use it? If you believe that government has taken the wrong course, educate your legislators, and if they won't listen, throw them out and elect someone who promises a revision of the course. If you conclude, after reading this book, that your vote might not be counted correctly, then you have decisions to make.

Why vote?
Whether or not you choose to vote, do you demand the *right* to vote?
Is your country what you want, or is it becoming something else?
How important is voting?
Is your vote in danger?
What would the founders of this country ask you to do?
Will you choose to engage?

"The liberties of our country, the freedom of our civil Constitution, are worth defending at all hazards; and it is our duty to defend them against all attacks. We have received them as a fair inheritance from our worthy ancestors: they purchased them for us with toil and danger and expense of treasure and blood, and transmitted them to us with care and diligence. It will bring an everlasting mark of infamy on the present generation, enlightened as it is, if we should suffer them to be wrested from us by violence without a struggle, or to be cheated out of them by the artifices of false and designing men."

— Samuel Adams

Chapter 1 footnotes

1 – InfoPlease.com: History and Government, U.S. Elections, Election Statistics: "National Voter Turnout in Federal Elections: 1960–2000" *Source:* Federal Election Commission. Data drawn from Congressional Research Service reports, Election Data Services Inc., and State Election Offices. http://www.infoplease.com/ipa/A0781453.htmls

2 – WNYC radio interview: with Jeet Heer, graduate student at York University in history and frequent contributor to the Boston Globe on American culture, explaining the influence of the intellectual icon Leo Strauss. May 22, 2003

3 – International Herald Tribune , 15 May 2003; "The long reach of Leo Strauss Neoconservatives." According to Pfaff, Deputy Defense Secretary Paul Wolfowitz, and Abram Shulsky of the Pentagon's Office of Special Plans took their doctorates under Strauss. Another neoconservative, William Kristol, studied under Strauss protogé Allan Bloom. Jeet Heer disputes this, saying that while Wolfowitz may have taken classes with Strauss, he took him main influence from Allan Bloom.

Chapter 2
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris

with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar

2
Do Voting Machines Ever Get it Wrong?

I refer to this chapter as the "I don't believe there is a problem" chapter. I wrote this obese section for the people who, when you give them the short but horrifying version, insist on minimizing the problem. When you jump into the fray, you'll soon meet them: You tell them about an election that lost 25 percent of its votes, and they say "that's just an isolated incident." When you add that another election had a 100 percent error, they call it a "glitch." When you tell them a voting machine was videotaped recording votes for the opposite candidate than the one selected, they say, "There are problems in every election."

No. We are not talking about a few minor glitches. This chapter contains a compendium (and it is by no means complete) of real miscounts by voting machines, which took place in real elections. Almost all of them were caused by incorrect programming, whether by accident or by design.

And if you run into anyone who thinks we are hallucinating these problems, I have included a "super-sized" footnote section, so you can invite them to examine sources and look them up themselves.

Of course, I realize that you're one of the good guys, and it won't take you long to see the magnitude of the problem. If you get a little light-headed after seeing all the miscounts, you have my blessing to skim, or quit reading altogether and just go on to the next chapter. Lest you get depressed after seeing what keeps happening to our votes — you know, the ones that Thomas Jefferson argued so eloquently for, the votes that define whether we have a democracy or not — don't be. Solutions and suggestions for what we can do about this problem are scattered abundantly through the rest of this book.

* * * * *

Voting machine companies claim these things are amazingly accurate. Bob Urosevich, who has been president of three different voting machine companies under five different corporate names, said in 1990 that his company's optical scan machines had an error rate of only "one-thousandth of 1 percent."[1]

At that time, Urosevich was with Election Systems & Software (ES&S; then called American Information Systems). Recently, the same Urosevich (now president of Diebold Election Systems, formerly called Global Election Systems) gave an even more glowing endorsement of his company's touch screen accuracy.[2] "Considering the magnitude of these elections, which includes more than 870,000 registered voters within the four Maryland counties, we are very pleased with the results *as every single vote was accurately counted*," he said. [emphasis added]

When Chuck Hagel accepted his position as chairman of American Information Systems, now called ES&S, he offered a rousing endorsement: "The AIS system is 99.99 percent accurate," he assured us.[3] A little later, he left this position and ran for the U.S. senate seat in Nebraska, a seat he won in the biggest upset of the 1996 general election. Hagel's victory was tallied by his previous employer's computer voting machines.

But do these claims hold up?

- According to *The Wall Street Journal*, in the 2000 general election an ES&S optical scan machine in Allamakee County, Iowa, was fed 300 ballots and reported 4 million votes.[4]

- Better than a pregnant chad — these machines can actually give birth! In the 1996 McLennan County, Texas, Republican primary runoff, one precinct tallied about 800 votes, although only 500 ballots had been ordered. "It's a mystery," declared Elections Administrator Linda Lewis. Like detectives on the *Orient Express*, officials pointed fingers at one suspected explanation after another. One particular machine may have been the problem, Ms. Lewis said. That is, the miscounted votes were scattered throughout the precincts with no one area being miscounted more than another, Ms. Lewis also explained. Wait — some ballots may have been counted more than once, almost doubling the number of votes actually cast. Aha! That could explain it! (Er…excuse me, exactly *which* ballots were counted twice?) "We don't think it's serious enough to throw out the election," said county Republican Party Chairman M.A. Taylor. Size of error: 60 percent.[5]

- Here's a scorching little 66 percent error rate: Eight hundred and twenty-six votes in one Tucson, Arizona-area precinct simply evaporated, remaining

A Quick Primer on Voting Systems

Raise your hand — Raise your voice — Put sticks in a box — Elections have been used to decide various questions for at least 2000 years. In ancient Greece, they voted by putting white ("yes") or black ("no") stones in a bucket. Early voting methods (still used in some settings) included shouting out "Aye" or "Nay," raising hands, or depositing objects to be counted.

Paper ballots — The first known use of paper ballots in an election in the U.S. was in 1629, to select a church pastor. **The Australian paper ballot system** was considered a great innovation: Standardized ballots are printed at government expense, given to voters at the polling places, and people are required to vote and return the ballots on the spot. No, this wasn't invented in America: The Australians came up with this procedure, which is now the most widely used voting system in the world.

Lever machines — Lever machines made their debut around 1890 and became popular throughout the USA by the 1950s. They've been out of production since 1982 and are now being phased out.

Punch cards — Punch cards also date back to the 1890s, but really became stylish around 1964, when we learned to program computers to count punch card votes. By the 1970s, punch cards had become the most widely used system in America. The Help America Vote Act (HAVA) mandates that punch card voting be eliminated by 2004 or, if a waiver is requested, by 2006.

Optical scanning (Also called "mark sense") — When voting on an optical scan system, you fill in the dot on paper ballots, and a computer reads them. Some optical scan systems have you connect a dot to a candidate by drawing a line. These ballots are fed into a scanner, which records the vote and provides a computer tally of the totals.

Touch screen and "DRE" machines: "DRE" stands for "Direct Recording Electronic." Most DRE systems involve touching a computer screen to record your vote. Some systems involve turning a wheel or pushing a button on a computer, instead of touching a screen. Touch Screen/DRE machines are the newest voting system, and they are sleek and fun and convenient. Without proper audits, they represent a horrifying risk to proper vote tabulation because most of them are not properly auditable.

Voting Systems (continued)

Some manufacturers, like Avante and AccuPoll, pioneered in developing touch screen voting systems that can be audited properly. However, many officials succumb to lobbying and yes, accept financial contributions from manufacturers that produce unauditable systems, purchasing the riskier systems instead.

Internet Voting — Almost no one believes that Internet voting is ready for prime time, but that hasn't stopped some companies from trying to talk everyone into it. And they are succeeding, to the dismay of computer security experts. As currently developed, Internet voting, like touch screen/DRE voting, is not auditable by proper accounting methods and carries with it a host of other security risks.

Telephone Voting — Yes, some systems have been developed to pick up the phone and vote! While this book does not spend much time on telephone voting systems, they, too, are counted by computer software and are not, at this time, properly auditable.

unaccounted for a month after the 1994 general election. No recount appears to have been done, even though two-thirds of voters did not get their votes counted. Election officials said the vanishing votes were the result of a faulty computer program. Apparently, the software programming error and the person who caused it are still at large. [6]

- Some voters aren't so sure that *every single vote* was accurately counted during the 2002 general election in Maryland. "I pushed a Republican ticket for governor and his name disappeared," said Kevin West of Upper Marlboro, who voted at the St. Thomas Church in Croom. "Then the Democrat's name got an 'X' put in it." No one will ever know whether the Maryland machines counted correctly because the new Diebold touch-screen system is unauditable.[7]

- Honolulu, Hawaii: Tom Eschberger, a vice president of ES&S, said a test conducted on the software and the machine that malfunctioned in a Waianae precinct in the 1998 general election showed the machine worked normally. He

Dozens of protesters chanted, "Gringos get out!" at ES&S technicians, and Venezuelan President Hugo Chavez accused ES&S of trying to destabilize the country's electoral process..

said the company did not know that the machine wasn't functioning properly until the Supreme Court ordered a recount, when a second test on the same machine detected that it wasn't counting properly. "But again, in all fairness, there were 7,000 machines in Venezuela and 500 machines in Dallas that did not have problems," he said.[8]

- Dallas, Texas: More than 41,000 votes were not counted during the 1998 general election because of incorrect programming. A recount was done and ES&S took the blame. Democrats picked up more than 1,000 votes, not quite enough to overturn the election.[9]

- Caracas, Venezuela – May, 2000: Venezuela's highest court suspended elections because of problems with the vote tabulation for the national election. Venezuela sent an air force jet to Omaha to fetch experts from ES&S in a last-ditch effort to fix the problem. Dozens of protesters chanted, "Gringos get out!" at ES&S technicians. Venezuelan President Hugo Chavez, whom U.S. officials would very much like to see unseated, accused ES&S of trying to destabilize the country's electoral process. Chavez asked for help from the U.S. government because, he said, the U.S. recommended ES&S. [10]

- For the third time in as many elections, Pima County, Arizona, found errors in the tally. The computers recorded no votes for 24 precincts in the 1998 general election, but voter rolls showed thousands had voted at those polling places. Pima was using Global Election Systems machines, which now are sold under the Diebold company name. [11]

- "It was like being queen for a day — but only for 12 hours," said Richard Miholic, a losing Republican candidate for alderman who was told that he won the Lake County, state primary election. He was among 15 people in four races affected by an ES&S vote-counting foul-up in the Chicago area. [12]

- Officials in Broward County, Florida, had said that all the precincts were included in the Nov. 5, 2002, election and that the new, unauditable ES&S touchscreen machines had counted the vote without a major hitch. The next day, the

County Elections Office discovered 103,222 votes had not been counted. Broward Deputy Elections Supervisor Joe Cotter called the previous day's mistake "a minor software thing." [13]

- An Orange County, California, election computer made a 100 percent error during the April 1998 school bond election. The Registrar of Voters Office initially announced that the bond issue lost by a wide margin when in fact it was supported by a majority of the ballots cast. The error was attributed to a programmer reversing the "yes" and "no" answers in the software used to count the votes. [14]

- Illinois Democrat Rafael Rivera said, "I knew something was wrong because when I looked up the results in my own precinct it showed zero votes. I said, `Wait a minute. I know I voted for myself.'" The problem cropped up during the Lake County election held April 1, 2003. Clerk Willard Helander blamed the problem on ES&S, the Omaha company in charge of operating Waukegan's optical-scan voting machines. Rivera said he felt as if he were living an episode of *The Twilight Zone*. No votes showed up for him, not even his own. "It felt like a nightmare," he said. [15]

- A computer program that was specially enhanced to speed the November 1993 Kane County, Illinois, election results to a waiting public did just that — unfortunately, it sped the wrong data. Voting totals for a dozen Illinois races were incomplete, and in one case they suggested that a local referendum proposal had lost when it actually had been approved. For some reason, software that had worked earlier without a hitch had waited until election night to omit eight precincts in the tally. [16]

- Ten days after the November 2002 election, Richard Romero, a Bernalillo County, New Mexico, Democrat, noticed that 48,000 people had voted early on unauditable Sequoia touch-screen computers, but only 36,000 votes had been tallied — a 25 percent error. Sequoia vice president Howard Cramer apologized for not mentioning that the same problem had happened before in Clark County, Nevada. A "software patch" was installed and Sequoia technicians in Denver *e-mailed* the "correct" results. [17]

  Not only did Cramer fail to mention to Bernalillo County that the problem had happened before in Nevada — just four months later, Sequoia salespersons

failed to mention it again while making a sales presentation to Santa Clara County, California! A Santa Clara official tried to jog their memory and specifically asked whether Sequoia had experienced a 25 percent error in any election. According to the minutes of this meeting[18], "Supervisor McHugh asked one of the vendors about a statistic from Bev Harris saying there was a 25 percent error rate...No one knew where this number came from and Sequoia said it was incorrect."

The Santa Clara meeting, above, was held Feb. 11, 2003. Just 18 days before, in Snohomish County, Washington, at a meeting called because Sequoia optical scan machines had failed to record 21 percent of the absentee votes,[19] I asked about the 25 percent error in Bernalillo County. The Sequoia representative was well aware of the problem, replying quickly that *that* 25 percent error was caused by something quite different from *this* 21 percent problem. OK. *Nothing to see here — move along*.

Sequoia's failure to disclose a known error when asked about it during a sales meeting really got me wondering:

How often do voting companies lie about known errors when they are making sales presentations?

Not often, it turns out. They don't have to lie — because our election officials *don't ask*! That's right. When deciding to buy voting machines, our representatives *don't ask* whether the machines count accurately. And only occasionally does anyone bother to ask whether the machines can be tampered with.

Decisionmaking in Action
Marion County, Indiana, Voting Technology Task Force
Meeting Minutes July 30, 1999
Election Systems & Software - Global Election Systems - MicroVote

Mr. Cockrum asked a series of questions to each vendor.
- How do you recommend instruction of voters to become familiar with your system?
- How many machines per voter/precinct?
- Could your system handle split precincts?

As a citizen, you can attend meetings like the Marion County Voting Technology meeting, below. Had Mr. Cockrum, or anyone else who attended the meeting, known about errors caused by these machines, much better questions could have been asked.

Before anyone runs out to spend a few million tax dollars on machines that may actually take away your vote, try questions like this:

Has your vote-counting system ever lost thousands of votes without flagging the error?

- In Seattle, a malfunction caused voting-machine computers to lose more than 14,000 votes during the November 1990 election. Individual ballots were counted but not the votes contained on them. The computer program didn't catch the problem, nor did any of the election officials. A Democratic candidate noticed the discrepancy after the election was over and demanded an investigation. "It was mechanical or electric malfunction with the card reader," said Bob Bruce, then superintendent of elections for King County. "We'd lost the 14,000 votes. We've got them back now. Hallelujah! The prodigal votes have come back. Now we have to make sure we don't have too many votes." [20]

- A software programming error caused Dallas County, Texas's new, $3.8 million high-tech ballot system to miss 41,015 votes during the November 1998 election. The system refused to count votes from 98 precincts, telling itself they had already been counted. Operators and election officials didn't realize they had a problem until after they'd released "final" totals that omitted nearly one in eight

(continued)
- Could your systems handle school board elections?
- Does your system allow for party crossover voting?
- What is the recount capability?
- Is your system tamper proof?
- Can your system be leased or does it need to be purchased?
- What is the percentage of availability of spare machines?
- What are the advantages?
- There being no further business before the Voting Technology Task Force, Chairwoman Grant adjourned the meeting.

votes. The system vendor, ES&S, assured voters that votes were never lost, just uncounted. The company took responsibility and was trying to find two apparently unrelated software bugs, one that mistakenly indicated precinct votes were in when they weren't, and another that forgot to include 8,400 mail-in ballots in the final tally. Democrats were livid and suspicious, but Tom Eschberger of ES&S said, "What we had was a speed bump along the way." [21]

Here's a question that you shouldn't have to ask about a company involved in the voting process:

Have any of your employees been called to testify in grand jury proceedings related to your voting machines?

- In Polk County, Florida, County Commissioner Marlene Duffy Young lost the election to Bruce Parker in November 1996 but regained the seat after a court-ordered hand recount. After the recount, county commissioners unanimously voted to ask for a grand jury probe. Testifying were Todd Urosevich, a vice president with American Information Systems Inc. (now ES&S), the company that had sold the county its ballot-counting equipment. The machines had given the election to Parker (a Republican) but a hand recount revealed that Young (a Democrat) had won. Todd Urosevich said his machines were not responsible for the miscount. [22]
- A grand jury was convened in Stanislaus County, California, to determine what caused computerized voting machines to misreport election results in the November 1998 election. The grand jury concluded that an ES&S computerized counting system misccounted the votes for three propositions. A hand recount of the ballots resulted in Measure A, a state proposition, being reversed: ES&S machines had reported that it had lost badly, but it had won. According to Karen Matthews, county clerk recorder and registrar of voters, the problem occurred because of a programming error in the software produced by ES&S. [23]

A follow-up question should be:

Will you reimburse the county if we have to go to court or pay for a grand jury probe into your errors made by your voting machines?

More questions:

How often has your voting system been subject to programming errors? Can you give me some examples of when this has happened, and tell us what steps you took to make sure it could not happen again?

- In Knoxville, Tennessee, a software programming error caused more than 40,000 votes cast during 15 days of early voting for the 1996 general election to be lumped together, instead of separating the vote tally into city and non-city ballots. Voters considered this programming error to be an outrage, because it caused one of the ballot items to fail when it was voted on county-wide. [24]

- In the Oct. 16, 2001, Rock Hill, S.C., city election, computerized vote counters were programmed incorrectly, skipping hundreds of votes cast. In a number of precincts, the ballot-counting software ignored votes for council members when they should have been included, causing omission of 11 percent of the votes cast for these races. In all, voting irregularities were found in seven of the city's 25 precincts. [25]

At its heart, our body of law is on the side of the voter. Our entire governing system is based on the sanctity of the vote. It is not excusable for votes to be counted improperly because of "programming errors." Almost all states have statutes that say something like this:

"If voting machines are to be used, they must count the vote *properly*."

Federal Election Cmmission (FEC) regulations require that the manufacturer take responsibility for providing appropriate training to local personnel to ensure that votes are counted correctly. If a system is so complicated that programming errors become "inevitable" or "to be expected," the system must not be used!

The next question will elicit disclosure of past programming errors (or cause sales people to lie, providing fodder for product liability lawsuits):

How many instances have you had in which votes were counted incorrectly because of programming errors by your own personnel?

- In Union County, Florida, a programming error caused machines to read 2,642 Democratic and Republican votes as entirely Republican in the September 2002 election. The vendor, ES&S, accepted responsibility for the programming error and paid for a hand recount. Unlike the new touch-screen systems, which eliminate voter-verified paper trails, Union County retained a voter-verified paper trail. Thus, a recount was possible and Democratic votes could be identified. [26]
- In Atlanta, Georgia, a software programming error caused some votes for Sharon Cooper, considered a "liberal Republican candidate," not to register in the July 1998 election. Cooper was running against conservative Republican Richard Daniel. According to news reports, the problem required "on-the-spot reprogramming." [27]

Decisionmaking in action

From Indiana Election Commission Minutes — August 7, 2001

- Mr. Long asked if the master PEB [electronic ballot] is precinct unique.
- Mr. Long asked if a county would be able to add or replace a voting unit in a precinct.
- Ms. Christie asked if that override could be done at the precinct level
- Mr. Long asked if the central office of the county would program the PEBs.
- Mr. Long asked if the vendor would have a person on site in the county for each election.
- Mr. Morgan asked about other ES&S DRE voting systems operating in other states.
- Ms. Christie asked what the vendor's customers are using for absentee ballots.
- Mr. Perkins asked about training provided by the vendor.

Follow-up question: ***How can computerized vote-counting possibly be considered secure from tampering when "on-the-spot reprogramming" can be used to alter vote totals?***

Here is a question no one from the Indiana Election Commission asked:

How often has your equipment malfunctioned?

- Among the problems outlined by the Democratic Party in the infamous Florida election of 2000: When a polling machine, which counts and reports the tally by modem, resulted in a DeLand precinct's reporting that presidential candidate Al Gore had *negative* 16,022 votes, the vendor blamed it on a "faulty memory card" (more on this later). The computerized vote tally gave the Socialist Workers Party candidate almost 10,000 votes — about half the number he received nationwide.[28]
- In November 2002, a voting machine was caught double-counting votes in South

(continued)
- Mr. Valentine asked if election night reporting could be reported electronically.
- Mr. Valentine asked if the data could be altered to match the State's format
- Mr. Simmons stated that he had a question about the technology for absentee voting
- Mr. Long asked for the Election Division's recommendation on the voting system
- Mr. Perkins asked if the staff had contacted any of the references or other States listed in the vendor's material provided to the Election Commission. (Mr. Valentine stated that staff had not done so at this time.)
- Mr. Cruea asked if the system had been used in an election
- Mr. Long moved that the Commission approve the iVotronic DRE Voting System for certification. Mr. Morgan seconded the motion.
- There being no further discussion, the Chair called the question, and declared that with four members voting "aye" (Mr. Cruea, Mr. Long, Mr. Morgan and Mr. Perkins), and no member voting "nay", the motion was adopted.

Dakota. The error was blamed on a "flawed chip." ES&S sent a replacement chip; voters demanded that the original chip be impounded and examined. Who was allowed to examine it? Citizens? (No.) Experts that we choose? (No.) ES&S? (That's it.)[29]

- Then there is the case of the 3.9 million extra votes during the 2000 election in Allamakee County, Iowa. Final reporting of the state's election-night results were held up until 4:15 a.m. The county's lone voting machine was fed about 300 absentee ballots. But the optical-scanning device reported it had counted a few million extra ballots. The county auditor tried the machine again but got the same result. Eventually, the machine's manufacturer, ES&S, agreed to have replacement equipment sent. Republicans hoped that the tiny but heavily Republican county would tip the scales in Mr. Bush's favor, but tipping it by almost four million attracted national attention. "We don't have four million voters in the state of Iowa," said Bill Roe Jr., county auditor. Todd Urosevich of ES&S said "You are going to have some failures."[30]

"But they are "TESTED and TESTED and TESTED again!"

This is the official rebuttal when you ask whether machines can miscount. More on this "testing" later, but for now, suffice it to say that the ultimate invalidation of

Decisionmaking in action

Indiana Secretary of State Election Commission Minutes 8/7/01

- Ms. Robertson, Co-General Counsel of the Election Division stated that ES&S had submitted its application to the Election Division, and that the system had passed approval by both Wyle Laboratories, the independent testing authority for voting system hardware and firmware and Metamor, the independent testing authority for voting system software.
- Ms. Robertson explained that under Indiana law, voting systems that involve software are required to have an escrow agreement. Mr. Valentine, Co-Director of the Election Division indicated that he believed that the Division had received the escrow agreement for this voting system but they would have to follow up with the vendor to ensure that.
- Ms. Robertson stated that ES&S had met all other requirements under Indiana law.

the testing a voting machine endures would be *a machine that can't count!*

The sub-bar starting on page 29 documents the "arduous" testing these machines go through. This is a state meeting to certify election machines. Nowhere do officials ask the manufacturer to list or explain known errors in tabulation during actual elections. Nowhere do they ask any questions about anti-tampering security.

Election officials and voting machine companies can argue 'til they are blue in the face about the excellence of the certification process and why all this testing means we should "trust" their machines. But if, even after certification and testing, the machines get it wrong, the testing isn't doing its job. Machine tallies in actual elections must be properly and robustly audited. Deal-breaker. End of discussion.

Sometimes, errors show up before or during certification tests but are ignored.

• Dan Spillane, a test engineer for the Votehere touch screen voting system, says he flagged more than 250 system-integrity errors, some of which were critical and could affect the way votes were counted — known errors, yet this system passed every level of certification without a hitch. Spillane claims he brought

(continued)
- The Chair recognized Robb McGinnis of ES&S who introduced Jack Black and Pat Whalen also of ES&S.
Mr. Whalen then explained that as stated earlier, the voting system had:
- passed the testing requirements of the independent testing authority.
- been approved by both Wyle and Metamor.
- He stated that the voting system had been assigned a NASED (National Association of State Election Directors) number.
- Chris gave a description of the ES&S Model 100 version 4.5.5 certification demonstration.
- Moved by Viken, seconded by Brock to certify the ES&S Model 100 firmware version 4.5.5 optical scan ballot counter for precinct and central count use. Passed.
- Adjourned.
Joyce Hazeltine, Secretary of State - Chris Nelson, Recorder

his concerns up to all levels of VoteHere management but was ignored. Just before the system went through certification testing, the company fired him to prevent him from flagging the problems during certification, Spillane contends. He filed a lawsuit for wrongful termination, which is still pending. [31]

- According to the *Las Vegas Review-Journal*, a member of the Nevada Policy Research Institute's Advisory Council reports the following: "In July 1996, a public test to certify Clark County's Sequoia Pacific machine for early voting was conducted. During the test, a cartridge malfunctioned; also, the examiner (selected by the state) had difficulty casting his vote. He had to vote 51 times rather than the designated 50, an option not afforded the voter should the machine malfunction in an actual election. In spite of these malfunctions, the machine was given certification—the equivalent of declaring it accurate, reliable and secure." (Clark County then trotted right out and bought the machines.) [32]

Even after certification and testing, the machines get it wrong:

- In Conroe, Texas, congressional candidate Van Brookshire wasn't worried when he looked at the vote tabulation and saw a zero next to his name for the 2002 primary. After all, he was unopposed in the District 2 primary and he assumed that the Montgomery County Elections Administrator's Office hadn't found it necessary to display his vote. He was surprised to learn the next day that a computer glitch had given all of his votes to U.S. Rep. Kevin Brady, who was unopposed for the nomination for another term in District 8. A retabulation was paid for by ES&S, the company that made the programming mistake. The mistake was undetected despite mandatory testing of the program before and after early voting. [33]

- In Tennessee, a computer snafu in the August 1998 Shelby County election temporarily stopped the vote count after generating wildly inaccurate results and forcing a second count that continued into the morning. State Sen. Roscoe Dixon huddled with other politicos around a single copy of the latest corrected election returns, which quickly became dog-eared and riddled with circles and "X"s. "This system should have been checked, and it should have been known that the scanner couldn't read the cartridges," Dixon said. [34]

- Pamela Justice celebrated her re-election to the school board in Dysart, Arizona, in the March 1998 election. But because of a software programming error in the

county's computer, there had been a mistake in the unofficial election results. The computer had failed to count 1,019 votes from one precinct. When those votes were added in, Justice lost the election to her opponent, Nancy Harrower. "We did an accuracy test before election day and the computers worked fine," said Karen Osborne, county elections director.[35]

"That's what's puzzling about it. It's one of those deals where you can test it one minute and it's working fine, and you can test it the next and it's not."

- A computer defect at the Oklahoma County, State Election Board left more than a dozen state and county races in limbo during the 1996 general election. A final count was delayed until sometime the next morning while technicians installed new computer hardware. "Our memory pack receiver doesn't want to talk to our computer, basically," Sanderson said. Despite several trial runs with computers the week prior to the election, the problem didn't surface until 7:05 p.m. — five minutes after the election board attempted to begin its count. "That's what's puzzling about it," Sanderson said. "It's one of those deals where you can test it one minute and it's working fine, and you can test it the next and it's not."

  Two hundred and sixty-seven precincts (and two close races) were involved. "We could count it by hand, but I'm not going to do that," Sanderson said. "We're just going to wait here until we can do it electronically, so there will be no question" that the election's integrity was upheld. Really.[36]

- The manufacturer of Baltimore's $6.5 million voting system took responsibility for the computer failures that delayed the November 1999 city election results and vowed to repay the city for overtime and related costs. Phil Foster, regional manager for Sequoia Pacific Voting Equipment Inc., said his company had neglected to update software in a computer that reads the election results. Although it tested some programs, the company did not test that part of the system before the election. Before Sequoia agreed to reimburse the city for the problems — a cost that election officials said could reach $10,000 — Mayor Kurt L. Schmoke had threatened a lawsuit against the company.[37]

- In a 1998 Salt Lake City election, 1,413 votes never showed up in the total. A software programming error caused a batch of ballots not to count, even though

they had been run through the machine like all the others. When the 1,413 missing votes were counted, they reversed the election. [38]

Has anybody been studying error rates?

Not really. Most errors are detected only when they are caught during "canvassing" (when voter rolls are compared with vote tallies). Many of the errors listed in this chapter were found *only* because the number of votes cast did not match the number of voters who had signed in.

Because hardly anyone audits by comparing actual ballot counts with machine tallies, we are not likely to catch other kinds of errors unless something bizarre shows up (candidate gets zero votes, or the Wild-Eyed Radical Party gets 60 percent of the vote, for example).

The frightening thing is this: For every machine miscount we catch, there must be a hundred we never notice, simply because the number of voters is the same as the number of votes and nothing looks unusual. And only discrepancies in number of voters vs. number of votes can prove a machine miscounted when there is no paper trail — on those systems, if you had 100 votes cast (55 for Mary and 45 for Idiotman) but the computer says you have 100 votes, 48 for Mary and 52 for Idiotman, he wins. End of story. People can gripe about it, but that's all they can do: gripe.

Shortly after the election of 2000, the California Institute of Technology and the Massachusetts Institute of Technology mobilized a team of computer scientists, human-factors engineers, mechanical engineers and social scientists to examine voting technology. Here are voting system error rates, as estimated by the Caltech/MIT Voting Technology Project report, issued in July 2001: [39]

Most lost votes — Congressional and gubernatorial races

1. Lever machines 7.6% — 1.5% for presidential races
2. Touch screen machines 5.9% — 2.3% for presidential races
3. Punch card 4.7% — 2.5% for presidential races
4. Optical scan 3.5% — 1.5% for presidential races
5. Hand-counting 3.3% — 1.8% for presidential races

However, the Caltech/MIT error estimates omit two issues that are critical to system integrity: tampering and programming errors.

Tampering: Every voting system can be tampered with (later chapters will cover this in more detail). When scrutinizing opportunities for malfeasance, you build an "attack tree." To do that, you see if you can compromise the system. The following considerations affect how easy it is to compromise a system and how likely it is that someone will try:

- How much can be stolen.
- How many strategies can be found.
- How many people would be required to compromise the system, and who has access.
- How likely it is that tampering will be detected.

Unless we start auditing the machines using a voter-verified ballot, in some robust manner, we are moving toward more and more vulnerable systems. Based on the above factors, from most to least vulnerable:

1. Internet
2. Touch screen or DRE
3. Punch card (being phased out)
4. Optical scan
5. Hand-counting (being phased out)
6. Lever machines (being phased out)

Errors: Although the Caltech/MIT study looks at how many votes are lost (for example, ballots that show no vote because the machine failed to record the voter's preferences, or because the voter made a mistake or was confused), it fails to account for risks such as incorrect programming. The more complex the system, the greater the potential for errors. Some errors, like a touch-screen machine that fails to boot up, are discovered immediately. The more dangerous errors are those that can pass unnoticed. Based on system complexity, the most and least vulnerable systems to programming error are:

1. Internet
2. Touch screen or DRE
3. Optical Scan

4. Punch card (being phased out)
5. Hand-counting (being phased out)
6. Lever machines (being phased out)

Everything changes if we start doing proper auditing. In a few locations, such as California, a paltry 1% of precincts are randomly audited, but only for machines that produce an audit trail. In Washington state, candidates can select up to three precincts per county for audits, but unless this audit compares the paper trail to the machine, it is not a valid audit of machine accuracy.

Let's quit calling these things "glitches" and "snafus"

A word about the term "computer glitch." Glitches seem to have no owner and bring with them an aura of expectability, if not respectability. The proper term is *incorrect programming*, which demands accountability.

A Compendium of Voting Machine Errors

- 1950s, Louisiana — The shape of things to come: When automated voting machines were brought into the state as a way to reduce election fraud, then-Gov. Earl Long said, "Gimme five (electoral) commissioners, and I'll make them voting machines sing `Home Sweet Home.'" [40]

- 1971, Las Vegas, Nevada — Machines declared Democrat Arthur Espinoza to be the winner of a seat on the city assembly, but Republican Hal Smith challenged the election when he determined that some votes had not been counted because of a faulty voting machine. After unrecorded votes were tallied, Smith was declared the winner. [41]

- September 1986, Dallas, Texas — Voting system reports fluctuated. The number of voters changed on various report printouts, but votes for individual candidates remained the same. The problem was attributed to a computer-programming error. Note the date on this report: Officials have been expressing concerns about computerized vote-counting for nearly two decades.

  "With paper ballots, I can make the numbers add up..." said Assistant Texas Attorney General Bob Lemens. "We are running into much tougher problems here."

Texas Attorney General Jim Mattox said the computerized vote-counting clearly has the potential for fraud. "I can't send a reasonably good programmer to look at this system and determine that it is properly tabulating the ballots," Mattox said. [42]

- 1986, Atlanta, Georgia — The wrong candidate was declared the winner. Incumbent Democrat Donn Peevy was running for state senator in District 48, which straddled Barrow and Gwinnett counties. The machines said he lost the election. After an investigation revealed that a Republican elections official had kept uncounted ballots in the trunk of his car, officials also admitted that a computerized voting program had miscounted. Peevy insisted on a recount. "When the count finished around 1 a.m., they [the elections board] walked into a room and shut the door," recalls Peevy. "When they came out, they said, 'Mr. Peevy, you won.' That was it. They never apologized. They never explained." [43]

- November 1988, Hillsborough, Broward and Dade counties, Florida — A dropoff was observed in Senate votes from the previous general election, but only in counties that used computerized vote-counting machines. Counties without computerized vote-counting showed a 1% dropoff, while counties with computerized voting showed a dropoff of 8%. "Something stands out there like a sore thumb," said Michael Hamby, executive director of the Florida Democratic Party. [44]

- November 1989, Lima, Ohio — Representatives of Sequoia Pacific, makers of the voting machine software for Lima, failed to appear as requested, and election results were delayed until someone could work out the programming error and recount the votes. Nobody was quite sure how many races were affected, but the mayoral race and the school board races were in question for nearly a week after the election. [45]

- November 1990, Seattle, Washington — Worse than the butterfly ballot, some Democratic candidates watched votes alight, then flutter away. Democrat Al Williams saw 90 votes wander off his tally between election night and the following day, though no new counting had been done. At the same time, his opponent, Republican Tom Tangen, gained 32 votes. At one point several hundred ballots added to returns didn't result in any increase in the number of votes. But elsewhere, the number of votes added exceeded the number of additional ballots counted. A Republican candidate achieved an amazing surge in his absen-

tee percentage for no apparent reason. And no one seemed to notice (until a determined Democratic candidate started demanding an answer) that the machines simply forgot to count 14,000 votes.

Incorrect programming caused machines to count ballots cast without counting any of the votes on the ballots. The miscounts were sporadic and thus hard to spot, and the errors disproportionately favored just one party. King County's election manager recommended a countywide recount. [46]

- 1994, New Orleans, Louisiana — Voting machine tests performed and videotaped by candidate Susan Barnecker demonstrated that votes she cast for herself were electronically recorded for her opponent. This test was repeated several times with the same result. (The video footage of this incident can be seen in Dan Hopsicker's documentary video *The Big Fix, 2000*, Mad Cow Productions). [47]

- November 1996, Bergen County, New Jersey — Democrats told Bergen County Clerk Kathleen Donovan to come up with a better explanation for mysterious swings in vote totals. Donovan blamed voting computers for conflicting tallies that rose and fell by 8,000 or 9,000 votes. The swings perplexed candidates of both parties. For example, the Republican incumbent, Anthony Cassano, had won by about 7,000 votes as of the day after the election but his lead evaporated later. One candidate actually lost 1,600 votes during the counting. "How could something like that possibly happen?" asked Michael Guarino, Cassano's Democratic challenger. "Something is screwed up here." [48]

- November 1996, Thurston County, Washington — An inexplicably large number of people went to the polls but did not vote in the hot House contest. A whopping 11.5% of Thurston County voters ignored the congressional race — nearly twice as many no-votes as other races in Thurston county and twice as many no-votes as other counties had. Bob Van Schoorl, Thurston County's chief deputy auditor, said, "We have absolute confidence our machine is counting appropriately." J.R. Baker, Democratic challenger Brian Baird's campaign was not satisfied. "They have not gone through any special testing to see if their machines are adequately counting the votes. Perhaps they need to do sample hand counts of precincts and compare them with the machine." [49]

• November 1996, Guadalupe County, Texas — Officials discovered a voting computer counted more votes in the presidential election than the number of ballots cast. Guadalupe County Elections Administrator J.R. Perez said the problem was with new software for the county's Business Records Corp. Eagle vote-counting system. Perez said a problem was identified with the software before the election, and he thought it was fixed. "I had no reason to believe the system was not tabulating right," Perez said. [50]

• July 1996, Clark County, Nevada — According to a Las Vegas Review-Journal article, a technician removed thousands of files from the tabulation sector of the program during the vote count "to speed up the reading of the count." Reconfiguring a computer program that affects the tabulation of votes is prohibited without prior state verification. [51]

• December 1997, Akron, Ohio — Scrambled votes: Ed Repp won the election — no, cancel that, a software programming error was discovered — Repp actually lost. (Look, twins!) Another error in the same election resulted in incorrect vote totals for the Portage County Board election. (Make that triplets!) Turns out the bond referendum results were wrong, too. [52]

• August 1997, Oklahoma — Computers gave the election to the wrong candidates, twice. The private company hired to handle the election for the Seminole Nation announced results for tribal chief and assistant chief, then decided that their computer had counted the absentee ballots twice, so they posted a second set of results. Tribal officials then counted the votes by hand, producing yet a third, and this time official, set of results. Each set of results had a different set of candidates moving on to the runoff election. [53]

• Tucson, Arizona —

1984 - 826 legitimate ballots were discarded in Oro Valley because of a computer error. The error wasn't discovered until after the deadline for counting them.

1996 - Software programming error mixed up the votes cast for two Republican Supervisor candidates.

1997 - More than 8,300 votes in the City Council race were initially left uncounted because of defective punch-card ballots, which were provided by the voting machine company.

1997 - The city had to hand-count 79,000 votes because of a manufacturing defect in the ballots, provided by the voting machine company.

1998 - 9,675 votes were missed in the tabulation. After canvassing, officials realized that no votes had been recorded for 24 precincts even though voter rolls indicated thousands had voted at those polling places. Global Elections Systems tried to figure out why the computer failed to record the votes. [54]

A breathtaking number of snafus caused candidates to liken the election to the movie "Groundhog Day," with every day starting all over...

• November 1998, Clearwater, Florida — The voting computer crashed on election night. Republicans who lost complained that the crash could have corrupted files, skewed data or lost votes. Tom McKeon, a county commissioner candidate, said "There's no guarantee the votes went to the right candidate." Elections Supervisor Dot Ruggles said it was not the first time such a crash had occurred. [55]

• November 1998, Franklin County, Ohio — One candidate was incorrectly credited with 14,967 votes; another received 6,889 in error. Deborah Pryce and John R. Kasich gained 13,427 votes and 9,784 votes, respectively, after election officials hand-checked vote totals in 371 machines that were affected by a software programming error. A spokesman for Danaher Corp., which supplies electronic voting machines to the county, told the board that such a problem had never before happened in Franklin County. No one caught the error while downloading the data into voting machine memory cartridges, which record the actual vote on Election Day. [56]

• November 1998, Washoe County, Nevada — A breathtaking number of snafus in the Washoe County registrar's office caused candidates in Reno to liken the election to the movie *Groundhog Day*, a movie in which the lead character relives the same day over and over again. Count votes. Computer failure. Go to court. Recount the votes. Software error. Back to court. Start over counting, and so on. [57]

• December 1998, Canada — What was billed as a historic first for the Canadian Wheat Board turned into an embarrassment as a software programming error threw the election results into question. The firm hired to count the ballots an-

nounced that it had detected a flaw in the computer program that tabulated results for the agency's first-ever board of directors. [58]

- September 1998, Kansas City, Kansas — Republican John Bacon, a staunch conservative, celebrated a resounding victory for the 3rd District Kansas Board of Education seat, defeating moderate Republican Dan Neuenswander by 3,018 votes. Two weeks later Neuenswander learned that the race was virtually dead even with the margin of loss being a mere 24 votes. No one offered any explanation for the descrepancy.[59]

- August 1998, Memphis, Tennessee — In the governor's race, a software programming error in Shelby County began crediting votes to the wrong candidates. Computer cartridges containing 295 individual precinct results were taken to a central location because the scanner couldn't read the cartridges. The system that was shut down had posted the incorrect results to newsrooms across the city that had computer links to the data. At least one television station broadcast the bogus results. Which brings up a question: Why were newspaper and TV hooked directly up to computerized voting machines? [60]

- November 1998, Chicago, Illinois — One hundred eight of 403 precincts were not counted. A pin from the cable connecting the ballot reader to the counting computer apparently got bent after three-fourths of the precincts had been counted correctly. No one could explain how a pin inside a cable became bent during the middle of the count. Democrats requested a full recount; a judge disallowed it. [61]

- November 1998, Honolulu, Hawaii — A state senate investigation was conducted into the 1998 election and the malfunction of ballot-counting machines in seven precincts at once. ES&S acknowledged the error and paid more than $250,000 for the recount, in which the biggest expense was hand counting, Vice President Todd Urosevich said. ES&S financial officer Richard Jablonski said ES&S would have saved a lot of money if it had been permitted to just do a machine recount, giving voice to a financial incentive for voting machine companies to get rid of the paper trail. [62]

- November 1999, Norfolk, Virginia — Machines showed totals of zero even though votes had been cast. Edward O'Neal, vice chairman of the Norfolk Electoral Board, attributed the discrepancy to incorrectly programmed computer chips: "Somehow, they lost their ability to count the votes," he said. [63]

- April 1999, Port Washington, Wisconsin — A new computer system gave the wrong election results to news media. The initial results showed that Renea Krueger had won the election for town clerk. In reality, Susan Westerbeke won the election. "Nothing is wrong with the computer. The final printout gave the correct results," said Harold Dobberpuhl, Ozaukee County Clerk. The system receives information from a modem but also requires some manual entry. The error occurred when the person inputting the information simply dropped the digit "2."[64]

- November 1999, Onondaga County, New York — Computers gave the election to the wrong candidate, then gave it back. Bob Faulkner, a political newcomer, went to bed on election night confident he had helped complete a Republican sweep of three open council seats. But after Onondaga County Board of Elections staffers re-checked the totals, Faulkner had lost to Democratic incumbent Elaine Lytel. Just a few hours later, election officials discovered a software programming error had given too many absentee ballot votes to Lytel. Faulkner took the lead.[65]

- March 2000, Shelby County, Tennessee — Computer problems halted the voting at all 19 of Shelby County's early-voting sites during the 2000 Republican presidential primary, forcing officials to use paper ballots (supposed to be provided by the voting machine company as a backup, but for some reason they were unavailable when they were needed). Election officials had to make voters wait in line or tell them to come back later. Because early voting turnout in this election was six times normal, this snafu affected about 13,000 voters. If there was a beneficiary of the problem, it likely was George W. Bush, who needed to defeat John McCain in Tennessee: Shelby County, which contains the urban Memphis population, usually votes less conservatively than the rest of the state.[66]

- November 2000, Arapahoe County, Colorado — Officials agreed to reconfigure the vote-reading machines for a recount because they had been set wrong and therefore did not read all of the votes. Because Democrats wanted the additional recounts, they had to pay the bill, which came to about $11,000.[67]

- November 2000, Denver County, Colorado — Electronic cartridges from four voting machines malfunctioned and voting officials mistakenly assumed those machines were not used, but there were 300 votes on the machines.[68]

• Crozet, Virginia (anecdotal report from a voter) — "When I pushed the button beside 'No' the machine registered my vote as a 'Yes.' I tried this a couple of more times and got the same result. Finally, I poked my head outside the curtain and asked the "attendant" what I should do... whenever I made my choice, the opposite choice lit up. He suggested then that I should intentionally push the wrong button..." [68b]

• November 2000, Volusia County, Florida — A clerk in one precinct could not reach election headquarters to report that the computer had shut down, so the clerk turned the computer off, then turned it back on, accidentally erasing 320 votes. This was discovered only when workers counted all ballots by hand. Election supervisors across Florida say the phone clog happens during most presidential elections, but few people notice. [69]

• November 2000, Davidson County, North Carolina — A computer error allowed election software to count about 5,000 early and absentee ballots twice. A reporter brought the discrepancy to light during the county election board's official canvass. The incorrect vote totals appeared only on the official report sent to the state Board of Elections in Raleigh. Vote totals listed on the Davidson County Web site were correct. [70]

• November 2000, Glenwood Springs, Colorado — At a special city council meeting held just after the election, Mayor Skramstad announced that the Garfield County Clerk and Recorder asked that he read a press release. It stated, "The Garfield County Clerk and Recorder wishes to inform the public that she is continuing to experience difficulty with the ES&S Inc. software utilized for tabulating election results. I will receive a corrected computer chip this evening. On Friday, November 10th…my office will utilize a new chip to count the ballots for Precinct 20 and re-tabulate the results…I anticipate this process will take most of the day. Thank you for your patience during this process." Signed Mildred Alsdorf. [71]

whenever I made my choice, the opposite choice lit up. He suggested then that I should intentionally push the wrong button...

• November 2000, San Francisco, California — In polling place 2214, machines counted 416 ballots, but there were only 362 signatures in

the roster and the secretary of state found only 357 paper ballots. [72]

• February 2000, Manatee, Florida — A power surge was reported to be the cause of incorrect computerized vote tallies. A hand count was performed. And because the hand count showed that a candidate lost by just two votes, another hand count was done. All results, including two hand counts, were completed within 48 hours. [73]

...internal checks revealed that the system had under- and over-reported hundreds of votes. The voting machines worked fine, they just tabulated wrong. "The machines performed terrifically," said Robert J. Urosevich, president of Diebold Election Systems. "The anomaly showed up on the reporting part."

• November 2000, Albuquerque, New Mexico — A software programming error in New Mexico led officials to withhold about 60,000 ballots from their vote count. According to an AP wire service report: "Their (voting) machines have a problem in the database," elections bureau director Denise Lamb said, "and they can't count any of the straight-party ballots." [74]

• November 2000, Allegheny County, Pennsylvania — City Councilwoman Valerie McDonald reported that machines in Pittsburgh's 12th and 13th wards and other predominantly black neighborhoods malfunctioned on Election Day. They began smoking and spitting out jammed and crumpled paper. Poll workers felt the machines had been intentionally programmed incorrectly and had been sabotaged. Whether or not it was sabotage, what is clear is that the spit-and-polish image so carefully crafted in election company press releases didn't seem to apply to the African-American precincts that day. Poll workers in the 12th and 13th wards waited hours for repair, and voters who couldn't spend the day at the polling place were rendered politically voiceless. [75]

• February 2000, Passaic, New Jersey — About 75 percent of the voting machines in the city of Passaic failed to work when the polls opened on Election Day, forcing an undetermined number of voters to use paper ballots during the morning hours. Independent consultant, V. Thomas Mattia, a Philadelphia voting machine supervisor who later examined the machines concluded the problem was due to sabotage, which led a Democratic candidate to refer the matter to the FBI.

Mattia later reversed himself. "I believe that it was an oversight, and there was no fraud involved," Mattia stated in the letter. Freeholder James Gallagher, who had referred the matter to the FBI based on Mattia's previous suspicions, said that he was surprised by the reversal, and needed more information about why the expert changed his mind. [76]

- November 2001, Buffalo, New York — The poll book and tally sheet show 96 Republicans signed in to vote at the polling place in Ohio Elementary School, but when the machine was checked, it tallied 121 votes for mayor: 74 for David Burgio and 47 for Mary Kabasakalian.[77]

- April 2002, Johnson County, Kansas — Johnson County's new Diebold touch screen machines, proclaimed a success on election night, did not work as well as originally believed. Incorrect vote totals were discovered in six races, three of them contested, leaving county election officials scrambling to make sure the unofficial results were accurate. Johnson County Election Commissioner Connie Schmidt said that internal checks revealed that the system had under- and over-reported hundreds of votes. Schmidt said the voting machines worked fine, they just tabulated wrong. "The machines performed terrifically," said Robert J. Urosevich, president of Diebold Election Systems. "The anomaly showed up on the reporting part."

  The problem, however, was so perplexing that Schmidt asked the Board of Canvassers to order a hand re-count to make sure the results were accurate. Unfortunately, the touch screen machines did away with the ballots, so the only way to do a hand recount is to have the machine print its internal data page by page. Diebold tried to re-create the error in hopes of correcting it. "I wish I had an answer," Urosevich said. In some cases, vote totals changed dramatically.[78]

- November 2002, Palm Beach, Florida — A Florida woman, a former news reporter, discovered that votes were being tabulated in 644 Palm Beach precincts, but only 643 precincts have any eligible voters. An earlier court case in Florida found the same discrepancy, and the reason for it was never satisfactorily explained.[79]

- November 2002, New Jersey — A reporter in New Jersey observed 104 precincts with votes in an area that has only 102 precincts. "Ghost precincts," no matter what

the official explanation, do not provide the transparent accounting needed to protect voting integrity."[79]

- November 2002, Comal County, Texas — A Texas-sized lack of curiosity about discrepancies: The uncanny coincidence of three winning Republican candidates in a row tallying up exactly 18,181 votes each was called weird, but apparently no one thought it was weird enough to audit.[80]

- March 2002, Palm Beach County, Florida — Touch screen machines sometimes froze up when voters selected which language to use. Phil Foster from Sequoia Voting Systems said that was a software programming error. Elections Supervisor Theresa LePore also said she heard that some people touched one candidate's circle on the screen, only to see an X appear by another candidate's name. [81]

- August 2002, Clay County Kansas — A squeaker — no, a landslide — oops, we reversed the totals — and about those absentee votes, make that 72-19, not 44-47. Software programming errors, sorry. Oh, and reverse that election, we announced the wrong winner — The machines said Jerry Mayo ran a close race in the county commissioner primary but lost, garnering 48 percent of the vote, but a hand recount revealed Mayo won by a landslide, earning 76 percent of the vote. [82]

- November 2002, Adams County, Nebraska — Adams County Election Commissioner Chris Lewis says she will be meeting with representatives of ES&S to further discuss "what went wrong" on November 5th. During the General Election, Adams County was the last in Nebraska to have election results, due to both machine and software glitches. ES&S has talked about some compensation for the election problems including paying for election worker overtime and not charging for programming adjustments. The board went into executive session to discuss their options, including seeking a refund from ES&S. Lewis said, "no one wants a lawsuit." [83]

- November 2002, Dallas, Texas — When 18 machines were pulled out of action in Dallas because they registered Republican when voters pushed Democrat, Judge Karen Johnson, a Republican, quashed an effort to investigate the accuracy of the tally. [84]

- November 2002, Scurry County, Texas — Scurry County poll workers got suspicious about a landslide victory for two Republican commissioner candidates.

They had a new computer chip flown in and also counted the votes by hand — and found out that Democrats actually won by wide margins, overturning the election.[85]

Same tallies, same county:
18181
18181
18181

• November 2002, Miami, Florida — Fuzzy math in Miami: On November 10, the *Miami Herald* listed the following figures for the total votes cast at the Democrat-friendly Broward County Century Village precinct in the general election:

1994: 7,515
1998: 10,947
2002: 4,179

Yet an accountant called Century Village and was told that their occupancy has remained stable (around 13,000 residents) since the complex hit capacity in 1998. [86]

• March 2002, Medley, Florida — Voting machines gave the town council election to the wrong candidate. The cause was attributed to a software programming error by a voting machine technician. County Elections Supervisor David Leahy said he was concerned because the computer did not raise any red flags, and humans had to spot the error.[87]

• November 2002, Baldwin County, Alabama — No one at ES&S can explain the mystery votes that changed after polling places had closed, flipping the election from the Democratic winner to a Republican in the Alabama governor's race. "Something happened. I don't have enough intelligence to say exactly what," said Mark Kelley of ES&S. Baldwin County results showed that Democrat Don Siegelman earned enough votes to win the state of Alabama. All the observers went home. The next morning, however, 6,300 of Siegelman's votes had disappeared, and the election was handed to Republican Bob Riley. A recount was requested but denied. [88]

• November 2002, North Carolina — Computer misprogramming overturned the House District 11 result in Wayne County. A mistake in the computer program caused vote-counting machines to skip over several thousand party-line votes,

both Republican and Democratic. Fixing the error turned up 5,500 more votes and reversed the election for state representative. [89]

- November 2002, Monterey, California — California machines that can't add: The problem in Monterey, California, was that the department's mainframe computers refused to add the results of early absentee votes and those cast on touch-screen computers prior to Election Day. "We didn't have any problems whatsoever during our pre-election tests," said the elections official. [90]

- November 2002, Gretna, Nebraska — This crushing defeat never happened: Vote-counting machines failed to tally "yes" votes on the Gretna school-bond issue, giving the false impression that the measure failed miserably. The measure actually passed by a 2-1 margin. Responsibility for the errors was attributed to ES&S, the Omaha company that provided the ballots and the machines. [91]

- November 2002, South Carolina — A software programming error caused more than 21,000 votes in the squeaker-tight race for S.C. commissioner of agriculture to be uncounted, an error margin of 55 percent. Only a hand-count was able to sort it out. Good thing there were paper ballots. [92]

- November 2002, Taos, New Mexico — Software programming error caused machine to count the wrong names: In Taos, New Mexico, just 25 votes separated the candidates in one race; another race had a 79-vote margin. After noticing that the computer was counting votes under the wrong names, Taos County Clerk Jeannette Rael contacted the programmer of the optical machine and was told it was a programming error. [93]

- November 2002, Pennsylvania — One hundred percent error tabulating Libertarian votes: In Pennsylvania, a voter reported that he had followed his conscience and voted Libertarian. When he reviewed the results for his precinct, though, the Libertarian candidate received zero votes. Two ways to look at this: Unimportant, just a vote; or, a 100 percent error. Either way, why bother to vote? [94]

- November 2002, New York — Voting machine tallies impounded in New York: Software programming errors hampered and confused the vote tally on election night and most of the next day, causing elections officials to pull the plug on the

vote-reporting Web site. Commissioners ordered that the voting machine tallies be impounded, and they were guarded overnight by a Monroe County deputy sheriff. [95]

• November 2002, Tangipahoa Parish, Louisiana — "I can't say every precinct had a problem, but the vast majority did" — Tangipahoa Parish, Louisiana, Clerk of Court John Dahmer said at least 20 percent of the machines in his parish malfunctioned. "One percent might be acceptable, but we're not even close to that," Dahmer said. He said 15 employees worked to combat the malfunctions. [96]

• November 2002, Maryland — Vote Republican (read "Democrat") — In Maryland, a software programming error on Diebold touch screen machines upset a lot of voters when they saw a banner announcing "Democrat" at the top of their screen, no matter whom they voted for. [97]

• November 2002, New Jersey — Forty-four of forty-six machines malfunctioned in Cherry Hill, New Jersey: Election workers had to turn away up to 100 early voters when it was discovered that 96 percent of the voting machines couldn't register votes for mayor, despite the machines' having been pre-tested and certified for use. [98]

• November 2002, North Carolina — Trying to find 300 voters so they can vote again: In Wake County, North Carolina, one out of four new touch-screen voting machines failed in early voting, losing 294 votes. The machines were shut down before Election Day, so election workers looked for the 294 voters to ask them to vote again. (A paper trail would have solved this problem.) [99]

• November 2002, Florida — Bill McBride was a tough guy to vote for: One voter said that he tried 10 times, and every time he pressed McBride the Jeb Bush choice lit up. He could only get his vote to light up the McBride choice when he pressed a dead area of the screen. No paper trail was available, so no one really knows who got any of the votes — regardless of which candidate lit up. Similar problems were reported in

Trying to find 300 voters so they can vote again (a paper trail would have solved this problem)...

various permutations, for various candidates, by several Florida voters, and an identical problem was noted in Texas. [100]

When all else fails, use duct tape (that was the only way it would feed the votes through)

- November 2002, New Jersey — "What the hell do I do with this?" A bag full of something that looked like rolls of cash register tapes was handed to the Mays Landing County Clerk. A computer "irregularity" in a New Jersey vote-counting system caused three of five relay stations to fail, leaving a single county clerk holding the bag for a hand count. [101]

- November 2002, Ascension Parish, Louisiana — An elections official gnashed his teeth as more than 200 machine malfunctions were called in. The Parish Clerk said his staff was on the road repairing machines from 5 a.m. to 9 p.m. In one case, a machine wasn't repaired until 12:30 a.m. Wednesday. "A mechanic would fix a machine, and before he could get back to the office, it would shut down again," Bourque said. [102]

- November 2002, Sarpy County, Nebraska — A call-in report I received on election day reported that in Sarpy County, Nebraska, they had to use duct tape to stick something under the machine — that's the only way it would feed votes through. [103]

- November 2002, St. Bernard Parish, Louisiana — All the king's horses and all the king's men…couldn't put the tally together again: With a 34-vote margin separating the two justice of the peace candidates in St. Bernard Parish, the machine ate 35 absentee votes and left everyone guessing about the outcome of the race. The ballots became inaccessible when the system locked up; even the technician couldn't get at them. [104]

- November 2002, Georgia — In one Georgia county, ballots in at least three precincts listed the wrong county commission races. Officials shut down the polls to fix the problem but didn't know how many wrong ballots were cast or how to correct errant votes. In another, a county commission race was omitted from a ballot. Cards voters needed to access machines malfunctioned. Machines froze up and dozens were misprogrammed. [105]

• November 2002, Ohio — A vote-counting machine malfunctioned with 12 of Crawford County's 67 precincts left to count. A back-up vote-counting machine was found, but it also could not read the vote. Election workers piled into a car and headed to another county to tally their votes. [106]

• November 2002, Pickens County, South Carolina — Two South Carolina precincts worked to extract information from the computer: Pickens County was unable to get totals from two precincts because of computer glitches. [107]

• November 2002, Georgia — Election officials lost their memory: Fulton County election officials said that memory cards from 67 electronic voting machines had been misplaced, so ballots cast on those machines were left out of previously announced vote totals. No hand count can shine any light on this; the entire state of Georgia went to touch-screen machines with no physical record of the vote. Fifty-six cards, containing 2,180 ballots, were located, but 11 memory cards still were missing two days after the election: Bibb County and Glynn County each had one card missing after the initial vote count. When DeKalb County election officials went home early Wednesday morning, they were missing 10 cards. [108]

• November 2002, Nebraska — U.S. Senate Candidate's ballot was pre-voted for his opponent: Charlie Matulka, the Democratic candidate for U.S. Senate in Nebraska, arrived at the polls to vote for himself. When he looked at the optical scan ballot he was given, he discovered it had already been filled out — for his opponent, Chuck Hagel, giving Nebraska the most newfangled voting of all — not just electronic voting, but *automatic* voting! [109]

• November 2002, Marina del Rey, California — In posh Marina del Rey, California, one precinct had no voting booths, the voting machine was broken, voters couldn't get their cards into one machine, and someone broke the puncher out of the machine. So voters were told to vote in public. [110]

• November 2002, Nebraska — Candidate for governor finds vote-counting computer asleep: Paul Rosberg, the Nebraska Party candidate for governor, eagerly took advantage of a Nebraska law that lets candidates watch their votes being counted. He first was invited to watch an optical scanner machine, which had no counter on it, and then was taken into the private room, where he was al-

lowed to watch a computer on a table with a blank screen. So much for public counting of votes. [111]

- February 2003, Everett, Washington —If there was any doubt that Republicans were right to ask for a recount of some Snohomish County absentee ballots from November's general election, it was erased by one sobering number: 21.5 percent of the ballots cast in 28 selected precincts were not counted. The Snohomish County Auditor's Office recounted 116,837 absentee ballots Thursday after county officials discovered that the optical scan ballot-counting machines had miscounted. The cause was attributed to a faulty "read head" on each of two optical scanner machines, causing them to fail to read ballots with blue ink. The machines had passed the test on blue ink before the election. The Sequoia representative could not recall that the read head problem had ever happened before.

  When asked how many machines of the same make and model number Sequoia has in the United States, she said "about 1,500." When asked how many years they'd been in use, she said about six years. "Why, then," asked a citizen, "would this unheard-of problem happen at exactly the same time in exactly the same place on two different machines at once?" The Sequoia rep said she had no idea.[112]

* * * *

Phew! Had enough? Well, while you are resting from marathon of error, consider these points:

1) "Logic & Accuracy" tests did not prevent these problems.

2) It doesn't matter if the miscounts were accidental or intentional, the results were the same: Citizen's votes were not counted as cast.

3) The information on these preceding pages is the result of only a few hours research. Space constraints prohibited me from devoting more pages to this topic. Suffice it to say, I only scratched the surface of the voting machine Encyclopedia Errata.

Chapter 2 footnotes

1 – *The Omaha World-Herald* , 15 June 1990; “Vote Confusion Blamed on Human Error”
2 – Company press release: PR Newswire 12 September 2002; “Diebold Touch-Screen Voting Terminals Perform Well in Primary Elections”
3 – *The Omaha World-Herald*, 21 April 1992; “Omaha Firm Taps North Platte Native”
4 – *The Wall Street Journal* , 17 November 2000; “Fuzzy Numbers: Election Snafus Went Far Beyond... ”
5 – Associated Press, in the *Dallas Morning News*, 13 April 1996; “Vote tally miscounted in runoff...”
6 – *The Arizona Daily Star* , 8 December 1994; “826 votes vanish in Oro Valley precinct...”
7 – *All Africa*, 11 November 2002; “US Polls Plagued With Glitches”...‘While the American government has been too quick to attack most Zimbabwean elections won by the ruling Zanu-PF party, its own polls continue to be marred...’; Also reported in *The Washington Times*, 6 November 2002; “Glitches cited at some polls...”
8 – *Honolulu Star Bulletin*, 3 February 1999; “Voting checks failed to detect fault twice; A flawed ballot counter passed a manual check and a mechanical test”
9 – *The Dallas Morning News*, 11 November 1998; “Election system company apologizes, offers partial refund Fixes proposed for problems that led to undercounts” (related articles Nov. 5 and 28)
10 – *Honolulu Star Bulletin*, 6/7/2000; “Firm admits errors in counting votes for Hawaii, Venezuela”
11 – *The Arizona Daily Star*, 11 Nov. 1998; “Computer fails to record 9,675 Pima County votes”
12 – *Chicago Tribune*, 4 April 2003; “Returns are in: Software goofed Lake County tally misled...”
13 – *The Post-Standard*, 5 Dec. 2002; "More Florida Blunders; Precious Votes Should Be Counted”
14 – *Newsbytes News Network*, 24 April 1998; “Feature - Glitches Of The Week”
15 – *Chicago Tribune*, 4 April 2003; “Returns are in: Software goofed...”
16 – *Chicago Tribune* , 6 November 1993; “Kane Election Results Just Didn’t Compute”
17 – *Albuquerque Journal*, 19 November 2002; “County Certifies Vote Tally”
18 – Notes on “Workshop” on Voting Machine Security for Santa Clara County Supervisors, 11 Feb. 2003; see http://verify.stanford.edu/dill/EVOTE/sc-2-11-2003.html
19 – *The Everett Herald*, 20 Jan. 2003; “County to Discuss Ballot-Counting Foul-up”
20 – *The Seattle Times*, 22 November 1990; “Thousand of Lost Votes Turn Up in Recount”
21 – *The Dallas Morning News* , 6 November 1998; “Computer glitch led to omitted votes”
22 – *The Tampa Tribune*, 2 May 1997; “Grand jury probes contested election”
23 – *Newsbytes News Network*, 4 June 1999; “Glitches of the Week”
24 – *The Knoxville News-Sentinel*, 8 November 1996; A betrayal of voters; “Disaster over early votes on unification demands action”
25 – *The Herald*, Rock Hill, SC , 25 October 2001; “The city election foul-up”
26 – *The Bradenton Herald*, 17 September 2002; “Sometimes the old ways are best”
27 – *The Atlanta Journal; The Atlanta Constitution*, 23 July 1998; “Election ’98 - Cobb glitch delayed tabulations statewide”
28 – *Orlando Sentinel*, 7 October 2001; “Election Goal: Low Profile, Changes Aim to Keep Day Fiasco-Free”
29 – NPR: *Morning Edition*, 6 November 2002; “Analysis: Senate races in Minnesota and South Dakota”
30 – *Wall Street Journal* , 17 November 2000; “Fuzzy Numbers: Election Snafus... ”

31 – *Daniel B. Spillane vs. VoteHere Inc*., filed in King County, Washington case # 03-2-18799-8SFA
32 – *The Las Vegas Review-Journal*, 19 July 1998; "The Clark County vote: How secure is it?"
33 – *Houston Chronicle*, 16 March 2002; "Candidate zeroes in on computer glitch"
34 – *The Commercial Appeal*, 7 August 1998; "Vote Totals..."
35 – *Newsbytes News Network*, 20 March 1998; "Feature - Glitches of the Week"
36 – *The Daily Oklahoman* , 6 November 1996; "Big Computer Glitch Causes Election Hitch"
37 – *The Baltimore Sun*, 4 November 1999, "Manufacturer of voting system assumes blame for Baltimore's Election Day glitch; Failure to test software resulted in breakdown, delays in vote"
38 – *The Salt Lake Tribune*, 25 June 1998; "Commission Primary Recount..."
39 – Caltech/MIT Voting Technology Project, July 2001; www.vote.caltech.edu/
40 – *The Virginian-Pilot and The Ledger-Star*, 25 August 1997; "Warner Doggedly Pursues Divisive Election Inquiry"
41 – *The Las Vegas Review-Journal*, 30 November 1994; "Voter fraud allegations continue"
42 – *The Dallas Morning News*, 24 September 1986; "Dallas Officials Deny Election Fraud Claim
43 – *The Atlanta Journal - The Atlanta Constitution*, 3 September 1998; "Elections Board Case: Candidate's lawyer knows the feeling"
44 – *Atlanta Journal; Atlanta Constitution*, 11 November 1988; "Thin Lead Allows Mack to Proclaim Victory in Senate Race"
45 – *The Plain Dealer*, 10 November 1989; "Tally mix-up still under investigation"
46 – *Seattle Post-Intelligencer*, 20 November 1990; "Recount of All Election Returns Recommended"
47 – The Las Vegas Review-Journal, 19 July 1998; "The Clark County vote: How secure is it?" and *The Big Fix, 2000*, Video by Dan Hopsicker, Mad Cow Productions
48 – *The Record*, 16 November 1996; "Bergen County Paper Ballots Finally Counted..."
49 – *Seattle Post-Intelligencer*, 16 November 1996; "Democrats Seek Recount in 3rd District - Thurston County in Question.
50 – *San Antonio Express-News*, 8 November 1996; "Computer glitch skews Guadalupe vote results"
51 – *The Las Vegas Review-Journal*, 19 July 1998; "The Clark County vote: How secure is it?"
52 – *Newsbytes News Network*, 9 December 1997; "Feature - Glitches of the Week"
53 – *Newsbytes News Network*, 5 August 1997; "Glitches of the Week
54 – *The Arizona Daily Star*, 20 November 2001; "Year-old Votes Discovered in City Precinct Box"
55 – *The Tampa Tribune*, 6 November 1998; "Computer crash leads to countywide recount of votes"
56 – *The Columbus Dispatch*, 8 December 1998; Tallies from November Election Change..."
57 – *The Las Vegas Review-Journal*, 12 November 1998; "Washoe's nightmare"
58 – *Winnipeg Free Press*, 9 December 1998; "Glitch forces recounts in CWB vote"
59 – *The Kansas City Star*, 19 August 1998; "Ballot tally change 3,000-vote error..."
60 – *The Commercial Appeal* , 7 August 1998; "Computer Glitch Delays Final Vote Total..."
61 – *Chicago Daily Herald*, 6 November 1998; "Computer glitch leads to vote error"
62 – *Honolulu Star Bulletin*, 10 Marchl 1999; "Vote Recount to Cost $250,000" http://starbulletin.com/1999/03/10/news/story9.html
63 – *The Virginian-Pilot and The Ledger-Star*, 3 November 1999; "Tallying-machine malfunction leads to Norfolk Recount"
64 – *Newsbytes News Network*, 22 April 1999; "Glitches of the Week"
65 – *The Post-Standard*, 4 November 1999; "Faulkner Outlasts Vote-Counting Glitch..."
66 – *The Commercial Appeal*, 5 March 2000; "Computer Glitch Hampers Voting ..."
67 – *Denver Post*, 29 November 2000; "Recount confirms Polis won seat..."

68 – *Denver Post*, 28 November 2000; "Recount adds 300 'lost' votes"
68b – *The George Loper Home Page*, letter to the editor, 30 November 2000; "Voting Irregularities in Crozet, Virginia." http://loper.org/~george/archives/2000/Nov/30.html
69 – *St. Petersburg Times*, 17 November 2000; "Busy signals taunt clerks at precincts"
70 – *Greensboro News & Record*, 15 November 2000; "Davidson Computer Glitch Doubled Votes..."
71 – Minutes of City of Glenwood Springs Special City Council Meeting Nov. 9, 2000
72 – *The San Francisco Chronicle*, 11 February 2002; "2000 election finds work was sloppy"
73 – *Sarasota Herald-Tribune*, 10 February 2000; "Election recount makes no change"
74 – AP Online, 8 November 2000; "Ballots Withheld in New Mexico"
75 – *Pittsburgh Post-Gazette*, 4 May 2001, "Hearing Gets Landslide of Voting Problems"
76 – *The Record*, 23 February 2000; "Expert Finds No Sabotage in Election, Reverses Stance..."
77 – *Buffalo News*, 18 October 2001; "Voting Snafu Won't Change Mayoral Primary"
78 – *The Kansas City Star* , 5 April 2002; "Election errors unnerve Johnson County official"
79 – Call in reports; Nov 2002 election; See also: Dr. Rebecca Mercuri's work on voting machines, where she has similar reports: www.notablesoftware.com
80 – *Deseret News*, 9 November 2002; "Texans tally triple match in exceptional election"
81 – *The Palm Beach Post*, 14 March 2002; "Human goofs, not machines, drag vote tally into next day"
82 – Associated Press,reported in the *Wichita Eagle*, 22 August 2002; "Mayo won by a landslide... Election reversed..."
83 – *YorkNewsTimes.com*, 20 Dec. 2002; "Omaha election systems firm to pay for county election problems" (also found in meeting minutes)
84 – *The Fort Worth Star-Telegram*, 30 October 2002; "Democrats to appeal voting case ruling"
85 – *Houston Chronicle*, 8 November 2002; "Ballot glitches reverse two election results"
86 – *Miami Herald*, 10 November 2002; and call in report from a Miami accountant
87 – KRTBN Knight-Ridder Tribune Business News: *Miami Herald*, 4 April 2002; "Despite New Voting System, Human Error Mars Medley, Fla., Council Election"
88 – *Mobile Register*, 28 January 2003; "Voting Snafu Answers Elusive"
89 – *The News & Observer* , 9 November 2002; "'Winners' may be losers"
90 – *Monterey Herald*, November 2002
91 – *Omaha World-Herald*, 6 November 2002; "A late night in Sarpy; glitches delay results"
92 – *The Herald*, Rock Hill, SC , 7 November 2002; "Machine glitch keeps votes from being counted"
93 – *Albuquerque Journal*, 7 November 2002; "Taos To Recount Absentee Ballots"
94 – 01 November 2002; Citizen report on the VoteWatch forum: http://pub103.ezboard.com/fsoldiervoicefrm44.showMessage?topicID=1.topic
95 – *Democrat & Chronicle* (Rochester, NY) , 7 November 2002; "John squeaks out victory"
96 – *The Baton Rouge Advocate*, 7 November 2002; Voting machine glitches worrisome..."
97 – *The Washington Times*, 6 November 2002; "Glitches cited at some polls..."
98 – *Newsday*, 06 November 2003; "Voting glitches"
99 – *The News & Observer* Raleigh, NC, 31 October 2002; "Machines lose 294 early votes"
100 – Votewatch citizen reports; http://www.votewatch.us/election_2002_findings.htm
101 – *Newsday*, 06 November 2003; "Voting glitches"
102 – *The Baton Rouge Advocate*, 7 November 2002; Voting machine glitches worrisome..."
103 – Call in reports; Nov 2002 election

104 – *The Times-Picayune*, 7 November 2002; “Machine snag leaves race up in the air ; Trapped absentee ballots delays news of JP winner until today”
105 – AP Online, 5 November 2002; “Glitches Hit High-Tech Voting Systems”

106 – *Telegraph-Forum*, 6 November 2002; “Glitch sends vote count to Richland”
107 – *Associated Press*, 06 November 2002; “Equipment causes voting problems in several counties”
108 – *Atlanta Journal - Constitution*, 8 November 2002; “2002 ELECTION: 2,180 Fulton ballots located after tally 67 memory cards misplaced...”
109 – 06 November 2002; interview with Charlie Matulka, Democratic candidate for U.S. Senate in Nebraska
110 – VoteWatch report, www.votewatch.us
http://pub103.ezboard.com/fsoldiervoicefrm10.showMessage?topicID=3.topic
111 – 07 November 2002; Interview with Paul Rosberg, candidate for Nebraska governor
112 – Citizen meeting in Snohomish County, 23 January 2003

Chapter 3
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris

with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar

3
How Do You Verify Voting Machine Accuracy?

If we solve this problem, the rest of this book is moot. However, before we get to solutions, two things:

1) I keep saying we can't verify the accuracy of these things. What do the voting machine companies have to say about this? How do our politicians explain it? We should at least listen to the company line, so the first part of this chapter will discuss the official explanations.

2) If you are in the high-tech community, you may be just dying to suggest technological solutions. Before you start explaining that cryptography, redundant systems, or a secret pin number are the answer, let me explain: Cryptography doesn't solve the problems either nor does redundancy or a receipt with a pin number.

But don't just take my word for it — We have included a discussion of open source and other technological solutions later in this book.

We put this chapter here, because after reading the little shop of horrors in the previous chapter, you might want to hear some good news. And to cut to the chase: We favor a hybrid system — touch screen machines with a voter-verified paper ballot, with an audit that compares the two against each other.

The official line on voting machine verification:

Indeed, they can't be properly audited, but what you'll hear from the manufacturers is this: "Each machine creates an internal facsimile of each vote, and if there is any question, we can simply print out each vote for a hand recount."

And what about the voter being able to see that his vote was recorded the way he cast it? Well, absolutely, the voter verifies his vote, they tell us. After making his selection for each ballot question, the votes appear on the screen and the voter confirms his choices.

Saying the machine creates an internal facsimile of each vote is just a fancy way of saying that the data in the machine can be printed out one vote at a time. Think of it this way: Suppose you have an address book on your computer, and it lets you print a full page with a single record, or a list of all the records. Now, suppose you have an error in your computer records, and instead of "John Doe," you typed "Joxn Doe." Whether you print his record as a single page, or you print out a list, he will appear both places as the erroneous "Joxn Doe."

If incorrect programming caused the machine to record your vote for Truman as a vote for Dewey, it's not going to help to have the machine print a copy of its own incorrectly recorded vote.

Now let's look at the "voter verified" issue. It's nice that you can review your choices and confirm them. However, what you are looking at is just a screen display. The screen says "Voted for Truman, correct?" — you press "Confirm" — but that does nothing to prove that the software inside the black box instructed the memory card to record your vote correctly.

The solution is simple: All major voting machine manufacturers say they have machines capable of printing ballots. From the beginning, Avante and AccuPoll have provided touch screen machines that print a paper ballot. If the machine prints a ballot that shows your vote: "Truman" but inside the machine, the software interprets your vote as "Dewey," all we have to do is devise a way to compare the paper ballots, which you have independently verified, to the machine counts, and the machine miscount will show up.

Optical scan machines have ballots, but if we don't look at them, we can't say we verified the machine count. Running the ballots through the machine again won't prove anything — if the software is programmed incorrectly, the same error will probably appear when you run it through a second time. Running it through a different machine may not help, either — if both machines use the same software, they might both give you the same error.

Another answer you'll hear is that we don't need to compare the paper ballot, which you have verified, with the machine tally, because the voting system has been so carefully tested. That claim is debunked in the Chapter 5.

Why is comparing the paper trail to the machine count so important?

When you verify the accuracy of a count — points in a beauty pageant, dollars in your bank account, or votes cast in an election, it is called doing an *audit*. So

what, exactly, is an audit? Can we just make up our own rules as we go along? Who has expertise in proper auditing procedures?

Auditing is an accounting function. Proper auditing include the following:

• Independent data sources

• Transparency (meaning the accounting process is transparent to everyone)

• For systems that are part of the public commons, like voting, scrutiny by "many eyes"

Computerized vote-counting systems fail on all of these criteria, but this is easily correctable, if we take appropriate actions.

Comparing two <u>independent</u> data sources

In auditing, you prove one set of data is correct by verifying it against a matching set of data that comes from a different source.

Example - Paying taxes:

Tax authorities require you to keep independent verification.

1) You fill out a report when you file your taxes ("Source 1"). You may keep a computerized record of your deductible expenses and your expenditures, using a program like *Microsoft Money*. ("Source 1a"). Why are these two sources not independent? Because only one person (you) has verified them.

2) You also have independent records, like bank statements (verified by your bank) and receipts (verified by the vendor) ("Source 2").

To do a proper audit, the IRS uses your tally, but backs it up with a document trail that is verified independently, by banks and vendors.

Independent Auditability in Voting:

Punch card and optical scan systems

1) You enter your vote on a punch card or optical scan ballot. This is "source 1"

2) The actual record containing your intent is counted by a software program on a computer. This is "source 2."

3) No one, however, is allowed to look at source 1. We can only look at source 2, the computer tally.

As described above, the vote count is never verified at all. Although we have two independent sources, we refuse to allow anyone to look at a more important source, the voter-verified ballot. Using this system, we cannot know whether the machine is correctly recording our votes.

However, we can easily correct this problem by regularly, thoroughly comparing the computer count with a hand-count of the ballots.

Touch screen, DRE, Internet and vote-by-phone systems

1) You enter your vote into a computer, using a touch screen, keyboard buttons or a wheel. The screen, or the phone system, provides a digital representation of your vote and asks you to confirm it. However, you cannot see your vote actually being recorded. (Source 1)

2) The computer transmits your vote to a second system, creating a redundant record in case the power goes out, or so that people can look at another version of the vote repository. (Source 1a)

3) The computer tallies up the votes that it recorded. (Source 1b)

4) The computer prints a summary of the votes, and the election official uses this summary to represent the physical record of the vote (Source 1c)

5) The computer also can create a facsimile of each vote it has recorded, an individual "ballot" for each vote cast. (Source 1d)

Note that the system just described is not auditable, because it does not keep any record verified by any party independent of the computer.

Asking you to "verify" your vote by saying yes to a computer screen is exactly the same, in terms of data integrity, as asking you to tell an election official your vote, which she then asks you to repeat while never letting you see what she wrote down. That procedure is absurd and would be trusted by no one, yet it is exactly equivalent to the touch screen system.

If the touch screen prints a ballot that you verify, which is saved in a secure ballot box, a proper audit can be done by comparing the machine count (source 1) to the voter-verified ballots (source 2).

Transparency

Proper auditing requires transparency. Just ask an IRS auditor whether you can get by with handing him a shoebox full of indecipherable receipts with no explanation. Not likely. You either have to organize it and explain it clearly, or it gets thrown out.

Transparency somehow evaporated when we privatized our vote-counting system.

Discrepancies they cite are explained away by technicians who are not sworn election officials citing "glitches" in the programming that we cannot see. Sometimes technicians fly in to "replace a chip" (yet we have no idea what's on the chip). In one news account, in which logs showed 48,000 votes cast, but only 36,000 recorded, a technician *e-mailed* the "correct" results for the missing votes, claiming it did not change the outcome, though no one would ever know, because an audit trail didn't exist.

Trust is critical, so transparency is especially important. The Declaration of Independence does not say "Governments are instituted among men, deriving their just powers from the consent of the computer programmers."

No matter how clever the cryptography, no matter how great the open source program is, unless ordinary citizens with no computer expertise can see with their own eyes that votes are being counted accurately, the audit system fails the transparency test.

In a democracy like ours, you don't need to be a lawyer to sit on a jury. You shouldn't need to be a computer programmer to count a vote.

scottxyz
DemocraticUnderground.com

"Many eyes"

The "many eyes" method is a great way to eliminate conspiracy and prove that a system is trustworthy.

Elections are simply no good unless we believe they are accurate. The Soviet Union held elections while under communism, but no one believed they were valid. According the *London Guardian*, Saddam Hussein held elections, too and reported that he had garnered 100 percent of the votes. I assume that no one wants elections like these.

"Many eyes" simply means that we let as many independent parties as possible view the vote-counting. The more eyes on the count, the less room for shenanigans. We do not want a system that only a few software engineers can verify. We require something that you, I, the mailman and our kindly senior citizen volunteers can attest to. "Of the people" does not also say, "as long as they are computer programmers."

I spoke with Christopher Bollyn, a reporter who has written several articles about the erosion in integrity of our voting system as it migrated to computerized counting. He described an election he witnessed in France which illustrates "many eyes" perfectly:

- Voters cast ballots on paper, and when it comes time to count, the room becomes crowded with citizens.
- As many citizens as can fit in the room are allowed to watch the counting. Sworn election officials, some from each party in the election, in front of all the observers, count the ballots into piles of 100.
- Each set of ballots is placed in a bag.
- Then, one bag at a time, the election officials count the ballots, announcing each one.
- They tally up one bag and move to the next, until all are done.
- It takes a relatively short time to count 1,000 votes, and by having many election precincts throughout the country, all of France can be counted in a matter of hours, in front of thousands of eyes.

I think you'll agree that the above system creates very little suspicion about the vote-counting procedure. Compare the trust gained by inviting many eyes, in the above example, with computerized vote-counting systems used in the USA right now:

• Computer programmers, who are not certified election officials, create a software system that will interpret and record the votes.

• The software program then takes its interpretation of the votes and adds them up inside a black box.

• The programming is done at a factory in Nebraska, or Vancouver, Canada, or Texas, or California, but citizens cannot look at the software.

• A copy said to be the program used in actual elections is then shipped to Huntsville, Alabama, where a testing facility examines it, but the tests are a secret and no one is allowed to interview the testing personnel.

• Then the secret code is sent to the secretary of state for each state that authorizes it, but no one really looks at the source code here. The secretary of state keeps the secret code locked in escrow.

• Election officials cannot view the vote recording or tallying because it happens inside a computer.

• Citizens can't see it, candidates can't check it and sometimes the results are wrong.

We don't use proper audit procedures and we don't pass the "many eyes" test, even if our elections are error-free (they are not) or honest (we can't count on that).

You cannot allow a system so fundamental to democracy to become opaque. Such a system will lose the trust of the people it must serve.

Following are suggestions for legislative reform to allow us to verify voting machine accuracy. Each of these suggestions deserves reasonable debate by a group that includes, at a minimum, people with accounting experience, people with programming experience and some ordinary citizens.

Suggestions:

One bill, as of the writing of this book, that holds promise is HR-2239 introduced by congressman Rush Holt. It needs stronger language to make the voter-verified paper ballot the legal representation of our vote, and beefed-up auditing procedures need to follow.

1) Require **voter-verified paper ballot** for all voting machines.

2) We favor a 100% audit of the paper ballots againt the machine count. There are ways to make this cheap and efficient. See *A Modest Proposal* later in the book.

3) If we decide not audit 100% of the precincts, we certainly need to develop robust auditing.

a) Require **spot-check audits** to compare voter-verified totals against voting machine totals. These totals should match exactly for touch screens, and very closely for optical scan machines.

b) **Discretionary audits**:

(1) Allow parties to select a percentage of precincts to audit.

(2) Allow election workers to audit any results deemed unusual.

(3) Allow the media to audit any precinct it deems of interest at their own expense.*

(4) Allow any citizen to audit any precinct, at their own expense.*

*If a significant error is found, the recount cost is born by the governemnt.

c) **Triggered audits** (hand counts)

(1) Insufficient randomness (e.g. three candidates get 18,181 votes; poll book shows voters arrived in alphabetical order; every Republican wins by exactly 3 % of the vote; the results of one machine vary widely from other machines at the same precinct)

(2) Breach of security (e.g. ballot box or memory cards misplaced, unusual time lag between poll closing and delivery of memory cards/ballot boxes to counting location)

(3) Digital signature of software doesn't match the certified version.

(4) Too close to call: Less than 1% spread

4) **Discrepancies** — Expand the audit if the difference between machine count and manual count is excessive, *whether or not the identified discrepancy would overturn the election*. For example, in a normal audit, if you were examining randomly pulled purchase orders, and discovered an anomaly, you would pull

a larger sample of purchase orders. Further discrepancies would trigger an audit of all purchase orders.

Voting machines which are found to have miscounted must be reported to the voting machine company, the elections board, the candidates, and the media.

Chapter 4 describes many potential ways to rig the black boxes. Election-tampering has been with us for 2,000 years, and is unlikely to go away just because we have entered the computer age.

When you look at paper ballot systems, you can see that many of the standard procedures they use were specifically designed to deter fraud. The same care needs to be given when setting up procedures for black box voting.

Isn't this time consuming?

If we are unwilling to make sure our voting machines count accurately, we shouldn't use them. The biggest objection to proper auditing is that it takes too much time, so some ideas follow for ways to run a relatively tamper-proof system efficiently and with minimal cost.

Implementation ideas

1) The simplest method is to have the touch screen systems print a paper ballot which is easily read by voters and election workers, but also contains a machine-readable bar code.

When the polls close, election workers can scan the bar code. This will take two poll workers approximately forty minutes to do an entire precinct. This gives us a 100% audit at the polling station

This is the cheapest, quickest and most secure method. Note, however, that the bar code scanner should not be from the same manufacturer as the voting machine.

2) Precinct counting: Bring in a second shift one hour before the polls close. After the normal day's work is done, let the tired folks go home. Second shift manually counts the ballots at the precinct level.

Limit the audit to national representative races, major state offices and a random selection of 1-5 propositions, judges and/or state committees, to start.

More exhaustive auditing would be optional depending on volunteer level.

3) Require **"vote audit" duty**, similar to jury duty. It can be during evenings and weekends only, so that it doesn't conflict with jobs. This might even get more people to start voting.

3) Pay poll workers to show up for one **extra day** for auditing duty.

The biggest objection to doing enough auditing to ensure system integrity is that it adds new things to do. Well, democracy is messy. The machines are new, and we certainly are willing to invest extra days to train poll workers for them. If the only way we can use machines safely is to audit their accuracy, let's put at least as much effort into that as we do into trying to learn how to use the machines.

Chapter 4
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris

with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar

4
Can These Things Be Rigged?

Election-rigging is nothing new. We've been conducting elections for more than a dozen centuries, and at one time or another, every system ever designed has been rigged. In fact, election tampering is so universal that it is simply to be expected.

We're a flawed species. The best in us shows up in our desire to make our government "of the people, by the people and for the people." The worst in us shows up when, no matter what the system, somebody figures out how to cheat.

The Fine Old Tradition of Vote-Rigging[1]

How to rig paper ballots

Because at first there was little voter privacy, candidates tried to pay people to vote for them.

People used to wander around town with their ballots, where the slips of paper got into all kinds of trouble. Similar problems can crop up with absentee voting. In the 2000 presidential election in Oregon, according to *The Wall Street Journal*, "unidentified people carrying cardboard boxes popped up all over Portland, attempting to collect ballots. One group set up a box at a busy midtown intersection. Outside the Multnomah County election office, a quartet of three women and a man posted themselves in the middle of the last-minute rush of voters. The county elections director says she was incredulous when she spied people gathering ballots. Nobody knows what happened to the ballots after that. [2]

The Australian paper ballot system, which keeps all ballots at the polling place, sets a very high standard: privacy, accuracy and impartiality when properly administered. It's difficult, but not impossible, to rig this system.

How to rig the Australian Paper Ballot system:

(1) Create a set of rules for which votes "count" and which do not.

(2) Make sure your team is better trained — or more aggressive — than the other team.

(3) Fight against miniscule flaws on ballots for your opponent and defend vigorously the right to count your own candidate's ballots.

According to the 1910 *Encyclopedia Britannica* entry for voting machines, a really well-coached vote-counting team used to be able to exclude as many as 40 percent of the votes. For this reason, some states insist on written standards for counting paper ballots.

Another way to rig paper-ballot elections is to gain unauthorized access to the ballot box. These boxes are supposed to be carefully locked, with an airtight chain of custody. Typically, sealed ballot boxes must be transported with a "chain of custody" form that includes the signatures and times in which they are in the custody of each official. However, chain of custody sometimes mysteriously disengages, and the "seal" is a little twisty-wire that does not take a master burglar to penetrate.

In San Francisco, ballot box lids were found floating in the bay and washing up on ocean beaches for several months after the November 2001 election. "Beachcombers find them on sand dunes west of Point Reyes. Rowers come upon them bobbing in the bay. The bright red box tops that keep washing up around the Bay Area are floating reminders of a problem in San Francisco, the remnants of ballot boxes that somehow got beyond the control of the city's embattled Department of Elections," reports the San Francisco Chronicle. [3]

According to a San Francisco citizens group that publishes reports under the name "First Amendment Defense Trust," the June 1997 vote on the 49ers football stadium was well on its way to losing. The defeat could not be announced, however, until after the "extremely late delivery of over 100 ballot boxes which turned out to have an abundance of 'yes' votes." The delay was attributed to ballots that somehow got wet and had to be dried in a microwave oven, causing great suspicion. When the tardy

The ballot box seal is a little twisty-wire that does not take a master burglar to penetrate...

ballots showed up, so dramatic was the shift to "yes" that the bond, worth $100 million to contractors, was passed by a narrow margin.[4]

New votes kept showing up; when 202 more votes came in (oddly, they were cast in alphabetical order) Lyndon Johnson was declared the winner...

The most famous person caught tampering with paper ballots was president Lyndon Johnson, who defeated the popular former Texas Governor Coke Stevenson in the 1948 Democratic senate primary. Johnson trailed Stevenson by 854 votes after the polls closed, but new ballots kept appearing. Various witnesses describe watching men altering the voter rolls and burning the ballots. Finally, when 202 new votes showed up (cast in alphabetical order), Johnson gained an 87-vote margin and was declared the winner.

LBJ's campaign manager at the time, John Connally, was publicly linked to the report of the suspicious and late 202 votes in Box 13 from Jim Wells County. Connally denied any tie to vote fraud.[5]

According to a bio for R. Doug Lewis,[6] who currently heads an outfit called The Election Center, Lewis managed affairs for John Connally. You will meet R. Doug Lewis in the next chapter; he is currently the most powerful man in America when it comes to influencing voting procedures, though he is a private individual who has never been elected to represent us.

Rigging the lever machines

Lever machines are being phased out. They are not particularly accurate, and they are inauditable and cumbersome. But they are not easy to tamper with. One inhibiting factor is their sheer size. It is impossible to tote one of these big metal contraptions around unnoticed, and the job of moving them is so immense that it happens only at election time and requires several beefy guys and a truck. Private access to lever machines is not easy to come by, but it can be done.

To rig a lever machine, you buy off a technician or one of the caretakers who has custody over the machines. Just file a few teeth off the gear that matches the candidate you don't want, causing the machine to randomly skip votes, and you'll improve your own candidate's chances immensely, though not precisely.

Lever machines are not complex and tampering is not invisible, but if no one looks for it, tampering sometimes goes unnoticed for years.

At least lever machines cannot be rigged on a national scale. Their unauditable, not very accurate, riggable problems have at least been confined to small geographic areas.

Rigging Punch Cards

One way to rig a punch card system is to consolidate ballot-counting in one location so that precincts are mish-mashed together. Then, the bad guys pick someone to add punches to the cards with votes for the other candidate. The double-punched cards become "overvotes" and are thrown out.

In the 2000 general election in Duval County, Florida, according to the *Los Angeles Times*, "a remarkable 21,855 ballots were invalidated because voters chose more than one presidential candidate."[7] These overvotes were never examined in the Florida recount and they came primarily from a handful of black precincts who pooled their votes for counting.

Another way to rig punch cards is to get into cahoots with the card manufacturer. Punch card manufacturers sometimes get both the punch card order and the printing contract for ballot positioning. If they can print punch card batches that are customized for each area, an unscrupulous card manufacturer can rig the cards. There are two ways to do this, and it is difficult to detect either method without a microscope:

(1) Adjust the die that cuts the card so that perforations make the favored candidate easier to punch out, or the undesired candidate's chads hard to dislodge. It is possible to die-cut the favored candidate so that his chads can be dislodged with a strong puff of air!

(2) Affix an invisible plastic coating to the back of the undesirable candidate's chads. They will not dislodge easily, and may even snap back into place after being punched.

Most of the previous methods can be observed and, for the most part, no special training would be needed to realize something was amiss, if you happened to catch someone in the act. Not so with rigging computers:

Cyber-Boss Tweed — 21st Century Ballot-Tampering Techniques

"Subverting elections would be extremely unlikely and staggeringly difficult," said Georgia Secretary of State, Cathy Cox, when interviewed about Georgia's touch screen voting system. "It would take a conspiracy beyond belief, of all these different poll workers.… I don't see how this could happen in the real world."[8]

My premise, though, is this: An insider, someone with access, can plant malicious computer code without getting caught. In this chapter, we will scrutinize my theory and see whether we can knock it down.

Just as we know that banks will have robbers, that blackjack tables will have card-counters and that embezzlers will slip in amongst the bean-counters, so we should expect to find vote-riggers among the software engineers who program and test our electronic voting machines and among the poll workers who have access to them.

Certainly, human nature did not change just because we entered the age of computers. Every other kind of voting system has been tampered with. Why wouldn't computerized vote-counting be a target?

Who might want to tamper with elections?

Political candidates:

Most people, when they think of election-tampering, think of candidates who cheat. Yet it seems to me that few candidates are likely to possess the combination of motive and cash to rig their own election. I believe that vested interests behind the candidate are more likely suspects, and the candidate need not even know.

True believers:

A bigger danger, I think, are the radical political activists or religious zealots, especially if they happen to be endowed with giant wallets. "True Believers" may feel that the end justifies any means; some are very wealthy, and some congregate in radical groups where they can pool their cash and push their agenda.

The more polarized we become politically, the greater the motive for "True Believers" to decide to take matters into their own hands. Some religious sects, like Christian Reconstructionists, are suspicious of the Constitution, sometimes

openly contemptuous of it. Zealots of any kind may truly believe they are "helping" the rest of us by imposing their candidates on us. You do not need to hand a zealot a bribe, and the candidate they select never even needs to know his election was rigged.

Hackers — like mountain climbers — just want to show they can do it. (But watch out for zealots with wallets)

Gambling interests:

For many years, the U.S. had a fairly stable gambling industry — independent bookies, race tracks, Las Vegas, Reno, then Atlantic City and, later, Native American gambling casinos. Now, gambling rights have turned into a brawl, with some tough players involved who are seeking riverboat gambling rights, the right to compete with Native American casinos, and just plain liberalized and legalized gambling in communities all over America. Some of the characters attracted to the gambling industry have criminal records and mob ties and may not be squeamish about little things like buying elections.

Hackers:

More accurately called "crackers," they get their kicks by compromising legitimate software systems. These people may not need bribe money or a cause; like climbing a mountain, they just want to see if they can do it. If working alone, a hacker may be the least dangerous tampering risk because the payoff is often just the bragging rights.

A senior engineer working for one of the companies told me that in 2001, during development of a voting system that was later certified for use, programmers boasted about how to change votes from Democrat to Republican choices, or vice versa. It is unknown if this problem was ever fixed. And herein lies the problem: Programmers who like to hack also like to talk about it, which can make them a target for bribery or extortion.

Profiteers:

Electronic voting systems give a small number of people access to a great number of votes. We should anticipate that ballot-tampering on a massive scale, which is possible if you control the counting software, will attract the all-star players.

In the old days, a city boss might want a particular candidate to win, perhaps throw a few construction contracts his way, take a kickback. But high-volume tampering provides a motive for a much different clientele.

- **Defense contractors**, who stand to make billions if they get the right candidate into a high enough office
- **Highway contractors**, who garner hundreds of millions on freeway and bridge projects
- **Oil companies**, who can benefit from vast new pipelines all over the world, if they select candidates likely to vote for open exploration and geopolitically strategic development
- **Global financiers**, who gain power and profit when international trade policies are set up to favor their interests
- **Pharmaceutical companies**, who want legislative protection for pricing policies and product patenting, and protection from international competition
- **Privatizers** —
  - **Investment holding companies**, who stand to gain control over privatized retirement and pension funds
  - **Water companies**, who want politicians to turn over public water projects
  - **Education companies**, who can sell private education and testing services with the right legislative support
  - **Health-care insurers and providers**, who want to retain control over medical services and reduce malpractice costs

So much to spend, so few techies to corrupt. Where to begin?

Well, for starters, you could send your own compromised programmer into a voting machine company toting a resume. But suppose I am a political operative for a wealthy and powerful, but ethically challenged, corporation and I just want to

"Should things go wrong at any time, the people will set them to rights by the peaceable exercise of their elective rights." —Thomas Jefferson, 1806

buy off an employee. How would I access an engineer, and how would I know whom to approach?

"When ballot-tampering can be done on a massive scale, we should anticipate that it will attract the all-star players — the billion-dollar multinationals. "

I set out to answer that question. I figured that if a middle-aged woman like me, who has never done a "covert op" in her life, working on the Internet in her spare time, could find the people who program our voting machines, then certainly a corporation like Multinational Profiteers LLC must already know who they are.

How would you find someone to bribe?

You can locate software engineers who once worked for voting machine companies by looking at online resumes and job-search sites. The resumes often have home phone numbers. You can call them up and say you are writing an article, and ask them exactly how a machine can be rigged. And they will tell you!

I know. I did this.

You will find software engineers who currently work for voting machine companies by finding any example of the company e-mail. For example, ES&S publishes this e-mail address at its official Web site: info@essvote.com.

- **ES&S** employees have e-mail addresses that end in essvote.com.
- **Diebold**: dieboldes.com and gesn.com.
- **Sequoia**: sequoiavote.com.
- **Hart Intercivic**: hartic.com.

If you enter the last part of the e-mail in a search engine and click every link you'll find people who submitted information to high-school reunion sites ("I work as a programmer for a voting machine company now!" they write proudly.); you'll find voting machine programmers who post comments on forums, join listservs, create personal Web pages and post their wedding plans on the Internet. One guy even listed his hobbies and his favorite vacation spots.

I located more than eight dozen voting-company employees. I also found the home phone number for someone in human resources at ES&S, who in turn has

access to contact information, including the home phone number, for every single employee. This took three hours to accomplish.

How would you choose someone to approach?

For $80 you can run a background check. That will give you a person's Social Security number, which opens up more information. You can also run a credit check. Doing this, you find out if the programmer has a gambling problem, has gotten into credit-card debt, is over her head in student loans, has had run-ins with the law, likes fancy cars, is overcommitted on a mortgage. Additional searches reveal political affiliations and even lead you to people who are disgruntled or believe they will soon be fired.

Assuming someone with programming know-how has access to voting machines or their software code:

• What tampering methods are most likely?

The following is a short discussion of possible ways to attack specific weaknesses found in Internet voting systems, optical-scan systems and touch-screen / DRE systems, and a longer discussion of methods that might apply to any computerized vote-counting system.

Tampering opportunities unique to Internet voting

Military voters in 14 states are scheduled to begin voting on the Internet in 2004. Some cities, like Manatowoc, Wisconsin, and Liverpool, England, are eager to vote by Internet, and some groups even want to vote by telephone!

Despite looming Internet-based elections, Internet voting advocates are difficult to find, even among techies. Companies like VoteHere claim that encryption techniques are a key to Internet voting security. Encryption won't protect these systems from software programming errors, though, and some attack approaches won't be impeded at all by encryption.

Rigging an Internet election is as simple as "DoSing" a server. Denial of Service attacks can knock out servers in targeted areas, and no amount of en-

cryption will help. Suppose you connect to the Internet using AOL, but on election day your AOL access numbers don't work. Can you vote on the Internet?

A January 2003 election.com contest in Toronto, Canada, was disrupted by a malicious attempt to shut down the computer system. According to CBC News, "Earl Hurd of election.com said he believes someone used a 'denial of service' program to disrupt the voting – paralysing the central computer by bombarding it with a stream of data... 'We had one log-in attempt that corrupted the ability of everybody to get access to our servers,' he said...When asked if a second ballot might be delayed by another act of computer vandalism, election.com conceded that the culprit might strike again. 'Unless he died in the last few minutes because of the evil thoughts in my brain, he or she is still out there,' Hurd said." [9]

And imagine, if you will, how the most elaborate encryption could solve this: a power outage. Whether by design or by accident, a power outage would stop Internet voting in its tracks.

Other ways to tamper with Internet voting can't be solved by computer scientists at all because they are human problems. How many people will have to vote with their spouses looking over their shoulders? Worse yet, many people connect to the Internet at work: Do we really want employees to cast their vote next to their union leaders or their bosses?

Tampering opportunities unique to optical-scan machines

People thought optical-scan machines could not be rigged, but there are anecdotal reports of possible rigging with these machines as far back as 1980.

An election official I spoke with from California reported that in her county, Jimmy Carter soundly defeated Ronald Reagan during the 1980 presidential election. However, the computer tally from the optical scanner reversed the results, giving Carter's votes to Reagan and vice versa. By doing a hand-audit using the paper ballots, they were able to straighten out the results, but when she requested that the state of California do more hand audits to see how widespread the problem was, she was ignored.

Where can you find a programmer to bribe? I located eight dozen voting industry insiders. This took 3 hours.

Most people believe that optical-scan machines are tamperproof because they provide a voter-verified paper ballot, but many states prohibit election officials from using the ballots to check the machine count. If you don't use the paper trail to audit the machines, optical scan machines are no safer than paperless touch screens.

Tampering with computerized voting systems

After the 2000 election, coached by vendors and cheered on by groups like The Election Center, the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED) — and bullied into buying new electronic voting machines by the Help America Vote Act (HAVA) — the U.S. began a stampede toward electronic voting.

In the above list of computer voting enthusiasts, here is a group you won't find: computer security experts. Computerizing systems to make them both accurate and tamper-proof clearly requires expertise in computer science. Why, then, are computer security experts opposed to the systems we are rushing out to buy?

A total of 1,212 technologists have endorsed the *Resolution on Electronic Voting* so far, and no comparable group of computer scientists — in fact, no technology group at all — has embraced the opposite side.

Resolution on Electronic Voting

"As a result of problems with elections in recent years, funding is being made available at all levels of government to upgrade election equipment. Unfortunately, some of the equipment being purchased, while superficially attractive to both voters and election officials, poses unacceptable risks to election integrity — risks of which election officials and the general public are largely unaware.

"We are in favor of the use of technology to solve difficult problems, but we

"Computerized voting equipment is inherently subject to programming error, equipment malfunction and malicious tampering..." — Professor David Dill, Stanford University

know that technology must be used appropriately, with due attention to associated risks. For those who need to upgrade, there are safe, cost-effective alternatives available right now, and the potential for vastly better ones in the future. For these reasons, we endorse the following resolution:

"Computerized voting equipment is inherently subject to programming error, equipment malfunction, and malicious tampering. It is therefore crucial that voting equipment provide a voter-verifiable audit trail, by which we mean a permanent record of each vote that can be checked for accuracy by the voter before the vote is submitted, and is difficult or impossible to alter after it has been checked. Many of the electronic voting machines being purchased do not satisfy this requirement. Voting machines should not be purchased or used unless they provide a voter-verifiable audit trail; when such machines are already in use, they should be replaced or modified to provide a voter-verifiable audit trail. Providing a voter-verifiable audit trail should be one of the essential requirements for certification of new voting systems."

David L. Dill
Professor of Computer Science
Stanford University

To sign the resolution yourself, go to:
http://verify.stanford.edu/dill/EVOTE/statement.html

It's not just the quantity of computer experts who have endorsed this demand for a voter-verifiable audit trail that is impressive, but the quality of expertise they represent. They include renowned experts such as Eugene Spafford, Professor of Computer Sciences and CERIAS Director at Purdue University, and Ronald L. Rivest, from the Massachusetts Institute of Technology; Peter Neumann, Principal Scientist for SRI International, who has studied computerized voting security for nearly two decades; Arnold B. Urken, from Stevens Institute of Technology, who founded the very first national certification and testing lab for computerized voting machines; and Dr. Rebecca Mercuri, one of the most famous analysts of voting-machine technology,

But that's not all. Add Douglas W. Jones, associate professor and former chairman of the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems, from the University of Iowa; Charles Van Loan, professor and chairman of the Department of Computer Science at Cornell University; and Martyn Thomas, Professor in Software Engineering at Oxford University.

One thousand two hundred and twelve *for* providing a voter-verified, tamper-resistant audit trail, *zero* computer scientists *against*. And these are not just academics. They include industry experts such as Susan Landau, senior staff engineer for Sun Microsystems Inc.; Patrice Godefroid, Distinguished Member of Technical Staff for Bell Laboratories and Lucent Technologies; and Thomas O'Meara, Lead Software Engineer with General Motors.

You may wonder why I'm going on about this, and it is for this reason:

Lack of Trust: A Dangerous Thing

Take away trust in the voting system, and all bets are off. Our vote is the underpinning for every law, every expenditure, every elected person. Both conservatives and liberals insist on a trustworthy voting system, and each side is already suspicious of the other:

A sampling of opinions from online forums...

"When some hacker living in his grandmother's basement is mysteriously elected senator or governor of a state, politicians will finally admit current computer voting machines are too corruptable even for them.[11] (From FreeRepublic.com, a conservative forum)

"What is really needed is for the hacker community to attack this. If the next election showed the winner to be Nader or the National Socialist Party, the "traceless" voting machines would get thrown out the nearest window."[12] (From Bartcop.com, a liberal forum)

"Elections without evidence see their legitimacy drain away like blood from a sliced jugular."[13] (from slashdot.com, a computer programming forum)

"Voter fraud is by and large a Democrat specialty."[14]

"Vote fraud is without a doubt their (Republican) MO. 'Election' 2000 should have made that manifest to anybody."[15]

After being presented with the urgent concerns of literally hundreds of learned professionals from industry and leading universities, and after being offered the voter-verified paper trail feature at no extra charge, Santa Clara County, California, purchased unauditable touch-screen voting machines anyway.

"They've created this whole UFO effect," said Jesse Durazo,[10] a registrar of voters for the county who is not versed in computer science. He was not persuaded by 1,212 of the nation's top computer scientists, choosing instead to follow advice from voting-machine vendors (who make millions with every sale) and NASS (which is sponsored by voting-machine company money).

"They've created this whole UFO effect," said a registrar of voters who is not versed in computer science. He was not persuaded by 1,212 of the nation's top computer scientists, choosing instead to follow advice from voting-machine vendors ..."

Durazo may believe that fears of election manipulation are overblown, but programmers I interviewed insist otherwise.

Rigging elections through "back doors"

Hiding functions in software programs is called putting in a "back door." The engineers I interviewed were able to invent back doors faster than I could write them down! Through interviews, I compiled the following incomplete list of voting-machine rigs and showed it to two different experts who work for voting machine companies. They told me that all of these methods are possible. They also said most of them would not be solved by the redundant data collection methods touted by manufacturers, nor would they be caught by the certification and testing process.

Some of the engineers I interviewed were so confident they could compromise electronic voting machines that they offered to rig the machines on live TV! Two different software engineers, who worked for different voting machine companies, told me they'd sabotaged the voting software themselves, just to see if they could. One programmer asked if we could have a contest to see which manufacturer's machines could be tampered with the fastest. One guy wanted to know if *Hustler* magazine publisher Larry Flynt, who once offered a $1 million

reward for anyone who could "out" a Republican having an affair (during the Clinton impeachment drive), might be persuaded to offer a bonus for a voting machine programmer who could rig four brands of voting machines at once.

One method to rig a machine involves casting a unique combination of votes which executes a program. This technique can use very short code and is almost undetectable, even if certifiers actually look for it.

10 Approaches to tampering with a voting machine

1. Create a program that checks the computer's date and time function, activating when the election is scheduled to begin, doing its work, and then self-destructing when the election is over.

   It is possible to write hit-and-run code that changes the *original votes*, then destroys itself. It can pass testing because it is activated only on election day.

2. Create a dummy ballot using a special configuration of "votes" that launches a program when put through the machine. Quite diabolical, actually: You rig the election by casting a vote! You could extend this to all machines using the same software version by embedding the program in setup functions, performed innocently by poll workers thinking they are just "testing the machine," or you could put it on the "ender card" which is run through some systems to close and lock down the election. It could also be done with touch-screen machines, by casting a certain unusual combination of votes.

   This technique can use very short code and is almost undetectable even if certifiers actually look for it. Moreover, the software is not examined rigorously during certification, and even if it were, the software that's certified may not be the same as what's in the actual machines.

3. Create a replacement set of votes, embed them on a memory card or chip, and arrange for someone with access to substitute the card or chip after the election. Computer chip substitutions are performed with surprising frequency because of "software programming errors." Yet only *one* version of a program is supposed to be allowed on machines, and it is not supposed to be changed without recertification. But in real elections, technicians sometimes replace voting-machine chips, explaining that the originals were "malfunctioning." One

If at first you don't succeed, there are always other ways...

"I can't help but think of new ways to hack an election using electronic voting. My current favourite is a video-cable dongle which swaps two rectangles on the screen. How this might help one candidate to illicitly obtain votes intended for another is left as an exercise for the reader. I'm all for computer-assisted vote counting, but taking out the physical audit trail is reckless.

nonpartiskan
FreeRepublic.com

"Lets say that a rogue programmer (or even the CIO) at an electronic voting machine company decides to include the following 'Spock pinch' Easter egg:

"If you place your fingers on two or three pre-determined locations (e.g. opposite corners) while making a vote selection, then all current (or subsequent) votes are changed such that 1/3 of all votes go to your preferred choice.

"This 'feature' would be essentially impossible to find in logic testing, and would not depend on the egg programmer knowing anything beforehand about what the vote questions would be, when the vote would take place or even how many 'test' votes were done.. All you would need would be someone who could make it to the polling station at the appropriate time in the voting process (beginning or end) to activate the egg.

"Without a voter verified paper trail, it would be almost impossible to verify that such a cheat had been used. — remember it could also be encoded in the prom firmware of the machine — not just the truly soft software, and it could sit there for years, until an appropriately critical vote occurred (or an appropriately large bribe was paid)."

BlackCopterControl
slashdot.com

"Guard with jealous attention the public liberty. Suspect every one who approaches that jewel.

— Patrick Henry June 5, 1778

such chip replacement took place in the 2002 general election in Scurry County, Texas. When election officials became suspicious about a Republican landslide, they hand-counted the ballots and found that the machine was miscounting; ES&S sent a new chip down and installed it, and the correct count reversed the election, giving it to the Democrat.

Another chip replacement was done in 2002, also by ES&S, in South Dakota, where technicians discovered a machine double-counting certain votes.

During the 2002 general election in Georgia, dozens of memory cards (the equivalent of ballot boxes) were "misplaced," representing thousands of votes. Most, but apparently not all, showed up, but because there were no voter-verified paper ballots, no one knows whether the cartridges that reappeared were identical to those on which the votes were cast.

4. Overwrite the approved program with new commands by installing upgrades or "patches" that have not been carefully tested and scrutinized. I interviewed many election officials who said that unexamined program overrides are routinely put on both optical-scan and touch-screen systems.

   I asked Paul Miller, an official from the Washington State Secretary of State's election division, what the procedures are for tracking program updates. He told me that tracking and examining program updates is "not an issue."

   Michael Barnes, from the elections division in Georgia, admitted that Diebold Election Systems and the Georgia Secretary of State's office put program changes on all 22,000 voting machines shortly before the 2002 general election. He said that the patch was examined by Georgia's independent examiner for voting machine software, Dr. Brit Williams, but Williams told me that he never looked at the source code on the patches.

   Sandy Baxter, Election Supervisor for San Juan County, Washington, who used an optical-scan system, told me that she would get a disk in the mail, sometimes without any instructions, so she installed it. She said that these program changes have sometimes been haphazardly distributed — some areas received them, some didn't.

Because these interviews with officials demonstrate that there is no real security for "patches," *which can overwrite the entire vote-counting program with an illicit one,* I have included full transcripts of the interviews mentioned here in the Appendix. *Any time a program is changed, it can change things you don't see.* For some reason, people supervising the voting system don't think anyone needs to examine and recertify the code on the updates. The kindest way to describe this attitude is "clueless."

5. Include a layer of software that is insulated from certification testing. Diebold voting machines use Microsoft Windows, but when examining the code, no one looks at the files associated with Windows. By embedding malicious programs in the Microsoft operating system instead of the voting software, a hacker can skip right through certification controls.

   Some Diebold machines run old versions of Microsoft operating systems, like Windows 95 and Windows 98, which are not recommended, even by Microsoft, for use in security-sensitive applications.

   In testimony before the U.S. House of Representatives Committee on Science on May 22, 2001, Douglas W. Jones, former chairman of the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems, and an associate professor of Computer Science at the University of Iowa, specifically warned that the Windows operating system could be used as a vehicle for tampering with the vote.

   In Georgia, just prior to the election in November 2002, an unexamined set of Windows files was installed on every voting machine in the state.

6. Work with an unscrupulous vendor for your components. Manufacturers are not required to disclose who their vendors are. Some companies reportedly use components from Russia or the Philippines. Others share components from vendors in the USA who are not scrutinized by independent testing authorities.

Whenever I made my choice, the opposite choice lit up. He suggested then that I should intentionally push the wrong button...

7. Find a video-game programmer to tamper with the video card. Because so many people create video games, the source codes are fairly readily available. A good game pro-

grammer can make the screen do one thing while the innards do something else.

8. Have your technicians obtain files from an Internet site. Tell them how to troubleshoot using a batch of replacement files that reside on a server. Anyone who gains access to the server can replace one with another — for example, replacing the central counting program with a file of the same name that contains a variation of the program, giving plausible deniability if the tampering is caught.

"The voting machines are, in fact, buggier than hell. The software running them is not very stable code, and that's why there is [sic] so many problems..."

9. Add a field into the program that attaches a multiplier to each vote, based on party affiliation, rounding one party slightly up and the other slightly down, using a decimal so that when votes are printed one by one (which is almost never done), they round off and print correctly, but when tallied, the total is shaved. For example: "Affiliation = Democrat; multiplier = 0.85...Affiliation = Republican; multiplier = 1.15." This will create totals that correlate with demographics.

10. Buy a tech and plant him as a poll worker in a key precinct where your competitor's machines are used. Have him go through the training and then have him flub the election by preventing machines from booting up on time, or causing them to crash and then blaming it on the manufacturer. If things really get messed up, have him call the press and grant interviews.

No, no, don't stop me now…

11. Using wireless technology embedded in the voting machine, network it with other machines. Monitor the election results on a remote basis as the contest proceeds and send your adjustment in when the election nears its end. (Idea: Have a programmer put in a special access code that allows us to launch an .exe program by dialing a number on our cell phones!)

12 People who have worked around touch screen know that rubbing them can screw them up big time).

And almost everyone who works on computers know that strowng magnets and magnetic storage don't mix.

The Red-White-and-Blue Screen of Death?

> **Vote.exe has caused a general protection fault in America.com. All work since 1776 may have been lost. Please close the republic and try to reboot.**

"All I have to remember is 18181. How many Republican candidates can come up with the exact same number of votes? As many as you want, but you would think that they could come up with at least a few different numbers."

LiberalProgressiveDemInTexas
DemocraticUnderground.com

"WOW! what a nice, neat, algorithm ... make a mistake voting for the Republican - no problem (vote stored in the bit-bucket)... make a mistake voting for the Democrat - ERROR, please re-vote! Every tenth good vote for the Democrat - ERROR, please re-vote!

bimbo
FreeRepublic.com

18,181...18,181...18,181...
ahaha...ahaha...ahaha...
[**1**2345678] [**a**bcdefg**h**]

"My default assumption is that anyone who uses the words 'proprietary' and 'our' to describe their voting technology has either the intent to commit voting fraud or to be an accessory to it, and the results of any election done with it are inherently suspect.

alizard.
slashdot.com

13. Put a back door into the compiler used for the source code(a compiler is used to "compile" software code from a high-level programming language into faster machine language). The source code can be clean, but no one looks at the compiler, and with this method, the digital signature (a method for detecting changes in software after certification) will remain intact.
14. Switch the card used to start up the machine. For some models, this overwrites the voting program with a new one.

"PALM BEACH COUNTY - Some precincts reported problems with electronic cards used to activate touch-screen machines. Backup cards worked." (AP / Miami Herald, Saturday, March 15, 2003)

15. Compromise the binary code, below the level of the source code, which will not be detectable even with a line-by-line examination of the source code and won't be solved by using a digital signature.

Source code: // really no idea on how to resolve rollback failure... :(perhaps praying :) //

16. Make your ROM eraseable; The firmware is supposed to be sealed into a non-eraseable ROM, but some voting machines can "flash" the ROM when you boot them up with an updated card, and this means the ROM is rewriteable.

17. Accidentally put a few bugs in the software. Software engineering is like writing music or creating a painting. It is inspired, sometimes in the middle of the night, and in the wee hours things slip past the best of them. Sometimes engineers just don't catch bugs in the code. Or perhaps, a programmer plays with bugs for a hobby…

Bugs in the Code

Voting machine source code has apparently turned into the digital equivalent of "The Blob," with such massive code, around a million lines long, that no one really catches all the "bugs."

With such bulbous source code, who would notice a few *malicious* lines that can be explained away as "bugs?"

Voting machine software engineers speak openly about the bug problem. Whether the bug is accidental or not, these bugs clearly can affect the accuracy of the count.

"ES&S's machines are not tampered with. I've seen them in action. They are, in fact, buggier than hell. The software running them is not very stable code, and that's why there is [sic] so many problems with the machines." This was a comment posted on the VoteWatch forum by "Lightfinger." Certainly, not a bullet-proof source, but this was on the day of the 2002 general election and is food for

thought; he also posted names of programmers and where they traveled that day, facts I confirmed later with news accounts and another source at ES&S.

Here are examples of actual voting machine software bugs. These are just a tiny fraction of those we found — and we only looked for those that *programmers pointed out in their comment notations*:

Found on Internet voting source code, called votation

// really no idea on how to resolve rollback failure... :(perhaps praying :) //

Found these comments in Diebold source code files:

Fix bug in VIBS causing Straight Party races not to work properly.

Fix problem with race stats results not being sent correctly.

Fixed bug in BallotDLG when ballot with the votes appears after touching Start button or anywhere else on the screen couple of times.

Revert improvement in detection of invalid smart cards

Fixed minor bug when internal keyboard did not work properly.

Build results offline then upload. Fixes crash when uploading results.

Fix problem with transfer sending wrong precinct id

Fix problem with not closing election after setting for election.

Fixed problem that caused an error when view ballot results.

Fixed problem in FileUtil that did not correctly determine if path was empty.

Fixed problem in PollBook for Closed Primary Elections.

Work around problem reporting zero totals when runing [sic] on Win95 units and Win98 units upgraded from Win95

Fix bug with starting PollBook when main and def. Directories do not match.

Fix problem with incorrectly determining whether an election is a primary.

Re-download will clean up all database, result and audit files.

Fix bug uploading candidate totals

Fixed election counter on the admin screen to always check for the records under the result folder when starting election.

Fixed problem in Poll Book where it fails to clear totals.

Fixed bug that did not accumulate write-in votes.

Handle failure of some files during upload.

Fix bug in validating ResultFile

Ballot station remembers opened election (again)

Truly fixed the bug in LanSelView

Enter a start condition. This macro really ought to take a parameter, but we do it the disgusting crufty way forced on us by the ()-less definition of BEGIN.

But do the bugs ever make it into the software used in elections?

Yes. That's why "patches" (replacement computer files) are so common. For a stunning list of bugs in the computers sent out for use in real elections, see the interview with Rob Behler in chapter 9

Chapter 4 footnotes

1 – Testimony before the U.S. House of Representatives Committee on Science, May 22, 2001; "Problems with Voting Systems and the Applicable Standards by Douglas W. Jones, University of Iowa Associate Professor and Former Chair of the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems. http://www.house.gov/science/full/may22/jones.htm

2 – *The Wall Street Journal*, 17 November 2000; "Fuzzy Numbers...Who Was Collecting Ballots In Oregon? "

3 – *The San Francisco Chronicle*, 19 February 2002; "S.F. voting system in shambles, mistrusted / Errors, mismanagement, instability"

4 – *San Francisco Election Fraud: June 1997 Stadium Bond Election*, http://brasscheck.com/stadium/; also *The San Francisco Chronicle*, 19 February 1997; "Supervisors Pass Ball to S.F. Voters..."

5 – Great thanks to the researchers at DemocraticUnderground.com for helping me source this widely reported story. Sources: *Worldnet Daily:* "Vote Early, Vote Often" by Kay Daly; http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=16460 and, from the Kansas Taxpayers Network, "The Chad Farce," by By Karl Peterjohn; http://home.southwind.net/~ktn/karl104.html; and the LBJ biography Means of Ascent, by Robert Caro. The connection with John Connally can be found at http://www.swt.edu/~lf14/conspire/lbj.html . and in his bio, http://www.tsha.utexas.edu/handbook/online/articles/view/CC/fcosf.html.

6 – Thanks to researchers Fredda Weinberg and Hedda Foil from DemocraticUnderground.com for uncovering the links between Connally and the Johnson vote fraud, and finding documents on the connection of R. Doug Lewis to Connally. University of Virginia Center for Government Studies, "Presidential Selection: A Guide to Reform": Doug Lewis bio, managed affairs for John Connally: appendix. http://www.centerforpolitics.org/reform/

7 – *Los Angeles Times*, 12 November 2001; "Election 2000: A recount..."

8 – *Creative Loafing*, 2 April 2003; "High-Tech Train Wreck?"

9 – *CBC News*, 5 Jan 2003; "Computer vandal delays leadership vote."

10 – *Wired News*, 1 Feb 2003; "Silicon Valley to vote on tech"

11 – FreeRepublic.com, by "Servant of the Nine"

12 – Bartcop.com, by "Barney Gumble."

13 – slashdot.com, by Effugas

14 – slashdot.com, by "ccmay"

15 – DemocraticUnderground.com, by "BurtWorm"

16 – VoteWatch.com, "buggy as hell" by "Lightfoot"

News Update

Some people reported problems with the chapter 3 PDF and upon checking I discovered the file was corrupted. I have uploaded a new file and that has fixed the problem.

Word has reached us that the Democratic National Committee has endorsed a "voter-verifiable audit trails" for the next election in 2004. This is not quite what we want, the explicit words "paper ballot" are missing and nothing else will do. After all, we are dealing with politicians and lawyers, so words *are* important, but they are headed in the right direction.

Our site was shut down for about 8 hours on Friday by our ISP due to a bogus spam complaint. I persuaded them to bring the site back up, but we were still denied access to the site and were told to find another provider. After being cleared by SpamCop.net and after a few email from supporters, the ISP reversed itself and returned full control of the site to us.

Finally, if you would like to help support the author and the publisher in defraying our expenses (band-width, distribution, research, legal fees, etc.), you may do so in one of three ways:

1) A single contribution.
2) A subscribing contribution.
3) By passing along this book or hosting it on your own web site.

A single contribution of any amount can be made via PayPal, credit card, check or money order. A subscribing contribution of $1.95 a month can be made the same way.

For how to make a contribution, please go to our support page at:

www.blackboxvoting.com/bbv/support.html

or email me at david@plan9.org

Thanks!

David.

Chapter 5
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris

with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar

5
How Are These Machines Tested?

When you apply your energy to fighting for trustworthy voting machines, one of the first rebuttals you'll hear is the certification argument. It goes like this: Trust the machines, because they are "tested and tested and tested again." This usually comes with a pat on the head and a condescending, "We know best."

You'll also discover that your opponents use canned rebuttals. If you know what questions to ask, the certification procedures implode. What we are looking for here, if certification is to mean anything at all, is a line-by-line examination of the source code. This, in itself, will not make the system secure. But doing a pseudo-examination of the system, spot-checking a few selected items without looking at the source code, or running automated diagnostics, is worse than no examination at all since it gives people false comfort.

What good is it to "certify" a system if you have never examined the secret, proprietary formula that tells the machine what to do and how to record your vote? A thorough examination should include looking at how the vote-counting program interacts with operating systems and other devices, like video cards — and it must be done by a human being, who can evaluate what each line of code does, not by a machine, which can only look for patterns.

I tried to find out who does the critically important "eyes on the code" examination. Who takes it apart and puts it all together again to see what every line does? Without that, secret "back doors" can be put in the code, telling the machine to do one thing while you think it is doing another.

Who are the people who test and test and then test again?

- The state
- An independent state voting machine examiner (sometimes)
- A National "ITA" (Independent Testing Authority): Wyle Laboratories, Ciber Labs.

Does the state examine the source code?

State certification checks the manual provided by the manufacturer. They review voting machine specifications against state guidelines to see that the machine follows the law. Is it accessible to the disabled? Does it prevent people from voting more than once?

When you ask about state testing of the software code itself, everyone hurries forward with their prepared rebuttal: "We do a Logic and Accuracy test (L&A)," they'll say. No, that's not what I asked.

Does anyone at the state level do a line by line examination of the source code?

Well, no. At least not in Georgia. Not in Washington State. Not in Indiana. So far, I haven't found a single state that does an eyes-on examination of the source code.

Logic and Accuracy tests

The L&A test is called a "black box" test; examining the source code is called "white box" testing. According to Arnold B. Urken, who founded Election Technology Laboratories, the first voting machine testing lab, white box testing — eyes-on examination of the source code — should be mandatory if certification is to mean anything. Urken was so adamant about this that he refused to certify ES&S (then called AIS), because the company would not allow him to examine its code.

L&A testing tells you nothing about tampering, and it can't be counted on to catch software programming errors. In an L&A test, you run test ballots through the machine. If it counts correctly, it passes the test. Some touch-screens use an auto-

Secret "back doors" can be put in the code, telling the machine to do one thing while you think it is doing another....

mated program to simulate someone casting test votes.

Now, if you are a suspicious type (read: a student of human nature), you might wonder how hard it would be to slide through an L&A test. Not surprisingly, many creative computer experts have thought about this, too. To get around an L& A test, an ethically challenged person might:

When machines lose 25 % of their votes, it's clear that the L&A test didn't do the job.

- Set the program to activate only towards the end of election day, using the date and time function of the computer. Because the L&A test is done before the election (and sometimes also after the election), the miscount will occur only during the election itself.
- Put a multiplier in the tabulation code, tied to party affiliation, set to activate only when in "election mode." (I was surprised to find that many of these machines require the administrator to tell the machine when it is in "test mode" and when it is in "election mode." This has to be one of the silliest security holes in the system. Why would you *tell* the machine when it is being tested?)
- Activate a program by casting a ballot with a specific configuration. The AccuVote optical scan machines made by Diebold (Global Election Systems) use a specially configured card to start an election and signal to the computer that the election is finished with an "ender" card. Because the code is proprietary, we are not allowed to see what functions are activated by the ender card. This card is a perfect target for introducing alterations at the end of the election.
- Set an "Easter egg" to hatch only when activated by remote access.

In fact, we already know that L&A tests do not catch hundreds of miscounts.

What about the independent state examiner?

When I spoke with Michael Barnes, an elections official with the Georgia's Secretary of State's office, he said that Dr. Brit Williams from Kennesaw University, the independent examiner for the state of Georgia, does the voting machine certification for Georgia. I called Dr. Williams, who told me that he doesn't certify for the state, saying the Secretary of State's office does it. He also said he does not examine the source code.

Harris: "I have questions regarding the certification of the machines used in Georgia during the last election."

Dr. Williams: "For the state of Georgia – I don't do certification. The law gives the Secretary of State the authority to say what systems are certified and what are not. What I do is an evaluation of the system. The FEC publishes standards for voting systems. We have national labs that examine for compliance with the FEC and if they are in compliance, certification is issued by NASED. Once that's done it's brought into the state and I evaluate them as to whether or not the system is in compliance with Georgia rules and regulations. Then the Secretary of State takes that report, in combination with the others, and certifies it."

He described a procedure where teams of people with a test script checked out each machine, but the tests seem to focus on the hardware. They test the printer, the card reader, the serial port, the screen calibration and then perform an L&A test.

My question remains: Who looks at the source code?

Dr. Williams: "We don't look at source code on the operating system anyway. On our level we don't look at the source code, that's the federal certification labs that do that."

Well, then, I guess they just meant "test and test."

I went to the ES&S Web page, which proclaimed that its voting machines were tested by Wyle Laboratories. David Elliott, of the Washington State Elections Division, said that Wyle is a very reputable firm that tests aircraft systems. Both Michael Barnes and Brit Williams, from the state of Georgia, said that Wyle Laboratories tests their voting machines.

I looked up Wyle Laboratories, and I came across a surprising article. It turns out that Wyle decided to *stop testing* voting machine software in 1996, citing bloated code that was more than 900,000 lines long. I called Edward W. Smith at Wyle Labs, who confirmed that Wyle no longer tests voting machine software. Wyle only tests hardware and firmware.

Can you drop it off a truck? How does it stand up to being left in the rain? Good things to know, but some of us also want to know that someone has examined every line of the source code to make sure no one tampered with it.

What is "firmware?"

Firmware is programming that is stored in read-only memory (ROM) or programmable ROM (PROM). It is created and tested like software.

Wyle Laboratories is responsible for testing the firmware, and after it is certified it is not to be changed without reexamination, so you can imagine my surprise when I ran into these comments, written into the source code files for Diebold Election Systems by its programmers:

"Remove SCWinApi module till pass WYLE certification."[1]

And because the version sent to Wyle for certification is supposed to be *the* version, and after certification the voting machines are supposed to use *only* the officially certified version, you might wonder at this comment:

"Merge WYLE branch into the stable branch."[1]

Why are we are removing things before we send them to Wyle, and why are we merging the officially certified version back into something else? Just wondering.

I called Diebold to ask, but no one returned my call.

I guess this stuff is just "tested."

Who does look at the software source code?

By visiting the Election Center Web site, I discovered that a lab called Ciber, Inc. tests voting machine software. Another lab, called SysTest, is also authorized to certify software, but all the major companies seem to be certified by Ciber.

Who owns Wyle Laboratories?

Wyle Laboratories and Wyle Electronics were once related. At one point, there also seems to have been a Wyly Laboratories.

PR Newswire 06/26/1995: New Name - Old Name **Wyle Electronics - Wyly Laboratories**

Texas billionaires Sam and Charles Wyly were the ninth-biggest contributors to George W. Bush in 2000, and Sam Wyly bankrolled the dirty tricks that wiped out John McCain's lead during the South Carolina primary. I wondered if the Wyly brothers are involved in Wyle (pronounced Wyly). I found many Wyly companies, and at least two companies called Wyly E. Coyote, but never found a link between Texas Bush-pal Wyly brothers and Wyle Laboratories.

I did find a link between Wyle Laboratories and prominent, ultra-right wing, monied interests. William E. Simon, along with Richard Mellon Scaife and the Coors family, has been one of the primary supporters of the Heritage Foundation and its derivatives.

And I did find conflict of interest. You would expect that a company who certifies our voting machines would not have its owners running for office. You would also expect that no one who owns the certification company would be under criminal investigation. You'd be disappointed.

Shortly after Wyle Laboratories split off from Wyle Electronics in 1994, controlling interest was acquired by William E. Simon & Sons, a firm owned by a former Secretary of the Treasury, William E. Simon and his son, Bill Simon, a candidate for governor of California in 2002, whose firm was convicted of defrauding investors.

Shortly before the election, in August 2002, William E. Simon & Sons was convicted of fraud and ordered to pay $78 million in damages. In what is surely record time for our glacial judicial system, the conviction was overturned in September 2002. The reason? William E. Simon & Sons had partnered up with someone who was a criminal and no one could tell who was the guiltiest.[2]

Recently, Wyle Laboratory shares held by William E. Simon & Sons were bought out. Now Wyle Laboratories is a wholly owned subsidiary of LTS Holdings, Inc., an entity I can find no information about, controlled by individuals whose names are not available.

I thought the certification process would involve, say, an expert in voting putting on a white lab coat, brushing away the voting machine employees and independently, painstakingly, testing the accuracy and integrity of the software. After all, our voting system is at stake. Surely, Ciber holds the answer. I decided to give them a call but found out that the public is not allowed to ask Ciber any questions.

When Wyle's division in Huntsville, Alabama, stopped testing voting machine software in 1996, that certification process went to Nichols Research, also of Huntsville, Alabama. Shawn Southworth tested the voting machine software for Nichols Research.

But Nichols Research quit doing it and voting software examination went to PSInet, of Huntsville, Alabama. Shawn Southworth tested the voting machine software for PSInet.

PSInet ran into financial difficulties. Voting software certification was taken over by Metamore, in Huntsville, Alabama, where Shawn Southworth handled it.

Metamore no longer does software certification for voting machines. Now it is done by Ciber, of Huntsville, Alabama. Shawn Southworth is in charge of it.

I called to talk to Shawn Southworth, but his assistant told me that she was supposed to refer all questions back to The Election Center. The only person at The Election Center who is authorized to answer questions about certification procedures is R. Doug Lewis. I left a message for Southworth anyway, but he did not call me back.

I looked up Shawn Southworth on the Web. I found pictures of his motorcycles and I found pictures of him at the beach. Though I'm sure he is eminently qualified (but we're not allowed to ask his credentials), no one has yet convinced me that Shawn Southworth should be entrusted with the sanctity of the vote-counting for all of America.

Who selects the certifiers?

The NASED ITA Technical Sub-Committee of the Voting Systems Board is a small group of people who select the certification agencies. This group looks to R. Doug Lewis of The Election Center as their leader.

What government agency is the Election Center connected with? None: The Election Center is a private corporation. Who runs the Election Center? A man named R. Doug Lewis, who was not elected by anyone.

"The ITAs <u>do not</u> and <u>will not</u> respond to outside inquiries about the testing process "[3]

What are the credentials of R. Doug Lewis? With some persistence, I located a bio for Doug Lewis,[3] but all it said was that he was an assistant to the president in the White House (doesn't say which president); that he ran campaigns for various important politicians (doesn't name any of them); that he headed the Democratic Party for the states of Texas and Kansas (doesn't say what years), and that he consulted for the petrochemical industry (doesn't say what company). With a little more digging, I found that he "managed affairs" for former Texas governor John Connally.

But who is R. Doug Lewis? Through the Election Center, he organized the National Association of Secretaries of State (NASS), which is heavily funded by voting machine vendors; he organized the National Association of State Election Directors (NASED), he is very active with the International Association of Clerks, Recorders, Election Officials and Treasurers (IACREOT), and he set up the training programs for election officials. When election officials want to know if these voting machines can be trusted, they ask: R. Doug Lewis.

I'm sure R. Doug Lewis is a terrific guy (the feeling apparently isn't mutual; he hangs up on me when I call him). But what I do want to know is this: What specific credentials qualify him for the critical work of overseeing the security of voting systems in the United States? Who appointed him?

The Election Center has specific instructions about this. Here they are:

"The ITAs DO NOT and WILL NOT respond to outside inquiries about the testing process for voting systems, nor will they answer questions related to a specific manufacturer or a specific voting system. They have neither the staff nor the time to explain the process to the public, the news media or jurisdictions. All such inquiries are to be directed to The Election Center..."[3]

So I called The Election Center, and was told the only person who could answer my questions was R. Doug Lewis.

Harris: "Mr. Lewis, I understand that your organization is the one that, basically, certifies the certifiers of the voting machines, is that correct?"

Lewis: "Yes."

Harris: "Do you have anything in writing that shows that a line-by-line examination of source code was performed by either Ciber or Wyle?"

Lewis: "No. But that's what they do. They go line by line. They're not trying to rewrite it."

Harris: "Where can I get something in writing that says they look at the code line by line?"

Lewis: "I don't know where you'd find that."

Harris: ... "Let me be more precise. Are you saying that Wyle and Ciber do a line-by-line check on the code, and the way it interacts with the system, to make sure that no one could have put any malicious code into the voting machine software?"

Lewis: "Oh. That's what you're talking about. I don't know if they do a line-by-line check to see if there's a problem."

Harris: "Who can I speak with at Ciber and Wyle?"

Lewis: "I don't think anyone there could answer your questions."

Harris: "Who do you speak with at those labs?"

Lewis: *(muttered)* -"Shawn S....... at Wyle."

Harris: "Okay, who at Ciber?"

Lewis: "No, Shawn S....... is at Ciber. And the person at Systest would be Carolyn Coggins —"

Harris: "Who should I ask for at Wyle?"

Lewis: "Wyle tests the hardware."

Harris: "But they also test the firmware, don't they?"

Lewis: “Jim Dearman at Wyle.”

Harris: “I couldn’t quite catch the name of the person at Ciber. Did you say Shawn S..... what was that last name?”

Lewis: (*muttered*)”Shawn Sou.....”

Harris: “I’m sorry, I couldn’t understand you. What is that name again?”

Lewis: (*muttered*)”Shawn South.....”

Harris: “How do you spell that?”

Lewis: (m*uttered very fast*)”Southw....“

Harris: “I’m sorry, you’ll have to slow down. How do you spell that?”

Lewis: (*quietly*)”S—o—u—t—h—w—[ard?]” (I was never able to understand him. I looked it up on the Web. The correct spelling of the name is Shawn Southworth).

Harris: “I have one more question: Prior to taking over The Election Center, you owned a business that sold used computer parts, which ended up going out of business. Shortly after that you took over The Election Center. Did you have any other experience at all that qualified you to handle issues like the security of national elections?”

Lewis: “Oh, no, no, no. I’m not going to go there with you.”

Harris: “I have newspaper articles published shortly after your computer reselling company went out of business that refer to you as an expert in election systems. What else did you do that qualified you to take over your current position?”

Why should we trust anyone? Why can’t we just verify the accuracy of these machines?

Lewis: “My background is that I

owned a computer hardware and software business. I've never claimed to be an expert. That's the reason we have laboratories, nationally recognized laboratories."

Lewis's used computer reselling business was called Micro Trade Mart, which appears in the Texas Franchise tax database this way:

Micro Trade Mart Inc.
Director: R. Doug Lewis
President: R. Doug Lewis
This corporation is not in good standing as it has not satisfied all state tax requirements.

Lewis ran Micro Trade Mart from 1986 through June 1993. I pulled the corporate documents for The Election Center, a Virginia corporation, and found that it was originally started by a group of individuals in Washington, D.C., but I could not find their names. Lewis became Executive Director of The Election Center in 1994.

I don't know why R. Doug Lewis, after holding the position of "Assistant to the President in the White House,"[4] spent eight years selling used computers.

All I really want to know is: What qualifies him to certify voting machine certifiers, and why must everyone, including the media, talk *only* to R. Doug Lewis when they want to find out how our voting machines are tested?

And now for the rudest question of all: Why should we trust anyone? Why can't we just verify the accuracy of these machines, using a voter-verified paper trail and a robust audit procedure?

* * * * *

Professor David Dill, of the computer science department at Stanford University, tried to get answers about source code certification as well. According to an e-mail he sent me, Dr. Dill has also become concerned that there seems to be *no* eyes-on examination of the code.

As far as I can tell, voting machine software is never actually examined by anyone. Not in the only truly meaningful way: by examining the source code itself line by line.

Chapter 5 footnotes

1 – Source code files for Diebold Election Systems, cvs.tar, Accutouch directory, VoterCard.cpp,v

2 – *The San Francisco Chronicle*, 6 August 2002: "…Though Republican candidate for governor Bill Simon insists he knew nothing of his former investment partner's criminal background, an investigation ordered by Simon's accounting firm revealed four years ago that the man was a convicted drug dealer. ... Even a quick Internet search would have shown that Paul Edward Hindelang's 1982 conviction for smuggling 500,000 pounds of marijuana into the country had been splashed over the front pages of Florida newspapers…and court records show that William E. Simon and Sons…and their partners, as well as his attorneys and accounting firm, spent nearly $1 million in so-called due diligence research on Hindelang and others involved.

3 – NASED Web site, *NASED General Overview for Getting a Voting System Qualified*. http://www.nased.org/ita_process.htm

4 – University of Virginia Center for Governmental Studies National Symposium, professional credentials of R. Doug Lewis.

Chapter 6
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris

with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar

6
Following the Money Trail: Who owns these companies?

Elections In America – Assume Crooks Are In Control
By Lynn Landes

> "Only a few companies dominate the market for computer voting machines. Alarmingly, under U.S. federal law, no background checks are required on these companies or their employees. Felons and foreigners can, and do, own computer voting machine companies.
>
> Voting machine companies demand that clients sign 'proprietary' contracts to protect their trade secrets, which prohibits a thorough inspection of voting machines by outsiders. And, unbelievably, it appears that most election officials don't require paper ballots to back up or audit electronic election results. So far, lawsuits to allow complete access to inspect voting machines, or to require paper ballots so that recounts are possible...have failed.
>
> As far as we know, some guy from Russia could be controlling the outcome of computerized elections in the United States."

* * * * *

This is the article that triggered my interest in voting machines. How hard can it be to find out who owns these companies?

It turns out that tracing ownership is very nearly impossible. As soon as you scrape the mud off the window to look at who's in there programming the voting machines, they pull the shades down. Talk about privatization.

Cast of Companies and Characters

Election Systems & Software (ES&S)
Former names:
American Information Systems (AIS) (Changed name to Election Systems & Software in 1997)
Business Records Corp. (BRC) (Acquired by American Information Systems in 1997)
Data Mark Systems (Changed name to American Information Systems in 1984)
Founders: Bob Urosevich, Todd Urosevich, Jim Lane

Current, former key people:

Directors, President/CEOs: Bob Urosevich, Chuck Hagel, William F. Welsh II, Aldo Tesi.
Vice Presidents: Tom Eschberger, Todd Urosevich, Jim Lane
Chief Financial Officers: S. Michael Rasmussen, Thomas O'Brien, Mike Limas

Diebold Election Systems
Former names:
Global Election Systems (Acquired by Diebold Jan. 2002)
I-Mark Systems (Acquired by Global Election Systems in 1997)

Current, former key people:

President/CEOs: Bob Urosevich, Howard Van Pelt
Vice Presidents: Larry Ensminger
Chief Financial Officers: S. Michael Rasmussen

Sequoia Voting Systems
Former names:
Sequoia Pacific
Business Records Corp. (acquired product line and software in 1997. ES&S was prohibited by antitrust regulations from purchasing BRC in its entirety, so the BRC acquisition was split up between ES&S and Sequoia.)
• Currently a division of: De La Rue (England)

Current, former key people:

President/CEOs: Peter Cosgrove, Tracey Graham
Vice Presidents: Kathryn Ferguson, Mike Frontera
Regional manager: Phil Foster

Advanced Voting Systems
Former names:
Shoup Voting Systems

Current, former key people:

President/CEOs: Ransom Shoup, Howard Van Pelt
Vice President, CFO: Larry Ensminger

VoteHere
Founder: Jim Adler
Directors include:
Robert Gates — Former CIA Director, dean of the Bush School of Government and Public Service at Texas A&M University.
Admiral Bill Owens — Defense Policy Board, SAIC.
Ralph Munro — Former Secretary of State for the state of Washington; his protegé, Sam Reed, is current Secretary of State

Election.com
Former names:
Votation.com
Controlling ownership: Osan Ltd., a holding company owned by a group of Saudi investors based in the Cayman Islands. Recently sold to Accenture.

Hart Intercivic
Chairman/CEO: David Hart
CFO: Ted Simmonds

The Good Guy List:

Avante (Produces paper trail, good accuracy, good disclosure)
CEO, Founder: Kevin Chung

Accupoll (Produces paper trail, needs certification in some states)
CEO, co-founder: Dennis Vadura
President, co-founder: Frank Wiebe

Chuck Hagel
Poster Boy for Voting Machine Vested Interests

He stunned them with his upsets. Nebraska Republican Chuck Hagel came from behind twice during his run for the U.S. Senate in 1996. Hagel, a clean-cut, crinkly-eyed, earnest-looking millionaire, had achieved an upset win in the primary against Republican Attorney General Don Stenberg, despite the fact that he was not well-known in the state. According to CNN's *All Politics*, "Hagel hoped he could make lightening strike twice" — and he did: Hagel then defeated popular Democratic Gov. Ben Nelson, who had led in the polls since the opening gun.

The *Washington Post* called Hagel's 1996 win "the major Republican upset in the November election." Hagel swept all three congressional districts, becoming the first Republican to win a U.S. Senate seat in Nebraska in 24 years. "He won counties up and down the politically diverse Platte River Valley and topped it off with victories in Omaha and Lincoln," reported the *Hastings Tribune*. [2]

What the media didn't report is that Hagel's job, until two weeks before he announced his run for the senate, was running the voting machine company whose machines would count his votes. Chuck Hagel had been chairman of American Information Systems ("AIS," now called ES&S) since July 1992.[3] He also took on the position of CEO when co-founder Bob Urosevich left in November 1993.[4]

Hagel owned stock in AIS Investors Inc., a group of investors in the voting machine company. While Hagel was running AIS, the company was building and programming the machines that would later count his votes. In March, 1995, Hagel stepped down as chairman of AIS; on March 31, he announced his bid for U.S. Senate.

When Hagel won what *Business Week* described as a "landslide upset," reporters might have written about the strange business of an upstart senator who ran his own voting machine company. They didn't because they didn't know about it: On Hagel's required personal disclosure documents, he omitted. When asked to describe every position he had held, paid or unpaid, he

mentioned his work as a banker, and even listed his volunteer positions with the Mid-America chapter of the American Red Cross. What he never did disclose was that he'd been chairman of his own voting machine company.[5]

We never learned about conflict of interest with voting machines, because Hagel failed to disclose his positions with the company that counted his votes.

Six years later, when asked about his ownership in ES&S by Lincoln's Channel 8 TV News, Hagel said he had sold that stock. If so, the stock he says he sold was never listed as one that he'd owned. Nowhere does he mention owning stock in AIS Investors, Inc. and nowhere does he mention the salary he earned from American Information Systems.

This is not a gray area. This is lying. Hagel's failure to disclose his ties to the company whose machines counted his votes was not brought to the attention of the public, and this was a material omission: Reporters surely would have inquired about it as they researched stories about his amazing upset victories.

It is therefore understandable that we didn't know about conflicts of interest and voting machine ownership back in 1996, and perhaps we would never have chosen to herd every precinct in America toward unauditable voting, had we known. Certainly, we would have queried ES&S about its ties to Hagel before allowing 56 percent of the U.S. to count votes on its machines.

In October 2002, I discovered Hagel's connection with ES&S. I found that not only had he not disclosed his involvement through his required filings, but he *still* had undisclosed ownership of ES&S through its parent company, the McCarthy Group.

The McCarthy Group is run by Hagel's campaign finance director, Michael R. McCarthy, who is also a director of ES&S. Hagel hid his ties to ES&S by calling his investment of up to $5 million in the ES&S parent company an "excepted investment fund." This is important because senators are required to list the underlying assets for companies they invest in, unless the company is "excepted." To be "excepted," the McCarthy Group must be publicly traded (it is not), and very widely traded (it is not).

Hagel continued to own a stake of up to $5 million in the ES&S parent company but, for six years, he has characterized it as an "excepted investment" and has never mentioned its ownership of the company that counts his votes.

Charlie Matulka, Hagel's opponent in 2002 for the U.S. Senate seat, finally got fed up. He called a press conference in the rotunda of the Nebraska Capitol Building on October 23, 2002.

"Why would someone who owns a voting machine company want to run for office?" Matulka asked. "It's like the fox guarding the henhouse."

"Why is Hagel allowed to even get close to a voting machine other than to cast his own vote? This is an outrageous example of conflicted interest."

Email from news department staff member, ABC-TV affiliate, in Lousiana

Matulka wrote to Senate Ethics Committee director Victor Baird in October 2002 to request an investigation into Hagel's ownership in and nondisclosure of ES&S. Baird wrote back, in a letter dated November 18, 2002, "Your complaint lacks merit and no further action is appropriate with respect to the matter, which is hereby dismissed."

Neither Baird nor Hagel ever answered Matulka's questions, but when Hagel won by a landslide his Web site did boast that he had beaten Matulka by one of the widest margins ever.

While Hagel's staff boasted, Matulka dug his heels in and asked for a recount. He figured he'd lost, but asked how much he'd need to pay to audit the machine counts. It was the principle of the thing, he said. Matulka received a reply from the Nebraska Secretary of State telling him that Nebraska has no provision in the law that allows a losing candidate to verify voting machine counts by comparing machine tallies with paper ballot counts.

In January 2003, Hagel's campaign finance director, Michael McCarthy (also an owner of ES&S), finally admitted that Hagel had ownership ties to the voting machine company. Hagel had lied, ignored, and then tried to kill the story, and when the story was finally told, his staff tried to claim there was no conflict of interest.

"[Hagel's Chief of Staff Lou Ann] Linehan said there's nothing irregular about a person who used to run a voting-machine firm running for office. 'Maybe

if you're not from Nebraska and you're not familiar with the whole situation you would have questions,' she says. 'But does it look questionable if there's a senator who is a farmer and now he votes on ag issues? Everybody comes from somewhere.'"

Two points, Ms. Linehan: A senator who is a farmer, if he follows the law, *discloses* that he is a farmer on his FEC documents. Then, if he votes oddly on a farm bill, people scrutinize his relationship with farming. Second, the farmer's own cows aren't counting his votes. Anyone with an I.Q. bigger than a cornhusk knows the real reason Hagel hid his involvement with American Information Systems on his disclosure statements.

Chuck Hagel and the Senate Ethics Committee

In October 2002, when I discovered Hagel's history with voting machines, I compiled a set of public documents including photocopies of the omissions in his personal disclosure statements, obscure newspaper articles that documented who did what and when, and corporate records for ES&S. I faxed the photocopies to 3,000 editors with a short synopsis of the significance of this story. At the time, Hagel was running for office, and the HAVA act, which mandates purchase of machines like those made by ES&S, was in its final stages of consideration.

No one touched the story.

HAVA was signed by President Bush at the end of October, and Hagel was reelected in November.

In January, I learned that Hagel might be planning a run for the presidency in 2008. An article printed in *The Hotline* quoted a prominent GOPer saying "It means Chuck's running for president in 2008." The article says Hagel's Chief of Staff, Lou Ann Linehan replied: "It's abundantly clear that many people think that's a possibility for Senator Hagel."[6]

Enter one Victor Baird, counsel for the Senate Ethics Committee. I found his name in Senator Hagel's disclosure documents, in letters repeatedly requesting clarification on certain unexplained investments.

I began with a nonconfrontational question. "What is meant by "widely traded" in the context of an "excepted investment fund?" Baird said that it generally refers to very diversified mutual funds.

I asked Baird why there were no records of Hagel's ties to the voting machine company in his disclosure documents. Was he aware of this? Had he requested clarification from Hagel? I knew I had struck a nerve. Baird was silent for a long time, and then said quietly, "If you want to look into this, you'll need to come in and get hold of the documents."

Hagel has never been called upon to answer for material omissions about his relationship to the voting machine manufacturer.

Something in his tone of voice made me uncomfortable. I did not get the impression that Baird was defending Hagel.

I rummaged through my media database and chose a respected Washington, D.C., publication called *The Hill*, where I spoke with reporter Alexander Bolton. He was intrigued, and over the next two weeks we spoke several times. I provided source material and he painstakingly investigated the story.

Unfortunately, when Bolton went to the Senate Public Documents Room to retrieve originals of Hagel's 1995 and 1996 documents, he was told they had been destroyed.

"They said anything over five years old is destroyed by law, and they pulled out the law," said Bolton.

But the records aren't quite gone. Hagel's staff told Bolton they had obtained the documents from Senate Ethics Committee files. I located copies of the documents at Open Secrets — a Web site where they keep a repository for FEC disclosures.

Bolton found out that in 1997, Baird had asked Hagel to clarify the nature of his investment in McCarthy Group. Hagel had written "none" next to "type of investment" for McCarthy Group. In response to Baird's letter, Hagel filed an amendment characterizing the McCarthy Group as an "Excepted Investment Fund," a designation for widely held, publicly available mutual funds.

According to Bolton, Baird said that the McCarthy Group did not appear to qualify as an "excepted investment fund."[7] Then Baird resigned.

Here's what happened: Baird met with reporter Alex Bolton, told him that Hagel appeared to have mischaracterized his investment in the voting company

parent firm, and then Hagel's staff met with Baird. This took place on Friday, Jan. 25, 2003. Hagel's staff met with Baird again on Monday, Jan. 27. Bolton came in for one final interview Monday afternoon, just prior to submitting his story to *The Hill* for Tuesday's deadline.

Baird had just resigned, it was explained, and Baird's replacement, Robert Walker, met with Bolton instead, urging a new, looser interpretation of Hagel's disclosures — an interpretation that did not mesh with other expert opinions, nor even with our own common sense.

Where was Victor Baird? Could he be interviewed at home? Not really. Bolton was told that he still worked for the Senate Ethics Committee, just not in a position that could talk to the press.

In a nutshell:

- Hagel omitted mentioning that he received a salary from American Information Systems in his 1995 disclosure document*.
- He omitted mentioning that he held the position of Chairman in his 1995 documents. He also omitted his CEO position; the instructions say to go back two years, that position was in 1994.
- He omitted mentioning that he held stock in AIS Investors Inc. in his 1995 and 1996 documents, which list stocks held and any transfers or sales.
- He apparently transferred his investment into ES&S' parent company, the McCarthy Group, and he disclosed investments of up to $5 million in that. However, he omitted the required itemization of McCarthy Group's underlying assets. When asked what kind of investment it was, he just wrote "none."
- When asked by Baird to clarify what the McCarthy Group was, he decided to call it an "excepted investment fund," the only category that allows senators to omit listing the underlying assets of what they own.
- When Baird failed to go along with Hagel's odd description of the McCarthy Group as an "excepted" fund, Baird suddenly was replaced by a new Ethics Committee director who did support Hagel's interpretations.

*In July 2003, in response to questions from the *Seattle Times*, Hagel produced a document that he claims showed he disclosed his position. If so, he still did not disclose the salary he received, or the stock that he held in the "interim" statement, a statement which does not appear to be available in any public recowrds.

Hagel has never been called upon to answer for material omissions about ownership in AIS Investors Inc., nor for his omissions about the positions he held with the company.

Could there have been another reason for Baird's resignation?

Perhaps. Baird had announced in December 2002 that he intended to resign at the end of February 2003.[8] But for some reason he changed his mind and left the position he had held for 16 years a month early and in the middle of the day.

Pressure to kill the story

When I spoke with Bolton the day he broke the Hagel story, he told me that something happened that had never occurred in all his time covering Washington politics: Someone tried to muscle him out of running a story. Jan Baran, perhaps the most powerful Republican lawyer in Washington, D.C., and Lou Ann Linehan, Senator Chuck Hagel's Chief of Staff, walked into *The Hill* and tried to pressure Bolton into killing his story. He refused. "Then soften it," they insisted. He refused.

Bolton is an example of what is still healthy about the consolidated and often conflicted U.S. press. Lincoln's Channel 8 TV News is another example — it was the only news outlet that reported on Matulka's allegations that Hagel had undisclosed ties with the voting machine company scheduled to count their votes.

The 3,000 editors who ignored faxed photocopies of Hagel's voting machine involvement, and especially the Nebraska press who had seen the documents and had every reason to cover the story but chose not to inform anyone about the issue, are an example of what is wrong with the media nowadays. This is not, ultimately, a story about one man named Hagel. It is a story about a rush to unauditable computerized voting using machines manufactured by people who sometimes have vested interests.

Hagel for president?

Hagel's aspirations to higher office have been known to insiders for some time. He was on the short list, along with Dick Cheney, for the vice president position on the George W. Bush ticket in 2000.

Here's what Dick Cheney had to say when he learned that Hagel was also being considered for the vice presidential slot: "Senator Chuck Hagel represents the quality, character and experience that America is searching for in national leadership."

According to an AP wire report, Sen. Chuck Hagel thinks he's capable of being an effective president and says he isn't afraid of the scrutiny that comes with a White House bid.

"Our citizens may be deceived for awhile, and have been deceived; but as long as the presses can be protected, we may trust to them for light."

—Thomas Jefferson to Archibald Stuart. 1799

"Do I want to be president?" Hagel commented, "That's a question that you have to spend some time with...I'm probably in a position as well as anybody — with my background, where I've been, things that I've gotten accomplished." [9]

* * * * *

Whether or not Hagel is in a position to run for president, the company he managed is certainly in a position to count most of the votes. According to the ES&S Web site, its machines count 56 percent of the votes in the U.S.

Chapter 6 footnotes

1 – Excerpted from article at *Common Dreams*, 16 Sept. 2002, "Elections in America: Assume Crooks Are in Control" by Lynn Landes

2 – *The Washington Post*, 13 January 1997; "Brothers in Arms..." *CNN AllPolitics*, 5 Nov 1996; Hagel scores big upset for Republicans. *Business Week*, 10 July 2000; "Chuck Hagel...landslide upset." *Hastings Tribune*, 6 November 1996, "Hagel savors upset win" http://www.cnweb.com/tribune/old/nov96/nov6/nov6_hagel.html

3 – *The Omaha World-Herald*, 21 April 1992; "Omaha Firm Taps North Platte Native"

4 – *The Omaha World-Herald:* 3 June 1994;."Welsh Named Top Executive..." Hagel took over as interim CEO from Bob Urosevich in November 1993. William F. Welsh III took the CEO position from Hagel in June 1994. Hagel remained as Chairman.

5 – United States Senate Public Financial Disclosurefor New Employee and Candidate Reports: Chuck Hagel, 1995. Hagel resigned his chairmanship of American Information Systems on March 15, 1995 and announced his candidacy for the U.S. Senate on March 31, 1995.

6 – *The Hotline*, 3 January 2003; "White House: Hagel cares about the U.S. and yes, all mankind."

7 – *The Hill*, 29 January 2003; "Hagel's ethics issues pose disclosure issue"

Chapter 7
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris

with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar

7

The first public look – ever – into a secret voting system

Author and historian Thom Hartmann writes:[1]

> "You'd think in an open democracy that the government – answerable to all its citizens rather than a handful of corporate officers and stockholders – would program, repair, and control the voting machines. You'd think the computers that handle our cherished ballots would be open and their software and programming available for public scrutiny...
>
> You'd be wrong.
>
> If America still is a democratic republic, then We, The People still own our government. And the way our ownership and management of our common government (and its assets) is asserted is through the vote...
>
> Many citizens believe, however, that turning the programming and maintenance of voting over to private, for-profit corporations, answerable only to their owners, officers, and stockholders, puts democracy itself at peril."

* * * * *

Historians will remind us of a concept called "the public commons." Public ownership and public funding of things that are essential to everyone means we get public scrutiny and a say in how things are run.

When you privatize a thing like the vote, strange things happen.

For example, you can't ask any questions.

Jim March, a California Republican, filed a public records request[2] in Alameda County, California, to ask about the voting machines they had entrusted with his vote. The county's reply[3]:

> "Please be advised that the county will not provide the information you requested...The County will not allow access or disclose any information regarding the Diebold election system as any information relating to that system is exempted from the PRA (Public Records Act)...The system provided by Diebold Election Systems Inc. ("DESI") is a proprietary system that is recognized as such in the contract between the County and DESI...
>
> ...The County contends that the official information privilege in section 1040 of the Evidence Code is applicable because the information requested was acquired by the County in confidence and the County is required to maintain its confidentiality. Any copying or disclosing of such information would violate the license agreements..."

When I called ES&S to ask the names of its owners, the company simply declined to take my call.

When former Boca Raton, Florida, mayor Emil Danciu requested that Dr. Rebecca Mercuri, perhaps the best-known expert on electronic voting in America, be allowed to examine the inner workings of Palm Beach County's Sequoia machines, the judge denied the request, ruling that neither Mercuri nor anyone else would be allowed to see the code to render an opinion.[4]

When best-selling author William Rivers Pitt interviewed Dr. David Dill, a professor of computer science at Stanford University, about his experience with voting machines, Pitt got an earful about secrecy:[5]

Dr. Dill says that when he started asking questions, he got answers that made no sense. "It is frustrating because claims are made about these systems, how they are designed, how they work, that, frankly, I don't believe," says Dill. "In some cases, I don't believe it because the claims they are making are impossible. I am limited in my ability to refute these impossible claims because all the data is hidden behind a veil of secrecy."

When members of the California Task Force on Electronic Voting tried to find out how the machines were tested, Wyle and Ciber (the primary "Independent Testing Authorities" – ITAs) declined to answer.

"If you go to their Web pages, it says, 'If you'd like to know something about us, please go to hell' in the nicest possible way."

— Dr. David Dill
Stanford Univ.

"We wanted to know what these ITAs do," said Dill. " So we invited them to speak to us...They refused to come visit us. They were also too busy to join us in a phone conference. Finally, out of frustration, I wrote up ten or fifteen questions and sent it to them via the Secretary of State's office. They didn't feel like answering those questions, either."

If the ITAs won't answer questions, what about the manufacturers? "What testing do the manufacturers do?" asks Dill. "If you go to their web pages, it says, 'If you'd like to know something about us, please go to hell' in the nicest possible way."

* * * * *

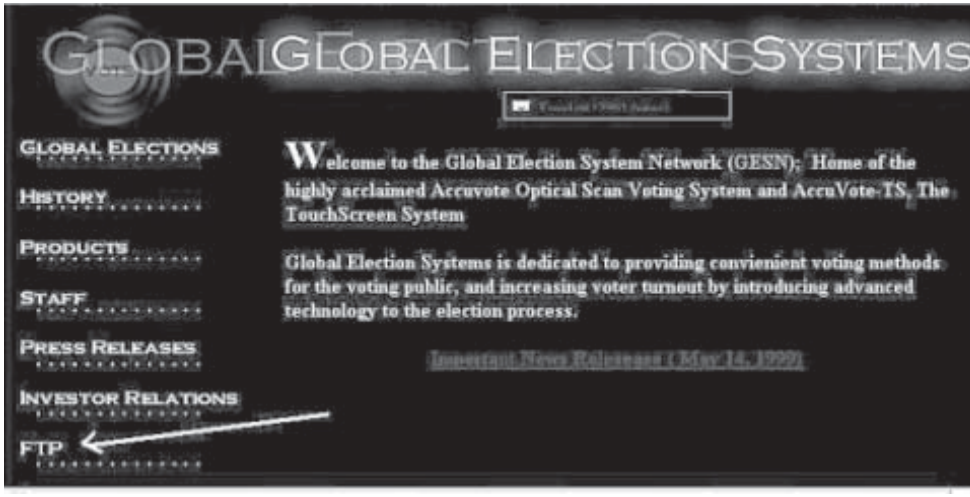
You can't examine a machine or even look at a manual. David Allen, one of the many computer techs who helped coach me through the writing of this book, also happens to be my publisher.

"These things are so secret we're supposed to just guess whether we can trust them," he said. "We've got to get our hands on a technical manual somehow."

I promised him, somewhat doubtfully, that I'd try calling some programmers to see if I could find one to cooperate. I was most interested in ES&S — at that time, I hadn't done much work at all on Diebold Election Systems. I entered "@essvote.com" into the Google search engine, looking for e-mails which might give me names I could contact, and found a few dozen employees who work for ES&S.

I felt cowardly about calling them. What would I say? "Hey, let me see a manual?" So I stalled by convincing myself that I should find as many names as possible. I got some from Sequoia. Then I entered "Global Election Systems" and found some old documents with e-mails ending in "gesn.com."

On page 15 of Google, looking for anything with "gesn" in it, I found a Web page. (You can still find this page at www.archive.org for GESN.com. The FTP link still appears.)



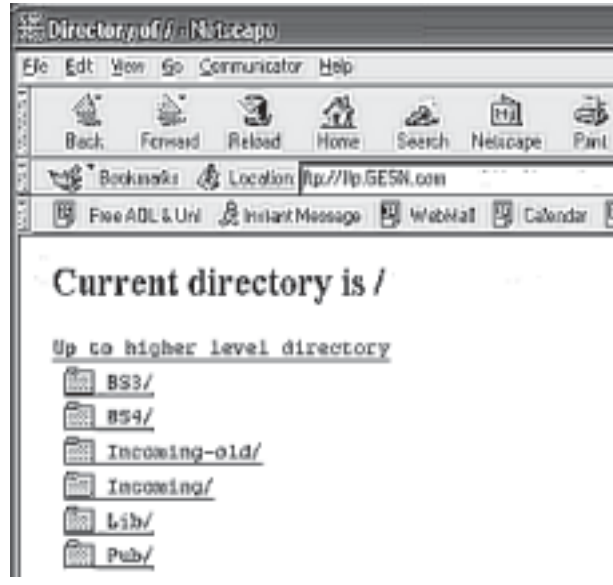
I clicked "press releases" to see what kind of claims this company was making. Then I clicked all the links. I clicked the link called "FTP" and it took me to a page full of files.

I called my publisher, David Allen.

"What am I looking at?"

He took one look at the page and snorted incredulously. "Incredible stupidity."

"Click 'Pub'" he suggested. We did, and began wandering through the files. What follows is the first detailed look — ever — into a secret voting system.



Noun or verb?

What do you do when you find 40,000 secret files on an unprotected file transfer site on the Internet? Probably just look and go away. But what if you have pledged allegiance to the United States, and to the republic for which it stands?

What if you knew that the devil went down to Georgia on Nov. 5, 2002, and handed that state an election with six upsets, tossing triple-amputee war veteran Max Cleland out of the U.S. senate in favor of a candidate who ran ads calling Cleland unpatriotic? Suppose you knew that in Georgia, the first Republican governor in 134 years had been elected despite being behind in every poll, and that African American candidates fared poorly even in their own districts? Knowing this, suppose you saw a file called "rob-georgia," looked inside, and found instructions to replace the Georgia voting program files with something unknown.

I don't know about you, but I'm a 52-year old grandma and I never expected to have to make a choice like this. I wanted someone else to take care of it. *We need investigators like Woodward and Bernstein*, I thought, so I called the *Washington Post*. Of course, Carl Bernstein isn't there any more, but I left a spicy message on Bob Woodward's voicemail. Never heard from anyone. I learned that *Washington Post* reporter Dan Keating was doing a story on voting machines, so I called him.

"So, will you call Diebold and find out what 'rob-georgia' is?" I asked.

"No."

"Why not?"

"Because I don't think 'rob-georgia' could possibly mean rob Georgia," he said.

I left a somewhat more agitated message on Bob Woodward's voicemail and submitted my experience to a Web site called *Media Whores Online*.

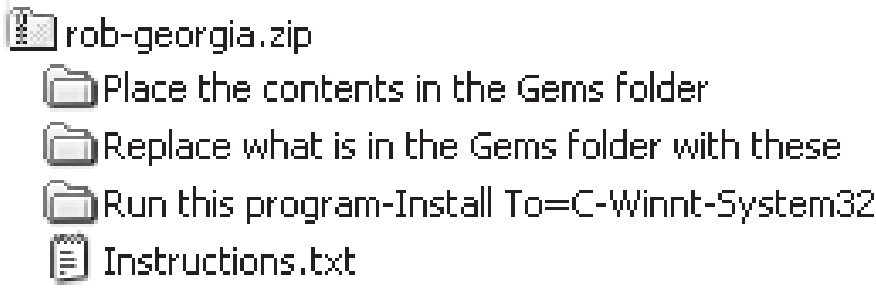
These files might contain evidence. These files might go away. I called people in various places around the world and urged them to go look at rob-georgia. I thought long and hard. And then I downloaded the files, all 40,000 of them. It took 44 hours nonstop. I gave them to someone I trust, who put them in a safe deposit box, and there they sit to this day.

Why in the world would an ATM manufacturer like Diebold leave sensitive files hanging out there on an unprotected Internet site? I made a few phone calls, which confirmed that Diebold *knew* the site was unprotected, and found out that the site had been there for years. (See appendix for interviews with Guy Lancaster, Josh Gardner and Kerry Martin.)

I kept asking if anyone knew who Rob was. Everyone told me there was no employee named Rob in Georgia.

Perhaps rob was a verb?

"rob-georgia" is a zip file with whole bunch more files inside it. It seems to be some sort of a program modification, which is a great way to slip any damn thing you want into a voting machine without anybody noticing. Here's what I saw when I clicked it:



Why did they replace voting machine stuff? *Did* they replace voting machine files? Googling around with various "Georgia, voting machine, Diebold" search words, here's what popped out:

> ***16 Sep 2002*** **Memo** from Chris Riggall (press secretary for Georgia Secretary of State Cathy Cox): "Diebold programmers developed a patch which was applied to the units deployed in Hall and Marion counties, and we were pleased that not one freeze was reported among the tens of thousands of votes cast there. Unfortunately, we simply did not have the time to apply the patch to the demo units, but that is now occurring to all units in all counties and the last increment of shipments from Diebold had this fix loaded before leaving the factory."[6]

A program modification was needed because the touch screens were freezing up, crashing the machines. Makes sense. The problem must be a big one to justify modifying the progam on all 22,000 voting machines in Georgia. But wait a minute —

"*Before being considered for acquisition in Georgia,*" states the Media Backgrounder put out by the Georgia Secretary of State Press Office, [7] "*...software is examined for reliability and hardware is subjected to a variety of 'torture tests.' The state testing examines both hardware and software for accuracy and reliability, and mock elections are conducted on the equipment, witnessed by county election officials.*" The document names Wyle Laboratories and Ciber, Inc., citing their "extensive experience in NASA-related testing."

So how did these NASA-testing labs miss something so obvious that all 22,000 voting machines had to have a program modification to keep them from crashing?

"*It is Diebold Election Systems, Inc. policy that the only acceptable level of conformance is Zero Defects,*"[8] Diebold wrote to certifier Wyle Laboratories in its latest touch-screen certification documents. Okay, we all know that 'zero defects' is one of those terms that sounds good and doesn't happen. But we ought to at least hold Diebold to this: *"The manufacturing test location, test date, and inspector initials will be recorded on a label on every voting machine."*

Whose initials, from the factory, are on the Georgia machines? Anyone's?

In its RFP soliciting purchase by the state of Georgia, Diebold submitted the following in its "Schedule for Deployment": [9]

"Prior to our GEMS™ hardware installation at each Georgia county, the hardware will be staged in McKinney, Texas for software integration and testing."

1. Hardware testing: Wyle Labs
2. Software testing: Ciber Inc.
3. Every machine tested at Diebold factories
4. Rigorous testing on arrival at the Georgia warehouse
5. Testing when delivered to each of Georgia's 159 counties

As part of the installation process, Diebold promised that all software and drivers (small programs which "drive" specific pieces of hardware such as printers, touch-screens, modems) would be loaded prior to being shipped to Georgia. and according to the Georgia Secretary of State Media Backgrounder:

"*Before leaving the factory, <u>each</u> touch screen terminal receives a diagnostic test.*"

If they "staged the hardware" and did software integration and testing and loaded everything and then tested each voting machine before shipping it to Georgia, why did every one of the machines need modifications, in order not to crash, *after* they reached Georgia?

The machines were shipped to Georgia in June 2002. And once they arrived, we are told, there was more testing:

"*Upon arrival at Diebold's central warehouse in Atlanta, each unit was put through a diagnostic sequence to test a variety of functions, including the card reader, serial port, printer, the internal clock and the calibration of the touch screen itself. These tests were audited by experts from Kennesaw State University's Center for Election Systems.*" This statement, on Georgia Secretary of State letterhead, remains posted on the state's Web site as of the writing of this book.

"*After shipment to each of Georgia's 159 counties, county acceptance testing (which consists of the same types of diagnostic procedures) was performed by KSU staff on each voting terminal*."

Was this testing rigorous? Yes, rigorous, they promised. According to the Media Backgrounder: "*Georgia's multi-tiered election equipment testing program, among the most rigorous in the nation*."

Could someone take a moment to do the math with me? If this testing is "rigorous," might we expect them to invest, say, 10 minutes per machine?

The testing described by Diebold and Secretary of State documents adds up to every touch screen unit being tested three times *before* it gets to the renowned "logic and accuracy" test.

> **22,000** machines x **10** minutes = **220,000** minutes
>
> **220,000** minutes x **3** times = **660,000** minutes.
>
> Divide by **60** minutes = **11,000** hours.
>
> Divide by **40**-hour work week = **275** work weeks, or **68** months
>
> **68** months divided by **12** = **5.7** years
>
> Amount of time available for acceptance testing: **4** months
>
> **NOW ADD PEOPLE:**
>
> **68** months divided by **4** = **17** people working **40** hours per week for **4** months doing nothing but rigorous testing.

Do you believe they did all the testing they claim to have done? Call me a skeptic. I want to see the payroll records on that.

What does all that modifying at the last minute do to security? Wait — don't program modifications need to be recertified? How many people had to get access to these machines to do this? Was this legal?

And what exactly was in rob-georgia.zip?

With so many unanswered questions, we decided to ask the public officials responsible for voting systems in the state of Georgia about these program modifications.

Feb. 11 2003: Interview with Michael Barnes, Assistant Director of Elections for the state of Georgia:[10]

> **Harris:** "I want to ask you about the program update that was done on all the machines shortly before the election."
>
> **Barnes:** "All right."
>
> **Harris:** "Was that patch certified?"
>
> **Barnes:** "Yes."
>
> **Harris:** "By whom?"
>
> **Barnes:** "Before we put anything on our equipment we run through state certification labs, and then, in addition to that, we forwarded the patch to Wyle labs in Huntsville ... Wyle said it did not affect the certification elements. So it did not need to be certified."
>
> **Harris:** "Where's the written report from Wyle on that? Can I have a copy?"
>
> **Barnes:** "I'd have to look for it I don't know if there was ever a written report by Wyle. It might have been by phone. Also, in Georgia we test independently at Kennesaw University — a state university."
>
> **Harris:** "Can I see that report?"
>
> **Barnes:** "You'd have to talk to Dr. Williams, and he's out of town. He's in Lincoln. Dr. Williams is on the National Association of State Election Directors (NASED) certification, and I think he's also at Kennesaw University. He does the certification for the State of Georgia."
>
> **Harris:** "Was this new patch tested with a Logic and Accuracy test, or was it tested by looking at the code line by line?"
>
> **Barnes:** "Logic and Accuracy, and also they verify that our version is identical and also any software is tested through Ciber and Wyle."
>
> **Harris:** "But Wyle decided not to test the patch, you say. Was this patch put on all the machines or just some of the machines?"

Barnes: “All the machines.”

Harris: “So every machine in Georgia got this program update.”

Barnes: “Yes, every one of the machines used on election day in November. If it had been sent out to counties prior already, Diebold and their technicians went out and manually touched every machine. Some of the machines were still at the manufacturer, they did the patches on those.”

Harris: “How long did it take to do patches on — what was it, around 22,000 machines?”

Barnes: “It took about a month to go back out and touch the systems.”

Harris: “Can you tell me about the procedure used to install the patches?”

Barnes: “The actual installation was a matter of putting in a new memory card. [memory card: like a floppy disk, but shaped like a credit card. Sometimes called PCMCIA card.] It took about one and a half minutes to boot up... [discussion of slots and memory cards]. They take the PCMCIA card, install it, and in the booting-up process the upgrade is installed.”

Harris: “Where did the actual cards come from?”

Barnes: “Diebold gave a physical card — one card that activates each machine. There were about 20 teams of technicians. They line the machines up, install the card, turn on, boot up, take that card out, move on, then test the machine.”

Harris: “Were people driving around the state putting the patches on the machines?”

Barnes: “Yes.”

Harris: “What comment do you have on the unprotected FTP site?”

Barnes: “That FTP site did not affect us in any way shape or form because we did not do any file transferring from it. None of the servers ever connected so no one could have trans-

ferred files from it. No files were transferred relating to state elections."

Harris: "How do you know that no one pulled files from the FTP site?"

Barnes: "One voting machine calls the servers and uploads the info. We don't allow the counties to hook up their servers to a network line."

Harris: "I notice that one of the things the network builder put on the [county] machines was a modem."

Barnes: "The only time you use the modem is on election night. That is the only time the unit was used, was election night when they plug it into the phone...[details on preparation of vote databases]"

Harris: "Having the screens freeze up is a pretty severe error — how did 5% of the machines get out of the factory with that? How did they get through Wyle testing labs?"

Barnes: "All I know is that the machines were repaired."

Harris: "How do you know that the software in the machines is what was certified at the labs?"

Barnes: "There is a build date and a version number that you can verify. Kennesaw University did an extensive audit of the signature feature — Dr. Williams and his team went out and tested every machine afterwards to make sure nothing was installed on them that shouldn't have been."

Harris: "They tested every one of 22,000 machines?"

Barnes: "They did a random sampling."

Feb. 12 2003: Interview with Dr. Britain Williams, Kennesaw Election Center, an organization funded by the Georgia Secretary of State.[11]

Harris: "I have questions regarding your certification of the machines used in Georgia during the last election."

Dr. Williams: "For the state of Georgia — I don't do certifica-

tion. The law gives the Secretary of State the authority to say what systems are certified and what are not. What I do is an evaluation of the system...[details on certification]"

Harris: "What was your involvement in certifying the program patch that was put on? Did you actually certify the patch, or did you determine that it was not necessary?"

Dr. Williams: "Part of our testing program is when these machines are delivered, we look at the machines and see that they comply. And in the process of doing that — representatives of Kennesaw University did this — we found about 4-5 percent of the machines were rejected, not all because of screen freezes, but that was one of the problems."

Harris: "It was the screen freezes that caused them to issue a program patch?"

Dr. Williams: "Yes. The vendor [Diebold] created a patch addressing the screen freezing. It made it better but didn't completely alleviate the problem."

Harris: "Did you do a line-by-line examination of the original source code?"

Dr. Williams: "For the original — no. We don't look at the source code anyway; that's something done by the federal ITAs."

Harris: "Did you do a line-by-line examination of the patch?"

Dr. Williams: "The patch was to the operating system, not to the program *per se*."

Harris: "It only changed Windows files? Do you know that it didn't change anything in the other program? Did you examine that?"

Dr. Williams: "We were assured by the vendor that the patch did not impact any of the things that we had previously tested on the machine."

Harris: "Did anyone look at what was contained in the replacement files?"

Dr. Williams: "We don't look at source code on the operating system anyway. On our level we don't look at the source code; that's the federal certification labs that do that."

Harris: "Did you issue a written report to the Secretary of State indicating that it was not necessary to look at the patch?"

Dr. Williams: "It was informal — not a report — we were in the heat of trying to get an election off the ground. A lot was done by e-mails."

Harris: "What month did you install that program patch?"

Dr. Williams: "When we took delivery, we were seeing that the patch was on there."

Harris: "I have a memo from the Secretary of State's office that is dated in August [Sept. 16, actually], and it says that due to a problem with the screens freezing, a patch was going to be put on all the machines in Georgia. It references a Rebecca Mercuri report..[Dr. Williams discusses Dr. Mercuri]"

Harris: "...Apparently, someone had already taken delivery on these machines and they had already been shipped out around the state before the patch was applied, is that right?"

Dr. Williams: "The patches were done while we were doing acceptance testing. One of the things we looked for during acceptance testing was to make sure the patch was put in."

Harris: "But as I understand it, a team of people went around the state putting these patches on."

Dr. Williams: "By the time they put the patches in, the majority of the machines had been delivered. Actually, it was going on at the same time. When they started putting the patches in around the state, we tested the machines where they did that [put the patches in] at the factory."

Harris: "When I spoke with Michael Barnes, he said that you tested all the machines, or a random sampling of the machines, after the patch was put on."

Dr. Williams: "We had five or six teams of people with a test

script that they ran on each machine —"

Harris: "The test script did what?"

Dr. Williams: "The test script was generic. It was in two parts. One part tested the functionality of the machine. It was a hardware diagnostic; it primarily tested that the printer worked, that the serial port worked, that the card reader worked, tested the date and time in the machine, and to an extent checked calibration of the machine. Then if it passed all of those, it tested the election. We loaded a small sample election in, the same as the one used during certification testing, and we ran a pattern of votes on there."

Harris: "You mean a Logic and Accuracy test?"

Dr. Williams: "Yes. A little miniature election. If the machine passed, we wrote it up and sent the report back to the office. If it failed — if it froze up or there were other failures, and there were some of those, like the card reader was broken or the case was broken — then we didn't pass it."

Harris: "Can you tell me about the digital signature?" [A digital signature is used to show that no changes in the software were done.]

Dr. Williams: "That's part of the test that involves looking at the software — putting the patch on wouldn't change the digital signature."

Harris: "But if you put in a program patch, wouldn't that show that a change has been made?"

Dr. Williams: "No, because the patch was only in the Windows portion — there was no digital signature check on the operating system..."

[discussion of how a digital signature works]

Dr. Williams: "They write the source code and the source code is submitted to the federal lab. When it passes the lab they freeze the source code; at that point it's archived. Any change after that is subject to retesting."

Harris: "What was the security around the creation of the

cards used to implement the patch?"

Dr. Williams: "That's a real good question. Like I say, we were in the heat of the election. Some of the things we did, we probably compromised security a little bit. Let me emphasize, we've gone back since the election and done extensive testing on all this."

Harris: "Based on your knowledge of what that patch did, would it have been needed for all the machines of same make, model and program? Including machines sold to Maryland and Kansas that were built and shipped around the same time?"

Dr. Williams: "Yeah, but now the key phrase is with the 'same system.' Maryland ran a similar version with a different version of Windows and did not have this problem."

Harris: "So the program was certified by the federal labs even when it ran on different versions of the operating system?"

Dr. Williams: "Yes, they don't go into the operating system."

Harris: "There was an unprotected FTP site which contained software and hardware specifications, some source code and lots of files. One file on that site was called "rob-georgia" and this file contained files with instructions to 'replace GEMS files with these' and 'replace Windows files with these and run program.' Does this concern you?"

Dr. Williams: "I'm not familiar with that FTP site."

Harris: "Is there a utility which reports the signature? Who checks this, and how close to Election Day?"

Dr. Williams "We do that when we do acceptance testing. That would be before election testing."

Harris: "What way would there be to make sure nothing had changed between the time that you took delivery and the election?"

Dr. Williams: "Well there wouldn't — there's no way that you can be absolutely sure that nothing has changed."

Harris: "Wouldn't it help to check that digital signature, or checksum, or whatever, right before the election?"

Dr. Williams: "Well, that is outside of the scope of what some of the people there can do. I can't think of any way anyone could come in and replace those files before the election —"

Harris: "Since no one at the state level looks at the source code, if the federal lab doesn't examine the source code line by line, we have a problem, wouldn't you agree?"

Dr. Williams: "Yes. But wait a minute — I feel you are going to write a conspiracy article."

Harris: "What I'm looking at is the security of the system itself — specifically, what procedures are in place to make sure an insider cannot insert malicious code into the system."

Dr. Williams: "There are external procedures involved that prevent that."

Harris: "This is exactly what I want to know. If you know what procedures would prevent that, could you explain them to me?"

Dr. Williams "We have the source code. How can they prevent us from reviewing it? I have copies of source code that I've certified."

Harris: "But you said you do not examine the source code."

Dr. Williams: "Yes, but the ITA did it. The ITA, when they finish certifying the system, I get it from the ITA — someone would have to tamper with the source code before it goes to the ITA and the ITA would have to not catch it."

Of course, they just told us that the ITA never examined the program modifications made to 22,000 machines in Georgia.

Let's consider a few points here:

1. Tiny programs can be added to any program modification. The file "Setup.exe" launches many of these, some of which are ".dll" files, which stands for "dynamic link libary." These are small files that hide inside executable programs and can launch various functions (whatever the programmer tells them to do.) They can be set up to delay their launch until a triggering event occurs. There is nothing wrong with .dll files, but there is something very wrong with putting new.dll files into a voting machine if no one has examined them.

Other files, such as "nk.bin," also contain executables that can literally rewrite the way the system works. The nk.bin file is sort of like a mini-Windows operating system. If a programmer from Diebold modifies the nk.bin file and these modified files are put on the voting machine without being examined, the truth is, we have no idea what that machine is doing.

Also, any time you do a program modification, you can introduce a small trojan horse or virus that can corrupt the election.

(Hey! What's *this*?)

ClockFix.zip

2. The rob-georgia.zip folder includes a file called "setup.exe" that was never examined by certifiers. It contains many .dll files. The "clockfix" zip file is an nk.bin file. Someone should have looked at these.

3. Windows operating system: In order to use "COTS" software (Commercial Off The Shelf) without having certifiers examine it, the commercial software must be used "as is", with no modifications. If the patches that Barnes and Williams referred to were Windows patches, the moment Diebold modified them they became subject to certification. They did not come from Microsoft. They came directly from Diebold. Therefore, they were not "as is, off the shelf." Someone should have looked at these, too.

4. The rob-georgia.zip file contains two folders full of files that are not for Windows. GEMS is not part of the Windows operating system. You don't need to be a computer scientist to see this: Just look at the file names, which instruct the user to alter the GEMS program. Someone should have looked at these.

5. According to Dr. Williams, no one at the state level looked at these modifications, and according to Michael Barnes, no one at the national level looked at

them, either. In fact, no one has any idea what was on those Georgia voting machines on Nov. 5, 2002.

Georgia certified an illegal election. Now what?

* * * * *

As word spread about voting machine files found on an open FTP site, it became a favorite topic of conversation on internet discussion forums...

"This could make Watergate look like a game of tiddlywinks... Get a good seat. This could be quite a long ride!"

— TruthIsAll

Best disinfectant for secret vote-counting: Sunlight

Public examination of those files is the best thing that could have happened. It's the only way we can engage in an informed debate about voting machines.

I'm glad we got a look inside, but what we found was shocking. What you are about to read should divest you once and for all of the idea that we can "trust" secret voting systems created by corporations.

The Diebold FTP site contained computer files for systems marketed by Diebold Election Systems and, before that, Global Election Systems. These voting systems were used in real elections.

There is no reason to believe that other manufacturers, such as ES&S and Sequoia, are any better than Diebold — in fact, one of the founders of the original

Trust us: Here is the official statement from Diebold, issued by fax on Feb. 19, 2003:[14]

"The old Global Election Systems site has been taken down because it contained old, out-of-date material."

The facts: According to whois.sc, the site was actually owned by Diebold, and this "old" site had been taken down only days earlier, and some of its "old" files were date-stamped just three weeks before Diebold issued this statement.

ES&S system, Bob Urosevich, also oversaw development of the original software now used by Diebold Election Systems.

Because voting systems (except AccuPoll[13], which is open source) are kept secret, I am focusing on Diebold in the next several chapters only because we can't find out anything about the other vendors' systems.

"r o b - g e o r g i a . z i p ? Anonymous FTP access? LOL, unbelievable! This is beyond ridiculous, these people couldn't be trusted to secure your granny's system!"

— quimby

We do know that, according to internal memos from Diebold employees, ES&S was said to have a patent lawsuit pending against Diebold predecessor Global Election Systems at one time[13a]. That is not surprising, because ES&S founder Bob Urosevich brought technology over to Global Election Systems. If a patent lawsuit was filed, that would indicate that some part of the system was alleged to be identical. Also, Chapter 2 shows that Diebold, Sequoia and ES&S have all miscounted elections many times.

A word about "open source"

Very reputable programs, such as the Linux operating system, have been developed through "open source," letting the whole world examine the system and suggest improvements. Some advocates confuse what happened with Diebold's unprotected FTP site with open source. What Diebold did, though, is quite different.

If you never obtain public feedback to improve your software, what you have is horrific security, not an open source system. Hundreds of people have by now examined the Diebold files, but it's still not open source because no one has the slightest idea what Diebold has done to correct the flaws, if anything.

If the Diebold system had allowed everyone with expertise in security, encryption, hacking and database design to critique the software during development and then showed how it corrected the flaws, that would be open source. Such a procedure would no doubt arrive at a very simple and secure program with a voter-verified paper ballot to back it up. Australia has developed an open source voting program, and so has AccuPoll.

Instead, Diebold allowed only a small handful of programmers to look at its software. Then they put all the software (along with passwords and encryption keys) on an open Web site and left it there for several years, where crackers could download it, and people interested in elections could find out about it, but respectable experts and citizens groups were not told of its existence or allowed to examine anything.

I'm glad the files became available, but putting that kind of material on an unprotected Web site was "a major security stuff-up by anyone's reckoning."[12] That's how Thomas C. Greene, of *The Register*, describes what Diebold did, and he's right. Diebold's entire secret election system was available to any hacker with a laptop.

Did leaving these files on an unprotected Web site jeopardize elections?

Yes. If your elections officials tell you they still trust the system, give them a copy of this book. They were never made aware of the risks. Your congressperson may be equally unaware. In fact, well-meaning, election supervisors and congressmen generally know diddly about C++ programming, Microsoft Windows code or remote-access security. Even if they looked at the source code (which they are prohibited from doing), they don't have the expertise to evaluate it.

Trust us: "There's so many checks and balances in this process." — Linda H. Lamone

Maryland State Elections Board[15]

The facts: Poll-worker training won't compensate for insecure or flawed computer programs.

They trust the system because they think that someone else is minding the store — secretaries of state, for example, or state election directors. But none of that makes any difference if the innards of your voting system, including the passwords, IP information and modem configurations have been available to crackers for six years.

As you'll see, our certification system is fundamentally broken. The system is secret, relies on a few cronies and is accountable to no one. Worse, the certifiers have clearly given a passing grade to

software so flawed that it miscounts, loses votes and invites people to come in the back door to make illicit changes to anything they want. But even this inadequate certification system would be better than what we discovered is really happening:

"Are you serious? Please tell me you're not serious here?"

— DEMActivist

Diebold has been using software directly off its FTP site, without submitting it for certification at all.

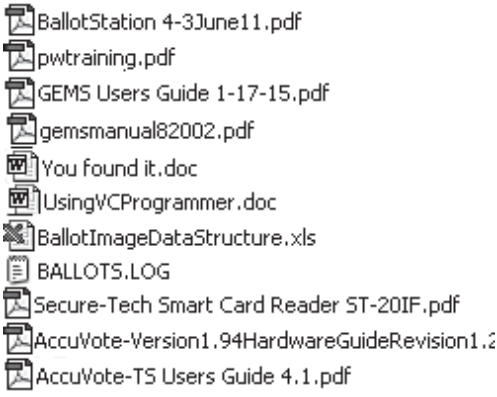
What a cracker could do with the files on the FTP site

If you want to tamper with an election through electronic voting machines, you want to play with:

Ballot configuration — Switch the position of candidates. A vote for one candidate goes to the other. This would be useful in precincts that favor one party or candidate over another.

Vote recording — Record votes electronically for the wrong candidate, or stuff the electronic ballot box.

Vote tallying — Incorrectly add up the votes, or substitute a bogus vote tally for the real one, or change the vote tally while it is being counted.



You'd want to find out as much as you could about procedures. No problem — the Web site contained the Ballot Station user manual, the Poll Worker Training Guide and at least two versions of the GEMS User Manual, along with the Voter Card Programming manual and hardware configuration manuals for the AccuVote touch screen system.

The "Technical Data Package" for the new AccuVote TSx system contains details on procedures and security measures (take with a grain of salt).

* * * * *

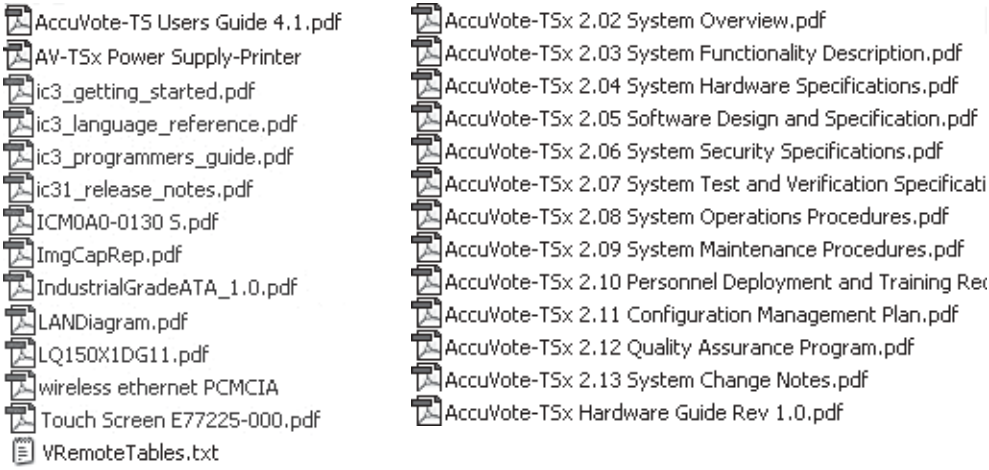
It would be helpful to play with elections in the comfort of your own home. Not a problem — full installation versions of almost all of the Diebold voting programs were on the Web site.

• **BallotStation.exe** (vote recording and precinct tallying, found in the BS folders)

• **GEMS.exe** (county-level tallying of all the precincts, found in the GEMS folders)

• **VCProgrammer.exe** (programs to sign in and validate voter cards)

Just about every version of the Diebold programs ever certified (and hundreds that were never certified) were available.



"You cannot build an idiot-proof voting system because idiots are so ingenious."

— ctdonath2

You'd want to know how to use the programs, so besides having all the installation and user manuals, all the "readme" files were available too.

It might be helpful also to know what kind of testing the voting system goes through, especially the details on the highly touted "Logic and Accuracy" testing done right before and after the election. After all, you'd want to make sure that whatever you do doesn't get caught. Not only testing procedures, but testing samples and instructions on how to do the testing were also provided on the Diebold FTP site.

You'd want to see some typical ballot configurations — or, better yet, get the data files created for actual elections. That way you'd know the positioning of the candidates on the ballot, and you could even get the candidate I.D. number used by the computers to assign votes. You could do test runs using real election files.

On the FTP site were files designated for counties in California, Maryland, Arizona, Kentucky, Colorado, Texas, Georgia, North Carolina, Kansas and Virginia. Some files, like one for San Luis Obispo County, California, were date-stamped on an election day (curiously, five hours before the polls closed).

The Diebold easy password method:

x110700-pimageneral.zip	password = pima
norfolk election.zip	password = norfolk
docs.zip	password = voter
ChrisBellis.zip	password = bellisc
Wyle.zip	password = wyle99
JuanR.zip	password = juan

Guessing passwords is easy. Many files are named for Diebold employees, and many passwords are just employee names.

The supervisor password for voting machines at the polling place was “1111.” When I saw this in the manual, it reminded me of buying a new briefcase. It comes with a "default" combination, but of course you change the combination as soon as you start using the briefcase.

1. Insert the Manager card into the card reader.
2. Enter the password 1,1,1,1,and touch "OK".
3. Remove card when instructed.
4. When the screen below appears, press the "End Election" button.

For some reason, Diebold’s voting machines were less secure than your briefcase. That’s because programmers hard-wired the password into the source code. That way, no one could change the password and anyone inside the polling place (the janitor, a crooked politician) could pretend to be a supervisor by entering "1111".

In case you need a fancy password, the files called “passwd” might come in handy. I don’t know if anyone found a use for the Diebold programmer passwords, but these were sitting there.

passwd

```
ken:Cx4JrK4Q4uebk
guy:APHmbSVeB5WQ6
tri:GwbsAUF5T1Q9Q
whitman:KnSetwE/DYtWM
nel:f1S7xcsCmmxBU
mike:X5oEayCP1CxN.
tomg:h8skrG2aFiuqg
bill:6bFseyII9RxVY
guest:cZm8UJv9sgzyc
```

passwd~

```
ken:Cx4JrK4Q4uebk
tri:UEGNh.UaiLRQk
dmitry:dyNCBK1jMDVDU
whitman:g8PfNAeGd9Ao6
kponti:b/tlxLF5aVUVE
denisel:b/tlxLF5aVUVE
ataa:b/tlxLF5aVUVE
josh:ZHwPOhd5is3JE
```

At the county election supervisor’s office, the results from all the polling places are tabulated using a program called GEMS and the password was in the user manual.

The election supervisor can change “GEMSUSER,” but later I’ll show you how even a ten year-old could change it right back.

Enter your user logon name and password (i.e. GEMSUSER).
At this point Windows will start.

Setting System Date and Time

After Windows starts, at the bottom right corner of the screen is the system

The password for the GEMS program is "GEMSUSER"

Supervisor access at the polling place is granted by the password 1111. Instead of allowing supervisors to control the password, it is written into the source code and printed in the manuals.

```
{
        //{{AFX_DATA_INIT(CSmartCardEmuDlg)
        m_ByAccLevel = '0';
        m_ID = _T("01234567890");
        m_Level1 = 1;
        m_Level2 = -1;
        m_Level3 = -1;
        m_Party = -1;
        m_PIN = _T("1111");
        m_Type = VOTER_CARD;
        //}}AFX_DATA_INIT
}
```

```
== ADMIN_CARD)) {
                st = VC_NOACCESS;
        } else {
                CVoterInfo writeVoterInfo;
                writeVoterInfo.m_CardType = VOTER_CARD;
                writeVoterInfo.m_Version = VCI_VERSION1;
                writeVoterInfo.m_ElectionKey = pVCardInfo->m_ElectionId;
                writeVoterInfo.m_VCenter = CVCenter(pVCardInfo->m_VCenterId);
                writeVoterInfo.m_DLVersion = pVCardInfo->m_DLVersion;
                writeVoterInfo.m_Reportunit = CDistrict(pVCardInfo->m_PrecinctId);
                writeVoterInfo.m_Baseunit = CBaseunit(pVCardInfo->m_PortionId);
                writeVoterInfo.m_CounterGroup = CCounterGroup(pVCardInfo->m_GroupId);
                writeVoterInfo.m_VGroup1 = CVGroup(pVCardInfo->m_VGroup1Id);
                writeVoterInfo.m_VGroup2 = CVGroup(pVCardInfo->m_VGroup2Id);
                strcpy(writeVoterInfo.m_PIN, "1111");
                strcpy(writeVoterInfo.m_Description, "");
                writeVoterInfo.m_Flags1 = (UCHAR)((pVCardInfo->m_Flags & 0x07) |
NEWTYPE_CARD);
                writeVoterInfo.m_Flags2 = (USHORT)(pVCardInfo->m_Flags >> 4);
                writeVoterInfo.m_VoterSN = pVCardInfo->m_VoterId;

                if (m_CardReader.Write(writeVoterInfo) != SMC_OK)
                        st = VC_FAILEDWRITE;
                else
                        st = VC_OKAY;
        }
    }
    if (m_CardReader.IsOpen()) {
```

Perhaps we should run some elections.

A cracker who wants to pretend he is the county elections supervisor might start by installing one of the GEMS vote-tallying programs on his home computer. GEMS is on the central computer at the county elections office. This is the software that creates the ballots before the election, and it also tabulates the incoming votes from the polling place when the polls close. The same GEMS program handles both touch screens and optical-scan machines.

If you were to select any of the many vote databases tagged to cities or counties, you could practice tampering with elections using real software and real vote databases.

Any computer that has Windows seems to work, but meticulous people would follow the instructions left on the FTP site and put the GEMS program on a Dell PC with Windows NT 2k installed.

So many versions of the GEMS program, so little time. A good version to start with would be GEMS 1.17.17 — according to NASED documents posted on the Internet by The Election Center, that was the officially certified version of GEMS during the general election in November 2002.

A folder called “Pima Upgrade” might be a good choice for a hacker living in Tucson, and the new 1.18 series was also available. An even newer program,

version 1.19, was put on the FTP site on January 26, 2003, just three days before it was taken down.

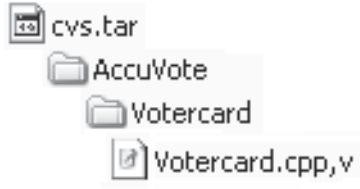
Faking your own touch screen machine

Suppose you wanted to simulate an actual touch screen voting machine. You need to activate those with a smart card, and the average desktop computer isn't set up for that. Put the word "votercard" into a text search on the Diebold files, and this pops up in a file called "votercard.cpp,v"

```
v3-10-19:1.5
v3-10-18:1.5
b1-1-3-votercard-hack:1.5.0.4
v3-10-17:1.5
v3-10-16:1.5
```

Well...what the heck is this file? What kind of file is a "cpp?"

The suffix "cpp" stands for "C++," and these files are source code. "Source code" contains the commands given to the computer that tell it how to execute the program. Many people are surprised to learn that source code files consist of English-like programming commands that people can read. After software engineers write the program, in this case in C++ language, it is then compiled to make it machine-readable.



The cvs.tar file that Diebold left on its Web site was a source code "tree" for the program used to cast votes on touch screens. The tree contains more than program commands; it includes the history of Diebold's software development process, going back all the way back to Bob Urosevich's original company, I-Mark Systems, through Global Election Systems, and including 2002 programming under Diebold Election Systems.

The Votercard.cpp,v, file is found in a directory called Votercard, in a cvs.tar directory called AccuVote.

Now, if I'm a cracker and I get the "Votercard.cpp,v" file off the Diebold Web site, and I'm running a computer that really isn't a voting machine but want to figure out how it works, here it is: a neat little program that can cancel out the card reader entirely. Diebold handed me the road map and helped me find it by naming it "votercard-hack." Any moderately skilled programmer will know how to paste it into the latest touch screen source code, recompile, install, and start playing around.

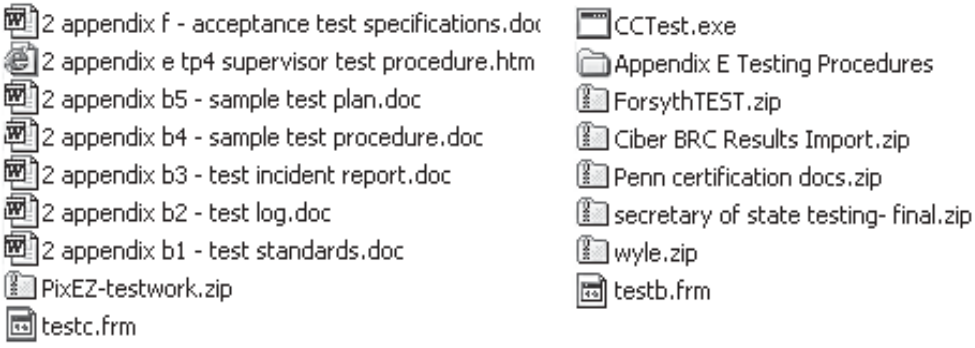
"Votercard-hack" takes you straight to the source code commands you need:

Leaving other people's pants unzipped

It's bad enough when you leave your own sensitive stuff on the Web. But Diebold exposed other people's confidential information, also. Diebold left 15,900 of Microsoft's proprietary Windows CE source code files on its public web site, ready to assemble like a set of legos.

The Microsoft Windows CE Platform Builder is a set of development tools for building a Windows CE operating system into customized gadgets. You are supposed to have a license to use it, and, according to Bill Cullinan of Venturcom Inc., a Waltham, Massachussetts-based Windows CE distributor and developer, the kit is certainly not free.

"The Platform Builder development kit for the new Windows CE .net runs about $995," he told me. "Earlier, the cost was up over $2,000."



"Stupid or evil?"
Though many companies maintain FTP sites, not many I am aware of store source code and customer files in plain sight.
— Atraides

Any cracker in the world could access the pricey Microsoft developer's platforms through the Diebold FTP site.

Despite a notice that says, "You may not copy the [Hewlett Packard] Software onto any public network,"copies of the Hewlett Packard software were on the public FTP site hosted by Diebold.

A document marked "Intel Confidential" pertaining to microprocessor development for personal PCs was on the FTP site, along with the Merlin PPC Sourcekit for personal PCs and the Intel Cotulla development kit, and board support packages for Microsoft Windows CE .NET and PocketPC 2002.

So, Diebold expects us to trust them with our vote, yet they are quite cavalier with other people's intellectual property and, as we will see in the next section, with people's personal information.

Parked on the Diebold FTP site: Private info on 310,000 Texans

Johnny May, perhaps the nation's leading expert on identity theft, has sobering information for you about the Internet and your security. Identity thieves can work anonymously from anywhere in the world and, armed with your social secu-

rity number and a few other details, can quite literally ruin your life. And all they need is your name, address and birthday to get your Social Security number.[16]

The files on the FTP site were a hodge-podge. During the writing of this chapter, I tried to take a more complete inventory.

Tucked into one folder, buried about three-deep in the directories, was a file that contained personal information for 310,000 Texans.

People have a right to privacy, even in the Internet age. Any woman who has an abusive ex-boyfriend will tell you that she doesn't want her apartment number published on an open web site. Child custody cases can get nasty. Thieves who find a database like the one left in the open by Diebold may try to sell the information.

In this file were birthdays. First, middle and last names. Street addresses. Apartment numbers. School districts. Political affiliations. Voting habits. Yes, I assume they will say it was some kind of voter registration file, but it doesn't look quite precisely like one. Each kind of information (name, zip code, etc.) is called a "field." This file had 167 fields, which included data from about three dozen elections, logged in over a period of several years by many different people. Ninety-five thousand people from Plano are in this file, and a couple hundred thousand more from Richardson, McKinney, Wylie, Dallas and surrounding areas.

Because of this file I know that Bob L. of Plano is a Republican and likes to do early voting, and that he and his wife are the same age. But does Bob know that Diebold hung his undies out the window for all to see?

Yes, I know. Someone will explain to me that you can buy voter registration files for a nominal fee. But that doesn't mean you can buy those lists and stick them on the Internet (and what was Diebold doing with this information anyway?).

And does Bob Urosevich, the President of Diebold Election Systems, know that his wife and daughter had their private information on that web site too?

And what do Diebold and the other guardians of our vote have to say about this?

"We protect the Bill of Rights, the Constitution and the Declaration of Independence. We protect the Hope Diamond. Now, we protect the most sacred treasure we have, our secret ballot."[17]

— Diebold CEO Wally O'Dell

"For 144 years, Diebold has been synonymous with security, and we take security very seriously in all of our products and services."

— Diebold web site

"Sometimes our customers use the FTP site to transfer their own files. It has been up quite some years. People go there from counties, cities, sometimes there is stuff there for state certification boards, federal certification, a lot of test material gets passed around."[18]

— Guy Lancaster
Diebold contractor, 2/03

...the current group of computer 'wizards" who are so shrilly attacking ... are no longer behaving like constructive critics but rather as irresponsible alarmists and it's getting a little old.

— Dan Burk
Registrar of Voters
Washoe County, NV
(from Diebold web site)

"They're talking about what they could do if they had access to the [computer program] code...But they're not going to get access to that code. Even if they did, we'd detect it." [19]

— Dr. Britain Williams

"Our ongoing investigation has found no merit to the insinuations of security breaches in our election solutions." [20]

Joe Richardson
Diebold spokesman
Feb 2003

Harris: (follow up question) "So if there were 20,000 files including hardware, software specs, testing protocols, source code, you do not feel that is a security breach?"

Richardson: *[shuffling papers]* "Our ongoing investigation has found no merit to the insinuations of security breaches in our election solutions." [20]

"The scientists are undermining people's confidence in democracy," Townsend said. "None of the critics is giving any credence to the extensive system of checks and balances that we employ internally."

Mischelle Townsend
Registrar of Voters
Riverside County, CA
Associated Press 8/17/03

"It is all fine and well to upload results over the internet, but we don't exactly have a lot of experience in internet security in this company, and government computers are crackers favorite targets."

Barry Herron
Diebold Regional Manager
Diebold internal E-mail - 2/3/99

Chapter 7 footnotes

1 – "If You Want To Win An Election, Just Control The Voting Machines" by Thom Hartmann: http://www.commondreams.org/views03/0131-01.htm. Thom Hartmann is the author of *Unequal Protection: The Rise of Corporate Dominance and the Theft of Human Rights* (www.unequalprotection.com)

2 – PUBLIC RECORD ACT REQUEST: Responding Agency: Alameda County Registrar of Voters filed by Jim March on July 29, 2003. http://www.equalccw.com/voteprar.html

3 – PUBLIC RECORD ACT REPLY: Responding Agency: Alameda County Registrar of Voters filed Aug. 8, 2003. http://www.equalccw.com/alamedafollowup.pdf

4 – *The Palm Beach Post:* 17 Sept. 2002; "Reno consults electronic voting foe"

5 – Unpublished interview of three experts on electronic voting, by William Rivers Pitt, author of *The Greatest Sedition is Silence*. Excerpted on Democratic Underground Aug. 1, 2003. Pitt also wrote *War in Iraq* and *Our Flag Too: The Paradox of Patriotism*.

6 – *The Risks Digest,* Vol. 22: Issue 25. Monday 23 September 2002: Memo from Chris Riggal, press secretary for Cathy Cox, Georgia Secretary of State.

7 – Georgia Secretary of State Press Office; Media Backgrounder: *Multilevel Equipment Testing Program Designed to Assure Accuracy & Reliability of Touch Screen Voting System*

8 – Diebold AccuTouch Technical Data Package TSx, final certification; *Appendix D: Quality Control Manual* and *Appendix E: Testing Procedures,* submitted to Wyle Laboratories for certification in Jan. 2003.

9 – RFP Sec 3.28, "Schedule for Deployment,"[#] submitted by Diebold Election Systems to the state of Georgia in March 2002.

10 – Feb. 11 2002: Interview of Michael Barnes, Assistant Director of Elections for the state of Georgia, by Bev Harris. Full unabridged interview can be found in the library at www.blackboxvoting.org

11 – Feb. 12 2002: Interview of Dr. Britain Williams, NASED certfication board, official voting machine certifier for the states of Georgia, Maryland

and Virginia, by Bev Harris. Full unabridged interview can be found in the library at www.blackboxvoting.org

12 – *The Register*, February 2003, republished Aug. 2 2003; "Computer ballot outfit perverts Senate race, theorist says" by Thomas C. Greene. http://www.theregister.co.uk/content/55/29247.html and (read also) http://www.theregister.co.uk/content/35/29262.html.

13 – AccuPoll voting system: http://www.accupoll.com/Products/Top10/index.html; "Non-proprietary hardware and open source software significantly reduce both initial acquisition and ongoing maintenance costs."

13a – Diebold internal Email, 4 April, 1999. From Ian Piper to Talbot Iredale.

14 – *The Baltimore City Paper*, 19 February 2003; "Ballot Check: Computerized Voting Comes Under Fire in Georgia and California" by Van Smith, and Salon.com, 20 February 2003; "Hacking Democracy" http://www.salon.com/tech/feature/2003/02/20/voting_machines/

15 – *The Baltimore Sun*, 25 July 2003; "New Study Says Maryland's Voting Machines Are Vulnerable to Hackers

16 – *The Guide to Identity Theft Prevention*, by Johnny May, CPP.Statistics on identity theft are available from the Federal Trade Commission Identity Theft Data Clearinghouse: "Figures and Trends on Identity Theft in Texas"http://www.consumer.gov/idtheft/statemap/texas.pdf (2001) and http://www.consumer.gov/sentinel/pubs/Top10Fraud_2002.pdf (2002).

17 – *Cleveland Plain Dealer*, May 2002, interview with Wally O'Dell. Sent out as a company press release in Sept. 2003.

18 – Interview with Guy Lancaster, 4 Feb 2003; According to Lancaster's web site, he was in charge of the site for Global Election Systems; Lancaster has a small computer consulting firm and was under contract to Global Election Systems. When Diebold bought Global in Jan. 2002, they transferred responsibilities for the site to a full time Diebold employee, but kept Lancaster on under a new contract.

19 – *Washington Post*, 28 March 2003; "New Voting Systems Assailed; Computer Experts Cite Fraud Potential "

20 – Interview with Joe Richardson, Diebold spokesman by Bev Harris, Feb 2003.

Chapter 8
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris

with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar

8
Who's Minding the Store?
A free press? Public officials? Anyone?

"Our citizens may be deceived for awhile, and have been deceived; but as long as the presses can be protected, we may trust to them for light."[1]

—Thomas Jefferson to Archibald Stuart. 1799.

* * * * *

Has the free press been reined in by corporate interests? Certainly not, I would have told you a year ago. You just have to make sure that you give them something newsworthy. Journalists are seekers of the truth, a balanced truth — this I still believe.

Managing editors understand that our government will become corrupt without critics, and that an honest and fearless press is the only method available to our citizenry to get at the truth — a year ago, I believed that they had such an understanding. But having seen the reluctance of some of our most important editors to consider issues of vested interests and electronic voting security, I have to say that mainstream press support for investigative reporting now barely has a pulse.

More insidious than failure to cover important stories as soon as they come out is this: Some members of the press now use their own failure to cover an issue as justification that the issue must therefore not have merit. "If what you say is true, why hasn't it been in the *New York Times*?"

Well I don't know. You'll have to ask the *New York Times* — in the meantime, I have a tape recording I'd like you to take a look at, a document you should see, some internal memos that someone should examine.

> "The press [is] the only tocsin of a nation. [When it] is completely silenced ... all means of a general effort [are] taken away."[2]
>
> —Thomas Jefferson to Thomas Cooper, November 29, 1802

Our press is far from "completely silenced," but its voice in matters of great importance has become, at the very least, muffled.

Investigative reporter Greg Palast did an important investigation into the illegal purge of over 50,000 citizens, who were not felons, from the Florida voter roles.[3] If your name was Bob Andersen of Miami, and Robert Anderson of Dallas was convicted of a felony, and you are black, there was a nasty likelihood that you would not be allowed to vote in Florida.

Explosive stuff. Proven stuff. Stuff that should be on the CNN news crawler, especially since these wronged voters, even after the case was proven, did *not* get their right to vote back in November 2002. Documented, confessed-to, photocopied facts that were validated in a court of law, but unfortunately, facts that were not covered at all by most news outlets.

One reason: Early on, some reporters called the office of Governor Jeb Bush and asked whether Florida had purged voters whose rights had been restored in other states, and Jeb's office told them it wasn't so. That was a lie, and documents proved it to be a lie, and an important part of the news story was, in fact, the uttering of that lie, but here's what happened: Reporters decided not to report the story at all, justifying their decision not to cover it by pointing to the lie, without checking to see if it was the truth. After all, it was a statement from the office of the governor.

That is not what our founding fathers had in mind when they envisioned the critical role that a free press must play to protect democracy. "No government ought to be without censors," said Thomas Jefferson, "and where the press is free, no one ever will...it would be undignified and criminal to pamper the former [the government] and persecute the latter [its critics]."[4]

But in today's media age, a Nebraska senator can have his votes counted by a company that he chaired and still partially owns, but even while he is actively running for office, the Nebraska press will not inform Nebraska citizens of his conflict of interest (the lone exception: Lincoln TV *Channel 8 News*).

This is huge... Why is it in a NEW ZEALAND paper?
— Sagan

Atlanta Journal-Constitution reporter Jim Galloway told me he felt that it was more important to write about a state flag controversy than to inform Georgia voters that an illegal program modification had been made to 22,000 voting machines right before an election.[5]

CNN, Fox News, MSNBC, ABC, CBS and NBC were unable to tear themselves away from promising us weapons of mass destruction in Iraq (a story that turned out to be false) in order to spend 30 seconds asking a single question about the integrity of our voting system, even after a Stanford computer science professor and more than one thousand computer security experts insisted that it could not be trusted.

When Diebold, with machines in 37 states, left its voting system out on the Web for six years (free for the hacking), not a single editor from the *Wall Street Journal* or *USA Today* or *Newsweek* magazine bothered to assign anyone to look at the files so they could form an opinion as to the importance of this security gaffe.

It wasn't because they didn't know. In my media database I have 451,000 editors and producers, and I have sent over 100,000 bulletins directly to the appropriate editors and producers, in which I offered documents, cited sources and listed phone numbers of many experts to call. Everyone got the material — investigative, political, government, high tech, national news journalists — many have been receiving regular updates since October 2002. Not only has most of the press done a poor job (or at least a delayed one) of informing American citizens about this issue; most reporters have not even looked at the documents to assess the credibility of this story.

So much for the mainstream news media minding the store. If you want to know where the free press is nowadays, here it is:

Alastair Thompson was a reporter for many years before starting his Internet news site, *Scoop Media* (www.scoop.co.nz) — which was launched out of a garden shed in Wellington, New Zealand and immediately won the New Zealand Internet Awards for "Best Online Writing" and "Best Content." Yeah, I know: It's just New Zealand, and only the Internet.

Thompson didn't wait for the *New York Times*. He broke the story of the Diebold security problems on February 10, 2003,[6] just 18 days after the FTP Web

site was discovered. Thompson covered the "rob-georgia" story, about last-minute program modifications on 22,000 Georgia voting machines, on February 13.[7] New Zealand's *Scoop Media* has consistently outpaced the U.S. media on the voting story, and ended up becoming part of the story itself when it published a worldwide link to all 40,000 Diebold files on July 8, 2003.[8]

"Does Palast have this?" Conason? Begala? Jimmy Breslin? Hunter Thompson? The Duke of Earl? Hell, I'm ready to send out a distress signal to the Thunderbirds!
— dedalus

Since the story broke, some good work has been done. Van Smith of *The Baltimore City Paper* published a detailed statistical analysis of anomalies in the November 2002 Georgia election,[9] even though he was working for a local paper in Baltimore, because he realized it was important. Maryland was planning to buy the same machines.

Salon.com has been writing about concerns with electronic voting for some time now, and Salon's tech writer, Farhad Manjoo,[10] has written several accurate and groundbreaking investigative stories.

Rachel Konrad of *The A.P.* has been covering this issue since an odd decision in Santa Clara County, California. Under great pressure from Silicon Valley computer experts, Santa Clara officials opted, grudgingly, for a "pilot project" in the future, aimed at just a few voters.[11] The county had been offered an option for voter-verified paper ballots by all of the major vendors at *no extra charge*, but they turned it down.

WiredNews.com has been tenacious about investigating and reporting this story and broke the story about the Diebold memos that you'll learn more about later.[12]

Julie Carr-Smyth of the *Cleveland Plain Dealer* wrote an astonishing report on voting machine vested interests; she discovered a visit by Diebold CEO Wally O'Dell, a member of the George W. Bush "Pioneers and Rangers," to Bush's ranch in Crawford, Texas — followed days later, by a letter in which O'Dell promised to "deliver the votes" for Bush in 2004.[13]

Erika D. Smith of the *Akron Beacon Journal* obtained a surprising revelation from Diebold's Mark Radke, who admitted that the new Diebold TSx machines,

to be sold in late 2003, will substitute wireless communication of votes for land-line modems. Radke all but admitted the system could be hacked when he made this startling (and cavalier) admission: "But even if that burst of election data were intercepted, all the hacker would get are unofficial results."[14] (Um, Mr. Radke? Hacking can put data in as well as take data out.)

If you want to find the free press nowadays, look to these folks, who prove we do have one, though it may not be quite where you've been looking for it. And if you really want to locate the free press, don a pair of hip boots and get one of those caver's hats with a light on it, wade into the Internet, shove the crud aside and you'll find some of the best investigative reporting ever.

Given the abundance of leads, the wealth of information on this topic, and its importance, this issue has largely been ignored. Is the paucity of news coverage because reporters have just now learned of the vulnerabilities of electronic voting? Is it because electronic voting is new?

Not exactly. The first major article about electronic voting appeared in *The New Yorker* fifteen years ago, by investigative reporter Ronnie Dugger.[15] He wrote of many of the same concerns you are reading about in this book — but no one paid much attention.

Though not covered in the mainstream press until late 2003, word of the Diebold FTP site spread through the Internet as soon as New Zealand's *Scoop Media* broke the news in February. And this, you see, is why true freedom of the press is so important: It informs the citizenry, and galvanizes us to engage in the scrutiny that is our duty. Thank goodness for the Internet, for without it this story would never have been fully exposed.

Despite a virtual blackout by major media outlets for nearly a year, ordinary people, like you, many of whom had never done any activism in their lives, made decisions to get involved in this issue.

This is an outrage, will the national press ever do what a 4th estate is supposed to do? Do we live in a free country or not?
—Annagull

Who's minding the store: I guess WE are

Efforts made by just a handful of people have gotten us to this point, where problems with voting

machines are at last reaching public consciousness. Drs. Rebecca Mercuri and Peter Neumann have put forth truly Herculean efforts, toiling nearly in the dark for fourteen years, while newspapers often chose to print press releases about how much "fun" it is to vote on machines instead of examining the more difficult subject matter brought to light by these computer scientists.

Never doubt that a small group of thoughtful, committed citizens can change the world. Indeed, it's the only thing that ever does.
— Margaret Mead

When news of the 22,000 illicit patches broke loose, a small contingent of Georgians decided to do something about it. I'm going to refer to them simply as "Georgia activists" because recently they asked me not to call them out by name. Those who have been following this issue closely will know who these individuals are; their efforts have been nothing short of heroic. But citizens in Georgia soon discovered that asking questions about our voting system is like trying to walk up the down escalator.

How many patches were done in Georgia?

When I began taking inventory of the Diebold FTP site, I found another folder called "Georgia062802.zip," which appeared to be a patch targeted for Georgia dated June 28, 2002. Another file, called "clockfix" modified Diebold's specialized Windows CE operating system in some undefined way.

Here's the thing about software patches: When you change software to correct a problem, the procedure is to assign a bug number. You test it. You document everything. You append a new number to the end of the release. Then it has to be approved. Writing up a fix, sticking it on the Internet, and then running around putting it on voting machines is not how it's done.

"Time to call out the geek militia ... Forget the militia, call out the whole damn geek army!"
— AdamFSmith

One of the Georgia activists hunted down the law and fired it off to me.

RULES OF OFFICE OF THE SECRETARY OF STATE ELECTION DIVISION
CHAPTER 590-8-1
CERTIFICATION OF VOTING SYSTEMS[16]

590-8-1-.01 Certification of Voting Systems.

11. Any modification to the hardware, firmware, or software of an existing system which has completed Qualification, Certification, or Acceptance testing in accordance with these Rules will invalidate the State certification unless it can be shown that the change does not affect the overall flow of program control or the manner in which the ballots are interpreted and the vote data are processed, and the change falls into one or more of the following classifications:

(i) It is made for the purpose of correcting a defect, **and test documentation is provided** which verifies that the installation of the hardware change or corrected **code does not result in any consequence other than the elimination of the defect.**

(ii) It is made for the purpose of enhancing the utility of the system or adding additional audit or report generating capability.

(iii) It is made for the purpose of enabling interaction with other general purpose or approved equipment or computer programs and databases, **and procedural and test documentation is provided** which verifies that such interaction does not involve or adversely affect vote counting and data storage.

(iv) It is made for the purpose of enabling operation on a different processor or of utilizing additional or different peripheral devices, and the software is unaltered in structure and function.

Georgia citizens have a right to be incensed. The state didn't bother to check what their voting system was doing when it counted their votes in the 2002 Georgia general election. This was a violation of the law, and Georgia taxpayers now realize that their votes may have been thrown out the window.

Suggestion: Why not contact the Carter Center? This organization, under the auspices of former President Jimmy Carter, seeks to prevent and resolve conflicts, protect freedom and enhance democracy. One of the Georgia activists

jumped on this, but the Carter Center told her that, according to its charter, it can only monitor elections *outside* the United States.

Ya!!! I never liked democracy anyway! Choose my leaders for me! — Skewthat*

A Georgia computer programmer contacted Lieutenant Governor Mark Taylor's office, which told her to send information, so she did, handing over a generous explanation about what was wrong with this picture, including the unprotected FTP Web site, rob-georgia, the Georgia law and the people driving all over the state administering unexamined program modifications before the election. But after that e-mail, they quit taking her calls.

Georgia activists began calling on local and state representatives, trying to get them to listen to the issues with electronic voting machines. They found that legislators were not enthusiastic about discussing computer security issues and usually were willing to give up no more than three minutes in the hallway, between sessions, to listen to concerns.

Now here we have an election chock-full of statistical anomalies, with who knows who uploading (or replacing) files on an open web site, and instructions to replace the voting program with something else, right before an election. Citizens were upset, but officials would not respond to them.

I spoke with Ben Betz, from People for the American Way, about the Georgia situation; he was referred to me by one of the activists. His group decided not to pursue the issue.

"Is there an attorney in this group?" Would it be feasable to have a class action lawsuit on behalf of Georgia voters? Perhaps a violation of civil rights suit? — MrHinkyDink*

Georgia activists made several attempts to meet with Secretary of State Cathy Cox but were allowed to speak with only with Assistant Director of Elections, Michael Barnes, who was less than helpful. They met with Tom Murphy, a former Speaker of the House in the Georgia legislature. "He knows where all the bones are buried," confided a self-appointed helper named Chris Hagin.

---

* Internet culture allows people to dish out political opinions under "screen names." The screen names, as well as the comments, can be entertaining.

Tom Murphy called upon Cox to meet with the activists, but she didn't; instead, Barnes told them (on March 6) that Cox would be booked up "until July."

What about the American Civil Liberties Union? Activists met with ACLU attorney C. Cooper Knowles, but he told them he couldn't take on electronic voting machines because he had fought against the punch cards. ACLU attorney Laughlin McDonald, director of the Voting Rights Project, apparently couldn't see how a case could be formed, saying "Where's the harm?" ("Harm" is a legal requirement needed for some types of lawsuits.)

Concern among citizens continued to grow. In New York, author Mark Crispin Miller asked what he could do to help. One of Miller's contacts, Denis Wright, lives in Georgia and began joining the agitation to have someone — anyone — look into irregularities with Georgia's voting system.

Wright filed a formal request to produce Georgia documents, which yielded this odd response to his simple query about the certification documents — you know, the ones that prove that we should just trust our votes to their secrecy:

From: Denis Wright
To: Kara Sinkule
Sent: Wednesday, March 19, 2003 9:33 AM

Hi Kara. Hope you are doing well.

I need some more help, please. I am hoping that I can get hard copies of the following documents, per the Freedom of Information Act:

1. According to state law, **any changes in the voting machine software (GEMS and Windows) require documentation in writing**. I would like to get copies of any such documentation.

2. **A copy of the actual certification letter from the lab** (certifying the version of the software which was used on election day) as well as any related memos, letters, etc...

* * * * *

From: "Tatum, Clifford" <ctatum@sos.state.ga.us>
Date: Tue Mar 25, 2003 11:39:40 AM US/Eastern
Subject: Open Records Request

Dear Mr. Wright:

Our office has received your request under the Georgia Open Records Act, O.C.G.A. § 50-18-70 regarding electronic voting information...

In response to your first category, we have determined that **no records exist regarding a change to software** used by the voting system.

In response to your second category, we have determined that **no records exist in the Secretary of State's office regarding a certification letter from the lab certifying the version of software used on Election Day.** Please be advised that any records of this type may have been submitted to the Georgia Technology Authority (GTA) in response to the Request for Proposal that was issued by GTA. Accordingly, a request for this type of information should be submitted to Gary Powell with GTA for response. By copy of this letter, I am advising Mr. Powell of your potential request...

Sincerely,

Clifford D. Tatum
Assistant Director of Legal Affairs
Election Division

What have we learned so far?

Uncertified program modifications present a serious risk to election security.

Georgia requires certification and reports for program modifications

- Rules of Office of the Secretary of State Election Division Chapter 590-8-1, Certification of Voting Systems, 11[16]

Diebold knew Georgia required recertification for modifications

- Diebold internal document: "Certification Requirement Summary"[17]

Officials admit modifications were made to Georgia voting machines

- Assistant Director of Elections Michael Barnes
- Chris Riggall, Press Secretary for Cathy Cox
- Kara Sinkule, Press Secretary for Cathy Cox
- Dr. Brit Williams, NASED Voting Systems Board Technical Committee

Officials admit that Georgia program modifications were not certified

- Michael Barnes
- Dr. Britain Williams

Officials admit there is no documentation for the program modifications

- Clifford Tatum[18]

Then, one official reverses himself and claims uncertified patches are impossible in Georgia

- Dr. Britain Williams: In response to my discussion of the Georgia program modifications on the BlackBoxVoting.com web site, Dr. Williams writes:

> "This comment ["A patch to the underlying operation system - Windows - can slip through without scrutiny."] **assumes that the State of Georgia allows changes and/or upgrades to the Microsoft operating system. This is not the case.**
>
> " ...This specific version of the operating system and the election software undergoes ITA* testing and State Certification *(sic)* testing. The State Certification is for this specific version of the Microsoft operating system and the Diebold election system. **After State Certification any change to either the Microsoft operating system or the Diebold election system voids the State Certification.**
>
> "If a change to either the Microsoft operating system or the Diebold election system becomes desirable or necessary, **this change voids the State Certification**. The revised system then must then go back through the entire ITA Qualification and State Certification."[19]

Next, two officials say no one downloaded anything from the FTP site

- Michael Barnes:

> "That FTP site did not affect us in any way shape or form because we did not do any file transferring from it. None of the servers ever connected so no one could have transferred files from it. No files were transferred relating to state elections."[20]

- Dr. Britain Williams

> "This [the Diebold FTP site] would have had absolutely no effect on the election system as implemented in Georgia. The State does

*ITA: Independent Testing Authority

not obtain its election system code from an FTP site or even from Diebold...The ITA, not the vendor and certainly not an open FTP site, provides the KSU [Kennesaw State University] Election Center with the source code, the object code, and various related files. "[19]

Then, Diebold officials decided that modifications were not done at all

• *Salon.com*: Joseph Richardson, a spokesman for Diebold, denied that a patch had been applied to the Georgia machines: "We have analyzed that situation and have no indication of that happening at all," he said.[21]

• Interview with Joseph Richardson:[22]

Harris: "Did you say, when interviewed by Salon.com, in reference to whether patches were put on machines in Georgia, "We have analyzed that situation and have no indication of that happening at all."

Richardson: "Well, that is what I said at the time, however, we have continued to investigate the matter and … (very, very long pause) Yes that is what I said to Salon.com."

Harris: "Do you stand by that now?"

Richardson: "We have continued to look into the matter."

Harris: "As you have continued to investigate this, do you have any new information as to whether patches were put on in Georgia?"

Richardson: "No."

Harris: "Has anyone thought to just call them up and ask? The Secretary of State's office?"

Richardson: "I can't say."

Harris: "What was the rob-georgia file? Who is responsible for it?"

Richardson: "I'm not privy to that information."

Harris: "Who would be able to answer that question?"

Richardson: "I can't tell you."

After this not very helpful exchange, I found myself back to my original question: *Who or what is "rob-georgia?"*

And then...

Date: Thu, 13 Mar 2003
From: "Rob Behler"

Hi Bev;

I read your recent article about Diebold Elections systems. Just wanted to let you know that I am the Rob in Georgia that they claimed they didn?t [*sic*] know about.

Thanks,

Rob Behler

And again, blessed are the whistle blowers.
They may save this democracy yet.
— concerned citizen

Chapter 8 footnotes

1 – Thomas Jefferson to Archibald Stuart. 1799

2 – Thomas Jefferson to Thomas Cooper, Nov 29, 1802

3 – *The Best Democracy Money Can Buy*, by Greg Palast (Pluto Press)

4 – Thomas Jefferson to George Washington, 1792

5 – Phone conversation between Bev Harris and Jim Galloway, March 2003

6 – *Scoop Media*, 10 Feb 2003; "System Integrity Flaw Found at Diebold Election Systems" http://www.scoop.co.nz/mason/stories/HL0302/S00052.htm

7 – *Scoop Media*, 13 Feb 2003; "Georgia's Last Minute 2002 Election Machine Fix" http://www.scoop.co.nz/mason/stories/HL0302/S00095.htm

8 – *Scoop Media*, 8 Jul 2003; "Sludge Report #154: Bigger than Watergate" http://www.scoop.co.nz/mason/stories/HL0307/S00064.htm

9 – *Baltimore City Paper*, 11 Dec. 2002; "Computerized Balloting is Taking Over Elections In Maryland—But Can We Trust the Results?"

10 – *Salon.com*, 5 Nov. 2002, "Voting into the void: New touch-screen voting machines may look spiffy, but some experts say they can't be trusted"; 20 Feb. 2003 "Hacking Democracy"; 23 Sept. 2003 "An open invitation to election fraud"

11 – *Associated Press*, 25 Feb. 2003 "Silicon Valley Wary of Voting Machine"

12 – *Wired News*, 7 Aug. 2003, "New security woes for e-vote firm"

13 – *The Plain Dealer*, 28 Aug. 2003 "Voting machine controversy Head of firm seeking Ohio contract committed to Bush victory "

14 – *The Beacon Journal*, 15 Aug. 2003 "E-Voting Becomes Touchy Topic" by Erika D. Smith

15 – *The New Yorker*, 7 Nov. 1988 "Annals of Democracy: Counting Votes" by Ronnie Dugger

16 – Rules of Office of the Secretary of State Election Division Chapter 590-8-1, Certification of Voting Systems

17 – Diebold internal document: "Certification Requirement Summary" Governing entity: Georgia

18 – Open Records Request, 25 Mar 2003, Response to Open Records Request from Denis Wright by Clifford Tatum, Assistant Director of Legal Affairs, Georgia Election Divison

19 – "Security in the Georgia Voting System," 23 Apr. 2003, by Britain J. Williams, Ph. D.

20 – Bev Harris interview with Michael Barnes, 11 Feb. 2003

21 – *Salon.com*, 20 Feb. 2003 "Hacking Democracy" by Farhad Manjoo

22 –Bev Harris interview with Diebold spokesman Joe Richardson, 26 Feb. 2003

Chapter 9
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris

with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar

9
Noun *and* Verb?

So, what or who is rob-georgia?

When you interview voting system officials, you spend twice as much time following up on their dodgy answers as you do asking the questions in the first place. Flip back to page 165, Chapter 8 and take a look at Joe Richardson, who I believe you might also find in *Webster's Dictionary* defining the word "stonewall." Compare him with Rob's straight-talking interview.

Meet Rob Behler:

Harris: "What was your position with Diebold in Georgia?"

Rob: "I was a server technician and then Product Deployment Manager for the Georgia project."

Harris: "What was the FTP site for?"

Rob: "One of the problems we had was an issue with the GEMS database. They had to do an update to it, so they just post the update to the Web site."

Harris: "What was rob-georgia?"

Rob: "I believe what that file was for, I did a — well, there were a ton of holes with the programs on those machines. When they all came into the warehouse, I did a quality check, this was something I did on a Saturday. I found that 25 percent of the machines on the floor would fail KSU testing —"

Harris: "What is KSU testing?"

Rob: "Kennesaw State University. We knew basically what they would be testing and the trick was to make sure the machines would pass the testing. So I went and checked a pallet and found it was bad. And I checked another, and another, and I knew we had a problem...

"I'd come in on a Saturday, I had two of my sons with me, and I thought, I'm going to just look, and it was bad.

"Then first thing Monday morning I raised the question, I said, 'Hey guys, we've got a problem — there's 20-25% of the machines that are palletized that are failing..."

How quirky. How did this batch differ from what was certified by the ITA labs and signed off on by Diebold quality control? Was this just a fluke, or a breakdown in the whole certification and testing system?

Harris: "What kind of problems were you seeing?"

Rob: "...One of the things we had wrong was the date wasn't sticking in the Windows CE. The real time clock would go to check the time on the motherboard, and it would have an invalid year in it, like 1974 or something...

"They had to do an update in [Windows] CE to fix all those dates. So the way we did that in the warehouse was, they would post whatever the update was on the FTP site. James [Rellinger] would go get the file and put it on the [memory] cards. Because you load everything through the PCMCIA cards. You boot it up using the card and it loads the new software...

"I went over to Dekalb [County]. We updated 1,800 machines in basically a day and a half. I still remember ol' Rusty, down at the warehouse, we ended up touching every single machine off the pallet, booting 'em up, update it, we had a couple hundred machines done when in comes a new update over the phone.

Harris: "You mean you used a modem or they called you on the phone?"

Rob: "No. A phone call. They'd say 'Oh, no, no, the way we had you do, that's not going to work, here's another thing to do. Okay, we just did a few hundred machines, now we gotta do it this way..."

Rob and I discussed how patches were downloaded. For some reason, the techs were told to use their own laptops to download files from the Diebold FTP Web site.

According to Rob, he was instructed by Diebold not to discuss anything with Georgia's voting machine examiner (Dr. Brit Williams) or other state officials. This was awkward because Dr. Williams was working alongside Rob at times, and when Dr. Williams asked questions, Rob made the mistake of answering. This infuriated Diebold managers. We'll get to the shouting and lying in a minute, but for now, back to downloading those program modifications:

Rob: "They used my laptop. It was not secure, either. They just used the laptop to repro the cards. Diebold never gave us anything [any laptops] with a PCMCIA slot, then they'd tell us, 'Go download this,' so we'd have to get out our own laptop to do it."

Harris: "Who instructed you about the FTP site? Was it a Diebold employee?"

Rob: "It was Diebold."

Harris: "Was it the people in Ohio or the people in Texas?"

Rob: "The people in McKinney [Texas]."

Harris: "Who were some of the Diebold people? Do you remember any names?"

Rob: "Ian. I remember one of the guys, Ian, I can't remember his last name. One of the main guys we dealt with was a guy named Ian. He was actually involved in the design of the motherboard. He was very much involved in trying to figure out how to fix the problems. So they sent us upgrades, but then after we did it KSU, still failed a ton of machines."

(Ian Piper was a stockholder in the company acquired by Diebold, Global Election Systems. The staff directory lists him as Manufacturing Manager, Research & Development division for Diebold Election Systems.)

Harris: "As I understand it, they send the system to Wyle labs for certification and also to Ciber to test the software. But from what

you are describing, I can't understand how the machines got through what they are telling us is 'rigorous testing.'"

Rob: "From what I understand, they ended up figuring out that the cards that we were loading, that fix that Diebold provided for us, well they were never tested, they just said, 'Oh here's the problem, go ahead and fix it.'"

Harris: "So what is your opinion about the certification testing?"

Rob: "No, it's not just that. NOBODY even tested it! When I found that out — I mean, you can't not test a fix — I worked for a billing company, and if I'd put a fix on that wasn't tested I'd have gotten *fired*! You have to make sure whatever fix you did didn't break something else. But they didn't even *test* the fixes before they told us to install them."

But Dr. Brit Williams told us this is not possible. "After state certification any change to either the Microsoft operating system or the Diebold election system voids the state certification," Williams assures us. "The revised system then must then go back through the entire ITA Qualification and State Certification."[1] And remember, before being shipped to Georgia, these machines go through testing. Rigorous testing.

Rob: "Look, we're doing this and 50-60 percent of the machines are still freezing up! Turn it on, get one result. Turn it off and next time you turn it on you get a different result. Six times, you'd get six different results."

Harris: "Can you give me an example of different results?"

Rob: "Meaning the machine does something wrong different each time you boot it up. One time and it would freeze on you, next time it would load the GEMS program but have a completely different type of error, like there'd be a gray box sitting in the middle of it, or you couldn't use a field."

Harris: "Was this all due to the clock?"

Rob: "I don't know for sure. They [the machines] were not originally doing it. Then they fixed the real time clock, and it was supposed to make it work normal. It fixed the clock problem — the clock problem had caused it to come up and not show the battery at

> one point...I mean, *you don't have the machine plugged in*, you boot it up, and it starts, and says it 'has no battery.' That's like saying, 'this morning I got out of bed and I stood up and I had no brain.'"

A memo from Talbot Iredale dated July 2, 2002, confirms the clock problem. "The new WinCE 3.00 release is now on the FTP site," it says. The memo directs the user to get a file called WCE300-020702.zip and says that the purpose of installing this modification is to "fix problem with getting and setting persistent Real Time Clock values," among other things. Iredale instructs the user to "Copy both the fboot.nb0 and the nk.bin files to a PCMCIA card and insert it into the bottom slot and then power the unit on," adding that this process will modify both the bootloader and the WinCE image.

"WinCE image" is a term is used to describe the specialized Windows operating system developed by Diebold for use with its touch screen system. It refers to an operating system, not a picture or an "image" in the traditional sense.

Not only was this modification to Diebold's customized version of Windows CE not certified, but Iredale also indicates at one point that he wants to avoid letting Wyle (the certifier for the touch screen firmware) look at Diebold's special Windows source code *at all*. In a memo dated April 15, 2002, Talbot writes: "We do not want to get Wyle reviewing and certifying the operating systems. Therefore can we keep to a minimum the references to the WnCE 3.0 operating system."

Whatever was on the special Windows system cooked up by Iredale and others at Diebold, it didn't seem to work very well:

Rob: "And then when we loaded the software to fix that, the machines were still acting *ridiculous*!

"I was saying, 'This is not good! We need some people that know what this stuff is supposed to do, from McKinney, NOW! These machines, nobody knows what they're doing but Diebold, you need some people to fix them that know what's going on. They finally brought in guys, they ended up bringing in about 4 people..."

You'd think that with such troubles, someone might follow standard company procedure and write up a "bug report."

"All bugs ever reported have bug numbers," wrote Ken Clark in a memo dated Jan. 10, 2003, pointing out that the whole collection can be found in "Bugzilla." So I went looking for Bugzilla reports from Georgia. My goodness. They weren't there!

Bugzilla report numbers 1150–2150 correspond with June–October 2002, but although hundreds of these bug numbers are mentioned in memos and release notes, I only found 75 Bugzilla reports for this time period, and none from Georgia. Strange. I was looking forward to reading the explanations about how computers can get up in the morning and announce that they have no brain. Aha! Here's a memo about missing Bugzilla files: It's dated 8 Jul 2002, from principal engineer Ken Clark:

S*ubject*: **bugzilla down, we are working on it.** "We suffered a rather catastrophic failure of the Bugzilla database," he writes. He warns that recovery of the bugzilla reports "will be ugly" and adds that "there will be a large number of missing bugs."

In a follow-up note on July 16, Clark says, "Some bugs were irrecoverably lost and they will have to be re-found and re-submitted, but overall the loss was relatively minor."

To understand the significance of these two e-mails, you must realize that among programmers, system backups are a religion. People are fired for not performing a daily backup. Some programming shops back up every shift! Because backups are critically important, expensive *automated* tape systems are employed to minimize any data loss. By our estimation, almost a thousand bug reports are missing, including all the Georgia bugs.

Rob: "When the machines came in, they came to us first. They were in the warehouse. We assembled them. They'd come in a box with a touchscreen, and another box with the booth. We assembled the machine and we ran it though a series of tests. We'd check the power cord, boot up the machine, check the printer, bar-code it, update Windows CE, then send it on to Brit. He did the KSU testing. The L&A [Logic & Accuracy] was done at the county level, right before the election."

Harris: "So…the L&A was not done at acceptance testing?"

Rob: "It got so there wasn't time. They did it before the election."

Now, supposedly, this L&A testing procedure is kind of a "mock election", which you do by entering practice votes. I pictured people pushing the touch screen and wondered how many test votes you push before your finger gets really tired. Not that many, apparently:

Rob: "The L&A testing — You would just enter, like, one vote and — you just choose one — you don't need to be specific on which one.

I see. One vote. But then I found out that some of their L&A test involves no touching at all:

6.1. Test Count

- performing a manual Logic and Accuracy Test
- performing an automated Logic and Accuracy Test

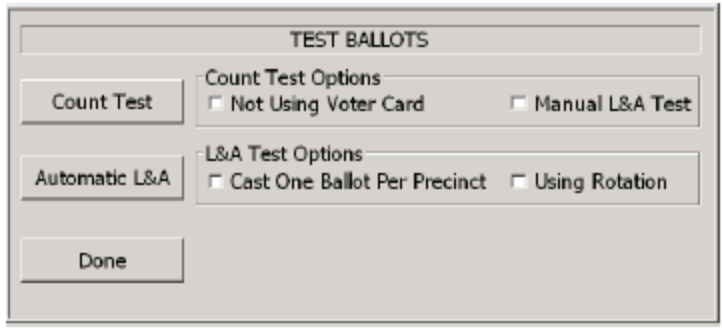


Figure 6-2: Test Ballots Screen

Ballot Station Users Guide: *"The automatic L&A test, on the other hand, allows a pre-determined combination of ballots to be automatically selected and marked, according to the voting options selected."*

Rob: "I worked there from mid-June to mid-July. The whole time they were upgrading the software and doing some sort of fix to it..."

"You've gotta go take care of this JS [junk shit] equipment, I told them. Finally, I raised it as high as you go, I raised it to Bob Urosevich, he's the head of it. [Urosevich is President of Diebold Election Systems]. I told him personally, 'This is bad, I don't see us putting an election on with these machines!'

"That's where they finally assembled the teams. They got some big ol' vans, we loaded up as many people as could fit in."

Question: Who paid for the vans? Diebold?

Who paid for the people piling into the vans?

Because now I'm having a hard time understanding why Diebold says it "had no indication" that these patches were done at all. Perhaps Diebold spokesmen can check with their own accounts payable department and then provide us with thorough, honest, and forthright answers about the Georgia program modifications.

If a private company, like Diebold, asserts its right to secret control of the public voting process, is it too much to ask for such a company to answer questions? I'm sure I am not the only one who finds this behavior intolerable.

Rob: ..."And then you know, ironically, later on right before I exited, they were scrambling for a date, they were trying to get us, the teams, into Fulton County to do Fulton County's 1,900 machines.

"They were in the most horrific spot. The place they warehoused them was like 1,900 machines in a little office space, there was no way we could get at them. The machines are like 58 pounds, and they had to bring them in, unstack them off the pallet, restack on the pallet. Talk about labor, talk about wasted money! It's like a warehouse and offices off Interstate 75, in Atlanta, I'm talking to this guy, he's a great guy, he's from Fulton County. Him and I were scheduling this, figuring it out how to get to these machines and

er of *WiredNews,* "denied that Rob ever mentioned patches to him and said, to his knowledge, no uncertified patches were applied to the machines. He said he would be very concerned if this happened."[2]

He should be concerned, because if Rob's story is correct, Diebold may have violated federal regulations. Patching systems after they've been certified opens the possibility for malicious code to be installed into the voting system, altering the results — which is precisely why it is against the law. The results of any election that used patched Diebold systems might be called into question.

The scenario that Dr. Williams has been reporting to state officials just does not correspond with what we are learning from Rob. Williams writes:

"Overall security of any computer-based system is obtained by a combination of three factors working in concert with each other:

"First, the computer system must provide **audit data** that is sufficient to track the sequence of events that occur on the system and to the extent possible, identify the person(s) that initiated the events."

But in the next chapter we will blow up the audit procedure.

"Next, there must be in place well defined and strictly enforced policies and procedures that **control who has access to the system**, the circumstances under which they can access the system, and the functions that they are allowed to perform on the system."

I must have missed the section of the operating manual that describes people piling into vans and driving around updating voting programs with uncertified patches, using cards they made on their own laptops.

"Finally, there must be in place **physical security**; fences, doors, locks, etc.; that control and limit access to the system."

Well, at least they have our voting machines under lock and key.

Back to the interview:

Rob: "They were actually swapping parts out of these machines that were on site. They'd cannibalize a machine with a bad printer or whatever, they'd grab the screen off of that to put on another

machine with a failing screen, they'd retest it. They were not just breaking them down, they were taking pieces off and putting it back together.

"Even the machines that are updated, that had the right release of the software, exactly like the company wanted it, you'd boot it up and all kinds of crazy things would happen. That led to my belief that when voting took place, there would be problems."

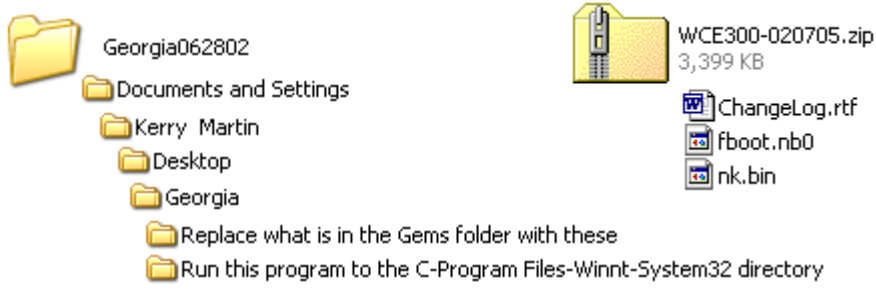
Harris: "Do you remember what release number it was?

Rob: "Release — I don't remember the number because what they did was it was always the date...

"The date was...let me see...**June 28**. No, the last one, the date that was supposed to be on there was **July 5**. There was about three updates, the CE software, the date that would come up would be the last. After that they came up with another fix, that's the August one at that point.

The more you examine this "electronic patch" thing, the more out of control it looks. From the memos, it appears there were so many patches that the garment might have changed color altogether:

Date: Thu, **13 Jun 2002**
Subject: WinCE 3.00 June 7th Release
From: "Talbot Iredale"
"The new WinCE 3.00 and bootloader are on the ftp site. The file is WCE300-020607.zip...



These files were found on the Diebold FTP site in January, 2003.

Date: Tue, **2 Jul 2002**
Subject**:** WinCE 3.00 July 2, 2002 Release
From: "Talbot Iredale"
"The new WinCE 3.00 release is now on the ftp site. The file is WCE300-020702.zip..."

Date: Thu, **4 Jul 2002**
Subject**:** WinCE 3.00 July 04, 2002 Release
From: "Talbot Iredale"
The new WinCE 3.00 release is now on the ftp site. The file is WCE300-020704.zip

Date: Fri, **5 Jul 2002**
Subject**:** WCE 300 - July 05, 2002 Release
From: "Talbot Iredale"
"...This is fixed in the July 05, 2000 (*sic)* release which is now on the ftp site."

Date: Thu, **8 Aug 2002**
Subject**:** WCE 300 - Aug 08, 2002 Release
From: "Talbot Iredale"
"The WCE300-020802 release is on the ftp site."

Date: Wed, **9 Oct 2002**
Subject**:** AV-TS R6 Bootloader and WinCE version numbers
From: "Ian S. Piper"
"...another method for determining the version number of the install files, prior to installation, is to view the creation date of the file on the flash memory card and compare it to the list below. (Unless you trust that someone has labeled the flash card correctly.) ...I've created a list of the file creation dates, and their versions...

Bootloader (filename "fboot.nb0")
Mar. 14th, 2001 Rev 1.00
Jan. 28th, 2002 Rev 1.01
Jun. 7th, 2002 Rev 1.02

Windows CE Image (filename "nk.bin")
May 25th, 2001 WinCE 2.12
Jan. 28th, 2002 WinCE 3.0
Jun 7th, 2002 WinCE 3.0
Jul. 2nd, 2002 WinCE 3.0

Jul. 5th, 2002 WinCE 3.0
Aug. 8th, 2002 WinCE 3.0

He adds, "Someone with the BallotStation install file archives can create a list of BS [Ballot Station software] versions if they want to bother."

There were more patches — the "clockfix.zip" patch is a little addition dated July 7, 2002. According a memo dated Aug. 6, 2002, Kansas may have caught a few bugs from Georgia:

Tuesday, August 06, 2002
Steve,

"It was believed that only units built for Georgia would be affected. However, Lesley had 38 units shipped to Johnson County around the same time, so she was affected as well. There should be no others (famous last words)..."

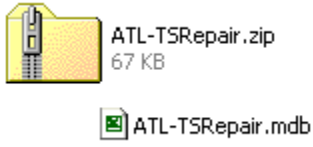
The techs were stitching new updates into the voting machines right up to Nov. 5, 2002 — Election Day and, apparently, even after the election:

...Rob: "...This is an example we did: We would plug it in, boot it 3 times, unplug it, boot it three more times. I wrote a sheet on this.

"This guy came in from McKinney, he was about the second in command. He's a good friend of Bob Urosevich. About second to Bob, at least now, he got a promotion. Greg? Something like that. He flew in and I went to Dekalb County and I tested and together we went through, and we wrote down every single error, and he booted them himself, and was looking at the results and seeing how sporadic they were. and we found out of the machines we tested, about 75% of the machines had different sporadic things.

The date on this file is Nov 11, 2002 — just six days after the general election. The file it appears to be "repairing" corresponds with the database used to count the touch screen (TS) votes in GEMS.

It is passworded and I have not opened it; and therefore I don't know what kind of repair it is making.



Certification Requirements Summary

Governing Entity	Certification Required	Need NASED #	Need Wyle Cert	Need CIBER Cert	Modification Requires Recertification	Submission Form Required	Technology Escrow Required
Alabama	☑	☑	☐	☐	☑	☐	☐
Alaska	☐	☐	☐	☐	☐	☐	☐
Arizona	☑	☐	☐	☐	☐	☐	☐
Arkansas	☑	☐	☐	☐	☐	☐	☐
California	☑	☑	☑	☑	☑	☑	☑
Colorado	☑	☐	☐	☐	☑	☐	☐
Connecticut	☑	☑	☐	☐	☐	☐	☑
District of Columbia	☑	☐	☐	☐	☐	☐	☐
Florida	☑	☑	☐	☐	☑	☐	☐
Georgia	☑	☑	☐	☐	☑	☐	☐

This document was found in a file from the Diebold FTP site. As you can see, any change to the software required recertification.

He was working with me and we were writing them down, we literally wrote everything down."

" — Greg Loe is his name. [Greg Loe, Controller] I drove him out there. Brit [Dr. Britain Williams] was there, KSU was doing their testing. **They were bombing these machines out left and right.**"

"I'm telling him, 'They're all like this.' At this time I was working 150 hours in 2 weeks. I was there all the time with these machines, that's the reality of it. The techs were working overtime trying to fix them. We couldn't get enough from the factory because so many were bad. You'd get a shipment of 300, but 75 were bad; they couldn't put them out fast enough to replace all the defects...

Harris: "I understand they did a big demonstration during the summer, with the machines."

Rob: "I was there when they told me I needed 1,100 machines for a demo. I thought, 'The trick is coming up with 1,100 machines that actually work."

Harris: "Do you know who was writing the fixes?"

Rob: "He had a weird name. He came out of Canada...— That's it! Talbot Iredale, [he] would actually fix it and say, 'Oh, here's the problem,' and stick it on the FTP site. We'd grab it, stick it on the card and make a bunch of copies and use it."

"...They produced it and got it to us in 24-48 hours. If I'd known they hadn't tested it, I simply wouldn't have installed it! My background tells me that's a no-no...

Let's revisit the concept of locks, keys, fences and warehouse security

Harris: "How secure were the machines, from what you saw?"

Rob: "I'll tell you something else — we didn't have badges. People could just walk right in and get to the machines."

Harris: "Do you think anybody could have tampered with a machine, if they wanted to?"

Rob: "Well, when we did the quality control check, we'd open it up. They have a little box for the printer. We would find the key still in the printer. Someone could literally take that. We found cards left in the machine. [Voter cards activate the vote; memory cards store the votes.] I wondered what would happen if the wrong person got it..."

Harris: "Were there any protections to keep you from duplicating memory cards, or to have them serial numbered or whatever?"

Rob: "The memory cards, you can just duplicate them. You have to have the proper info on the card for the machine to boot up, but you can just make copies of the cards."

If what Rob is describing sounds pretty slipshod to you, you're not alone. In a September 2003 letter by a member of the Georgia Elections Board to Cathy

Cox (Secretary of State), we learn that voting machine security is rather lacking.

"A missing DRE (*touch-screen voting machine*) for the State Board of Elections is tantamount to a missing ATM for a bank," J. Randolph Evans states in his letter. He then goes on to report that voting machines have been found in hallways, stairwells, and trunks of cars.[3]

* * * * *

Now every good fiasco has a little shoutin' and lyin'. This one has it all — office politics, regular politics and people scrambling to protect the company checkbook.

Harris: "When I asked Diebold if there was anyone named Rob in Georgia, they said no. Did they know about you?"

Rob: "They knew me and they knew me well. I met Bob Urosevich [President of Diebold Election Systems] a couple different times, and Ian, and then Greg Loe, he got promoted, he was basically Bob's right-hand man..."

"You know one of the main things that really just made me so upset, they were just, like, 'This Brit guy, don't even speak to him, it's a political game, you've gotta play the politics.' Well, he walks in and says, 'What are you guys doing?'

"I said, 'We're putting in an update.' He said, 'Will it change what it does?' We said, 'Just do your normal test, we're supposed to get the machines ready for you.'

"He tells someone at the office and they freaked out. They were like, 'What the heck are you doing???'

"I wasn't supposed to talk to him at all, I guess. The guy had a flannel shirt on, he was kicking it and he was very genuine and open and there we are in the same room together, but because I actually spoke to him I got reprimanded. They said, 'If they ask you any question, you gotta say, 'Talk to Norma, to one of us...'''

Harris: "What did you say to him, anyway?"

Rob: "He [Williams] said he wanted to talk to me, so I met him in this little side office and [he] asked me what was going on. I basically said I was updating the machines, doing a quality check making sure the machines are the same, making sure they had the the right release of Windows.

"Essentially, when I got back there was a meeting called. Urosevich was in it with a conference call. I went in, la-dee-dah, thinking I'd been doing a great job and it caught me by surprise. It just totally blew me away that they would be so incensed, and just absolutely angry about something so frivolous as the basic information I gave Dr. Williams. I've never been told to shut up so many times by so many people."

Harris: "You mean, 'shut up in this meeting,' or 'shut up' by not talking to other people?"

Rob: "I'll tell you exactly, I'll give you a quote — this came from Urosevich: He said, 'We don't need *you* airing our dirty laundry!'"

"It was during that meeting the details came to light for me about patches and certifying them. I wasn't aware of that before. There was this big discussion about what needed to be certified. In the course of trying to determine whether they needed to be certified, they were saying, 'What do we tell Kennesaw State?' Everybody went around and gave opinions except for James Rellinger, who didn't know. Wes [Krivanek], Norma [Lyons], Darrell [Graves], Bob [Urosevich] on the phone, each gave opinions on how it should be spun as to what we were trying to do. During the course of the conversation I said, 'Can't we just tell them? What's wrong with that?'"

"[they said], 'No no you can't do that, it may be a certification issue!' We were sitting around tables with Urosevich on speaker phone, trying to decide whether to tell the truth, half the truth, or a complete lie."

Georgia had just ordered up $53.9 million in voting machines, and the ink on the check wasn't quite dry.

"If they started erring in mass quantities, Kennesaw State's going to raise a red flag, the secretary of state's going to raise a red flag and Diebold wouldn't get paid," Behler told Kim Zetter of *WiredNews*. "I understand if a company has

information they need to keep under tight lip. But when you sit around discussing lying to a client in order to make sure you're getting paid . . . it's an ethics issue."

> **Rob**: "The rumor around the office was that Diebold lost maybe $10 million on the Georgia thing. I mean, they only sold the machines for what, $2,000 or $2,500, and then you have to build them and then you're paying people $30 an hour and you are out touching 22,000 machines *four times* — there's no way they didn't lose money on this deal...
>
> "The gist of the conversation was, you screw around with this and they might decide not to pay us."

How credible is Rob Behler?

Dr. Brit Williams told *WiredNews* that Behler was a disgruntled employee who was fired from the project by Diebold and Automated Business Systems and Services.

Rob's personnel records discredit this assertion.

"'He was released because his part of the project was completed,'[ABSS vice president for the southwest region Terrence] Thomas told *WiredNews*, explaining that there was no performance issue with Behler's work.

James Rellinger, a Diebold contractor who worked with Rob, also rejects Williams' interpretation of events. Rellinger told *WiredNews* that both Diebold and ABSS seemed happy with Rob's work.

But there are additional reasons to believe Rob:

• I spoke with Rob in March 2003. He had no way of knowing which files were sitting on the Diebold FTP site in January 2003 since he had not worked for the company in months — yet in his interview, he mentions specific electronic patch files, and I was able to find the files he mentioned among those on the Diebold web site. The file dates matched exactly, and the information in the accompanying release notes supports Rob's story. (This, by the way, directly contradicts Diebold's claims that these files were not used in an actual election.)

• Rob could not know that internal memos from Diebold would surface. He recalled that people with the names "Talbot Iredale" and "Ian" were involved with the fixes. Now we know that memos written by Talbot Iredale and Ian Piper

reveal patches just like those reported by Rob. These 2002 memos, which were revealed in August 2003, contain 13-character passwords for the matching files on the Diebold FTP site — files which had never been opened because they were locked with complex passwords. The passwords in the memos open the patch files found on the FTP site in January 2003.

• I interviewed Rob in March 2003; Kim Zetter from *WiredNews* interviewed him in September 2003; I interviewed him again in October. He never evaded questions and his answers stayed consistent over this six-month period.

• Rob was told to download information to his laptop. He has saved several files. He has the notes taken while demonstrating problems to Greg Loe and has provided a copy of his notes (and a videotaped deposition) to a lawyer who is working on a case with Georgia activists.

Rob: "...I went into this Diebold thing with no real knowledge of the voting industry. When I left, I not only had a complete grasp, but I had a complete disrespect for these machines.

"And with the folks in the office who were so — you know, 'I'm the political person, you have to know how the system works' — they were so much more concerned about their own self-importance, they were losing track of *do the machines count the vote properly*!

"Because that's what the people in Georgia need.

"And I'm one of them."

Rob jeopardized his employment future by stepping forward to tell us what really happened in Georgia. He has never asked for anything. This is especially impressive when you learn about a method that citizens like Rob can use to enrich themselves (albeit at the expense of the public interest).

In cases in which a government agency has spent taxpayer money based on fraudulent claims, the first citizens to file a *Qui Tam* lawsuit collect as much as 30% of the money mispent by the agency in question — in this case, for Georgia, nearly $54 million. The catch? The case must be filed under seal. No congressional investigation, no public disclosure, just a secret filing that may or may not get unsealed.

But citizens need to know the details about these voting machines. There are bills pending in Congress and states considering purchase as of this writing. Secreting the evidence away, so that a few citizens can line their pockets with

millions (and sidestep liability in the process, while leaving honest citizens, like Rob, hanging out the window), just seems wrong.

I told Rob about *Qui Tam*, and suggested that he consult someone for guidance to decide whether to pursue this path. He did. He consulted the Bible. He looked up what the Proverbs have to say, and shared their wisdom with me.

"I'm not interested in it," he decided. Now, Rob Behler is a man who is raising seven children with little material wealth. He could probably use 30 percent of $54 million. Instead, he has chosen to protect the security of your vote by telling the truth, publicly. In Rob Behler we meet the kind of quiet, patriotic citizen that makes us proud to be Americans.

Rob-Georgia: Epilogue

Harris: Do you remember the date when you got this job back in June?

Rob: Yes. June 24.

Hmmm.

Harris: Are you sure it was June 24?

Rob: Yes. June 24 to July 29.

Date on the rob-georgia files: June 4.

Twenty days *before* Rob was hired.

Back to Square One. Who or what is "rob-georgia?"

Chapter 9 footnotes

1 – "Security in the Georgia Voting System," April 23, 2003, by Britain J. Williams, Ph. D.

2 – *WiredNews.com*, 13 Oct. 2003; "Did E-Vote Firm Patch Election?"

3 – *Georgia Vine* Vol. III, Issue 18, 25 Sept. 2003.

Aug 18, 2003:
2004 Presidential election was offered for sale on E-Bay.
Asking bid: $99,999,999.99

Chapter 10
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris
with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar

10
Gently now...Carefully...Take the Lid Off and —
Eeeeew!

This chapter will be delving into unavoidably technical areas. This presents a challenge to the reader if, like me, you don't have a computer background. Even if you don't understand the specifics of the flaws uncovered, the gist of the problem is apparent. You will see our evolution from curiosity, to concern, to alarm as we unravel the voting system.

I certainly am not a programmer and, aside from looking at filenames, I wasn't much help in analyzing what was in the files. But by June 2003, Diebold voting files had begun to pop up in various places, and we learned that citizens all over the world are deeply interested in how their votes are counted.

Spontaneously, people began analyzing the voting system files, discussing them, and doing a little surreptitious comparison of their findings. *Hey, come over here, look at this ... We're trying to find out how our vote is counted!*

"This is dangerous," someone explained, to everyone's surprise. "Bad things could happen. Very bad things."

Can someone please explain to me how our "democracy" turned into something where ordinary citizens can get arrested just for looking at how their votes are counted? No, I'm not asking you to explain the "Digital Millennium Copyright Act" (DMCA),[1] which in Internet circles is almost as controversial as the Patriot Act. The DMCA was designed to clamp down on music swapping, but somehow it morphed into a tool that can eliminate free speech without due process and may punish copyright violations with jail time.

Some people say the DMCA might be used against any citizen who studies the software that counts his votes. What I want to know is this: How can we call ourselves a democracy if we are so afraid of the consequences that we don't dare to inspect our own vote-counting system? No, don't take this opportunity to

describe the DMCA law to me, or explain the history of how this came to be — what I'm looking for is an explanation of how *scaring people* who simply want to make sure their votes are counted properly can possibly be the right approach to a robust democracy.

Apparently, this peeking at how we count votes is dangerous and (possibly) forbidden — but no one seems to know for sure. Lawyers confess to uncertainty as to whether looking at vote-counting files found on an open Web site can be permitted.

For several months, I considered this issue. As of the writing of this book, I've not yet been able to get a straight answer out of anyone. Here is what *I* came to believe, after much thought: I think that examining our voting machine software is not only a legitimate activity, but it is also our civic duty. For queasier souls, I offer these statements in defense of this endeavor:

1) These files were publicly available.
2) Examining them is in the public interest.
3) Our objective is study and review, not copying and selling voting systems.
4) In a democracy, vote-counting should not be secret in the first place.

The Internet is alive with message boards, chat rooms and forums. People go to these Web sites to meet and converse with each other, using whatever name they choose so that they can feel free to express any opinion they like. One such forum is DemocraticUnderground.com (DU), a rapid-fire political discussion board with more than 30,000 participants. Because this kind of venue provides a feeling of safety and anonymity, citizens have been able to muster up the courage to examine our voting system.

I perused more than 5,000 comments about voting systems from DU, and I think you'll agree that the excerpts from the 75 posts that follow show a remarkable picture of democracy in action.

> "I haven't seen the Diebold machines or how they operate, but in my precinct, we have a numbered ballot we fill out that is scanned into a machine. In case of a questionable result, the numbered paper ballots can be used to verify results by

* In order to protect the innocent from the guilty, we have changed all the screen names.

> a hand count. The Diebold machines should have something similar."
>
> — "Cleaver"*

Three months later, "Cleaver" got a rude awakening. He learned that he has indeed been voting on Diebold machines and that a security breach was discovered right in his home county.

A lively discussion took place when programmers began looking at the source code itself:

> "What could this thing possibly be doing to need so much source code? I have built systems ten times more complex than any imaginable voting machine in 1/100th the source code space. Sometimes when programmers don't know what they are doing this is the result – lots of cut and pasted functions that are almost the same, tons of obsolete but not removed code ... Ugh."
>
> — "Romeo"

"Given that professional programming is complex by its nature and professional programmers are often messy tasteless people by 'normal' social standards, I'd be surprised if it didn't look like this. In fact, while the sample in question is small, it looks like at least half of the source is visual C++ generated from templates by click&drag, by virtue of its unpleasant-to-type words.

"Once the compiler gets hold of it, chops logicals and optimizes loops, you'll never know how crappy the source looked anyway. Believe it or not, there are actually contests (such as the infamous 'obfuscated C contest') to write the most convoluted and inscrutable programs possible."

— "mortal"

> "I don't think it's likely that you can prove anything with the source code. You won't find a function called "double_GOP_Votes" that does fake counting ... nevertheless, we could very well find backdoors, which aren't that uncommon, that would allow tampering."
>
> — "BettaWatchYerVote"

Some participants argued about the discussion process itself...

> "The thought struck me after reading the third or fourth message that this dialogue should not be on a public forum."
>
> — "ErgoWeAre"

> "Why not? This is the very underpinning of democracy we're discussing here. If there was ever a need-to-know issue for the general public, this is it."
>
> — "mortal"

Others suggested the most efficient ways to hunt for vote fraud:

"Have any empirical tests been done? Meaning, generate a large amount of output with the code, and analyze that output, looking for anything the least bit funny, then going back and then focusing on those funny results to look for foul play."

— "Ovaltina"

> "**Ok, so you've got your haystack and you're looking for the needle** ... Here's how I'd approach this problem:
> "...I'd begin by doing a bit of analysis on how the system is structured. Isolate the important data types (that voter info one is a good example) that someone might be interested in modifying...
>
> "After that, I'd go a few levels deeper with the functions that are doing the data modifications (look at the functions that are called by those functions.) I'd begin to chart out the "life of a vote" in the system...
>
> "...[I'd look for] code that does not appear to do what it's comments say it's supposed to do; code that is completely undocumented; any code that seems to be manipulating memory in "weird" or unnecessary ways. God help you because this is in C++."
>
> — "Bibbidi-Bobbidi-Boo"

One participant began to explore new legal issues...

"Discussion cannot be considered illegal under the DMCA.

"By making this third party code available freely, Diebold was violating the DMCA. If you would like, I could compile a quick list of third party companies and the files they are responsible for. Just those company names alone could provide you with multiple avenues of research...It's unfortunate that Diebold allowed Microsoft source code to be publically available on one of their FTP servers."

— "Clark Kent"

User manuals began to surface, answering many questions about how to operate the systems but sometimes raising new areas of inquiry.

> **"Look at this sentence**: *When you have finished entering the totals for a precinct, all Check values must be zero in order for you to proceed to the next precinct. If necessary, you can make up the difference by putting the number in the Check tally in the Times Blank field if the race is a Vote For One race. If not, you may have to perform some additional calculations to make the Check value equal zero.*"
>
> — "Jolio"

"I'm a technical writer, and even *I* can't figure out if that says what we think it says or not. Enter that one in the STC's "Worst Manual of the Year" contest. "

— "Crapper Dan!"

As time went on, a note of concern entered some comments:

> *"Why are they entering manual votes? If we have optical scanners reading absentee and touch screens reading polling votes (and the touch screens also read the challenge votes) — what is the purpose of manual entry?"*
>
> — "Jolio"

"My guess the optical scan machines may not be integrated into the same computer system as they are using to run the GEMS software. so (i am guessing) the data has to be entered manually. Even [if] the optical scan machines WERE on the same computer, it might be necessary to enter the

data manually if there is no standard protocol for transferring the data from the "optical scan" app to the GEMS software. Another possibility is write-in votes or provisional ballots."

— "K3Park"

"Write-ins, provisionals handled on the touch screen and most systems with touch screens are integrated with optical scan systems, but not all. That could be the reason for it, but if so...what security measures should it have, at a minimum? Because, manual entry might have a legitimate purpose for entering absentee votes, yet provide a back-door for tampering also."

— "Jolio"

"Unfortunately, a key piece is missing, manualentry.cpp — It's documented, but is not there."

— "Clark Kent"

"That's right... The code for GEMS Server is the key and it ain't here. Look, there's the code for the soon-to-be-hundreds-of-thousands of touch screen stations, and then there's the code for the servers."

— "Rummage"

"The system has a history of 'space' problems:

- Fixed problem with Accumulator not working with large elections (out of space).
- Fix problem with removing system.bin and AVTSError.txt files when removing old election files to make more room on the storage device.
- Add checking for minimum storage space free before allowing a ballot to be cast."

— "Lucille Goldman"

"*They have had one hell of a time with standard magnetic card readers. Programmer frustration comments are rampant in this series of modules.*"

— "*BlueMac*"

"It took 'em three years to log manual entries ... sheesh!
• Fix problem with wrong time being stored in the audit log.
• Add log entry for posting of manual results"
— "Lucille Goldman"

"I see the section on manual entry. Not a word in it on who is allowed to do it — presumably, must be someone with admin privileges, but I note this manual also has a section for remote access to the database (why does any election supervisor need to remote access their computer for voting program tasks?)

"And uh — wouldn't you say that a key event to log [in the audit] *after launching the election would be to log the closing of the election? Not a peep, they just go on and open another election."*
— *"Jolio"*

"You call that an audit log? Everybody's [logged in as] 'admin.'"
— "Lucille Goldman"

"More damning ... is that there doesn't seem to be a document detailing policies and procedures for security both at the user/institutional level and the hardware/software level. There needs to be a document detailing who is entitled to do what with the system."
— "Topper"

"The thing that disturbs me is the comment saying 'add this after it get backs from certification' (or however it's worded). While it's not necessarily nefarious doings — it could be they modified a function, and the mod was crashing, so they didn't want to insert the update it was 'stable' — the note does imply that there may be a non-certified build in use."
— "OutofTouch"

Of course, anonymous participants on an Internet message board are of no help at all if you want to document problems in a formal way. We know very little about these people's expertise or their credentials.

Among the advantages of this informal review format was the perception of protected freedom of speech, moderated to remove obviously disrup-

tive or libelous posts. The DU voting system discussions contained much postulating, backtracking, debating and sometimes plain old ignorance.

Internet forums differ from each other in character. The crowd at Democratic Underground includes many intellectuals, who like to step in to straighten out misinformation, and sometimes get quite fussy about insisting on sources for information posted. Even providing a source doesn't always suffice; a debate sometimes follows about the credibility of that source.

This public "open-source investigation" had many drawbacks, but it did attract intellectual talent and ultimately led to the first formal evaluations of the software outside the voting industry itself. One of the contributors explains how he came to be concerned about the Diebold software:

> "I'm the poor schmuck who configures brand new, untested, computer systems designed by teams of highly educated hardware engineers and loads brand new untested software designed by highly educated teams of software engineers and then performs the 'debug' to make them work together. The systems rarely, if ever, work the first time. It's been my job to be the final arbiter of the finger pointing battles between the two engineering groups who each claim the others product is at fault.
>
> "In short, I have to know enough about the hardware and the software to conclusively prove where the problem lies and then justify pulling overworked engineers off their new assignments to go back and fix something that was considered a 'done deal' under a closed out budget. Not an easy job."
>
> "...In order to survive, programmers tend to be extremely logical thinkers. They exhibit that logical thinking in the way they write their comments into the source code. Each section of code produced by a 'good' programmer has a 'plain english' explanation of what that section does. You might call it a 'professional courtesy' to other programmers who have to work with their code downstream. It's [looking at the comments] a shortcut that quickly lets you know where to focus your attention rather than study every line of code to find what you're looking for. That same logical attitude also drives them to 'ask questions' in their comments when they're asked to do something that's 'illogical' or perhaps they don't understand!
>
> "When you find comments [in the source code] that say things like [paraphrased to take the heat off of list moderators]:

'this is baloney, you don't have to do this, this function is already built in to XXXXXXX, just use the XXXXXX command'

or

'the (insert critical flag here) flag is broken so I did this and that to get around it'

and even things like

'I don't know why you want me to do this, it will let this and that happen....unless that's what you want to happen then I guess it's OK'!

"Comments of this type naturally lead a good programmer looking for problems to investigate what is going on in those routines.

Election systems are 'mission critical' in keeping the full force and power of the United States from falling into the wrong hands. The kind of crap in this code would make it, IMHO, unfit for even checking my e-mail."

— "GoodyTwoShoes"

Another contributor, known here under the screen name "Rummage," studied computer science under a Nobel laureate at Carnegie-Mellon University. In real life and under his normal name, he designs databases for critical applications in the medical field.

"So far, that's the story of the last few days... From databases with no foreign keys (read no referential integrity), unprotected transmission code, ample opportunity for buffer overruns right to PCMCIA slots for wireless modems. Not so much nefarious code as a system with so much opportunity for hacking/fraud as to invite cheating. "

"...as for structure and understanding the DB [database], there are no relationships and the Primary keys are not defined as Access Primary keys. This will make reconstructing the schema a little harder. I don't think a DBA [database analyst] designed this.

"No referential integrity — no autonumber primary keys... Bad for maintaining a reliable database — good for adding and deleting data at will."

— "Rummage"

With the Internet, you never really know whom you are dealing with; a fellow who joins a singles forum may think he's chatting up a buxom blonde named Inga from Denmark while he's actually charming a 400-pound farmer from Iowa named Ralph. I've spoken to many of the participants of the voting machine examination who seemed especially insightful, and they often have impressive credentials, but to most of the world they are anonymous so you can't really know. These informal forum discussions are more akin to casual conversation in the cafeteria than to academic research.

People outside the U.S. are keenly interested in these voting systems. Companies like ES&S and Diebold are marketing their products all over the globe, and some participants in the voting machine discussion confided to me that they are interested in U.S. elections because choices we make directly affect the rest of the world. Here are comments from a European participant who concurs with "Rummage" about weaknesses in the Diebold database design.

> "The fact that they're using Access disallows relationality ... When using a decent database, SQL Server Sybase etc, for example, constraints, triggers, stored procedures, packages, relationships, views, etc are all maintained inside the database — that's where all the business logic resides in a well crafted modern application.
>
> "With Access, however, you're dealing with basically a toy database, and since all of the above are missing, it is common to join tables on the fly using the data connection and SQL code embedded into the program itself...
>
> "... On another note, in a database system, since the system that's updating the database must write the logs, the user in this contect *(sic)* must have write capability to the log table. I could be wrong, but in Access, if you have write capability, you have delete capability...the security features are very limited.
>
> "Security is not something I would consider claiming to have for *any* Access-based application since about any user can gain access fairly easily ... and if you'd ever tried to upsize from Access you wouldn't be touting it as a good thing. Data types get changed, boolean fields don't translate, etc.
>
> "...Sorry, it's a useful tool for basic tasks but compared to a proper database, it's a toy. And it certainly shouldn't be used in a mission critical voting application."
>
> — "t_device"

On forums, people are free to make opinionated, dogmatic and sometimes mistaken statements, just as we do in casual conversation on the subway or in a bar. The Internet culture uses forums and message boards to consider perspectives and ideas, but never for a definitive answer. One reason: It all depends who's chatting that day.

> *"Dear 't_device' — Let's not get into a pissing match. My upsized applications run very nicely to this day. Yes, it's not perfect, but I've used ERwin for documentation and Access is much easier for smaller projects. You get the application running, produce the relational schema and put it on the server. You may choose to develop on the target system. I prefer my method. I hope we can treat each other respectfully.*
>
> *— "Lucille Goldman"*

"I believe we have been civil. If that's not the case, let me know. Apparently we have a difference of opinion. That's healthy. I have upsized a few Access apps and I've developed in it, so I'm not speaking off the top of my head ... Anyway, let's drop the Access better/worse convo and stick to the voting application."

— "t_device"

> "Go over to slashdot [Slashdot.org, a forum for computer people] and try talking about 'security' and 'Access' in the same breath and see how seriously they take you over there — they won't even dignify you with a response, they'll just laugh at you and spray you with onomatopoetic responses like this:
> =====
> slashdot comment:
> *choke*
> *wheeze*
> bwahahahahahahahahahahah
> *gasp*
> Wait, these things are already in use?!?
> *thud*
> ==========
>
> ...because all programmers know there is no security in Access."
>
> — "abcxyz"

> *If you want to know why Access is a bad idea.... ....just do a Google search for 'Access, vulnerability' and browse through the 951,000 hits!*
>
> *— "GoodyTwoShoes"*

Now THAT is a legitimate beef re Access… And the lack of referential integrity (which could have been done, but wasn't) only fuels my suspicions.

— "Rummage"

> *Good point about database audit log tables ... ... very easy to delete any entries. Though there should be some sort of audit ID (in any good database design) that records the sequence of audit log entries which would indicate that a log entry had been deleted.*
>
> *— "gandalf"*

Ahh, the audit log. The more people looked at it, the greater their surprise at the emphasis put on the audit log (by Diebold and its supporters) as a primary security device.

From Dr. Brit Williams*: "Overall security of any computer-based system is obtained by a combination of three factors working in concert with each other: "First, the computer system must provide audit data that is sufficient to track the sequence of events that occur on the system and,to the extent possible, identify the person(s) that initiated the events."[2]

"Generated entries on the audit log cannot be terminated or interfered with by program control or by human intervention."[3] Not quite. This statement is taken from the Diebold document used to sell its system to the state of Georgia, and it refers to a touch-screen audit trail. The server at the county that tabulates all the incoming votes (GEMS) is perhaps a more powerful tampering target, and altering the critically important GEMS audit log is quite easy.

> "Bev, in what way is it significant that the audit log can be rewritten? I'm puzzled by that, because as several people said (I among them) early on, physical control of a machine always means you can overwrite whatever you like. The trick is to keep the bad guys from gaining physical control."
>
> — "Mae West"

---

*Georgia's certification expert from Kennesaw State University.

"The significance is that in letters from certifiers and in documentation provided to certifiers and to the public, they took the curious position that the 'audit log' was a primary means of security protection."

— "BevHarris"

> "Hmmm…did they say in what way? Because if they said it as you implied here (i.e., the existence of an audit file is enough), that would actually be hilariously funny if it weren't so serious. Nerds the world 'round would be cleaning their keyboards and monitors after failing to laugh and swallow at the same time."
>
> — "Mae West"

Looking at the Microsoft Access database used in the main vote tabulation system at the county led to concerns about its audit log and the integrity of the GEMS program as a whole. Interest in the GEMS program began to take on a life of its own on the forums.

"Here's the best part... With GEMS (server) installed on my computer, I was able to create a user name ("me") with a password of my choosing ("mac") and assign myself ADMIN capabilities. This was without ever signing into GEMS....all I had to do was create a new database and I was in like Flynn.

— "BlueMac"

Another forum member pointed out that a database maintenance application might provide the security that GEMS appears to lack.

> "The votes end up in a database whenever there's a database, it makes sense that there would be a database maintenance application. Always preferable to have such an application controlling data entry, to control access and make sure everything agrees, catch entry errors, log activity, etc.
>
> "Without this data entry procedure, what would stop someone from going directly into the database and committing fraud that way? I think you said before that it's an Access database? So open up the database with Access and put your phony votes in. So what I'm saying is the mere ability to edit votes isn't all

> that menacing to me, because it doesn't say that there are no procedures to prevent it from being abused. Maybe elsewhere in the system, or maybe completely outside the system. "
>
> — "Ovaltina"

The GEMS program at the county, which pulls in all the polling place votes, would not be quite as vulnerable if a report was run directly from the voting machines themselves before any data was sent to the county tabulator. This report would have to be run *before* vote tallies begin and posted publicly at the polling place, so that chain of custody of the report does not become an issue. That way, if someone tampered with the central counting (even if they also tampered with the incoming data from the polling place), a red flag would pop up because numbers wouldn't match. Another forum member weighed in:

> "1. Full precinct reports are required by California state law as well as others. The Diebold system better be complying with requirement ...
>
> "2. There is no other auditing function in life that is similar to voting. Once the vote is cast, the identity of the owner of that vote is lost forever! In every other transaction described in these boards, the owner of the data is tied throughout the process. That is why banks can correct your account.
>
> "CA Code 19370 States... At the close of polls... at the precinct...One copy of the statement of return of votes cast for each machine shall be posted upon the outside wall of the precinct for all to see. "The return of votes includes each candidate's name and their vote totals at the precinct. During certification of voting machines, the Voting Systems Panels requires evidence that the procedures of each vendor include this process... "
>
> — "DanglingChad"

Well that makes me feel better. If someone tried to hack the GEMS program, promptly posted reports at each precinct in California (as long as they were printed before any upload of data) would make fraud at the central tabu-

lation stage significantly more difficult, though a clever insider could perhaps get around this excellent safeguard.

Unfortunately, as you'll learn in the next chapter, this procedure apparently was not followed in the 2003 California gubernatorial recall.

Why is it so important to have these printouts done before any data is transmitted to the county? A number of attack points open up while vote data is transmitted to the county by modem. Data transmission does not have to be one-way; the vote tallies might be intercepted, with a revised set zapped back into the polling-place machine during the transmission. Another attack method would be to intercept the vote data with a system that masquerades as the county tabulator, the risk of which is greater if the county transmits votes by wireless methods.

According to the Diebold memos, votes are sometimes transmitted with cell phones, opening up a host of security problems; interception by a spoofed GEMS tabulator is just one risk factor. Any time remote access is gained, the possibility for sending vote data the wrong direction (i.e., replacing the polling place data) arises.

> [In the AccuVote TSx Technical Data Package] "They also make reference to the precinct results being 'reconciled' with the results generated by GEMS at the county office. That's a nice warm fuzzy, if it's Gertrude the election worker taking the printout from the precinct and comparing it with the printout from the county. Unfortunately, I found this reference in a section that refers to the specifics of how the results are modemed in, and it is in a section that specifically deals with communications and the order in which they are transmitted. If the 'reconciliation' is done while this electronic transfer is taking place that's not too warm or fuzzy, is it."
>
> — "BevHarris"

Using the freedom of the Internet, intelligent, concerned citizens began to flesh out issues surrounding electronic voting systems for the first time, using a real system, the Diebold Election System, as their model. I say "for the first time" because until June 2003, only voting-industry insiders were allowed to look at the kind of information these citizens were discussing.

Most of us are given some amount of common sense (as long as sex or money isn't involved), and when we meet up in a group and bring our experiences into the picture, we can make some good, solid decisions. At DemocraticUnderground.com, people familiar with accounting and bookkeeping began to weigh in, and they sometimes took software engineers to task for their failure to understand basic accounting principles.

At issue in this conversation were statements by computer scientists that it was sometimes permissable to design tabulation systems in which totals could be manually overwritten.

> "Each and every vote should exist as a distinct and unadulterated record of one citizen's transaction, probably one or more copies should be generated simultaneously, and everything should be 'journalled' ...
>
> "Since voters are not allowed to recast votes, no possible set of circumstances can possibly exist to justify changing those records.
>
> "... Every change, every addition or subtraction to votes, has absolutely got to be a separate transaction. As a matter of fact, what reason should ever exist to make a change that has an intrinsic value of more than one?
>
> "If a fifty vote change has to be made, then you had better show fifty transactions ... If you need to cancel fifty votes, then you had better show which fifty votes that you are cancelling. Damn and double damn. There is absolutely no technical reason in the world why this cannot be done.
>
> "One vote today is the same as one vote in 1776, which is the same as one vote in 1876, which is the same as one vote in 1976, which should be the same as one vote in 2076.
>
> "What is so hard to understand about that for these computer geeks? "
>
> — "ItAllAddsUp"

A set of User Manual instructions caught my attention. In the GEMS User Manual we found a discussion of how touch screens handle the statistics for undervotes. That's fine, I suppose, but what was it doing in the instructions for how to do manual vote entries?

> "If you have an accounting document, and you are entering the revenues brought in from selling chocolate bars, you don't explain, 'by the way, the correct numbers for the salami sticks you sold should be calculated like this...'
>
> "An entry like that in the chocolate bars accounting instructions would make me go look at what the heck they are doing with the salami sticks.
>
> "By definition, doing manual entry means you are using some form of manual data. It is irrelevant to explain how a touch screen enters votes in a section describing manual entry for manual data. Irrelevant, and also inappropriate. You do not tell people to tinker with the math to make the check sum add up. This is the second such reference — if you'll recall, in the GEMS manual it talks about doing little "adjustments" to the math during manual entry to make sure the check sum is correct.
>
> "...Again, voting is accounting. The procedure they identify is exactly parallel to telling someone how to fudge an accounting log."
>
> — "BevHarris"

"Accounting practices are double entry, not only because of mistakes, but also fraud. Two sources are better than one. So there should be an accounting trail to verify results, especially when there is a question of accuracy ... It doesn't have to be paper but it should be a traceable source document."

— "Cleaver"

Most of all, citizens weighed in with demands for transparency. They chafed at corporate claims to privacy for votes that belong to all of us:

> Bottom line: Government has no business hiding behind proprietary computer code in proprietary voting machines. If the government wants us to use a number 2 lead pencil to mark the ballot, then we damn well better be able to examine that number 2 lead pencil ourselves. We should be able to buy a box of those very same, identical, number 2 lead pencils if we so desire. The paper used for the ballots has got to be paper that can be examined by any who wish. The boxes where the ballots are stuffed need to be made of commonly available

wood, nails, screws, hinges, etc. The boxes need to be able to be examined for false bottoms, hidden slots, etc."

— "ItAllAddsUp"

"States like Georgia have written provisions into their laws that make it impossible to get a machine in dispute adequately inspected. The Georgia law stipulates that three people, a patent attorney and two mechanics, be appointed by law to look at the *computerized* machines! This is tantamount to appointing two blind men and an attack dog to inspect the machine. If either of the 'mechanics' asks about how the machine works the attorney is there to tell them 'it's proprietary information', you're not allowed to know!"

— "GoodyTwoShoes"

Every now and then someone still pops up to tell us that the voting system topic has no legs, or that people just don't care about it. Then explain this: Voting system discussions at DemocraticUnderground.com became kind of an attraction. More and more people tuned in, but at the same time, the subject matter became increasingly technical, while the tone of discussions reflected more urgent concerns. Occasionally someone would sigh and raise their hand:

"Can anyone explain what is happening here in simple language for those of us who are non-techies? I can't make heads or tails about what you may have found here."

— "SkiBob"

Well, we're talking about the computer systems used to count our votes.

"But have you guys found anything? Everybody seems to be talking in very excited tones using terms I can't understand."

— "SkiBob"

(Sorry). Yes, people were finding things. Many of the things they found were eventually found also by researchers at Johns Hopkins and Rice universities,[4] in a report that ended up in *The New York Times*. It was the "increasingly excited tones," in fact, that directly led to the events that produced that report.

> "Attn: BevHarris... look at the cryptographic routines of the voting system. I've just started to go through this system and have a few little snide remarks to make..."

"Topper" was concerned about the possible use of a free, open-source cryptography program which is no longer supported.

> "The problem with using open source with no support is getting a timely answer to your question. Ergo, if there is a security problem during an election, you are stuck with fixing it—which you may not be able to do yourself in a timely fashion."
>
> — "Topper"

"Actually it's not so bad. I'm a programmer and have used that code before. It isn't very well documented and the code is very confusing due to some funky overuse of C++ templates.

"Some of the encrpytion modules are protected by patents which makes it less useful for me but it does appear to be based on an honest attempt to make an open source cryptography library available to everyone for no charge.

"However, I would have to agree that any kind of election software encryption should be based on a standard commercial or government supported encryption solution rather than someone's hobby encryption project."

— "MidniteMunchies"

> "I'm not sure any of the encryption is actually used anywhere ... Since you brought it up, I thought I'd see what algorithm they ended up using. The problem is, I've grepped all over the files, and I don't find any header file inclusions from the crypto library anywhere OTHER than the crypto library. I can't see where the other CVS modules call any of this stuff at all.
>
> "BTW: the library, while perfectly fine for free open source stuff (and I'm an OpenSSL user myself), is a remarkable mish-mash of acquired code. The rijndael.cpp is copied and pasted from the original rijndael.c reference implementation code, there is code copied and pasted from a textbook (dmac.h), the

idea.cpp code is again copied and pasted from the reference implementation idea.c, etc... Not bad for free, but....(apparently not live code anymore either).

"You know, they COULD have gone with OpenSSL — it's free, and supported by far, far more users (and corporate users, such as Apple and IBM for example). But, then again, it doesn't look like they are using any of it anyway..."

— "PoodieToot"

"Mystery solved...but...oh, no... I found what they are actually doing for encryption. They have their own implementation of DES in Des.h

"Here's the bad news...it looks like the DES encryption key is HARD CODED AS A MACRO!!!!!

"AAAAIIIIIIIEEEEEEEHHHHHHHH!!!!!!!!!!!!

"I'll leave discovery of aforementioned key as an exercise for the reader... Good God.....

— "PoodieToot"

"Ooorah!!!!!!! Yeah, I've found the DES.h file...and will start trolling through this...

"If you've hard coded your key and left it just like the public implementation, then it would not be that hard for a hacker to figure out how to get into your system."

— "Topper"

"It would end up as a static string in the executable file And you can tear the static strings out of an executable to view them faster than you can blink your eyes."

— "PoodieToot"

"In your best 50s announcer voice... ... now THAT'S real data security! (cough, cough)"

— "Romeo"

"These things actually use PCMCIA Cards? Huge potential security breaches! Think of the new stuff out there. This is Windows CE based code. Couldn't the existence of these drivers open up any one of these machines having a PCMCIA

based wireless network card installed surreptitiously, allowing remote access via airwaves?

"They're using simple PCMCIA ATA disks These things are basically notepad PC's and the security is almost non-existent. How many local governments will be up on the sophistication required to implement WEP with encryption and hiding SSID's for wireless networks? Heck, you wouldn't even have to hack the wireless network to get around these things, all that is necessary is to pop out one hard drive of results and pop in another with new results preconfigured."

— "Clark Kent"

"Wireless programming required? Are they nuts? i thought I'd been following all the "electronic voting machine" strategies but that's one I missed. I'm a techie, 36 years in the business, some of it with reading punch card votes and optical votes. Wireless programming capability is just plain nuts. That's a security hole the size of a 747.

"That would mean somebody could walk near the voting area (even outside the building), connect to the voting machines via wireless network, and make changes to the voting programs and/or the vote counts"

— "Razmataz"

"I think we've found a potential hole where somebody could alter results remotely with nothing going over any wire. Somebody needs to seriously wardrive elections sites using these things."

— "Clark Kent"

"Ah... That is serious bad news if they are running these terminals wirelessly and only relying on WEP for security. That is enough to fail a security audit at any fortune 1000 company.

"On the other hand, wireless can be extremely secure, more secure in fact that most wired communication if done properly and with the right equipment and design.

"To do it securely, would require fairly recent (and proprietary) technology..certainly not anything that is anywhere near 5 years old."

— "RescueRanger"

"You are assuming no encryption. Because this is wireless does NOT mean no encryption is being used. WEP anyone? Proprietary encryption perhaps? But then again it could be none is... "

— "spock"

"The onus is on the local election administrators, though I have my home wireless network locked down so tight most wardrivers will take one look at all of my security measures and drive on down the street to the guy who is advertising an SSID that is the default on the access point he installed and has never changed the admin password.

"Even I know that with 128 bit encryption using WEP, no advertised SSID, and a MAC Address list can still be cracked. MAC addresses can be spoofed relatively easily and brute force can break the 128 bit encryption if you've got the processor power. Even with encryption, it can be cracked. Now tell me how many of the local election boards you've had experience with are sophisticated enough to implement WEP, let alone MAC Address access lists etc. etc. etc.?

"Add to that the fact that there is a ton of code that could hold back door access and this thing is rife with potential abuse.

"Nope, this doesn't even compare to the potential for pushing out chads on hundreds of cards with a pin so they register as double votes and thus are spoiled ballots. The potential for abuse is magnitudes above this. If the government does not require an independent code review by at least three different companies, it's not doing its job."

— "Clark Kent"

"I trust you are aware... The chances of breaking 128 bit encryption with a brute force approach could very well take centuries with just about any computer on the planet?"

— "spock"

"A 128 bit encrypted file and the encryption level on WEP are two different things. I assure you, WEP is crackable. A PGP file with 128 bit encryption is, as you stated, not easily crackable. And when database files have passwords that are the name of the county where votes are counted, how secure is this system?

— "Clark Kent"

"Perhaps this programmer's comment in the Results Transfer Dialog file [TransferResultDlg.cpp] will answer that question for you: 'Changed the election.dbd file to only store ascii code not unicode to make it compatible between windowsNT/95/98 and WinCE. The convertion from acsii to unicode, if required, is done when the data is retrieved from the database. Note: This does not affect rtf data since it is always stored in ascii.'"

— "BlueMac"

"STRAIGHT ASCII???????? For compatibility with Windows 95/98/NT???? On February 15, 2001?????"

— "Clark Kent"

"Why not? ;o "

— "spock"*

"That's some encryption there! Straight ASCII for backwards compatibility on operating systems that are obsolete. This makes a lot of sense for a system we are supposed to trust the future of the world to."

— "Clark Kent"

"I believe it is talking about the unencrypted values for backwards compatibility when being viewed. But then again that's another problem with leaked source that may or may not be final, you can't be sure."

— "spock"

"And that's the problem with computer voting systems, isn't it... You can't be sure."

— "PoodieToot"

---

* ;o is a keyboard code meaning "wink"

"If I were the guys doing openssl, I'd be real pissed off right now. That blows chunks. I guess assigning a public/private key pair to each networked voting machine is too difficult for the people entrusted with the lifeblood of democracy?"

— "mortal"

"Seems a Congressional investigation should be next."

— "SPacific"

But a congressional investigation was not what came next, or even after next, or even next after next after next. If anything should have a congressional investigation in full view of TV cameras, the voting industry should, but as of the writing of this book, it hasn't happened.

What came next was a quiet phone call on a Sunday morning.

* * * * *

Over the course of a year, I consulted with about two dozen computer techs. Several are not on Democratic Underground because they are Republicans. I met one on Free Republic, a conservative forum. One was a former client of mine. Voting system integrity is a truly nonpartisan subject — Democrats, Republicans, Libertarians, and Greens — everyone but the Charlatan Party, I guess — all respond the same way when someone says, *By the way, we will no longer be auditing the vote, thank you*.

Among my sources is a computer programmer I'll call "Cape Cod."

The best programmers explain things in a very concise way. I'm stubborn enough that I'll keep asking until I understand the answer or the other person starts shouting at me, whichever comes first. But highly skilled programmers are extremely organized thinkers, and it is easy to follow their explanations. "Cape Cod" is such a person. His explanations of complex computer concepts follow this simple, linear fashion: *Here is A, and I'm going to take you to B. Take hold of A, and walk just this way, and I'll describe the scenery as we go. Now, here we have arrived at B; did you enjoy it?*

"Cape Cod" rarely calls me and has always been irritatingly discreet about his examinations of the Diebold files. When he calls, his clipped, East Coast voice provides no unnecessary words and gives very tidy explanations. He also never

calls unless he has something to say. He made one efficient, four-minute call to explain how a voting system might be able to cheat with 'zero reports,' for example:

"It's quite simple, really; your goal is to stuff the electronic ballot box while at the same time generating a report at the beginning of the election which tells you that zero votes have been cast, proving the ballot box has *not* been stuffed.

"Here's what you do: You stuff the ballot box by entering two vote totals that cancel each other out: 'plus 50 for Truman, minus 50 for Dewey.' You have thus created a spread of 100 votes between the candidates before the election begins — yet because +50 and -50 sum to zero, you have added no extra voters.

"To make the report read zero when you start the election, simply instruct the code to put a string of zeroes into the 'zero report' if there are any negative numbers in the ballot-stuffing area, but it must only do this if there are no other votes in the system. And by designing a database without referential integrity, you can arrange for the evidence of this ballot-stuffing area to fall off the radar."

(Did you understand that? I did — and he only had to explain it once.)

One Sunday morning while I was still in my bathrobe, I received one of "Cape Cod's" rare phone calls.

"Go to your computer. I want to show you something."

He proceeded to walk me through the process of rigging an election using a real Diebold program, with a version used in a real election, with a vote database for Cobb County, Georgia, found on the Diebold Web site.

Quick overview of GEMS: The GEMS voting software collects votes from the polling places, tabulates them and generates reports. GEMS is used for both optical scan ballots (where you fill in a dot, or draw a line to your choice) and touch-screen machines.

After the polls close, poll workers transmit the votes that have been accumulated to the county office. They do this by modem or by taking out the memory card (like a disk, but the size and shape of a credit card) and driving it over to the county office.

At the county office, there is a "host computer" (also called the "server"), which has the GEMS program on it. It receives the incoming votes and stores them in a vote ledger.

Bypassing the Supervisor Password

The GEMS User Manual tells us that the default password in a new installation is "GEMSUSER." If you install GEMS, click "new" and make a test election, then close it and open the same file in Microsoft Access, you will find an encrypted password in the "Operator" table. Anyone can copy an encrypted password from there, go to an election database and paste it into that using Microsoft Access. Using this method you can open any election database with the password "GEMSUSER."

You can grant yourself supervisor privileges by making yourself an "admin." You can add as many friends as you want. (I added 50 of mine and gave them all the same password, which was "password.")

Using this simple way to bypass password security, an intruder or an insider can enter the GEMS programs. However, you don't even need a password to go in the back door.

The GEMS program looks and feels very secure when you work with it. Running behind the GEMS program is a database using Microsoft Access. When you open an election in GEMS, it places an election database in a folder on your computer. Anyone who has Microsoft Access on their computer can open this election file, simply by double-clicking the file, going in the back door. This kind of access is not certified or authorized, but it can be done anyway.

If someone gains access to GEMS by getting at the computer in the county office, or by hacking in through the Internet or a phone line, they can get hold of this election file.

Back to "Cape Cod."

"Here's what we're going to do," he said. "We'll go in and run a totals report, so you can see what the election supervisor sees. Then I'll show you something unusual."

I opened the GEMS program and ran a totals report. Then I ran a detail report showing the results in each polling place.

"Now, open the file in Microsoft Access."

"Close out of GEMS?"

"No, Access is configured for multiple users."

OK, I didn't know that. Two people can wander around in the vote database at the same time without bumping into each other.

Remember that there are two programs: the GEMS program, which the election supervisor sees, and the Microsoft Access database (the back door) that stores the votes, which she cannot see.

When you open the election database in Microsoft Access, you will see that each candidate has an assigned number. One of the tables tells you the number for each candidate. You can then click a table called CandidateCounter, which will show you how many votes the candidate has accumulated for each polling place.

On this day, "Cape Cod" showed me another table in the Cobb County file, called SumCandidateCounter. This table had the same information as the first, but we observed that it had two complete sets of the same information. One set was marked by a flag, the number "-1."

Notice that this gives us three sets of votes.

"Change some of the vote totals in SumCandidateCounter."

I did, choosing votes from the set that did not have the "-1" flag.

"Now let's run a report again. Go into GEMS and run the totals report."

The totals report showed my new numbers, proving I could alter the report by going in the back door and replacing vote totals with my own in the unflagged votes in the SumCandidateCounter table.

"Now go back and look at that detail report."

The detail report had the original votes, not the ones I changed. It was drawing its information from either the CandidateCounter table or the flagged set in SumCandidateCounter. In accounting, this is called having two sets of books. (Or in this case, three. I never heard what the third set of books does. "Cape Cod" called it the "Lord only knows" table.)

"Why would it be good to have the detail report show the real votes while the summary shows the ones I changed?"

"This allows the system to pass a spot check."

Does this modification produce an audit trail?

Not if you go in the back door while the supervisor has the election open.

Any time you open the GEMS program, it will show up in the GEMS audit log. But suppose you want to erase yourself?

In the Diebold system, it seems that everyone uses the same name when they go into GEMS (they all call themselves "admin"), but I wanted to see whether I could become someone new, play around in GEMS and then erase myself from the audit log.

I created a new user by the name of "Evildoer." Evildoer performed various functions, including running reports to check his vote-rigging work, but only some of his activities showed up on the audit log. For some reason, a few of his activities omitted themselves from the audit log even before I tampered with it. But I wanted to erase *all* evidence that Evildoer had existed.

I went in the back door by double clicking the GEMS database on a computer with Microsoft Access loaded on it. I expected the audit log entries to be numbered automatically with something I could not edit. That way, if I erased some Evildoer activities, the numbers would still be there, marking an activity that had disappeared. I was surprised to find that I could just type new numbers over any of the GEMS audit log numbers, and I could also erase events altogether.

In every version of GEMS that I examined, the autonumbering feature was disabled, allowing anyone to add, change and delete items from the audit without leaving a trace. Soon, there was no trace of Evildoer in the audit log.

Going back into GEMS, I ran an audit report to see if Evildoer had indeed disappeared. As Verbal Kint, in the movie *The Usual Suspects* (1995) said, "The greatest trick the devil ever pulled was convincing the world he didn't exist."

Another thing that seemed improper in the GEMS program is this: You can enter *negative* votes. It is a simple matter to program the software so that it will never accept a negative number. Why should it? A vote total that is less than zero can only be illicit.

The entire process — bypassing the password, changing the vote totals, cleaning up the audit log — took less than 10 minutes.

* * * * *

During the month of June, I hadn't seen much of *Scoop Media*. But Scoop's publisher, Alastair Thompson, is never far from a phone when he smells something breaking.

"Hi, Bev. (New Zealand pronunciation, "Bivv"). Alastair here. (New Zealand pronunciation "Alasteh"). What's up?"

"Well, we have a pretty important story. With the GEMS program, using one of the databases found on the FTP site, we were able to rig it," I said.

"Hmm!"

"I'm writing it up. I'm not sure where I'm taking it, though."

"You know, I rather thought this might be a good time to publish the link," said Thompson.

—*Come again???* "What link?"

"Oh you know. To the files."

"The files from the FTP site?"

"It seems like a good time, don't you think? I think we should come out with your story at the same time. Get people to it, right?"

"To the link."

"Right."

"Alastair, that set of files is huge. Do you have the bandwidth?"

"Oh, I think we'll be all right.They have bandwidth to burn."

The story went out on *Scoop Media* on July 8;[5] Thompson ran one story about the hackability of GEMS, along with another editorial which he titled "Bigger than Watergate!" He has since been roundly criticized for that choice of title, but remember: Watergate took two years to get as "big as Watergate."

Just sixteen days after Thompson posted the article that brought the world to the link, *The New York Times* posted a scathing report on the Diebold voting system software, by computer security experts from Johns Hopkins and Rice University who had downloaded the files from *Scoop Media*. At least one new story came out in a major media outlet every day for the next two months. In

September, a report written by Pentagon contractor Scientific Applications International Corp. (SAIC) was published that detailed 328 security flaws in the Diebold voting system, 26 of which it deemed "critical."

Stories have now begun to surface about conflict of interest at the top of the company and secret lobbying efforts. People are starting to follow the money trail behind the voting machines.

"Bigger than Watergate." Ha!

Perhaps 50 years from now, some intrepid reporter in a far-flung corner of the world will be scoffed at for titling his article "Bigger than Votergate."

* * * * *

On July 24, 2003 *The New York Times*[6] ran an exclusive story about "stunning, stunning security flaws" uncovered by four researchers at Johns Hopkins and Rice universities. The report, titled "Analysis of an Electronic Voting System" described many of the same findings as those pointed out by the irreverent bunch at Democratic Underground. It was blistering. The Hopkins/Rice report quoted source code explaining its weaknesses, and delved into Diebold's smart card security and its source code architecture and provided the first detailed critique of Diebold's failure to use cryptography correctly. The report also revealed that one of the flaws had been pointed out by voting examiners five years ago and still had not been corrected.

Diebold Election Systems came out swinging:

• The software was never used in any election!

• Well it was used in some elections, another Diebold spokesman was reported to have said, by *WiredNews* reporter Louise Witt.[7] I called her to ask how solid this quote was. Rock solid, she said, but the quote was pulled a day later in favor of this: A small part of the software may have been used in some elections.

• The software is old and out of date, Diebold decided. An article in *The Plain Dealer* [8] pointed out that Diebold was preparing to sell Ohio its new TSx system, though the company admitted it might not be certified by purchase time.

Most of the people I've interviewed about this say the software cannot have been rewritten and tested in the short time since July 24 — or even in the 10

months since the last election. The problems exist in the program itself and patching them will not produce a sound voting system.

Nevertheless we are told by Diebold that the problems:

1) Are fixed

2) Were never a problem in the first place, because the Diebold software is surrounded by election procedures and physical security, which have effectively neutralized the problems all along.

There are weaknesses in the Hopkins/Rice report. Several sections seem to assume that touch-screen machines are connected to the Internet; nothing I've seen indicates that is the case. I have seen indications that the GEMS servers connect to the Internet, and GEMS also connects to a digiboard which, in turn, connects back to touch-screens with a modem when the election closes.

Before the election, GEMS loads ballots into the touch screens, but everything I've seen indicates that this is done using touch screens placed in the office near the GEMS machine, rather than loading the ballots over the Internet.

The criticism that the Hopkins/Rice report doesn't take into account all the election procedures is, in many ways, absolutely correct. It doesn't appear that the authors read the user manuals that go with the software; they apparently did not interview any election officials, either. Several of the concerns in their report prove unfounded when you find out more about election procedures.

Other areas of the report describe cracks that would be impractical or could not affect many votes at a time. The most publicized security flaw in the report has to do with making extra voter cards (or reprogramming one so that it can vote as many times as you want). These are valid concerns, but checking the number of voters signed in against the number of votes cast is a required safeguard in most states and would quickly reveal such a ploy. This type of hack would also be very difficult to achieve on a grand scale; you would have to make rigged smart cards and send people in to cast extra votes at hundreds of polling places at once, which gets into the crazy conspiracy realm.

The biggest taint applied to the Hopkins/Rice report is a conflict of interest on the part of one of its primary authors, Aviel Rubin.

Lynn Landes, a freelance reporter, revealed that Rubin had been an advisory-board member for VoteHere, a company that claims its software solves many of the problems in the Hopkins/Rice report.[9] Rubin also held stock options in VoteHere; he resigned and gave back his stock options, but not until after Landes published her article. Rubin told Landes that he had forgotten about this conflict of interest when he wrote the report.

Three more researchers — Dan Wallach, who is a full professor at Rice University and Adam Stubblefield and Yoshi Kohno, of Johns Hopkins — also wrote the report, and none of them appear to have any conflicts of interest. It seems unlikely that all three would help Rubin slant a report just to help him sell VoteHere software.

The importance of the Hopkins/Rice report:

1) It correctly identifies weaknesses in Diebold's software development process. The code is cobbled together to fix and patch. The correct way to produce quality software is to first develop a precise schema (structure) that says what the software must do; the development process must test against this schema to see that it performs flawlessly. Instead, Diebold's software engineers seem to make it up as they go, and this is evident both in the source code and in their internal memos.

2) It identifies very real security flaws that can jeopardize vote data, especially during transmission to the county tabulator.

3) The Hopkins/Rice report pushed media coverage into the mainstream. And because, when you are researching this story, you can't even sneeze without finding something new, coverage of the integrity of our voting system will continue to gather momentum. The longest leap forward in a single day was due to the Hopkins/Rice report.

4) The report triggered another evaluation, this time by the SAIC.

SAIC report

In August 2003, the governor of Maryland, which had recently placed a $55 million order for Diebold touch-screen machines, ordered an evaluation by Scientific Applications International Corp.[10] There are concerns with this report as well

— though the report is 200 pages long, two-thirds of it was redacted. In the small part that was made public, more sections were redacted, including everything about GEMS except a general statement that it was unsatisfactory.

If Rubin is said to have a conflict of interest, then SAIC has a whopper: The vice chairman of the SAIC, Admiral Bill Owens, is the chairman of VoteHere. Like the Rubin report, the SAIC report identifies many areas that VoteHere claims to have the solution for.

The SAIC report validates important findings in the Hopkins/Rice report and identifies many new areas of concern. Because it is heavily redacted, we don't know the details on all of the flaws it found, and many are specific to Maryland. Still, these words reverberate since Diebold's software is still being used in elections:

The system, as implemented in policy, procedure, and technology, is at high risk of compromise. Application of the listed mitigations will reduce the risk to the system. Any computerized voting system implemented using the present set of policies and procedures would require these same mitigations.

or to put it more succinctly. "328 security flaws, 26 deemed critical."

Chapter 10 footnotes

1 – Digital Millenium Copyright Act of 1998 http://www.loc.gov/copyright/legislation/dmca.pdf

2 – "Security in the Georgia Voting System," April 23, 2003, by Britain J. Williams, Ph. D.

3 – Georgia RFP Sales Proposal for Diebold Election Systems: Phase I, Tech Proposal.

4 – Analysis of an Electronic Voting System, Johns Hopkins Information Security Institute Technical Report TR-2003-19, July 23, 2003. http://avirubin.com/vote/

5 – *Scoop Media*, 8 Jul 2003; "Sludge Report #154: Bigger than Watergate" http://www.scoop.co.nz/mason/stories/HL0307/S00064.htm

6 – *New York Times* 24 July, 2003; "Computer Voting Is Open to Easy Fraud, Experts Say" http://query.nytimes.com/gst/abstract.html?res=F70A15F73E5B0C778EDDAE0894DB404482

7 – *WiredNews.com* 4 August, 2003; "More Calls to Vet Voting Machines" http://www.wired.com/news/politics/0,1283,59874,00.html

8 – *Cleveland Plain Dealer* 14 August, 2003; "Voting machines under review in Columbus" http://www.ohiocitizen.org/moneypolitics/2003/voting.htm

9 – *EcoTalk.org* 18 August, 2003; "Voting Machine Fiasco: SAIC, VoteHere and Diebold" http://www.ecotalk.org/VoteHereSAIC.htm

10 – "Risk Assessment Report Diebold AccuVote-TS Voting System and Processes" 2 September, 2003; Science Applications International Corp.

Chapter 11
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris
with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar

11
Election Procedures and Physical Security
These solve all the problems. (Really?)

San Diego County and the states of Maryland, Arizona and Ohio planned to buy new voting machines, and Diebold planned to sell the machines to them. All told, these contracts were worth over a quarter of a billion dollars. By August 2003, the following information was available to purchasing agents who represent the taxpayers:

- 40,000 Diebold voting system files were left on an unsecured Web site.
- 22,000 uncertified last-minute program modifications were put on voting machines in Georgia by Diebold Election Systems.
- Georgia machines malfunctioned so badly that it called the state's certification into question.
- The GEMS program did not prevent users from bypassing passwords, changing audit logs and overwriting vote tallies.
- Four computer scientists from two major universities exposed "stunning, stunning security flaws" in the touch-screen program.
- And by September, a report by Scientific Applications International Corp. (SAIC) had identified "328 security flaws, 26 of them critical" in the Diebold touch-screen voting system.

Your tax dollars are at risk. Therefore, your representatives (choose one):

a) Decided to hold off on purchasing voting machines until a thorough independent review could be performed on every manufacturer

b) Decided to buy voting machines from a manufacturer other than Diebold

c) Formed a task force to study the issue

d) Announced they were going ahead with the purchase anyway

Correct answer:

d) Decided to go ahead and buy the machines anyway.

I'll put some qualifiers on that: After the Hopkins/Rice report came out, Maryland Governor Robert Ehrlich commissioned a study by SAIC before deciding to purchase. He only announced he was going ahead *after* the SAIC report identified 328 security flaws, 26 of them critical. Ohio Secretary of State J. Kenneth Blackwell decided to hold off on his August 15 announcement of the approved vendors for his state's voting system, partly because of pending SAIC study but also because Sequoia Voting Systems was suing to get on the purchase list. A few weeks later, he put Diebold back on the approved vendor list. San Diego County, after a quick fly-in from Diebold representatives, said it was going ahead with the purchase but later said it might want to think about it. The state of Arizona, without offering an explanation, quietly announced that it would buy Diebold's voting machines.

Election officials hurried forward to explain to the media that all this criticism was just so much hooey; they trusted the machines and those computer scientists didn't know what they were talking about. Diebold announced, after the SAIC report gave it a failing grade, that the report (yes, the same one) said its voting system gave voters "an unprecented level of security."

The state of California decided to go ahead with its October 8 gubernatorial recall election, even though Diebold touch screens would be used in four counties (10 more counties would use Diebold optical scan machines) — and all 14 counties would use Diebold's GEMS county tabulation program.

Such confidence must be supported by a powerful factual underpinning, but so far I haven't been able to find it. Must we privatize the factual underpinning? Could someone please share the secret decoder ring with us so we, too, can see that these machines absolutely can be trusted?

Election officials give Diebold's encryption scheme a clean bill of health, but I'm not sure many of them can spell the word "algorithm," much less explain it. Why are we allowing election officials to pronounce an opinion on computer programming anyway?

I have yet to see any of Diebold's programmers answer a single question about these software flaws. Public-relations team, yes. Diebold software engineers? Total silence. That's OK, I suppose. Might as well do it under oath.

I, for one, would like to hear from technical writer Nel Finberg or principal engineer Ken Clark, who wrote the following e-mails two years before *Scoop Media* published my article about altering the audit log in Access:

> Subject**:** alteration of Audit Log in Access
> From**:** Nel Finberg
> Date: Tue, 16 Oct 2001
>
> "Jennifer Price at Metamor (about to be Ciber) [Independent Testing Authority –ITA– certifier] has indicated that **she can access the GEMS Access database and alter the Audit log without entering a password**. What is the position of our development staff on this issue? Can we justify this? Or should this be anathema?"
>
> Subject**:** RE: alteration of Audit Log in Access
> From: Ken Clark
> Date: Thu, 18 Oct 2001
> Importance: Normal
>
> "Its a tough question, and it has a lot to do with perception. Of course everyone knows perception is reality.
>
> "Right now **you can open GEMS' .mdb file with MS-Access, and alter its contents. That includes the audit log**. This isn't anything new. In VTS, you can open the database with progress and do the same. The same would go for anyone else's system using whatever database they are using. Hard drives are read-write entities. You can change their contents.
>
> "Now, where the perception comes in is that its right now very *easy* to change the contents. **Double click the .mdb file**. Even technical wizards at Metamor (or Ciber, or whatever) can figure that one out.
>
> "It is possible to put a secret password on the .mdb file to prevent Metamor from opening it with Access. I've threatened to put a password on the .mdb before when dealers/customers/support have done stupid things with the GEMS database structure using Access. **Being able to end-run the database has admittedly got people out of a bind**

though. Jane (I think it was Jane) did some fancy footwork on the .mdb file in Gaston recently. I know our dealers do it. King County is famous for it. That's why we've never put a password on the file before.

"Note however that even if we put a password on the file, it doesn't really prove much. Someone has to know the password, else how would GEMS open it. So this technically brings us back to square one: the audit log is modifiable by that person at least (read, me). Back to perception though, **if you don't bring this up you might skate through Metamor.**

"There might be some clever crypto techniques to make it even harder to change the log (for me, they guy with the password that is). We're talking big changes here though, and at the moment largely theoretical ones. I'd doubt that any of our competitors are that clever.

"By the way, all of this is why Texas gets its sh*t in a knot over the log printer. Log printers are not read-write, so you don't have the problem. Of course if I were Texas I would be more worried about modifications to our electronic ballots than to our electron logs, but that is another story I guess.

"Bottom line on Metamor is to find out what it is going to take to make them happy. You can try the old standard of the NT password gains access to the operating system, and that after that point all bets are off. You have to trust the person with the NT password at least. This is all about Florida, and we have had VTS certified in Florida under the status quo for nearly ten years.

"I sense a loosing *[sic]* battle here though. The changes to put a password on the .mdb file are not trivial and probably not even backward compatible, but we'll do it if that is what it is going to take. " — Ken

Subject**:** RE: alteration of Audit Log in Access
From: **Nel Finberg**
Date: Wed, 17 Oct 2001

"Thanks for the response, Ken. For now Metamor accepts the requirement to restrict the server password to authorized staff in the jurisdiction, and that **it should be the**

> **responsibility of the jurisdiction to restrict knowledge of this password**. So no action is necessary in this matter, at this time." — Nel

Resolution of the problem revealed in the "alteration of the audit log" leans heavily on local election officials to set up security around access to the GEMS computer. Setting aside the references to doing "end runs" around the voting system, do we really know whether the jurisdictions are able to restrict access to authorized staff? Here are three examples that make me wonder:

1. San Luis Obispo County, California: A vote database popped up on the Diebold Web site during the March, 2002 primary. It was tallied hours before the polls closed. Election officials can't explain how it got there.

2. Marin County, California: A cell phone was used to transfer a vote database. This is uncertified and insecure and apparently was never approved by anyone.

3. Volusia County, Florida: In November 2000, an unexplained replacement vote database overwrote the original votes, leading TV networks to erroneously call the presidential election for George W. Bush.

SLO County Mystery Tally

A vote tabulation saved at 3:31 p.m., five hours before poll closing for the March 5, 2002, San Luis Obispo County primary ("SLO County" to the locals) was found on the Diebold FTP site. SLO County Clerk-Recorder Julie Rodewald says that she doesn't know who put that file on the FTP site, and only two people have access to the GEMS computer — the Deputy Registrar of Voters and Rodewald herself.

The SLO file contains votes from a real election. It also contains a problem for Diebold, because in California it is illegal to tabulate votes before the polls close. According to California law, counties are allowed to begin counting mail-in and absentee ballots prior to election day, but results may not be posted before the polls close at 8 p.m.

This file contains an audit log which documents GEMS activities step by step for months leading up to the election, stopping precisely at 3:31 pm on March 5, 2002.

The votes in the file correspond with the final vote tally, which can be found on the San Luis Obispo County Web site for that election — but only about 40 percent of the votes had come in by 3:31 pm.

Was this file used for training? No one trains poll workers during an election. And why would you use real votes and a real file, during the middle of an election, for training?

Was this file part of a "Logic and Accuracy test?" It was date and time-stamped at 3:31 pm on election day. L&A tests are done a few days before the election.

Did company officials set the date forward for a Logic and Accuracy test? The audit log shows that this was an election, not a test.

Maybe the clock was off? It was for a different time zone? When it said 3:31 it was 8:31? Checking the date and clock is part of the election procedures, marked "important." But more than that, after the polls closed there were more votes.

How do the votes correspond to the final vote tally? The vote distribution parallels that of the final tally.

The SLO vote file was assigned a password and placed on a Diebold-owned Web site. The password was: "Sophia." Sophia Lee is a Diebold project manager.

"I live and VOTE in SLO County. I find this disturbing. Is there anyway we can get them to count the paper ballots, meaning the ones we put in the scanning machine, to verify the result?"

— "Cleaver"

Was Sophia Lee there that day? Yes, according to Rodewald. "An employee from Diebold was at the county Elections Office on the day of the primary to answer questions and help with any problems that might come up.

Did Sophia put that file on the Diebold Web site? "She's saying she did not post (the data) on election day," Rodewald said. "She

said it's something she never would have done."

Did Rodewald give Sophia access to the GEMS computer and the vote database? Rodewald says that neither she nor any of her staff put that file on the Diebold Web site, and she does not know how it got there. "Only the deputy (registrar of voters) and myself have access to the computer on election day or any day," Rodewald said.

Do we have a problem? Apparently.

1) Vote tallies were available for SLO County before the polling places closed. "We don't release those results. In fact, we don't even print results. We don't know what the results are until 8 p.m.," Rodewald said.

2) Security of the GEMS central count computer was breached when its midstream vote tabulation file was placed on an unprotected Web site. Yet we have been told that physical security is in place, limiting GEMS access to two county elections officials, placing the machine in a locked room that no one can enter and making sure it is not hooked up to the Internet or to the county network.

- The file is large and takes time to upload to an FTP site, even with a fast Internet connection. We have also been told that GEMS does not connect to the Internet. Somehow this large GEMS file from the midst of the SLO County primary election made its way from the "secure, inaccessible, locked-in-a-room, not-connected computer" onto the Diebold company Web site.

- This appears to have happened on election day, since the file is tagged to "sophia" and Sophia is a Diebold employee who was present at the San Luis Obispo County elections office on election day. Diebold denies that the results were posted on election day. "Diebold is trying to track down when the information was posted," said Rodewald. (If Diebold is trying to find out when it was posted, why does Diebold state that it was not posted on a particular day?)

Now let's look at the plausible explanation for how the votes got into the file: Rodewald says that the votes in the SLO file as of 3:31 pm in the afternoon on primary election day, March 5, 2002, were absentee votes, which were counted on March 1,2, 3 and 4. She says they are not votes cast at the polling place. Diebold said it was a back-up file. As the absentee and mail-in ballots are tabu-

lated, the county periodically "backs up" that data onto a computer disc, in case the main computer were to crash.

Diebold representatives now admit it was a "huge mistake" to have the data on a site that could be accessed by the public.

Accounting Minutiae

- In the SLO database, absentee votes are tagged with "1" and votes cast at the polling place are tagged with "0."
- This means all of the votes, if they are absentee votes, should be marked with a "1." But the first 15,000 votes in the database are all tagged with "0," which would indicate that they come from a polling place. The only way votes can get from a polling place into the GEMS program during the middle of an election is to have an E.T. moment and phone home. We don't want our voting machines to connect with their master before all the votes are cast.
- Enter strange accounting that gives me a headache: Rodewald says that there are precincts which have both polling places and absentee voters, but there are also about a hundred precincts where people cannot go to any polling place, but can only mail in a ballot to vote. These precincts are called "mail ballot" precincts. Mailed in ballots from the "mail ballot" precincts are called "polling place" ballots. (Correct accounting would call them "mail ballots" or "absentee ballots"— it would not call them "polling place" ballots.)
- Rodewald explained to me that you can tell the "mail ballot" precincts apart from the polling place ballots because they do not start with the letters "CON."
- So therefore, the votes marked "0" would be the "mail ballot" ones, right? Well, no. She then explained to me that no "mail ballots" were in this database, which she concedes is an authentic SLO County vote file.

Now this may sound like minutiae, but in accounting, precision is correct and confusion is incorrect. Because there are votes marked "0" in the database, it contains either votes from the polling place or "mail ballot" votes, both of which Rodewald told me are not in this vote database.

If Rodewald did not authorize placement of the SLO County vote database on the Diebold Web site, who did?

Why should Diebold employees be privy to midstream election tabulations? What was this file used for? Who put the file on Diebold's Web site?

Why should Diebold take any election vote file and keep it on a company Web site? (One California citizen, Jim March, posted the San Luis Obispo votes on his own Web site. Diebold demanded that he remove it, claiming the company had copyrighted San Luis Obispo's vote file.)

How did Diebold get access to this file? What mechanism was used to get this file off the GEMS computer? A CD burner? A zip drive?

Whether or not anything unscrupulous is involved with this file, it seems that unauthorized access was allowed into the system.

Transferring votes by cell phone

On October 8, 2003, I spoke with the California Elections Division to find out why, when citizens in California went looking for the polling place totals, which were supposed to be posted on the door at each voting location, they found nothing posted at all. I spoke with a "Mark Carrol," who said, "I have your answers." He told me that vote tallies don't have to be posted.

But, they do:

> CA Code 19370 States... At the close of polls... at the precinct...One copy of the statement of return of votes cast for each machine shall be posted upon the outside wall of the precinct for all to see. "The return of votes includes each candidate's name and their vote totals at the precinct. During certification of voting machines, the Voting Systems Panels requires evidence that the procedures of each vendor include this process... "

I asked Mr. Carrol about a set of memos indicating that Diebold has used cell phones to transfer vote results.

"That's not certified!" he said indignantly (and doubtfully).

Yup. I know.

"Not in California, they haven't," he said, after a stunned pause.

Yes, they have. In Marin and Tulare counties, according to the Diebold memos that no one wants you to see. He was silent for a long time, and I told him where to find the memos.

An investigative writer named Tom Flocco (www.tomflocco.com) saw the same memos as I did. In his blog he wrote:

"Diebold sales representative Steve Knecht wrote on April 12, 2000 that 'We are using cell phones in Tulare and Marin,' while also introducing a rather curious, unfamiliar electronic election official called a 'rover:' 'Rovers are the ones who are given the cell phone with the modem for end of night totals upload, not the precinct worker, at least in these two locations.'

"Guy Lancaster, Diebold software programmer, wrote on April 12, 2000, regarding cell phones: 'I know of no written instructions,' leading us to wonder if there were rules and traceable documentation, or why cell phones were being used in the first place ...

"[Diebold sales representative Juan Rivera wrote] 'Also, we did not have to dial the phone manually; the AccuVote did that just as if it was connected to the wall jack.'... So now we have private cell-phones, lap-top computers—and rovers, ostensibly uncertified by any government authority — but no one has reported or documented how or if this 'add-on' equipment or the individual rovers are registered, tested, certified, identified — or secured by state or federal authorities prior to an election...

"On April 17, 2000, Guy Lancaster wrote more about the Diebold AccuVote internal modem: 'We use what's called 'blind dialing' (ATX0) which means that it'll dial with nothing plugged into it. Thus if the AV won't work without this Dial Tone Emulator, then it's doing something in addition to providing a dial tone.' But Lancaster didn't get into what other actions he thought the software was affecting."

Dr. David Dill's* webmaster confirms cell phone data transfer

Dr. David Dill has been fortunate, with his "VerifiedVoting.org" Web site, to have a committed volunteer webmaster named Greg Dinger.

Dinger arranged for a friend to assist as an official pollworker and posted several interesting observations at a site set up by BlackBoxVoting.com for monitoring election reports (www.BBVreport.org — go there and tell us your own experiences).

---

* Dr. Dill is a professor of computer science at Stanford University.

"Ok, I have some news," Dinger writes. "For starters, this election has taught us some lessons. We need to make sure that we have our own people in every precinct possible — along with exit-poll staff and observors at the close of polls. They need to be trained in advance, they should be provided written materials that document what to watch for, and essentially equipped to be our eyes and ears.

"I just finished a lengthy phone call with a friend who worked at my precinct ... Basically, the people there (however well-intentioned) were ill-prepared for the task, were unaware that this e-voting controversy even exists ...

"At the end of the day, the "head" of the scanner was removed from the base. It was connected to some sort of cellphone for transmitting the results. Shocked, I asked her to repeat this: it appears that this phone was NOT connected, nor was the scanner connected to the landline that I observed in the polling place earlier in the day. It was wireless...

"During the transmission process, errors occurred. The phone apparently reported that a ballot was "stuck" in the reader. The precinct folks confirmed that this was not the case. There was a phone call placed to some "support number" which turned out to be a bad number. The lead precinct worker happened to have another phone number, reached some unidentified (to my friend) person, and eventually resolved the issue after a lengthy delay..."

"But she was VERY clear that this was a cordless phone (some sort of folding model) that was attached to the scanner at the end of the day." Dinger clarified that, according to his information, the cell phone was connected only during end-of-day processing. It worked like this:

"The precinct leader was provided a cordless phone of some sort. At the end of the day, she pulled the scanner out of the base and moved it to a table. Then the phone was attached (as I understand it) with a short cable.

"I do not believe the unit was built into the scanner, nor was it connected during the day."

I have some questions about transmitting votes by cell phone.

Why? Why do it? Can we not plug in a simple modem any more?

A well-financed operation can very easily penetrate the voting system with the right equipment and the correct information. Cell phones connect to the access tower with the strongest signal. It is relatively easy (but not inexpensive) to set up a rogue access tower. If you do, this cell phone will automatically communicate with you. You would then connect the call to your own GEMS server, load the real results, modify them and then call up the real GEMS server to upload your results.

Volusia County, Florida:

If Al Gore had publicly conceded on election night, would there have been a Florida recount? Would the "Help America Vote Act" ever have been passed, triggering the rush to touch-screen machines?

We'll never know, but thanks to an internal CBS report and an e-mail written by the vice president of Research and Development at Diebold Election Systems, we now know that the unexplained replacement of a set of votes on a Diebold optical scan machine in Volusia County triggered a premature private concession from Al Gore to George W. Bush and resulted in TV networks' erroneously calling the election for Bush instead of deeming it too close to call. The final "offical" tally showed Gore losing by 527 votes, though the hand recount stopped by the Supreme Court later gave the election to Gore.

Volusia County did a hand recount and straightened out the mistake. It is interesting to note that in the future there may be no paper ballots to recount, thus such a mistake would go uncorrected.

* * * * *

Fox News Network, 29 November 2000: Brit Hume, host:

"And now the latest from the 'Political Grapevine.'

"It seems a broken computer modem and a faulty memory card were culprits in the erroneous election-night call of George W. Bush as the Florida winner. A broken modem prevented some of Volusia County, Florida's results from being transmitted directly to headquarters.

"When the county tried to read the results themselves and relay them to headquarters, computers with a bad memory card caused it to appear for a time

that Al Gore had lost more than 16,000 votes, which seemed to put George W. Bush up by 50,000 — at that stage in the night, an insurmountable margin. Every network saw that as a basis for calling the state for Mr. Bush..."

Two questions:

1) Was it a "bad memory card" that produced the bogus 16,000-vote spread? Or is there another explanation?

2) Is it true that these 16,000 mystery votes caused the networks to call the election for Bush?

What are the symptoms of a bad memory card?

A memory card, as you'll recall, is like a floppy disk. If you have worked with computers for any length of time, you know that a disk can go bad. When it does, which of the following is most likely:

a) In the Word document you saved on the disk, the "bad disk" replaces some of the words you typed with different ones. If I was typing this document on a bad disk, for example, the "bad disk" might read this phrase correctly the first time: "In the Word document you saved..." but the second time, read it like this: "In the pot-bellied pig that you saved..." In your experience, is this likely?

b) In an Excel spreadsheet that you saved on the "bad disk," might it read a column of numbers correctly the first time: "1005, 2109, 3000, 450..." but the second time, replace one of the numbers like this: "1005, 2109, –16,022, 3000, 450..."?

c) Or is it more likely that the "bad disk" will do one of the following things: Fail to read the file at all, crash your computer, give you an error message, or make weird humming and whirring noises while your computer attempts unsuccessfully to read the disk?

For most of us, the answer is c). But according to news reports, the official explanation from Global Election Systems (now Diebold Election Systems) was that a "bad memory card" reported votes correctly in every race except the presidential race, where it mysteriously changed Gore's total to *negative* 16,022.

This kind of explanation gets my nose twitching. Really? Is that what a "bad memory card" does? If so, how many "bad memory cards" have been out there changing vote totals, unbeknownst to voters?

If the symptom of a corrupted memory card was arbitrary vote-changing, as explained to the media in Volusia County, we'd be in real trouble — according to Diebold sales representative Steve Knecht in an internal memo dated March 24, 2000, "Cards were corrupted throughout California at a rate exceeding our normal 1 in 100 that we've been seeing. Marin is now up to 8 cards corrupted out of 114." He reports a number of problems that must have had election officials pulling their hair out:

> "This issue [faulty memory cards], along with AccuVotes [AccuVote is a brand name for Diebold Election Systems optical scan machines] needing to be turned off and on repeatedly during the day to reset them, or AccuVotes just dying in the middle of the day due to Readers failing has gotten to epidemic proportions. Fresno, Marin, Tulare, and Humboldt all replaced about 10% of their units in the field on election day for a variety of reasons ... These corruptions and failures are no longer going to be seen as isolated and will begin impacting our reference selling ability and confidence in the product."

If the memory card failure has, at times, "gotten to epidemic proportions," we'd better hope that the symptoms certainly do *not* include randomly changing the vote totals.

According to an exchange between principal engineer Ken Clark and Donna Daloisio, who was systems administrator for Supervisor of Elections Gertrude Walker in St. Lucie County, Florida the following symptoms typify a corrupt memory card:

When beginning to upload results the following message appears: "PLEASE RE-INSERT MEMORY CARD."

If you take the memory card out and put it back in, you are likely to see this error: "PCT DATA ERROR OK TO CONTINUE?"

If you say yes, this message appears again: "PLEASE RE-INSERT MEMORY CARD."

When Daloisio described these symptoms, principal engineer Ken Clark shot back this diagnosis: "Garden variety corrupt memory card."

Apparently the story the media got about Volusia County's sudden vote discrepancy (because of a "faulty memory card") isn't quite the whole story.

On January 17, 2001, Volusia County employee Lana Hires asked the technical staff at Global Election Systems for help. She was being put on the hot seat over Al Gore's strange tally of negative 16,022 votes.

"I need some answers!" she wrote. "Our department is being audited by the County. I have been waiting for someone to give me an explanation as to why Precinct 216 gave Al Gore a minus 16022 when it was uploaded. Will someone please explain this so that I have the information to give the auditor instead of standing here 'looking dumb'... Any explantations *[sic]* you all can give me will be greatly appreciated."

Global Election Systems' John McLaurin tossed the question to Sophia Lee and Talbot Iredale. "Sophia and Tab may be able to shed some light here, keeping in mind that the boogie man may me *[sic]* reading our mail*. Do we know how this could occur?"

Talbot Iredale, senior vice president for research and development, has been with the elections company since 1991. He explains: "Only the presidential totals were incorrect." Iredale then hits us with this bombshell:

> "The problem precinct had two memcory *[sic]* cards uploaded. The second one is the one I believe caused the problem. They were uploaded on the same port approx. 1 hour apart. As far as I know there should only have been one memory card uploaded. I asked you to check this out when the problem first occured but have not heard back as to whether this is true."

Where did this second card come from? Iredale then gives a cursory nod to the official explanation given to the media:

> "Corrupt memory card. This is the most likely explaination *[sic]* for the problem but since I know nothing about the 'second' memory card I have no ability to confirm the probability of this."

---

* That's a damn curious remark!

Again, WHERE DID THE SECOND CARD COME FROM?

> "Invalid read from good memory card. This is unlikely since the candidates results for the race are not all read at the same time and the corruption was limited to a single race. There is a possiblilty that a section of the memory card was bad but since I do not know anything more about the 'second' memory card I cannot validate this."

There's that pesky second card again. He then suggests that perhaps the second card might have been — well — another way to say this would be "election tampering," I guess:

> "Invalid memory card (i.e. one that should not have been uploaded). There is always the possiblity that the 'second memory card' or 'second upload' came from an un-authorised source."

So, who is investigating this unauthorized source?

> "If this problem is to be properly answered we need to determine where the 'second' memory card is or whether it even exists.

But it turns out that this second card certainly did exist, at least at one time:

> "I do know that there were two uploads from two different memory cards (copy 0 (master) and copy 3)."

There were two uploads from two different cards.

- The votes were uploaded on the same port approxiately 1 hour apart.
- Only one memory card was supposed to have been uploaded.
- "Copy 0" uploaded some votes.
- "Copy 3" replaced the votes from "Copy 0" with its own.
- Iredale believes the second one is the one that caused the problem.
- The "problem": 16,022 negative votes for Al Gore

What effect did this have on the 2000 presidential election?

We know that the "problem" was noticed and corrected. An election worker noticed Gore's votes literally falling off the tally, and the number of votes in Pre-

cinct 216 was totally out of whack. Eventually, a manual recount was done. No harm, no foul?

That depends on how you look at things. I found a report called "CBS News Coverage of Election Night 2000: Investigation, Analysis, Recommendations prepared for CBS News."

"It would be easy to dismiss the bizarre events of Election Night 2000 as an aberration, as something that will never happen again," the report begins. "...But, this election exposed flaws in the American voting system, imperfections mirrored in television's coverage of the election results."

Yes. This election exposed flaws, but the imperfections were not really quite "mirrored" in television's coverage of the results. A more apt metaphor would be that the imperfections exposed the tip of an iceberg and then, with the HAVA bill, everyone in America decided to buy a ticket on the *Titanic*.

It is, as one of the computer scientists I've talked with likes to say, like "The Amazing Randi." Don't look there — look here! An illusion. Ridicule the dangling chads. Voter News Service blew it. Don't worry, we caught that crazy error of negative 16,022 votes, it made no difference. We'll give you the Help America Vote Act (HAVA) and promise $3.8 billion (much of which may never materialize) to prevent this fiasco from ever happening again.

Look over here: Chads are bad. Look over there: Let's vote on a black box!

Don't look there: No one paid much attention to the optical scan machines, which, we now know from Greg Palast's research, used different settings depending on whether you were in a minority district or an affluent suburb. White? Suburban? Set the machine to provide an error message if the ballot was overvoted, so the voter can correct it. Minority? Poor? Accidental overvotes discarded, thank you. Back that up with statistics, of course: "Too dumb to vote."

While we fixated on a butterfly ballot, no one asked about the GEMS program that counted 30 counties in Florida, or demanded to see "card number 3" from Volusia County, or asked who made this card and how it got past all the election procedures and physical security, or whether any other counties had a card number 3.

According to the CBS report, here is a chronology of how the election was called for Bush. You decide whether card number 3 made a difference:

7:00 PM: Most Florida polls close. CBS News' best estimate, based upon exit-poll interviews, shows Gore leading Bush by 6.6%. The Decision Desk decides to wait for some actual votes [i.e., voting-machine votes] to confirm the exit-poll results.

7:40 PM: Voter News Service (VNS) projects Florida for Gore.

7:48 PM: NBC projects Florida for Gore.

7:50:11 PM: CBS projects Florida for Gore.

7:52:32 PM: VNS *calls* Florida for Gore.

8:10 PM: CBS News analysts recheck the Florida race and feel even more confident about the call for Gore, based on data available at 8:10.

9:00 PM: A member of the CBS News Decision Team notices a change in one of the Florida computations. One of the estimates, the one based solely on tabulated county votes [tabulated county votes: In the Diebold system, this is the GEMS program], is now showing a Bush lead. The team discovers problems with the data.

9:07 PM: VNS reports county-tabulated vote data from Duval County that puts Gore in the lead in the tabulated-vote estimate. (This was an error.)

9:38 PM: VNS deletes the Duval County vote from the system, sending a correction to all members. Gore's total in Florida is reduced by 40,000 votes.

10:00 PM: CBS withdraws the Florida call for Gore.

10:16 PM: VNS retracts its Florida call for Gore.

At some point between 10:16 p.m. and 1:12 a.m., Bush took the lead.

1:12 AM: Associated Press, which collects its numbers separately from VNS, shows the Bush lead dropping precipitously. VNS differs.

Correspondent Ed Bradley began telling people in the CBS studio that there were irregularities and that many Democratic votes were still coming in.

1:43AM: Bradley points out that more than 30% of the vote remains uncounted in that Dade and Broward counties, both Democratic strongholds.

1:48 AM: Bradley does the math: "Bush is ahead by 38,000 votes. And still out there, about 5 percent of the vote is still out, 270,000 votes. So that's a big chunk of votes."

Bradley seeks additional information from the AP wire and from CBS News correspondent Byron Pitts.

What has not yet been discovered is an erroneous entry from Volusia county. The initial report from Precinct 216 subtracted votes from Gore's total and added votes to Bush's total.

2:00 AM: According to VNS, Bush leads by 29,000 votes. The CBS model predicts a very narrow Bush win.

Heavily Democratic counties have not weighed in yet. Ed Bradley is following the AP reports and talking about them to others at CBS, but CBS is not using that information.

2:09 AM: VNS adds Volusia County's incorrect numbers to its tabulated vote. This 20,000-vote change in one county increases Bush's VNS lead to 51,000 votes.

2:09:32 AM: Bradley sounds an alarm, but no one pays attention: "Among the votes that aren't counted are Volusia County. Traditionally they're…one of the last counties to come in. That's an area that has 260,000 registered voters. Many of them are black and most of them are Democrat."

2:10 AM: Brevard County omits 4,000 votes for Gore (Brevard also used GES/Diebold machines), but no one notices.

Bush's lead in the VNS count includes 16,000 negative votes for Gore and unspecified other voting problems such that Bush's lead appeared to increase by 20,000 votes in Volusia (plus the 4,000 missing from Brevard).

According to the CBS News report: "These 24,000 votes would have nearly eliminated the 30,000-vote final Bush margin the CBS News Decision Desk has estimated. ***There would have been no call if these errors had not been in the system."***

2:16 AM: John Ellis, who has been hired as an analyst for Fox, relying on information gathered from conversations with his two first cousins — George W. Bush and Florida Gov. Jeb Bush — and on VNS reports, calls Florida for Bush.

Ellis says he spoke to Jeb Bush shortly after all television networks initially declared Vice President Gore the winner of Florida, just before 8 p.m. ET elec-

tion night. He spoke to George W. Bush twice during the day and many times during the evening.

2:16 AM: NBC calls Florida for Bush.

2:16 AM: The AP lead for Bush drops by 17,000 votes, to 30,000. This 17,000-vote drop, occurring in only four minutes, is a Volusia County correction. But VNS does not use the correction, and no one at CBS is listening to Ed Bradley or watching the AP wire.

2:16:17 AM: Dan Rather talks with Bradley about the large number of votes still out in Volusia County.

2:17:52 AM: CBS calls Florida for Bush.

2:20 AM: ABC calls Florida for Bush.

2:47 AM: The AP reports that Bush's lead has dropped to 13,934.

2:48 AM: VNS shows the Bush lead at 55,449.

2:51 AM: VNS corrects its Volusia error, and Bush's lead drops to 39,606.

2:52 AM: The AP reports the Bush lead down to 11,090.

2:55 AM: Palm Beach County weights in with a large number of votes, and VNS reports the Bush lead down to 9,163.

3:00 AM: Rather preps viewers for a Gore concession speech: "We haven't heard yet from either Al Gore or from the triumphant Governor Bush. We do expect to hear from them in the forthcoming minutes."

3:10–3:15 AM:** Al Gore, exhausted from having, gone 50 hours without sleep, telephones Mr. Bush to concede.

3:10 AM: CBS begins investigating the VNS numbers. It also, finally, begins watching numbers from the AP. CBS also looks at the Florida Secretary of State's Web site. The three sets of numbers don't match, but all of them indicate the race is much closer. VNS does not yet analyze this dramatic change.

3:32 AM: From 3 a.m. until now, there is much talk about the expected Gore concession speech.

3:30-3:45 AM:* Gore boards a motorcade for a 10-minute journey to War Memorial Plaza in Nashville, Tennessee to deliver a concession speech to his supporters.

3:40 AM: Bush's lead drops to 6,060 votes.

Around this time, Gore Campaign Chairman William Daley places a call to CBS News President Andrew Heyward. Daley asks whether CBS is thinking about pulling back its call for Bush. Heyward wants to know what Gore is planning to do.

According to the CBS report, "Daley says, 'I'll get right back to you,' hangs up and does not call back. There is more talk in the studio between Rather and the correspondents about the peculiarities now emerging in the Florida vote count. They discuss the AP count of the decreasing margin for Bush."

3:48 AM: "Rather says, 'Now the situation at the moment is, nobody knows for a fact who has won Florida. Far be it from me to question one of our esteemed leaders [CBS management], but somebody needs to begin explaining why Florida has now not been pulled back to the undecided category.' He goes on to say, "A senior Gore aide is quoted by Reuters as confirming that Gore has withdrawn [his] concession in the U.S. President race."

3:45-3:55 AM:* Two blocks away from the plaza, Gore field director Michael Whouley pages traveling chief of staff Michael Feldman to tell him the official Florida tally now shows Bush up by just 6,000 votes, with many ballots left to be counted. By the time the Gore motorcade reaches the plaza, according to Agence France-Presse, he is down by just under 1,000 votes.

Gore did not, then, give the speech he had planned to give.

3:57 AM: According to CBS, the Bush margin has narrowed to fewer than 2,000 votes. CBS News President Heyward, who has been watching the Bush lead evaporate and listening to Rather and Bradley discuss the Florida situation, orders that CBS News retract the call for Bush.

4:05 AM: By this time, the other networks have rescinded the Florida call for Bush.

4:10 AM: According to CBS, Bush's lead drops to 1,831 votes, which is roughly where it remains until the first recount.

4:15 AM:* Daley calls Bush campaign chairman Don Evans, although the exact of their conversation aren't made public.

4:30-4:45 AM:* Gore makes a second telephone call to Bush to retract his concession, saying that he is waiting for all the results from Florida. "They had a brief conversation which shall remain private," said Gore spokesman Douglas Hattaway.

5:05 AM:* A Florida election official announces a recount, with the two candidates separated by a few hundred votes.

According to the CBS report, “the call for Bush was based entirely on the tabulated county vote” [i.e., GEMS or equivalent programs]. “There were several data errors that were responsible for that mistake. The most egregious of the data errors has been well documented. Vote reports from Volusia County.”

Four thousand votes for Gore were omitted from the county tabulation in Brevard County and in Volusia, 4,000 votes were erroneously counted for Bush and 16, 022 negative were recorded for Gore.

“The mistakes ... which originated with the counties, were critical,” says the report. “They incorrectly increased Bush’s lead in the tabulated vote from about 27,000 to more than 51,000. Had it not been for these errors, the CBS News call for Bush at 2:17:52 AM would not have been made.”

* * * *

If you strip away the partisan rancor over the 2000 election, you are left with the undeniable fact that a presidential candidate conceded the election to his opponent based on results from a second memory card (card #3) that mysteriously appears, subtracts 16,022 votes, then just as mysteriously disappears.

If this isn't disturbing enough, consider these three points:

1) We don't know if this was an isolated incident. It may have occurred in other locations, but in smaller, less spectacular totals.

2) The errors were correctable because paper ballots existed which allowed a hand recount. This will not be possible in a future devoid a paper ballots.

3) The fact that "negative votes" could be applied to a candidate's total, demonstrates such a fundamentally flawed software model that it calls into question the competence and integrity of the programmers, the company and the certification process itself.

Footnotes are coming.