Black Box Voting
Ballot Tampering in the 21st Century

By Bev Harris

Talion Publishing / Black Box Voting

ISBN 1-890916-90-0
Jan. 2004

www.blackboxvoting.org

Black Box Voting
330 SW 43rd St PMB K-547 • Renton, WA • 98055
Fax: 425-228-3965 • talion@ix.netcom.com • Tel. 425-228-7131

Dedication

First of all, thank you Lord.

I dedicate this work to my husband, Sonny, my rock and my mentor, who 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 right 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 reporter for a major news outlet, for telling me, "Mom, that is not a story. You have to prove it." And when I did prove it, for saying "This is good, Mom, but it's B-section. Get some more if you want it on A-1."

— Bev Harris

"What's being done to ensure that computerized voting systems are trustworthy? ... Bev Harris, author of the book "Black Box Voting," is the godmother of the movement."

— Hiawatha Bray
The Boston Globe

"Bev Harris ... found Diebold software – which the company refuses to make available for public inspection, on the grounds that it's proprietary – on an unprotected server, where anyone could download it...This in itself was an incredible breach of security...Why isn't this front page news?"

— Paul Krugman
New York Times

"Worried about computerized democracy? You should be. You may have already voted in 2004 — they just haven't yet told you whom you voted for. Bev Harris gives you the real skinny on the Gatesification of our ballot box."

— Greg Palast
Author, "The Best Democracy Money Can Buy"

"This book is already required reading for people to learn about electronic voting, in my opinion."

— Dr. David Dill
Stanford University Computer Science Professor

* * * * *

Black Box Voting: "Any voting system in which the mechanism for recording and/or tabulating the vote is hidden from the voter, and/or the mechanism lacks a tangible record of the vote cast."

The term "Black Box Voting" was coined by David Allen, who also collaborated on approximately 11 pages of the 239-page text, as follows: *ITAA meeting*: Author Bev Harris obtained info on the meeting from her sources and gave Allen the time, phone number and password. Allen taped the meeting, and provided the detailed notes in Chapter 16. Harris provided the ITAA document quoted in Chapter 16. Harris and Allen collaborated on the commentary on the meeting. Allen wrote part of the 2-page Internet voting section, and contributed his comments on a Talbot Iredale memo in Chapter 13: Volusia County. All research and writing for the remaining 228 pages is by Bev Harris with the help of 75 sources, 22 of whom are computer professionals.

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 everyone was saying "Enough, enough we can't take any more!"

This book was originally designed to be a handy little activism tool, an easy-to-understand introduction to the concept of electronic voting risks. It was to contain a history, interviews, and a discussion of theoretical vote-rigging. But as we were plugging along, researching the subject, it got a little too real — even for us.

C'mon over. No time to waste. We have a republic to defend.

Contents

1
I Will Vote

Anthony Dudly, a mulatto from Lee's Mill, North Carolina, believed that he was undereducated. He had a vision in mind for his children: They would become educated — all of them — and one day they would vote.

His country was struggling to recover from a war that had ripped the North from the South, forcibly rejoined them and ordered the Emancipation Proclamation. Now it was trying to decide what to do about voting rights for freed black citizens. Reconstruction Acts ordered voting rights for African-Americans in the South but not the North. The border states wanted nothing to do with black voters.

When the Fifteenth Amendment became part of the Constitution on March 30, 1870, guaranteeing black suffrage in all states, Anthony figured all that remained was to make sure his children got an education.

Anthony's children learned to read and write so well that they looked up the traditional spelling of their own name and changed it to "Dudley," and they also discovered that voting was not as guaranteed as the Constitution promised.

Politicians clashed over the rights of former slaves. Vigilante groups like the Ku Klux Klan found ways to prevent black citizens from voting. Will Dudley, one of Anthony's children, vowed that *his* children would go to college, and by golly, they were going to *vote*.

Will was not an affluent man, but he was a man of conviction, and all nine of his children went to college. Eight of them got their degrees. Will's third child, David, noticed something that caused him to put college life on hold. Around election time in Greensboro, North Carolina, black folks had become so intimidated that they often just locked the door and stayed home on Election Day. Even registering to vote could get you on the "list," and you might get a visit in the middle of the night.

A singular goal took over David's life, and he dropped out of college to drive all over North Carolina, persuading African-Americans to vote.

"We must have the courage to exercise this right," he said. "If we don't vote, we can never truly be a free people." David preached voting and the value of a good education until the day he died.

Jerome Dudley was David's youngest son, and he became the most pissed-off Dudley when it came to voting. It was 1964, nearly 100 years since Anthony had pinned his hopes on the Fifteenth Amendment, and people still were being cheated out of their votes.

The cheating took various forms. Sometimes "challengers" were posted at the voting locations, demanding answers to questions like, "Who was the 29th president of the United States?" before allowing citizens to vote. Sometimes a poll worker would tell you to step aside and let the "regular Americans" vote.

Jerome became student body president at North Carolina A&T State University, leading demonstrations to integrate schools and fighting for voting rights.

It was in this climate that Jerome's nephew was raised. Sonny Dudley spent his younger years projecting his voice in community theater; when he becomes passionate about a topic, he bellows so dramatically that he shocks everyone.

"I will vote for who I want, and no one's gonna stop me," he announced. He said it loud and said it proud, and then Sonny cast his very first vote, for Eldridge Cleaver.

This is the man I married, now 53 years old, a great, gentle bear of a family man. We watched the bizarre 2000 presidential election together, and while I ranted about the disenfranchisement of the Florida voters, Sonny just sat there with a quizzical look.

"But look what they are doing!" I said. "These are violations of

their right to vote!"

"Oh, they've always done that," he said quietly. "You just notice it because now they're playing games with the white folks, too. How's it feel?"

Not too good.

Two years later, something made me stay up all night.

"I just got curious," I told Sonny. "There's this article by a writer named Lynn Landes that says no one knows who owns the voting-machine companies. I did some research and found out that one of the owners is a Republican senator who is running for office right now. Does that seem right?"

"Heck, no!"

So I wrote it up and and posted it on my Web site, along with corporate papers and financial documents. A few days later I got a certified letter from lawyers for Election Systems and Software (ES&S), demanding that I remove information about ES&S ownership from my Web site.

Well yikes. Does *this* seem right?

Heck no, so I sent copies of the ES&S cease-and-desist letter to 3,000 reporters. Then it occurred to me that it might be a good idea to mention it to my husband.

"We can't afford a lawyer, you know," I said. "We might lose the house. Maybe I shouldn't have done that."

"It was Christmas," said Sonny, "and my son David was six months old." He speaks slowly and with great flourish, and it gets me impatient when he goes off on these tangents. "I was so broke that all I had in the refrigerator was a jar of pickles." He added a long pause for effect. "I went out in the back yard and cut a branch off a tree and decorated it." His voice softened. "Now what's the problem?"

He stood up, towering over me.

"My people *died* for the right to vote," he boomed. "I will vote for who I want, and *no one's* gonna stop me."

But I have a question: Can we trust these machines to let us vote for who we want?

Chapter 2
Can We Trust These Machines?

In the Alabama 2002 general election, machines made by Election Systems and Software (ES&S) flipped the governor's race. Six thousand three hundred Baldwin County electronic votes mysteriously disappeared after the polls had closed and everyone had gone home. Democrat Don Siegelman's victory was handed to Republican Bob Riley, and the recount Siegelman requested was denied. Six months after the election, the vendor shrugged. "Something happened. I don't have enough intelligence to say exactly what," said Mark Kelley of ES&S. [1]

When I began researching this story in October 2002, the media was reporting that electronic voting machines are fun and speedy, but I looked in vain for articles reporting that they are accurate. I discovered four magic words, "voting machines and glitch," which, when entered into the DJInteractive.com [2] search engine, yielded a shocking result: A staggering pile of miscounts was accumulating. These were reported locally but had never been compiled in a single place, so reporters were missing a disturbing pattern.

I published a compendium of 56 documented cases in which voting machines got it wrong.

How do voting-machine makers respond to these reports? With shrugs. They indicate that their miscounts are nothing to be concerned about. One of their favorite phrases is: "It didn't change the result."

Except, of course, when it did:

In the 2002 general election, a computer miscount overturned the House District 11 result in Wayne County, North Carolina. Incorrect programming caused machines to skip 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. [3]

This crushing defeat never happened. Voting machines failed to tally "yes" votes on the 2002 school bond issue in Gretna, Nebraska. This error gave the false impression that the measure had failed miserably, but it actually passed by a 2 to 1 margin. Responsibility for the errors was attributed to ES&S, the Omaha company that had provided the ballots and the machines. [4]

According to the *Chicago Tribune*, "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 had won a Lake County, Illinois, primary election. He was among 15 people in four races affected by an ES&S vote-counting foul-up. [5]

An Orange County, California, election computer made a 100 percent error during the April 1998 school bond referendum. The Registrar of Voters Office initially announced that the bond issue had lost by a wide margin; in fact, it was supported by a majority of the ballots cast. The error was attributed to a programmer's reversing the "yes" and "no" answers in the software used to count the votes. [6]

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. [7]

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. In the 2002 Clay County, Kansas, commissioner primary, voting machines said Jerry Mayo ran a close race but lost, garnering 48 percent of the vote, but a hand recount revealed Mayo had won by a landslide, receiving 76 percent of the vote. [8]

Apparently voting machine miscounts have been taking place for some time. In a 1971 race in 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. [9]

The excuses given for these miscounts are just as flawed as the election results themselves. Vendors have learned that reporters and election workers will believe pretty much anything, as long as it sounds high-tech. They blame incorrect vote counts on "a bad chip" or "a faulty memory card," but defective chips and bad memory cards have very different symptoms. They don't function at all, or they spit out nonsensical data.

In the November 2002 general election in Scurry County, Texas, poll workers got suspicious about a landslide victory for two Republican commissioner candidates. Told that a "bad chip" was to blame, they had a new computer chip flown in and also counted the votes by hand — and found out that Democrats actually had won by wide margins, overturning the election. [10]

We usually don't get an explanation for these miscounts. In 1986 the wrong candidate was declared the winner in Georgia. Incumbent Democrat Donn Peevy was running for state senator in District 48. 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. According to the *Atlanta Journal-Constitution*: "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." [11]

In a Seminole Nation election held in Oklahoma in August 1997, electronic voting machines gave the election to the wrong candidates twice. The private company hired to handle the election announced results for tribal chief and assistant chief, then decided that its computer had counted the absentee ballots twice. So the company 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. A different set of candidates moved on to the runoff election each time. [12]

If you insist on the right to vote for whom you want (and no one's gonna stop you), does it make a difference if misprogramming, rather than a human being, forces you to vote for someone you *don't* want?

News reports often explain miscounts as "software programming errors," with no follow up and certainly no outrage. Yet incorrect programming is more insidious than Mad Myrtle secretly stuffing the ballot box. At least when we vote on paper ballots, hand counted, we can hold someone accountable. We don't even know the names of our voting machine programmers.

A software programming error gave the election to the wrong candidate in November 1999 in Onondaga County, New York. 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 rechecked the totals, Faulkner had lost to Democratic incumbent Elaine Lytel. Just a few hours later, election officials discovered that a software programming error had given too many absentee ballot votes to Lytel. Faulkner took the lead. [13]

Akron, Ohio, discovered its votes got scrambled in its December 1997 election. It was announced that Ed Repp had won the election — no, cancel that, a programming error was discovered — Repp actually lost. (Look! Twins!) Another error in the same election resulted in incorrect totals for the Portage County Board election. (Make that triplets.) Turns out the bond referendum results were wrong, too. [14]

In a 1998 Salt Lake City election, 1,413 votes never showed up in the total. A programming error caused a batch of ballots not to count, though they had been run through the machine like all the others. When the 1,413 missing votes were counted, they reversed the election. [15]

* * * * *

Voting machine vendors claim these things are amazingly accurate. Bob Urosevich, who has headed 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." [16]

At that time, Urosevich was with 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 touchscreen accuracy.

"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. [17]

When Chuck Hagel accepted his position as chairman of American Information Systems, he offered a rousing endorsement: "The AIS system is 99.99 percent accurate," he assured us.[18]

But do these claims hold up?

According to *The Wall Street Journal*, in the 2000 general election an optical-scan machine in Allamakee County, Iowa, was fed 300 ballots and reported 4 million votes. 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 had hoped that the tiny but heavily Republican county would tip the scales in George W. Bush's favor, but tipping it by almost four million votes 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." [19]

November, 2003: Officials from Boone County, Indiana, wanted to know why their MicroVote machines counted 144,000 votes cast when only 5,352 existed.

"I about had a heart attack," said County Clerk Lisa Garofolo, according to the *Indianapolis Star*. "Believe me, there was nobody more shook up than I was." [20]

If you are an elections official, I hope this litany gives you pause. Do you really need this kind of stress?

With computerized voting, the certified and sworn officials step aside and let technicians, and sometimes the county computer guy, tell us the election results. The Boone County information technology director and a few MicroVote techs "fixed the problem." (For voting, I prefer the term "corrected.")

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, Lewis said. That is, the miscounted votes were scattered throughout the precincts with no one area being miscounted more than another, 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. Error size: 60 percent. [21]

Here's a scorching little 66 percent error rate: Eight hundred and twenty-six votes in one Tucson, Arizona-area precinct simply evaporated, remaining 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. [22]

Some voters aren't so sure that *every single vote* was accurately counted during the 2002 general election in Maryland.

According to the *Washington Times,* Kevin West of Upper Marlboro, who voted at the St. Thomas Church in Croom, said, "I pushed a Republican ticket for governor and his name disappeared. Then the Democrat's name got an 'X' put in it." [23]

No one will ever know whether the Maryland machines counted correctly because the new Diebold touch-screen system is unauditable.

Tom Eschberger became a vice president of ES&S not long after he accepted an immunity deal for cooperating with prosecutors in a case against Arkansas Secretary of State Bill McCuen, who pleaded guilty to taking kickbacks and bribes in a scheme related to computerized voting systems. [24]

Eschberger reported that a test conducted on a malfunctioning

machine and its software in the 1998 general election in Honolulu, Hawaii, showed the machine worked normally. He 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. [25]

Really?

Dallas, Texas: 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 one in eight votes.

In one of the nonsensical answers that we see so often from vendors, ES&S assured us 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 said, "What we had was a speed bump along the way." [26]

Caracas, Venezuela: In May 2000, Venezuela'a highest court suspended elections because of problems with the 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 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. had recommended ES&S. [27]

* * * * *

Some people, when you give them the short but horrifying version of the electronic voting issue, insist on minimizing the problem. 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. These are 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, hand them the footnote section, so they can examine sources and look them up themselves.

For the third time in as many elections, Pima County, Arizona, found errors in its tallies. 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 used Global Election Systems machines, which now are sold under the Diebold company name. [28]

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 touch-screen machines had counted the vote without a major hitch. The next day, the County Elections Office discovered 103,222 votes had not been counted.

Allow me to shed some perspective on this. Do you remember when we got excited about a missing ballot box found in a Dade County, Florida, church daycare center in the 2000 presidential election? [29] One hundred and three thousand uncounted votes represents about 1,000 ballot boxes. Broward Deputy Elections Supervisor Joe Cotter called the mistake "a minor software thing." [30]

If you are a candidate, you know that participating even in a small election means raising or borrowing money, passing out flyers, going door to door and standing in the rain at various events. How do you feel if your vote is not counted accurately?

"I knew something was wrong when I looked up the results in my own precinct and it showed zero votes," said Illinois Democrat Rafael Rivera, according to the *Chicago Tribune*. "I said, 'Wait a minute. I know I voted for myself.'"

The problem cropped up during the Lake County, Illinois, 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. [31]

Is this not alarming? These voting systems have miscounted our votes, flipping elections even when they are not particularly close. Even more alarming: We have no idea how many miscounts go unnoticed.

No legal authority permits privately employed technicians — often temporary workers — who are not sworn and don't work for the elections office, who sometimes are not even residents of the U.S., to determine the results of the election when there are discrepancies. Yet they do.

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 (more on that risky procedure later) and Sequoia technicians in Denver *e-mailed* the "correct" results. [32]

Not only did Cramer fail to mention to Bernalillo County that the problem had happened before in Nevada — just four months later, Sequoia salespersons also failed to mention it while making a sales presentation to Santa Clara County, California. A Santa Clara official tried to jog their memory. According to the minutes of this meeting, [33] "Supervisor McHugh asked one of the vendors about a statistic saying there was a 25 percent error rate. ... No one knew where this number came from and Sequoia said it was incorrect."

That meeting was held Feb. 11, 2003. Just 20 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,[34] 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 miscount 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. Here's what I mean:

Marion County, Indiana Voting Technology Task Force,
Meeting Minutes July 30, 1999

ES&S, 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?

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.

* * * * *

We know the machines have miscounted elections, but could this happen without being discovered?

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 happened to notice the discrepancy after the election was over, and he 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." [35]

At least two voting machine miscounts resulted in grand jury investigations. 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. [36]

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 miscounted 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. [37]

Who, exactly, must pay lawyers and court costs if errors made by a voting machine result in litigation? Is it the taxpayer?

If an elections official ruins an election — loses votes forever, or mishandles the voting so badly that no one can repair the error — we can fire that person. If an elections *machine* ruins an election, shouldn't we fire that voting system?

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 noncity 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. [38]

In the October 16, 2001, Rock Hill, South Carolina city election, voting machines were programmed incorrectly, skipping hundreds of votes cast. In a number of precincts, the 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. [39]

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*."

If a system is so complicated that programming errors become "inevitable" or "to be expected," the system must not be used. And yet the problems continue.

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 ballots, Union County retained a paper ballot. Thus, a recount was possible and Democratic votes could be identified. [40]

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." [41]

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

In November 2002, a voting machine was caught double-counting votes in South 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.) [42]

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

Election officials and voting machine companies can argue 'til they are blue in the face about the excellence of the certification process, but if the testing works, how did this happen: In Volusia County, Florida, during the 2000 presidential election, the Socialist Workers Party candidate received almost 10,000 votes — about half the number he received nationwide. Four thousand erroneous votes appeared for George W. Bush while at the same time, presidential candidate Al Gore received *negative* 16,022 votes. [43]

I think we should pause for a moment to digest this last example. In fact, if an electronic voting system, in this case a Diebold optical-scan system, can register *minus* votes in sufficient quantity to cause a candidate for president of the United States to erroneously concede to his opponent, we should examine the situation in more detail, don't you agree? We'll revisit this episode in a later chapter.

* * * * *

Sometimes, machines are given a passing grade even when they fail their testing. Dan Spillane, a senior 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 — yet this system passed every level of certification without a hitch. Spillane claims he brought his concerns up to all levels of VoteHere management but was ignored. Just before the system went through certification testing, Spillane contends, the company fired him to prevent him from flagging the problems during certification. He filed a lawsuit for wrongful termination, [44] which was settled by VoteHere, with details kept confidential. [45]

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 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.) [46]

The testing didn't work here either: 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 before and after early voting. [47]

What is supposed to happen in theory doesn't always happen in practice. 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. [48]

Here's another system they tested right before the election, but it miscounted anyway, flipping the election: Pamela Justice celebrated her re-election to the school board in Dysart, Arizona, in the March 1998 election. But 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. [49]

And if you're not yet convinced that our certification system doesn't work: 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.

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," County Election Board Secretary Doug 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, as reported by the *Daily Oklahoman*. "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." [50] Really.

Sometimes they omit testing key systems: 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. [51]

After every election, you will hear this happy refrain: "The election went smoothly." More recently, as we have brought concerns to light, this has become: "Though some people expressed concerns about the voting machines, the election went without a hitch."

Here's the hitch: You won't discover miscounts until you do the audit, which does not take place on election night, and errors sometimes aren't identified until several days later, if at all.

Most errors are detected only when voter sign-in sheets 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. But suppose 100 votes are cast, 55 for Mary and 45 for John, but the computer says you have 100 votes, 48 for Mary and 52 for John. John wins. How will we know the election was given to the wrong person if no one checks the paper ballots?

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. Touch-screens did not get high marks. Here are voting system error rates, as estimated by the Caltech/MIT Voting Technology Project report, issued in July 2001: [52]

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

The Caltech/MIT study omits three critical issues: programming errors, tampering and dirty politicking.

If we are going to use computerized systems, we need computer scientists to help us create safe voting systems. Dr. Rebecca Mercuri, now with Harvard University, and Dr. Peter Neumann from SRI International Computer Science Laboratory, are among the best known computer scientists in the elections field and were the first to really investigate electronic voting systems. They were joined by Dr. Doug Jones, a computer scientist from the University of Iowa, who became a member of the Iowa Board of Examiners for Voting Machines in 1994. For many years, these were the voices of reason in the mad dash to electronic voting. New faces have entered the fray within the last two years, but for more than a decade, much of the heavy lifting has been done by these three computer scientists.

They've done a stellar job, but computer scientists usually see this as a programming challenge, rather than an auditing problem or a decision about election procedures, and they tend to concentrate their attentions on touch-screen voting, though some of the most disturbing problems take place on optical-scan systems.

Because we have become over-reliant on input from this one type of expert, we have not adequately evaluated simpler, cheaper solutions, like going back to hand-counted paper ballots (perhaps using a computer as a printer, for legibility and accessibility).

Linda Franz, a voting integrity activist you'll meet later in this book, puts it more tactfully.

"Democracy builds from many pieces. We have an absolute need for accounting expertise, and part of the puzzle is the input of experts on good accounting practices. Computer scientists know the theory of plotting out the need before the design, and in current electronic voting systems, it doesn't look like the vendors have done much of that. How do we convince them that the system needs to be thought

out with the input of experts in many fields?"

Current voting systems suffer from a very poor understanding of accounting, and make no mistake about it, counting the vote is a form of accounting. We also need better input from candidates and campaign managers, from historians, from legal and civil rights people, and from the officials who run the elections.

"I often see overgeneralization [believing that expertise in one area translates into wisdom in other domains] with top performers in advanced technical fields," says leadership psychologist Dr. Susan Battley, who troubleshoots for organizations such as JP Morgan Chase and Brookhaven National Laboratory. "In reality, when high achievers overlook fundamental differences in skill requirements, it courts not just failure, but disaster." [53]

We may have such a disaster with current auditing systems. We've been using inappropriate statistical models for auditing, and this model (random spot-checks of a tiny percentage of the ballots) has now become the law in many jurisdictions. This can help catch random error, but a more robust procedure is needed to detect fraud.

November 2002, Comal County, Texas: A Texas-sized anomaly on ES&S machines was discovered when the uncanny coincidence came to light that three winning Republican candidates in a row tallied exactly 18,181 votes. It was called weird, but apparently no one thought it was weird enough to audit. [54] Comal County's experience shows why a simple, random, spot-check audit is insufficient.

Suppose you are an auditor but you must follow election audit rules. You are only allowed to spot check, and you can only look at 1 percent of the receipts. You see this:

$18,181 - Utilities
$18,181 - Advertising
$18,181 - Payroll

But you can't do anything about it, because according to the law, you can't audit any more. You have already looked at 1 percent of the receipts. If you try to pull the records on the $18,181 anomaly, party hacks object that you want to "audit and re-audit and then audit some more." A real audit allows you to look at any darn thing you want, even on a hunch, and when you spot an anomaly of any

kind, you get to pull all the records.

1950s, Louisiana: Ivory tower, meet raw politics. 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.'" [55]

Actually, accountants for Las Vegas casinos have better expertise on fraud-prevention techniques than computer professors. Accountants are never invited onto voting system task forces, nor were they called upon to testify when the Help America Vote Act, which prescribed new voting requirements, was being written. Hint hint. Nudge.

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, but they did it anyway. [56] In a real audit, people don't get to remove part of the bookkeeping system, and in the real world, people don't always follow instructions.

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 its occupancy had remained stable (around 13,000 residents) since the complex had hit capacity in 1998. [57]

A spot-check audit, in this case, will achieve nothing. Because there is usually no provision in the law to allow an audit based on anomalies, all a fraudster had to do was figure out a way to delete a block of votes and cook the sign-in books. Impossible, you say? Here's a five-letter method: b-r-i-b-e.

* * * * *

When a human being handles a voting system, you'll see mistakes, but when a computer handles the voting, you'll see some complete boondoggles.

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. [58]

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 (which were supposed to be provided by the voting machine company as a backup but were unavailable when 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. [59]

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." [60]

Question: Did this new chip go through certification? Nope. The only one who knew what was on this chip was some guy in Omaha. What Mildred didn't realize when she accepted that chip was that she had just opened the door for lawsuits, ultimately paid for by you, the taxpayer, and guaranteed to produce a great deal of stress for Mildred, the County Clerk and Recorder.

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 there was sabotage, 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 repairs, and voters who couldn't spend the day at the polling place were rendered politically voiceless. [61]

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. 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.

For no discernable reason, Mattia later reversed himself.

"I believe that it was an oversight, and there was no fraud involved," Mattia stated in a 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 had changed his mind. [62]

November 2002, Tangipahoa Parish, Louisiana: "I can't say every precinct had a problem, but the vast majority did," Tangipahoa Parish Clerk of Court John Dahmer said. He reported that 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. [63]

November 2002, Maryland: Vote Republican (read "Democrat") — In Maryland, a 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. [64]

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 pretested and certified for use. [65]

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 the vote-counting system caused three of five relay stations to fail, leaving a single county clerk holding the bag for a hand count. [66]

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. [67]

November 2002, Ohio: A voting machine malfunctioned with 12 of Crawford County's 67 precincts left to count. A backup 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. [68]

November 2002, Pickens County, South Carolina: Pickens County couldn't get totals from two precincts due to computer problems. [69]

November 2002, Georgia: 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. 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, they were missing 10 cards. [70]

What is a memory card? It's a ballot box. Electronic ballot boxes for the Diebold machines used in Georgia are about the size of a credit card. With the new electronic voting systems, you can pocket a dozen ballot boxes at once, slip one up your sleeve or tote 67 ballot boxes around in your purse.

An interesting (and suspicious) anomaly appeared with these missing electronic ballot boxes. I interviewed a Georgia computer programmer named Roxanne Jekot for this book. When Jekot quizzed Dr. Brit Williams, official voting machine certifier for the state of Georgia, during an August 22, 2003, public meeting, Williams explained that the memory cards were not lost, but had inadvertently been left in the machines.

Really? Something appears to be missing in this explanation. The procedure in Georgia for transmitting electronic votes from Diebold touch-screens is as follows: If you have seven voting machines at a polling place, each one has a memory card which stores its votes.

You take all seven cards and, one by one, put them into a single machine, which accumulates them and runs a report. When votes from all seven machines are accumulated, they are transmitted to the county tabulator. A printout of the accumulated results is run, and this is placed in an envelope with the memory cards. The envelope is then sealed, signed and delivered to the county.

Jekot raised this excellent question: If the votes are accumulated from all cards before transmitting to the county, this means all the votes would be transmitted as one batch. So why did 2,180 more votes show up when individual cards were "found" inside the machines?

I also have this question: If the procedure is to accumulate, print the report, place it into an envelope with cards, seal the envelope, sign it and then take it to the county, how is it that different people, at different polling places, forgot to do this 67 times in the same county?

Perhaps we should look into the Georgia election a little more.

* * * * *

November 2002, Nebraska — This example shows, I think, just how far we've deviated from the concept of fair and open election procedures. 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-scan machine, which had no counter on it, and then was taken into the private room, where he was allowed to watch a computer with a blank screen. So much for public counting of votes. [71]

* * * * *

"Take the rest of the examples out or put them in an appendix — this is just completely overwhelming," said an editor. So I did. All in all, I documented 100 of these examples, and could have continued for another 100 had space allowed, and our ability to tolerate this outrage permitted. See Appendix A for a continuing compendium.

3
Why We Need Disclosure of Owners

Elections In America – Assume Crooks Are In Control [1]
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. After all, how hard can it be to find out who owns these companies?

Chuck Hagel
Poster Boy for Conflict of Interest

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.

According to CNN's *All Politics*,[2] "Hagel hoped he could make lightning 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."[3] 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*. [4]

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. [5] He also took on the position of CEO when co-founder Bob Urosevich left in November 1993. [6]

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. [7]

When Hagel won what *Business Week* described as a "landslide upset," [8] 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 AIS. 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 disclosed was his salary from or stock holdings in the voting machine company

whose machines had counted his votes. [9]

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.

This is not a gray area. This is lying. Hagel's failure to disclose his financial relationship with the company 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. Had we known, perhaps we never would have chosen to herd every precinct in America toward unauditable voting. 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 that 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).

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 hen house."

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, Matulka dug his heels in and asked for a recount. He figured he'd lost, but he 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 allowing a losing candidate to verify vote tallies by counting the paper ballots.

In January 2003, Hagel's campaign finance director, Michael McCarthy, admitted that Hagel had ownership ties to ES&S. When the story was finally told, Hagel's 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," wrote Farhad Manjoo of *Salon.com*. "'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.'"[10]

Two points, Ms. Linehan: A senator who is a farmer, if he follows the law, *discloses* that he is a farmer on his Federal Election Commission 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.

Hagel was reelected in November. An article in *The Hotline* quoted a prominent GOPer predicting that Hagel would run for president in 2008. The article then quotes Linehan: "It's abundantly clear that many people think that's a possibility for Senator Hagel." [11]

I called Victor Baird, counsel for the Senate Ethics Committee, beginning with a nonconfrontational question: "What is meant by 'widely traded' in the context of an 'excepted investment fund?'"

Baird said that the term refers to very diversified mutual funds. I asked why there were no records of Hagel's ties to the voting 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."

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 publication called *The Hill,* where I talked 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 the documents. I located copies of the documents at OpenSecrets.org, a Web site that keeps a repository for FEC disclosures. 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." 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." [12] Then Baird resigned.

When Baird met with Bolton, he told him that Hagel appeared to have mischaracterized his investment. 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? Apparently not. Bolton was told that Baird still worked for the Senate Ethics Committee, just not in a position that could talk to the press.

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

Maybe. Baird had announced in December 2002 that he planned to resign at the end of February 2003. But he changed his mind and left the position he'd held for 16 years, a month early and in the middle of the day.

In a nutshell:

• Hagel omitted mentioning that he received a salary from American Information Systems in any disclosure document.

• He omitted mentioning that he held the position of chairman in his 1995 and 1996 documents, but says he included it in a temporary interim 1995 statement. The instructions say to go back two years. Hagel also held the CEO position in 1994, but omitted that on all forms.

• He omitted mentioning that he held stock in AIS Investors Inc. and also did not list any transfers or sale of this stock.

• He apparently transferred his investment into ES&S' parent company, the McCarthy Group, and he disclosed investments of up to $5 million in that. He omitted the itemization of McCarthy Group's underlying assets. Under "type of investment," he originally wrote "none."

• When asked by Baird to clarify what the McCarthy Group was, he decided to call it an "excepted investment fund."

• Baird failed to go along with Hagel's odd description of the McCarthy Group as an "excepted" fund

• Baird was replaced by a new Ethics Committee director who did support Hagel's interpretations.

• After this chapter was posted on the Internet, Hagel's staff sent a bulletin to the press saying that he did disclose his position with AIS. Several reporters simply accepted this misstatement at face value. In fact, Hagel's staff is referring to a temporary *interim* statement covering five months in 1995, which still omitted his stock holdings and salary from AIS and the CEO position. Somehow even the temporary disclosure of his ties to AIS disappeared from his final 1995 disclosure form. All of Hagel's 1995 and 1996 disclosure documents, including the temporary interim statement, contain material ommissions, and his final forms (the ones used by the press and the Senate Ethics Committee) omit *everything* about AIS.

Hagel has never been called upon to answer for these omissions.

Bolton told me that something had happened during his investigation of the Hagel story that had never occurred in all his time covering Washington politics: Someone had tried to muscle him out of running a story. Jan Baran, perhaps the most powerful Republican lawyer in Washington, and Hagel's Chief of Staff, Lou Ann Linehan 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 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.

Here's what Dick Cheney had to say when he learned that Hagel was also being considered for the vice presidential slot in 2000: "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.

"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." [13]

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.

* * * * *

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.

4
A Brief History of Vote-Rigging

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.*

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.

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-

* Douglas W. Jones, a University of Iowa associate professor of computer science, deserves more than a footnote here. We all know that election-tampering is a political reality, but it was not easy to find any authoritative information on specific techniques. Much of the material in this chapter was found by perusing Dr. Jones's work. [1]

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. Here's how you can manipulate this 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 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]

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]

Lever machines: These are being phased out. They are not particularly accurate, and they are unauditable 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 problems are confined to small geographic areas.

Punch Cards: One way to rig a punch card system is to add punches to the cards with votes for the undesired 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.

Another way to rig punch cards is to find a crooked card printer. Printing companies 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.

Another way to rig the punch card vote would be to tamper with the automated counting system.

* * * * *

These methods are clever, but computerized methods are more elegant. Using computers, you can manipulate more votes at once.

5
Cyber-Boss Tweed
21st Century Ballot-Tampering Techniques

With old-style voting systems, for the most part, no special training was needed to realize something was amiss. Not so with rigging computers, but many public officials don't understand this.

"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." [1]

My premise, though, is this: An insider, someone with access, can plant malicious computer code without getting caught. 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 a few ethically challenged individuals among the honorable programmers and technicians who work with our voting machines.

Certainly, human nature did not change just because we entered the age of computers. Sooner or later, someone's going to try to steal votes on these things.

What kind of cheaters are we looking for?

Candidates may not be the most likely people to cheat. 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.

Zealots are a bigger danger, especially if they happen to be connected to people 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. Zealots of any kind may 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 needs to know his election was rigged.

Gambling interests may not be squeamish about pulling strings. Gambling rights have turned into a brawl, with some tough players 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 the world.

Hackers, more accurately called "crackers," 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.

Profiteers can make billions by putting the right candidate into office. Electronic voting systems give a small number of people access to a great number of votes. If you control the counting software, ballot-tampering on a massive scale is possible. We should expect this to 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 different clientele.

Defense contractors stand to make billions with the right candidate. Oil companies benefit from new pipelines all over the world, if they select candidates likely to vote for open exploration and geopolitically strategic development. Highway contractors garner hundreds of millions on freeway and bridge projects. Global financiers gain power and profit when international trade policies are set up to favor their interests. Pharmaceutical companies want legislative protection for pricing policies and product patenting and protection from international competition. Investment holding companies stand to gain control over privatized retirement and pension funds.

* * * * *

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 crooked, corporation, and I just want to buy off an employee. How would I find and contact an employee, and how would I know whom to approach?

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, could find the people who program our voting machines, then certainly the bad guys must know who they are.

You can find 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, say you are writing an article and ask them how a machine can be rigged. And they will tell you. I know this because I did it.

You will find software engineers who currently work for voting machine companies by finding any company e-mail address. ES&S employees have e-mail addresses that end in "essvote.com." Enter "essvote" in a search engine, and you'll find people who submitted information to high-school reunion sites and 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 eight dozen voting-company employees this way. 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.

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.

How to compromise an Internet voting system

Some cities, like Manatowoc, Wisconsin, and Liverpool, England, are eager to vote by Internet. Among computer professionals, however, Internet voting advocates are difficult to find. Here's why:

Companies like VoteHere claim that encryption techniques are a key to Internet voting security, but encryption won't protect our vote from software programming errors.

Rigging an Internet election is as simple as "DoS"-ing a server. Denial of Service attacks can knock out servers in targeted areas, and no amount of encryption will help. (Let's take the technospeak out: Suppose you connect to the Internet using America Online, but on election day, for some reason, your AOL access numbers don't work. Can you vote on the Internet?)

A company that specializes in Internet voting, election.com, ran a January 2003 contest in Toronto, Canada, which was disrupted by a malicious attempt to shut down the computer system.

"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," CBC News reported. "'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." [2]

Even the most elaborate encryption can't solve a power outage. If some clown with a backhoe pulls the phone cables up out of the ground, how will you vote? If an ice storm takes out power in the city, will your modem work? If you forget to pay your cable bill and they turn it off on Election Day, what will you do?

If you can vote from the privacy of your home, you can sell that vote as well. Proof of how you voted would be as close as your printer.

And while we're talking about privacy, what if you neglect to put in the latest Microsoft patch? You know, the one that says "*A security issue has been identified that could allow an attacker to compromise a computer running Windows XP and gain control over it*."

Heck, if there is as much "spyware" out there as my spam claims,

Internet voting would mean big trouble. From what I can tell, a lot of people don't trust the privacy of their computer even when they are not doing something mission-critical, like casting a vote. Even if scientists make a safe system, how do we get everyone to trust it?

You might find other people voting for you. Read up on identity theft, which is getting worse every year. [3]

Dirty tricks will proliferate. Your elderly Aunt Martha may get convincing messages that send her to bogus voting sites which dispose of her vote. Come to think about it, beloved Aunt Martha is eighty-three years old. Learning to vote on the Internet might stress her out, and why should she have to?

Do you want to vote with your spouse looking over your shoulder? Many of us connect to the Internet at work: Do you really want to cast your vote next to your union leader or your boss?

And what about "technical difficulties?" You cast your vote and your computer screen turns blue and a message appears:

Iexplorer.exe has caused a general protection fault in vote.exe. Your system may be unstable. Save all your work, close all windows and reboot your system.

Ookay. Did your vote go through? How will you know?

If it didn't, will you be able to vote again? If you do and the same thing happens, then what? Where will we find enough people to staff the tech support desks on Election day? Will we farm the job out to a service company in Bombay? And if so, how secure is that?

People are out there pushing Internet voting, but this concept is flawed and cannot be repaired. Any money we would save closing down the polls would be lost trying to make the system secure and reliable, and new laws would have to be passed to deal with each problem that arises. People and agencies would have to be appointed to enforce those laws. Election law would come to resemble the tax code in complexity.

Bottom line? Voting for your favorite movie online may be cool, but it's no way to run the Republic.

How to compromise an optical-scan system

Optical-scan systems involve filling in an oval or drawing an arrow on a paper ballot, which then is fed into a scanner. People think

these systems can't be rigged because they have a paper ballot, but there are anecdotal reports of optical scan systems flipping elections 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 audits to see how widespread the problem was, she was ignored.

Most people believe that optical-scan machines are tamper-proof because they provide a paper ballot. But election officials generally don't use the ballots to check the machine count, and in some states it's against the law to do so. If you don't audit properly, optical-scan machines are no safer than paperless touch screens.

Some people think that all we need to do is vote absentee and the touch-screen problem is solved. Unfortunately it will not be solved until we actually look at those ballots. When you vote absentee, your ballot is usually run through an optical-scan machine. Hack either the scanner or the main accumulation and you take the election away, while ballots sit forlorn in a box that no one is allowed to open.

The official results come from the county, not the polling place, so if you adjust the optical scan data before it gets into the county accumulator, you've just rigged the election. No one's going to look at those paper ballots, but if they do a spot check, see below. I'll show you how a crooked programmer can create a safety net for spot checks.

The greatest danger is during the transfer of the vote from the polling place to a central counting facility. Optical-scan votes are vulnerable when transferred by modem or, by *cell phone*, as happened in Marin County, California, during the recall election on Oct. 7, 2003. [4]

Another way to compromise an optical-scan system is to attack the program that accumulates the votes from the polling place.

One way to do this would be to enable a double set of books. If the software keeps a duplicate set of records and uses the first set for the totals, and the second set for the real numbers, you can rig

the totals but keep the detail intact in case of spot checks.

With our current lack of auditing controls, anyone with access to the central count machine can hack an election, and this access may be available through telephone lines or Internet connections, allowing complete strangers to tamper. One way to deter this tampering, or detect it, is to audit the paper ballots against the totals.

More ways to compromise an electronic voting system

Hiding functions in software programs is called putting in "back doors." Visit any computer forum on the Internet, and you'll find that programmers can think up back doors faster than anyone can figure out how to test for them. I spoke with sources who had worked for voting-machine companies and who came up with one method after the next. Here are some of their ideas:

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 activates only on election day.

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 by embedding the program in the "ender card," which is run through some systems to close the election.

Create a replacement set of votes, embed them on a chip, and arrange for someone with access to substitute the chip after the election. Chip replacement took place in the 2002 general election in Scurry County, Texas. Another chip replacement was done in 2002, also by ES&S, in South Dakota, where technicians discovered a machine double-counting Republican votes.

Overwrite the approved program with new commands by installing upgrades or "patches" that have not been examined. I asked Paul Miller, an official from the Washington State Secretary of State's election division, about procedures for updates. He told me that tracking and examining program updates is "not an issue." *But any time a*

program is changed, it can change things you don't see.

Include a layer of software that is insulated from certification testing. Diebold voting machines use Microsoft Windows, but when examining the code, no one looked at the Windows files. By embedding malicious programs in the Microsoft operating system instead of the voting software, a hacker can skip right through certification. Some Diebold machines run old versions of Microsoft operating systems, such as Windows 95 and Windows 98, which are not recommended, even by Microsoft, for use in security-sensitive applications.

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.

Find a video-game programmer to tamper with the video driver. Because so many people create video games, the source codes are fairly readily available. A good game programmer can make the screen do one thing while the innards do something else.

Exchange files with support techs by putting them 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.

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 = 0.95 ... Affiliation = Republican; multiplier = 1.05." This will create totals that correlate with demographics.

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, 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.

Using wireless technology embedded in the voting machine, monitor the election results on a remote basis as the contest proceeds and send your adjustment in when the election nears its end.

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.

Switch the card used to start up the machine. For some models, this overwrites the voting program with a new one. In Palm Beach County, Florida, in a March 2003 election, some precincts reported problems with electronic cards used to activate touch-screen machines, but according to the news reports, "backup cards worked." [5]

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.

By the way, people who have worked around touch screens know that rubbing them can screw them up big time. And almost everyone who works on computers knows that strong magnets and magnetic storage don't mix.

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 apparently has 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? Just a bug. A glitch. Remember, it's easy and fun to vote on these machines.

Following are examples of actual voting-machine software bugs.

Found on Internet voting source code, called votation

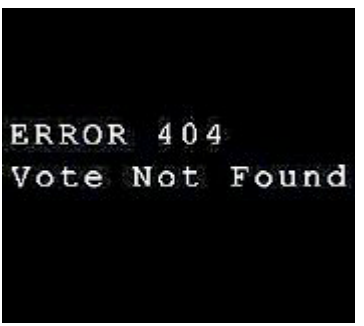
// really no idea on how to resolve rollback failure. :(perhaps praying :) //

Found these comments in Diebold source code files:

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

Diebold bugs, continued:

- 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.
- 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 bug uploading candidate totals
- 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.



Do the bugs ever make it into the software used in elections? Absolutely. That's why "patches" (after-the-fact program modifications) are put on the machines.