6
Who's Beholden to Whom?

Everyone thinks we got into this mess because of irregularities exposed during the Florida recount in November 2000. I disagree.

If you go back to Chapter 2 and delete all the Florida 2000 problems, you're still left with 97 out of 100 examples. This problem is not limited to Florida or the 2000 election, and it cannot be blamed on hanging chads or a butterfly ballot. The root cause of this problem is money.

Vendors and lobbyists leveraged the Florida fiasco to persuade well-meaning legislators to enact a sweeping election reform bill, the Help America Vote Act (HAVA), creating a gold rush to purchase new voting systems, under tight deadlines, using federal money. Vendors did not disclose to lawmakers that their optical-scan systems and touch screens had a history of glitches, bugs and miscounts, and because their computer code was kept secret and proprietary, even U.S. senators and representatives could not know about security flaws or learn just how broken the "certification and testing" system really is.

But I'm getting ahead of myself.

In later chapters, I'll take you inside one of our secret electronic voting systems, and you'll see just how little confidence they should inspire. By rights, we should demand an immediate moratorium on electronic voting, returning to paper ballots, hand-counted if necessary, until we solve underlying problems, such as certification that doesn't work and failure to audit properly.

The Election Center, a private entity that receives little federal oversight and is cozy with vendors,[1] provides training for county clerks and auditors.

The county election officials who purchase these systems are persuaded by a nonstop barrage of talking points, sales presentations and "training programs" provided by vendors and that strange little entity called The Election Center. They have been told to buy now or lose government funds and get fined. Most county officials are honest folks who have not been given the option to buy safer, more secure systems. They may not even know such systems exist.

Not all county officials are well behaved, however. According to one of our sources, who made sales presentations for a voting-machine vendor mentioned in this book, it is all too common for county buyers to hint at gifts ("That's a nice laptop ...") and, sometimes, place an empty envelope on the desk hoping it will be filled.

County officials must abide by what the regulators say, but the regulators keep getting hired by the vendors.

VoteHere hired former Washington state Secretary of State Ralph Munro, who helped to usher in his protegé, Washington's current secretary of state (and avid voting-machine advocate), Sam Reed. [2]

Former California Secretary of State Bill Jones is now a paid consultant for Sequoia Voting Systems. [3] Former Florida Secretary of State Sandra Mortham was hired by ES&S. She promptly got into hot water for being a lobbyist for both the state's counties and the company that sold them their touch-screen voting machines. [4]

Lou Dedier, the California official responsible for recommending which voting systems to buy, took a job with ES&S. [5] Diebold employs Deborah Seiler, a former assistant to California Secretary of State March Fong Eu. [6]

The three finalists for Ohio's 2003 voting-machine recommendations happened to be the companies that hired the most lobbyists. Diebold lobbyists Mitchell Given and Jonathan Hughes formerly worked for Ohio Attorney General Jim Petro, and six ES&S lobbyists showered Ohio county elections officials with gifts. [7]

While we're on the subject of cashing in, take a look at the commissions these companies pay. Sequoia paid $441,000 in a single year to John Krizka for selling voting machines to four Florida counties. Krizka sued, claiming Sequoia had stiffed him for $1.8 million. [8]

Amid these commissions, hope-filled envelopes, job offers and former bosses-turned-regulatees, some election officials don't seem to welcome input from scientists like Dr. David Dill, the Stanford computer professor who wrote, "... Some of the equipment being purchased, while superficially attractive to both voters and election officials, poses unacceptable risks to election integrity — risks of which election officials and the general public are largely unaware."

Dill urged a more prudent voting system, and his "Resolution on Electronic Voting" [9] garnered 1,212 endorsements by technologists. No comparable group of computer scientists — in fact, no technology group at all — has embraced paperless voting.

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

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

One thousand two hundred and twelve *for* providing a voter-verified, tamper-resistant paper ballot, *zero* computer scientists *against*. And these are not just academics. They include industry experts from Sun Microsystems Inc., Bell Laboratories and Lucent Technologies, and General Motors.

You may wonder why I'm going on about this, and it is for this reason: After being presented with the urgent concerns of so many learned professionals, and after being offered the voter-verified paper ballot feature at no extra charge, Santa Clara County, California, purchased unauditable touch-screen voting machines anyway.

"*They've created this whole UFO effect*," said Jesse Durazo,[10] registrar of voters, who is not versed in computer science.

Durazo was not persuaded by 1,212 of the nation's top computer scientists, choosing instead to follow advice from vendors.

A look at the regulators

State certification procedures rely on a procedure called the "Logic and Accuracy" (L&A) test. The L&A test is called a "black-box" test, whereas examining the source code is called "white-box" testing.

According to Arnold B. Urken, who founded Election Technology Laboratories, the first voting-machine testing lab, white-box testing — eyes-on examination of the source code — should be mandatory if certification is to mean anything. Urken told me that he refused to certify ES&S (then called AIS) because the company would not allow him to examine its source code.

In an L&A test, you run test ballots through the machine. If the machine counts correctly, it passes the test. Some touch screens use an automated program to simulate someone casting test votes.

You can practice with all the test ballots you want, but tampering with a program in such a way that it will pass the L&A test is as simple as hatching an egg. An "easter egg" is a tiny code embedded into the program which launches a function when triggered. When the egg receives a signal, it hatches — and the signal can be as simple as receiving a vote containing a special combination of choices.

Dr. Britain Williams, the official voting-machine examiner for the state of Georgia, described testing procedures that sound impressive.

"The law gives the Secretary of State the authority to say what systems are certified and what are not. What I do is an evaluation of the system. The FEC [Federal Election Commission] publishes standards for voting systems. We have national labs that examine for compliance with the FEC, and if they are in compliance, certification is issued by NASED [the National Association of State Election Directors]. Once that's done, it's brought into the state, and I evaluate them as to whether or not the system is in compliance with Georgia rules and regulations. Then the Secretary of State takes that report, in combination with the others, and certifies it." [11]

He described a procedure in which teams of people with a test script checked out each machine, testing the printer, the card reader, the serial port, the screen calibration.

I went to the ES&S Web page, which said that its voting machines were tested by Wyle Laboratories. David Elliott, Washington state's elections director, said that Wyle is a very reputable firm that tests aircraft systems. [12]

Sounds pretty good. Except that in Georgia, where Dr. Brit Williams oversees the testing, and Washington state, where State Elections Director and former NASED board member David Elliott is in charge, they have been using software *that was never certified at all*.

Diebold's Principal Engineer Ken Clark wrote a memo on January 14, 2002, describing his intent to avoid putting his newly modified software through California's certification process by fudging a version number. He wrote, "What good are rules if you can't bend them now and again?" [13]

Ahem.

But suppose for a moment that they actually do test the stuff. How bulletproof is this testing?

Both David Elliott (Washington state) and Brit Williams (Georgia) said that Wyle Laboratories tests their voting machines. But it turns out that Wyle decided to stop testing voting machine software in 1996, citing bloated code that was more than 900,000 lines long. I called Edward W. Smith at Wyle Labs, who confirmed this. Wyle only tests hardware and firmware. Can you drop it off a truck? How does it stand up to being left in the rain? Good things to know, but some of us also want to know that someone has examined the source code to make sure no one tampered with it.

Wyle says they don't test the software, but in a way, they do. Wyle tests the programs that go inside the optical-scan and the touch-screen machines. Because these programs are stored in read-only memory (ROM) or programmable ROM (PROM) chips, or flash memory, Wyle calls the programs "firmware" — basically, this is just industry jargon for software that doesn't reside on a hard drive.

After the program is certified, it must not be changed without reexamination, so you can imagine my surprise when I ran into these comments, written into the source-code files for Diebold Election Systems by its programmers:

"*Remove SCWinApi module till pass WYLE certification.*"

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

"*Merge WYLE branch into the stable branch.*" [14]

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

A lab called Ciber, Inc. tests the voting-system software. Another lab, SysTest, is also authorized to certify software, but all the major companies seem to be certified by Ciber. The software that sits on the county server and accumulates the votes as they come in from the polling places is tested by Ciber.

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

"The ITAs DO NOT and WILL NOT respond to outside inquiries about the testing process for voting systems, nor will they answer questions related to a specific manufacturer or a specific voting system from the public, the news media or jurisdictions. All such inquiries are to be directed to The Election Center..." [15]

What government agency is the Election Center connected with? None: The Election Center is a private, nonprofit entity set up during the late 1980s. Who set it up? Some people in Washington, D.C., whose names are not published. Who provided its seed money? No one seems to know. Who runs the Election Center now? A man named

R. Doug Lewis, who was not elected by anyone.

What are the credentials of R. Doug Lewis? With some persistence, I located a bio for Doug Lewis,[16] but all it said was that he was an assistant to the president in the White House (doesn't say which president); that he ran campaigns for various important politicians (doesn't name any of them); that he headed the Democratic Party for the states of Texas and Kansas (doesn't say what years); and that he consulted for the petrochemical industry (doesn't say what company). With a little more digging, I found that he "managed affairs" for former Texas governor John Connally.

The Election Center works with the National Association of Secretaries of State (NASS), the National Association of State Election Directors (NASED) and the International Association of Clerks, Recorders, Election Officials and Treasurers (IACREOT).

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

I called The Election Center to ask about certification and was told that the only person who could answer my questions was R. Doug Lewis.

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

Lewis: "Yes."

(This turns out not to be true; perhaps he misunderstood my question. The NASED ITA Technical Sub-Committee of the Voting Systems Board is a small group of people who select the certification agencies. This group does seem to work closely with R. Doug Lewis, but I am unclear as to who's in charge of whom.)

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

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

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

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

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

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

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

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

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

Lewis: (muttered) -"Shawn S....... at Wyle — No, Shawn S....... is at Ciber ... "

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

Lewis: (muttered) "Shawn Sou....."

Harris: "I'm sorry, I couldn't understand you. What is that name again?"

Lewis: (muttered) "Shawn South....."

Harris: "How do you spell that?"

Lewis: (muttered very fast) "Southw...."

Harris: "I'm sorry, you'll have to slow down. How do you spell that?"

Lewis: (quietly) "S-o-u-t-h-w-[ard?]" (I was never able to understand him. The correct spelling of the name is Shawn Southworth.)

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

Lewis: "Oh, no, no, no. I'm not going to go there with you."

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

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

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

Micro Trade Mart Inc.
Director: R. Doug Lewis
President: R. Doug Lewis

This corporation is not in good standing as it has not satisfied all state tax requirements. Lewis ran Micro Trade Mart from 1986 through June 1993. He became Executive Director of The Election Center in 1994.

I don't know why R. Doug Lewis, after holding the position of "Assistant to the President in the White House," spent eight years selling used computers. All I really want to know is: What qualifies him to certify voting-machine certifiers, and why must everyone, including the media, talk *only* to R. Doug Lewis when they want to find out how our voting machines are tested?

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

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

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

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

I called to talk to Shawn Southworth, but his assistant told me that she was supposed to refer all questions back to The Election Center. The only person at The Election Center who is authorized to answer questions about certification procedures is R. Doug Lewis.

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

And now for the rudest question of all

Why should we trust anyone? Why can't we just audit the accuracy of these machines, using the paper ballots and practical procedures?

7
Why Vote?

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

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

When the United States was formed, our founders had a clear idea what government should and should not be. The purpose of the government was to provide for the common good.

As Benjamin Franklin wrote, "In free governments the rulers are the servants and the people their superiors and sovereigns."

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

> "Government is instituted for the common good; for the protection, safety, prosperity, and happiness of the people; and not for profit,

> honor, or private interest of any one man, family, or class of men; therefore, the people alone have an incontestable, unalienable, and indefeasible right to institute government; and to reform, alter, or totally change the same, when their protection, safety, prosperity, and happiness require it."
>
> — John Adams, Article VII, Massachusetts Constitution

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

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

Most importantly, we must reach some approximate agreement about what we want, and that is done by placing people, initiatives and referenda on the ballot and casting our votes on them.

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

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

> "Nothing so strongly impels a man to regard the interest of his constituents, as the certainty of returning to the general mass of the people, from whence he was taken, where he must participate in their burdens."
>
> — George Mason
> Speech, Virginia Ratifying Convention, June 17, 1788

Trust is the element that keeps us from taking to the streets every time we disagree with something our government does. As long as we feel our representatives are deciding most things, and the very important things, the way we would ask them to, we are content. If we elected them in an election that all agreed was fair, but they make an egregious choice, one that many of us feel we cannot live with, our governmental system sanctions our protest. We reserve such behavior for unusual circumstances, knowing that when the next election rolls around, we can always vote them out.

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

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

> "That love of order and obedience to the laws, which so remarkably characterize the citizens of the United States, are sure pledges of internal tranquility; and the elective franchise, if guarded as the ark of our safety, will peaceably dissipate all combinations to subvert a Constitution, dictated by the wisdom, and resting on the will of the people."
>
> — Thomas Jefferson to Benjamin Waring, 1801

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

> "I like to see the people awake and alert. The good sense of the

people will soon lead them back if they have erred in a moment of surprise."

— Thomas Jefferson to John Adams, 1786

Democracy is for suckers?

Americans prefer to feel good. They want to believe that elections are fair, that machines count right and that people don't cheat. And yet, there are scholars even within our own country who might advocate, if not subverting the system, at least lying to the voters.

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

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

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

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

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

> "Unless the mass retains sufficient control over those entrusted with the powers of their government, these will be perverted to their own oppression, and to the perpetuation of wealth and power in the individuals and their families selected for the trust."
> —Thomas Jefferson to M. van der Kemp, 1812

> "No other depositories of power [but the people themselves] have ever yet been found, which did not end in converting to their own profit the earnings of those committed to their charge."
> — Thomas Jefferson to Samuel Kercheval, 1816

> "If once [the people] become inattentive to the public affairs, you and I, and Congress and Assemblies, Judges and Governors, shall all become wolves. It seems to be the law of our general nature, in spite of individual exceptions."
> — Thomas Jefferson to Edward Carrington, 1787

> "[We] should look forward to a time, and that not a distant one, when corruption in this as in the country from which we derive our origin will have seized the heads of government and be spread by them through the body of the people; when they will purchase the voices of the people and make them pay the price. Human nature is the same on every side of the Atlantic and will be alike influenced by the same causes."
> — Thomas Jefferson: Notes on Virginia Q.XIII, 1782

> "How long we can hold our ground, I do not know. We are not incorruptible; on the contrary, corruption is making sensible though silent progress."
> — Thomas Jefferson, 1799

Maybe you have never written a letter to your legislator. Perhaps you think that no matter what you do, they'll just do what they want anyway. But can you live with yourself if you do nothing? And what legacy will you leave your children? Later chapters focus on practical activism; this section is about your responsibility to engage.

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

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

Why vote? Is your country what you want, or is it becoming something else? Do you feel your vote is in danger? What would the founders of this country ask you to do? Will you choose to engage?

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

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

8
Company Information
(What you won't find on the company Web sites)

If anything should remain part of the public commons, it is voting. Yet as we have progressed through a series of new voting methods, control of our voting systems, and even our understanding of how they work, has come under new ownership.

> "It's a shell game, with money, companies and corporate brands switching in a blur of buy-outs and bogus fronts. It's a sinkhole, where mobbed-up operators, paid-off public servants, crazed Christian fascists, CIA shadow-jobbers, war-pimping arms dealers — and presidential family members — lie down together in the slime. It's a hacker's dream, with pork-funded, half-finished, secretly-programmed computer systems installed without basic security standards by politically-partisan private firms, and protected by law from public scrutiny." [1]

The previous quote, printed in a Russian publication, leads an article which mixes inaccuracies with disturbing truths. Should we assume crooks are in control? Is it a shell game?

Whatever it is, it has certainly deviated from community-based counting of votes by the local citizenry.

We began buying voting machines in the 1890s, choosing clunky mechanical-lever machines, in part to reduce the shenanigans going on with manipulating paper-ballot counts. By the 1960s, we had become enamored of the poke-a-hole method (punch cards). In the early 1980s, we saw the advent of fill-in-the-oval ballots, run through a scanner for tabulation (optical-scan systems). In the mid-1990s, we decided to try computers that mark votes using touch screens or dial-a-vote devices (direct recording electronic, or DRE, systems). Then we began experimenting with Internet voting.

We first relinquished control to local election workers, who managed lever machines and punch-card voting. With the advent of optical-scan systems, local election workers gradually gave up control to private, for-profit corporations and their programmers and technicians.

In a frenzy of mergers and acquisitions during the 1980s, local election-services companies sold control of our voting systems to a handful of corporations. During the 1990s, these corporations engaged in a pattern of setting up alliances and swapping key personnel that has given just a few people, some of whom have vested interests, far too much access to and influence over our voting systems.

This is not a computer-programming problem. It is a procedural matter, and part of the procedure must involve keeping human beings, as many of us as possible, in control of our own voting system. Any computerized voting system that requires us to trust a few computer scientists and some corporate executives constitutes flawed public policy. It doesn't matter whether they come up with perfect cryptographic techniques or invent smart cards so clever they can recognize us by sight. The real problem is that we've created a voting system controlled by someone else.

During the 1980s, mom-and-pop companies sold election supplies. That changed when the dominant player in the elections industry, Business Records Corp. (BRC), embarked on an acquisitions blitz. You'd almost think they wanted to corner the elections industry.

Business Records Corp. (BRC)

Business Records Corp. was a subsidiary of a Dallas, Texas, company named Cronus Industries Inc.,[2] which was owned by a consortium of wealthy Texas power brokers.

July 1984: BRC acquired Data Management Associates of Colorado Springs, Colorado, a closely-held concern that supplied county governments with computer software and services, and acquired David G. Carney Co., a closely-held San Antonio firm that marketed records-keeping services. Then it purchased the assets of C. Edwin Hultman Co., a closely-held Pittsburgh company that provided county-government information services. [3]

November 1984: BRC acquired Western Data Services Inc., a firm that provided on-line computer services to several hundred county and municipal governments, school districts and other governmental agencies in Texas. [4]

November 1984: BRC acquired Contract Microfilm Services and Business Images Inc. [5]

February 1985: BRC acquired Roberts & Son Inc. of Birmingham, Alabama, a firm which provided voting equipment and election materials to county governments. [6]

April 1985: BRC acquired Frank Thornber Co., a Chicago firm specializing in election-related services, equipment and supplies. [7]

November 1985: BRC acquired Dayton Legal Blank Co. [8]

December 1985: Cronus Industries Inc., the parent company of BRC, completed the purchase of Computer Election Systems Inc. of Berkeley, California. At that time, Computer Election Systems was the nation's largest manufacturer of election machines and related equipment. It provided election computer programs and equipment to more than 1,000 county and municipal jurisdictions. [9]

January 1986: BRC acquired Integrated Micro Systems Inc. of Rockford, Illinois. [10]

March 1986: BRC merged with Computer Concepts & Services Inc. of St. Cloud, Minnesota. [11] During the same month, it acquired Sun Belt Press Inc. of Birmingham, Alabama and merged it into Roberts & Son, one of the election- and voting-equipment companies acquired by BRC in February 1985. It also bought the government operations of Minneapolis-based Miller/Davis Company. The government portion of Miller/Davis provided legal forms, election supplies and office supplies to local governments in Minnnesota. [12]

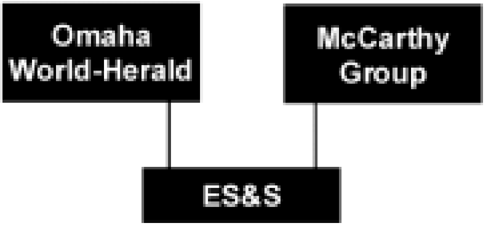
Business Records Corp. dominated the U.S. elections industry until 1997, when it was purchased by Election Systems and Software.

Election Systems and Software (ES&S)

Founded in Omaha, Nebraska, under the name “Data Mark Systems” by brothers Todd and Bob Urosevich, the company soon changed its name to American Information Systems (AIS). In 1984, the Uroseviches obtained financing from William and Robert Ahmanson, whose family piled up a fortune in the savings-and-loan and insurance industries. [13]

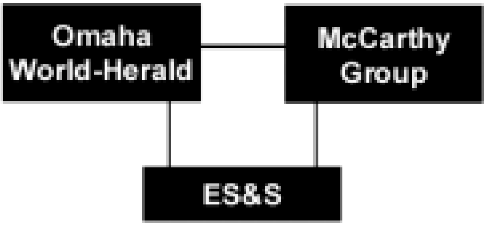
Howard Ahmanson Jr., a younger cousin of the AIS financiers, has parlayed his fortune into extremist right-wing politics, pushing the agenda of the Christian Reconstructionist movement, which openly advocates a theocratic takeover of American democracy. [14]

William and Robert Ahmanson appeared to be more moderate than Howard Jr. and invested money in theater and public broadcasting. In 1987, they sold their direct shares in the voting-machine company to the Omaha World-Herald (which took a 45 percent stake in the company) and the McCarthy Group (35 percent). [15]

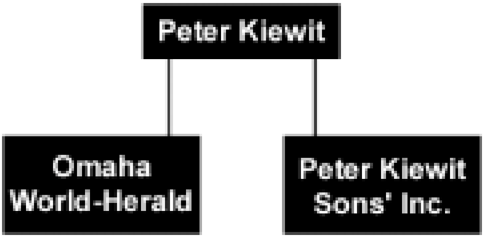


And here the fun begins — watch the bouncing ball ...

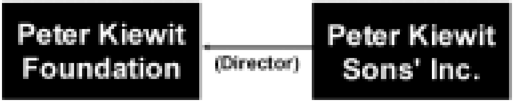
It turns out that the Omaha World-Herald has also been an owner of the McCarthy Group. [16]



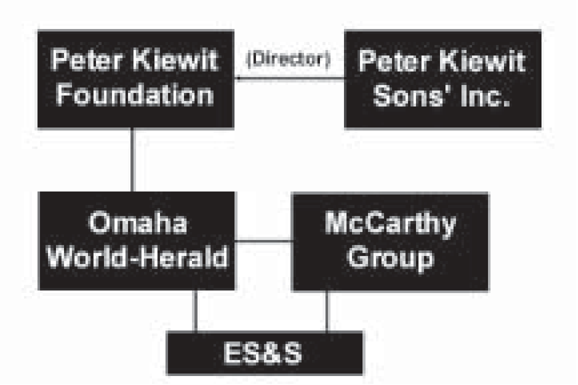
The Omaha World-Herald was owned by Peter Kiewit, the head of Peter Kiewit Sons' Inc., until his death. [17]



Before he died, Peter Kiewit set up the Peter Kiewit Foundation, requiring that at all times the foundation have a director from Peter Kiewit Sons' Inc. as a trustee.



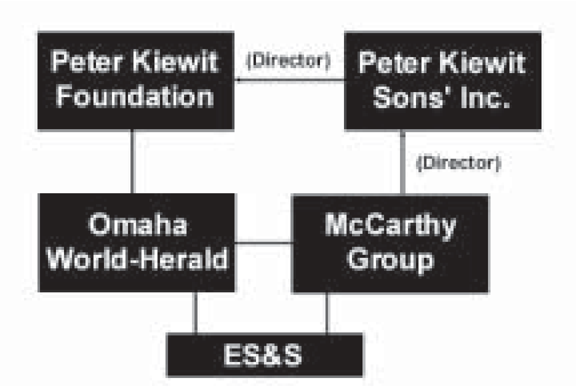
Kiewit arranged for the Omaha World-Herald stock to be purchased by its employees and the Peter Kiewit Foundation, which holds a special class of stock, giving it veto power over any sale proposal. The largest single stockholder in the World-Herald Company is the Peter Kiewit Foundation. [18]



Tracing ES&S ownership thus leads us to the World-Herald and then to the Peter Kiewit Foundation.

It also leads to the McCarthy Group, which is headed by Michael McCarthy. He came to Omaha to sell Peter Kiewit's ranch when he died. [36] Michael McCarthy assumed Peter Kiewit Jr.'s position as a director of Peter Kiewit Sons' Inc in 2001. [19]

The McCarthy Group shows up as one of the investments of a World-Herald subsidiary, in turn leading back to the World-Herald and the Peter Kiewit Foundation. Dizzy yet?



I became interested in Kiewit because if anything is less appropriate than Chuck Hagel's ties to ES&S, it would be a Kiewit relationship of any kind to any voting-system vendor. So who is Kiewit?

Peter Kiewit Sons' Inc. and its subsidiaries have been tied to a string of bid-rigging cases in as many as 11 states and two countries.

In an antitrust case that involved charges of bid-rigging in New Orleans, Kiewit pleaded no contest and paid $100,000 in fines and $300,000 in a civil settlement. In South Dakota, a Kiewit subsidiary pleaded guilty to bid-rigging on road contracts and paid a fine of $350,000. In Kansas, a Kiewit subsidiary was found guilty of bid-rigging and mail fraud on a federal highway project. The firm was fined $900,000 and a company official was sentenced to a year in jail. A Kiewit subsidiary paid $1.8 million for bid-rigging on a state highway project in Nebraska, and a Kiewit vice president was jailed. [20]

The Army Corps of Engineers at one point decided to bar Kiewit from bidding on all federal projects but later changed its mind. Kiewit builds munitions plants and military airstrips.

Does Kiewit have a political agenda? Absolutely. Kiewit's Jerry Pfeffer has spoken before Congress to ask for more privatization:

"Kiewit, based in Omaha, built more lane-miles of the Interstate Highway System than any other contractor," he said. "…We're active in toll roads, airports and water facilities …" [21]

Pfeffer, advocating privatization of the highway system, has stated glibly that "American motorists will gladly pay market prices to avoid congestion."

He goes on to suggest to Congress that Kiewit should get special tax treatment. Kiewit also owns CalEnergy Corp., has been involved with Level 3 Communications and is a quiet giant in telecommunications; underneath its highways, Kiewit lays fiber-optic cable and has been outfitting our roads with video surveillance cameras since 1993.

When the state of Oklahoma forbade Kiewit to bid anymore, Kiewit set up a different company called Gilbert Southern Corp. According to *The Sunday Oklahoman,* "Gilbert Southern Corp. recently submitted a sworn affidavit to the transportation department saying it had no parent company, affiliate firms or subsidiaries." [22]

But Kiewit owned Gilbert Southern Corp. lock, stock and barrel. When the state of Oklahoma found out, it yanked the contracts.

In another obfuscation, Peter Kiewit & Sons took contracts in Washington State under the guise of a minority-owned firm. The government thought it was giving contracts to a company owned by African-American women; actually, it was a bunch of white guys in Nebraska. Kiewit paid more than $700,000 in fines while denying liability or wrongdoing. [23]

Kiewit's corporate papers indicate that investigations and litigation are normal, saying there are "numerous" lawsuits. This is a handy thing to know: Apparently you can skip disclosure of pending litigation, if there's a lot of it.

This example illustrates why voting-machine vendors should be required to provide full disclosure on owners, parent companies, stockholders and key personnel. Kiewit has connections with both ES&S parent companies and has a track record of hiding ownership when it wants to, it has a powerful profit motive for getting the people it wants into office and it has broken the law in the past to achieve its goals.

We should require enough disclosure so that we can at least ask informed questions next time we buy voting machines.

In 1997, the company that had called itself American Information Systems bought elections-industry giant BRC and changed its name to Election Systems and Software. The Securities and Exchange Commission objected on antitrust grounds, and an odd little deal was cooked up in which the assets of BRC were shared between two voting companies: ES&S and Sequoia.

Sequoia Voting Systems

Sequoia Voting Systems has nearly jockeyed its way into position to grab voting-machine dominance away from ES&S and Diebold.

We are told to trust Sequoia's voting systems, along with the people who sell and service them. Well, come with me for a moment and let's do a little re-enactment. After this, you, the jury, can decide for yourself how much trust you want to offer Sequoia.

You be Philip Foster, Sequoia's southern regional sales manager and the project manager who oversaw Riverside County, California's first touch-screen election. I'll be your brother-in-law, David Philpot of Birmingham, Alabama.

I am going to hand you a manila envelope stuffed with $20,000 or $40,000 of kickback cash.[24] These envelopes are sealed, and I won't tell you what is in them. I instruct you to travel to Louisiana and place them in a drawer belonging to Louisiana state elections chief Jerry Fowler. You do so. And then you do it again. Five times.

If we are to trust Sequoia Voting Systems, we must believe that Phil Foster had no idea what was in those envelopes. Foster said in an interview that he did nothing wrong. He continued to work for Sequoia after these allegations were revealed.

Peter Cosgrove, Sequoia's chief executive officer at the time, decided that the allegations against Foster (two counts of conspiracy to commit money laundering and one count of conspiracy to commit malfeasance in office) were "without merit," so he continued to employ him.

"As a company, we believe the allegations against him are without merit," said Cosgrove, "and we believe the statements against him were made by convicted felons." [25]

Well that much is true. Both Foster's brother-in-law, David Philpot, and Louisiana's elections chief, Jerry Fowler, pleaded guilty. Fowler went to federal prison. Another participant in the scam, which reportedly cost Louisiana taxpayers $8 million, was New Jersey's Pasquale Ricci, who pleaded guilty to conspiracy to commit money laundering. [26]

When the charges against Foster were thrown out, the prosecutor appealed. State District Judge Bonnie Jackson upheld the dismissal of charges, ruling that prosecutors had failed to show the charges resulted from evidence collected separately from Foster's grand-jury testimony. Because he had been immunized, prosecutors could not use Foster's own statements against him. [27]

"My investigation of the charges reveals he hasn't done a thing in the world wrong," Foster's Baton Rouge lawyer, Karl Koch is reported to have said.

OK. Let us assume that Foster really had no idea what was in those envelopes. Forty thousand dollars is a minimum of four hundred $100 bills, a pile two inches thick. We are trusting these guys with our vote. Do we really want someone around our voting machines who is so naive that he doesn't understand the implications of sticking manila envelopes stuffed with two-inch-thick wads of something shaped like money into desk drawers belonging to election officials?

Of the big four voting vendors, Sequoia currently has the tidiest corporate ownership but the most recent indictment of an employee and the most prolific habit of hiring its own regulators.

Besides hiring former California Secretary of State Bill Jones, Sequoia hired Kathryn Ferguson, the elections official who helped purchase Sequoia machines for Clark County, Nevada, and Santa Clara County, California, as Vice President, Corporate Communications. In October 2003 she moved to Hart Intercivic. [28]

Michael Frontera, former executive director of the Denver Election Commission, went to work for Sequoia after awarding it $6.6 million in contracts from his own department. [29]

Alfie Charles, former spokesman for Secretary of State Bill Jones, is now spokesman for Sequoia Voting Systems. [30]

At the time of the bribery scandal, Sequoia Voting Systems was owned by Jefferson Smurfit Group, a company based in Ireland. In May 2002, Sequoia was purchased by Great Britain's De La Rue plc, and Phil Foster's loyal and trusting boss, Peter Cosgrove, was retained and promoted.

De La Rue is considered a blue-chip company. Its fortunes are heavily affected by politics, and it has at least one politically active investor.

It is the world's biggest commercial money printer. De La Rue was one of the first British companies to profit from the war in Iraq, earning a quick windfall when it received the assignment to print the new Iraqi bank notes. During the first Bush administration, De La Rue was called in toward the tail end of Sandinista rule in Nicaragua to create new money. [31]

De La Rue is also involved in Britain's national lottery, through its investment in Camelot Group plc. In this capacity, it enraged British citizens when they learned that Camelot had assigned its executives a 40 percent pay hike while reducing the funds allocated to good works. [32]

De La Rue would very much like to take Diebold's position, and not just in election systems. The firm also sells ATMs and smart cards and lists Diebold Inc. as one of its competitors. [33]

In July 2003, the U.S. Department of Justice launched an investigation into a U.S. division of De La Rue, alleging that it had engaged in an illegal price-fixing scheme in relation to the supply of holograms for Visa banking cards, violating US antitrust laws. In a statement, De La Rue said the "individual implicated" in the price-fixing allegation had "left the business in October 1999." [34]

One of the most aggressive investors in De La Rue stock is the hugely wealthy Australian Lowy family, who by March 2003 had picked up 5.5 million shares (just over 3%) through their private investment vehicle, LFG Holdings. Frank Lowy is Australia's second-richest man.

He is highly political, particularly with pro-Israel issues, and has come under fire for his company's payments to Lord Levy, British Prime Minister Tony Blair's "special envoy to the Middle East," which the Aussie billionaire authorized directly. At first, his payments raised suspicions of a "cash for access" intrigue at the highest level of British politics, but as the size of the payments (£250,000) became apparent, the Australian media began raising questions of "cash for foreign policy." [35]

The Lowy family contributes heavily to the Democratic Party. [36]

On August 4, 2003, Sequoia Voting Systems quietly announced a partnership with VoteHere Inc. for electronic ballot verification on its touch-screen machines. [37] It is amazing how much money the elections industry is willing to spend just to avoid giving us ballots we can read and use for audits. The VoteHere system provides a receipt with a code number on it, not a human-readable ballot. You get to check your single vote using a secret code.

If you believe this constitutes public counting of the vote then please meet me under the bridge at midnight and enter your special password into my PalmPilot, and I'll slip you a brown paper bag with some stock tips in it. Count on 'em. Trust me.

Instead of allowing the vote to be counted in the open, viewed by citizens, the VoteHere solution requires us to give control of our elections to a handful of cryptographers with defense-industry ties.

VoteHere Inc.

Like a Timex watch, this company takes a licking but keeps on ticking. Launched by a cryptographer named Jim Adler during the height of the dot-com boom, VoteHere hoped to usher us into the brave new world of Internet voting.

Adler picked up funding from Compaq Computer and Cisco Systems and Northwest Venture Associates, $15 million by November 2000. [38] He also did an honorable thing: He made his company's source code available for review.

Adler's Internet voting system did not fare well in a simple review titled "Vote early, vote often and VoteHere," a master's thesis by Philip E. Varner. After defining threats to the publicly available VoteHere system in such areas as completeness, privacy, verifiability, fairness and reliability, and creating an attack tree, Varner identified several weaknesses in the VoteHere system and concluded it was not ready for use. [39]

Undaunted, the entrepreneurial Adler charged ahead with a plan to have us try voting on totable Compaq iPAQ hardware using VoteHere software and online polling sites connected to the Internet. [40]

But his Internet plans did not materialize, and Adler also stopped making his source code available for public review. VoteHere persuaded places like Swindon, England, and the city of Suwanee, Georgia, to try the system and conducted an online advisory election for the Conservative Party in Sweden. But by 2003, it had few sales to show for six years of work and $15 million in outside investments.

I have seen no more sources of funding for VoteHere, nor much in the way of sales revenues, but one thing I did find was a board of directors spiked with power brokers from the defense industries.

For a long time, VoteHere's chairman was Admiral Bill Owens, a member of the Defense Policy Board and Vice Chairman of Scientific Applications International Corp. (SAIC), which did the Diebold review for the state of Maryland. Robert Gates, former CIA director and head of the George Bush School of Business at Texas A&M, was another director.

VoteHere may be trying to make a comeback with its Internet voting concept. It hired former Washington State Secretary of State Ralph Munro as its chairman. Pam Floyd, who had worked for Washington state elections director David Elliott, left to take a position with VoteHere for three years; she recently became Washington’s assistant state elections director, and she oversees Washington’s Internet SERVE project. Washington state is now leaving the door open (through legislation proposed by Munro crony and current secretary of state Sam Reed) to arrange for more Internet voting in the state.

In 2003, VoteHere decided to go after the innards of other vendors’ touch screens, perhaps hoping to become the Good Housekeeping Seal of Approval for electronic voting machines by claiming that its system verifies the integrity of the vote. This verification system is another way to avoid giving voters the paper ballots they are asking for.

I have always been a proponent of hybrid systems, combining voter-verified paper ballots with computers. Systems like VoteHere, though, make me wonder if we aren’t safer to go back to straight hand-counted paper ballots. Every time we propose a solution to solve a problem with computerized voting systems, a new salesman pops up with a different cure, new techno-jargon, a fresh sales pitch and friends in high places and starts lobbying our public officials. By the time we figure out the latest spin, it could be too late.

* * * * *

VoteHere had its eye on a Pentagon project called SERVE, designed to convert our armed forces over to Internet voting. Despite its clout, VoteHere did not win the contract. Instead, the contract was awarded to election.com and Hart Intercivic.

election.com

This company is no longer in existence, at least in its original form. I am including it so that you can see just how slipshod our government procurement system, which originally awarded the SERVE contract to election.com, really is.

According to its Web site, election.com was a global election software and services company which provided election services like voter registration and Internet voting.

Newsday's Mark Harrington discovered that election.com had sold controlling ownership to an unnamed group of Saudi investors who, he reported, paid $1.2 million to acquire 20 million preferred shares, for 51.6 percent of the voting power. The investment group was identified as Osan Ltd. [41]

I spoke with Amy Parker, press contact for election.com, in February 2003.

Harris: "Is the Newsday article, which states that 51.6% of election.com is owned by Osan Ltd, accurate?"

Parker: "No, that is not true."

Harris: "Is Osan Ltd. involved?"

Parker: "Osan Ltd. became the largest shareholder of election.com in December 2002 — that's an accurate statement — and after December 2002 Osan held 36.2% of all outstanding shares."

Harris: "Is Osan based in the United States, or where?"

Parker: "In the Cayman Islands."

Harris: "So when *Newsday* said they have controlling interest … "

Parker: "After December 2002, Osan held 36.2% of all outstanding shares. And that's equal to 58.2% of the voting power."

OK. So Osan actually owned *more* controlling interest than reported by Newsday. Why would we want our military votes counted by a Saudi-owned company?

At least, if it's approved by the Pentagon, one would assume that it's a pretty solid operation. But for some reason, election.com pulled the names of its directors off the Internet. There are ways to find pages that have been removed, so I did and began contacting directors. I soon received an e-mail from one of the directors which said simply: "You should call me."

I did, and he spoke with me at some length but only after getting my agreement not to reveal which director he was when I printed this interview.

Harris: "I notice they've taken the names off the Web. Are you still involved?"

Director: "No."

Harris: "Tell me about your experience with election.com."

Director: It looked like a hot company, [was] featured in *Red Herring* as one of the companies most going to affect the world and all that ... What happened is that Joe — they had a CEO named Joe, Joe something … "

Harris: "Joe Mohen?"

Director: "That's it. He ended up loving publicity too much. They put those machines in on the Democratic Convention, a giant waste of money, over a million, so Joe could get on TV. When they wanted to start going that way I got concerned. If they were getting into public elections, the market wasn't as huge [as elections in the private market, such as stockholder votes and union elections].

"Of course, the reason I got into it was we wanted to run a business, we wanted to become profitable. ... So the 2000 election in Florida happens, and they change their philosophy and want to do public elections. I said 'this isn't going to work.'

"Finally we get Joe to resign as CEO and we got the Number 2 guy [Charles Smith] to resign also. By this time we were about out of money." (He explained that they brought in a new CEO, who pumped in new money and got some contracts in Australia, but it wasn't long before they ran out of money again.)

Director: "Then, the guy we fired [Charles Smith] comes back with this Arab money. They wanted the board as well as the company. For $5 million, they bought the whole damn thing. At the time the Arab money came in, I made the motion to go ahead and dismiss our butts."

Harris: "What about Charles Smith? I hear he's the guy who represents the Arabs."

Director: "Charles Smith is the guy who we fired. He is sort of an Arab himself; I don't know why he has the name Smith." [According to his bio, Smith previously worked with Procter & Gamble in Saudi Arabia and with PepsiCo in Cairo.]

Harris: "Who else is in the group of investors?"

Director: "Nobody knows who this group is."

Harris: "How Saudi is Osan Ltd?"

Director: "Oh, it's all Saudi as far as I know. What do you know about the thing?"

Harris: "Just what I read in *Newsday*."

According to the *Newsday* article, Defense Department spokesman Glenn Flood, when asked how the department screens the background of contractors, said: "We don't look into that [country of origin] part of it ... It's the process we're interested in, not the company, unless they screw up."

Penelope Bonsall, director of election administration for the Federal Election Commission, told *Newsday* that tracking issues like election.com's change of control doesn't fall under the purview of any federal agency.

I decided to ask Amy Parker more about the Pentagon deal, but the conversation got derailed:

Harris: "With regard to the military contract, what will election.com be doing and what will Hart Intercivic do?"

Parker: "We're not the prime contractor on that project."

Harris: "Election.com is not the main contractor?"

Parker: "No."

Harris: "Who is, then?"

Parker: "That's Accenture."

Harris: "I spoke with Hart Intercivic, who has explained to me that Accenture does not make voting systems. What they do is procurement. They procured the contract and then subcontracted it to election.com and Hart Intercivic, is that true?"

Parker: "Yes."

Harris: "Accenture holds shares in Election.com also, doesn't it?"

Parker: "No.

Harris: "No?"

Parker: "Accenture, we have a formal strategic marketing alliance and as part of that they took an equity position."

Harris: "So Accenture holds shares in election.com, then."

Parker: "Yes."

On July 2, 2003, election.com announced that it had sold its assets to Accenture, turning the military SERVE project over to an Arthur Andersen spin-off and Hart Intercivic.

Hart Intercivic

You might get the impression that Hart Intercivic, a voting-system vendor based in Austin, Texas, is a cozy little family-owned operation, giving us real faces that we can hold accountable and trust with our vote. Not quite.

The chairman of Hart Intercivic is David Hart, whose family developed Hart Graphics, at one time the largest privately-held commercial printer in Texas.[42] Internet growth and the ease of putting documentation on disks and CD-ROMs reversed the company's fortunes.

"We began to see, in the later part of the '90s, a crack in the strategy," David Hart said. "The presses weren't staying busy." In looking for other work to fill the void, "we just ran into a wall. We were singularly unsuccessful." [43]

And it was here that the comfortable, family-owned company turned into a venture-capital- and government-privatization-driven election vendor. Hart Intercivic sells the eSlate, a dial-a-vote variation on the touch-screen concept that uses a wheel instead of a poke with a finger to register your vote.

The finances and managerial control of Hart Graphics were at one time closely controlled by the family, but Hart took a different approach to its election business. They lined up three rounds of venture capital and formed an alliance with a gigantic social-services privatizer.

For initial funding, Hart went to Triton Ventures, a wholly-owned subsidiary of Triton Energy, a firm that primarily exploits oil fields in Colombia. Triton, in turn, is a subsidiary of Amerada Hess. [44]

The $3.5 million awarded by Triton in 1999 didn't last long, but the Help America Vote Act, with its massive allocation of federal money, hovered just over the horizon. In October 2000, Hart picked up $32.5 million more from five sources. [45] In 2002, it raised another $7.5 million. [46]

RES Partners, which invested in Hart's second and third rounds, is an entity that represents Richard Salwen, retired Dell Computer Corporation vice president, general counsel and corporate secretary, who had also worked with Perot Systems and EDS. Salwen is a heavy contributor to George W. Bush and the Republican Party. [47]

Hart's most politically charged investor is an arm of Hicks, Muse, Tate & Furst, which was founded and is chaired by Tom Hicks. Hicks bought the Texas Rangers in 1999, making George W. Bush a millionaire 15 times over. Tom Hicks and his investment company are invested in Hart Intercivic through Stratford Capital. They are also heavily invested in Clear Channel Communications, the controversial radio-raider that muscled a thousand U.S. radio outlets into a more conservative message. [48]

In Orange County, California, and in the state of Ohio, Hart Intercivic entered into a joint enterprise called Maximus/Hart-InterCivic/DFM Associates, led by Maximus Inc.

Maximus Inc. is a gigantic privatizer of social services. It cuts deals with state governments to handle child-support collections, implement welfare-to-work and oversee managed care and HMO programs.

A Wisconsin legislative audit report found that Maximus spent more than $400,000 of state money on unauthorized expenses and found $1.6 million that Maximus couldn't properly document. These unauthorized expenses included a party for staff members at a posh Lake Geneva resort; $23,637 for "fanny packs" to promote the company, with the bills sent to the state; and entertainment of staff and clients by actress Melba Moore. Maximus settled for $1 million. [49]

Maximus jumped into the smart-card business and soon afterward entered the elections industry through an alliance with Hart Intercivic.

All this alliance-building and venture capital-seeking and political shoulder-rubbing is very nice for the big boys in Texas. However, it fundamentally changes the way we run our democracy. Do we really need to bring in Maximus, Hart Intercivic, DFM Associates, Triton oil, CapStreet Group, Dell Computers, Texas Growth Fund and the owner of the Texas Rangers just to count a vote?

The voting-machine industry has created such a byzantine path to computerized voting that it cannot possibly be cheaper or more efficient than voting in a much-simplified way.

What do we really know about the certifier, Wyle Laboratories?

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

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

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

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

Just before the election, in August 2002, William E. Simon & Sons was convicted of fraud and ordered to pay $78 million in damages. In what is surely record time for our glacial judicial system, the conviction was overturned in September 2002. The reason? William E.

Simon & Sons had partnered up with someone who was a criminal and no one could tell who was the guiltiest. [50]

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

Diebold Election Systems

By now, Diebold Inc., the owner of what is now arguably the largest voting-machine company in the U.S., has become famous for its vested interests and an idiotic written statement made by its CEO.

Diebold director W. H. Timken has raised over $100,000 for the 2004 campaign of George W. Bush, earning the designation "Pioneer." Bush supporters qualify as Pioneers if they raise at least $100,000, and Rangers if they raise $200,000. [51]

On June 30, 2003, Diebold CEO Walton O'Dell organized a fundraising party for Vice President Dick Cheney, raising $600,000 and many of our antennas. [52]

Julie Carr-Smyth, of *The Plain Dealer*, discovered in August 2003 that O'Dell had traveled to Crawford, Texas, for a Pioneers and Rangers meeting attended by George W. Bush. Then Smyth learned of a letter, written by O'Dell shortly after returning from the Bush ranch and sent to 100 of his wealthy and politically inclined friends, which said:

"I am committed to helping Ohio deliver its electoral votes to the president next year.'' [53]

Admitting that such candor was a mistake, O'Dell later told Smyth, "I don't have a political adviser or a screener or a letter reviewer or any of that stuff." [54]

O'Dell described Diebold "a model of integrity and reporting and clarity and disclosure and consistency" and said he hoped his company would not suffer because of his mistake. A model of integrity and — clarity? Disclosure, perhaps, if you count embarrassing leaks and the sharp hissing sound of security flying out the window.

Wally O'Dell's statement was ill-advised, if not downright arrogant. But while Wally O'Dell can write about delivering the vote, Diebold's programmers may be in a position to actually do so. Where do they come from?

Diebold Election Systems was formed when Diebold Inc. of Canton, Ohio, acquired a Canadian company called Global Election Systems Inc., headquartered in Vancouver, British Columbia. [55] In some ways, nothing changed. The manufacturing body of the elections company continued to be in McKinney, Texas, under the same management, and the programming brain continued to be in Vancouver, Canada, with the same programmers.

Two of these programmers, Talbot Iredale and Guy Lancaster, have been designing and programming voting machines for Diebold Election Systems Inc. and its predecessors since 1988. Iredale and Lancaster developed the ES-2000 optical-scan voting system currently used in 37 states. [56]

These two men worked for North American Professional Technologies (NAPT), a subsidiary of Macrotrends International Ventures Inc. Their assignment was to develop a computerized voting system.

Macrotrends and NAPT were marketed by Norton Cooper, who had been jailed for defrauding the Canadian government in 1974.[57] This did not keep him out of trouble; he became a stock promoter who sold so much stock in flawed companies though Macrotrends that Jaye Scholl, a writer for *Barron's*, portrayed him as a "hazard" and cautioned the well-heeled to avoid him at the golf course.[58] In 1989, members of the Vancouver Stock Exchange (VSE) ordered Macrotrends to cease any doings with Cooper [59] because his deals went south too often and *Forbes* had written an article describing the VSE as "The Scam Capital of the World," causing an erosion of confidence in the entire exchange.

Charles Hong Lee, a director of both Macrotrends and NAPT, was a childhood friend of Cooper's. In 1989 Lee was ordered to pay $555,380 in restitution when Lee was sued, together with Norton Cooper, by investors in a Macrotrends venture called Image West Entertainment. Cooper settled, but Lee failed to answer the complaint and also failed to list the lawsuit on his personal disclosure form with immigration officials. In 1994, Lee and his partner, Michael K. Graye, allegedly bilked 43 Chinese immigrants, mostly small businessmen, out of $614,547 more in fees than was authorized by the agreement. The unauthorized fees were paid to United Pacific Management Ltd., controlled by Graye and Lee. [60]

In 1991, NAPT and Macrotrends were reorganized, and the name was changed to Global Election Systems. At this time, Michael K. Graye became a director, a position he held for two years. Earlier, Graye had misappropriated $18 million from four corporations, but the law had not yet caught up with him. In 1996, Graye was arrested on charges of tax fraud, conspiracy to commit tax fraud, and money laundering, stemming from activities from 1987 through 1991 with four other companies. For Graye to make bail, a Hong Kong-based shell company called Nexus Ventures Ltd. obtained $300,000 from unwitting investors in Eron Mortgage. Before Graye's sentence could be pronounced in Canada, he was indicted in the U.S. on stock-fraud charges for his involvement with Vinex Wines Inc., a company he and Charles Hong Lee ran. Graye spent four years in prison on the charges related to Vinex Wines and was returned to Canada in May 2000; in April 2003 he admitted that he had misappropriated $18 million and committed tax fraud, and he was sent back to jail. [61]

These founding partners, along with Clinton Rickards (sometimes listed as C. H. Richards), set up Macrotrends, NAPT, and then Global Election Systems. During these early years, Iredale and Lancaster nurtured the ES-2000 optical scan voting system into existence.

The company appears to have washed its hands of Cooper, Lee and Graye. These criminals were involved a decade ago, so why is this relevant now?

It's important because it tells us something about the ethics and due diligence of both Diebold and Global Election Systems. If you are asking people to trust you with their votes, but convicted felons hired and managed the programmers who are now your key people, you have some explaining to do. If criminals who were managing your company were written up in *Barrons* and *Forbes*, publicly embarrassing everyone, we would expect that you would rid yourself forever of such people. If you then hire two more convicted felons, you have just demonstrated that we cannot trust you with our votes.

One such felon, a 23-count embezzler named Jeffrey Dean, who specialized in computer fraud, was made a director of Global Election Systems in 2000, and then was assigned to be the head of research and development, with access to all components of the most sensitive parts of the voting system. The other, a cocaine trafficker named John Elder, has directed the sensitive punch-card printing for both Global and Diebold, and has had involvement with the processing of incoming absentee ballots. Elder is still running the printing division for Diebold.

By 2001, Global Election Systems had grown substantially, but had accumulated a pile of debt. Diebold, Inc. began making arrangements to purchase the company in June 2001. Diebold made a sizeable loan to Global in 2001 and, according to securities documents, arranged to take over manufacturing of Global's voting machines when the Canadian firm could not come up with the cash to service its orders.

While Diebold was loaning money to Global, embezzler Jeffrey Dean remained a director of the company and, according to memos, was involved with the Windows CE system used in the touch-screens and the new 1.96 series optical scan software. He also was working on a project to integrate voter registration software with the GEMS central tabulation program, and he claimed to have developed a "ballot on demand" system which, he bragged to Diebold, could optionally connect a voter with the ballot — a feature which is certainly illegal and would remove voter privacy.

Global Election Systems was formally purchased by Diebold Inc. effective January 31, 2002, and at this time Jeffrey Dean became a paid consultant to Diebold Election Systems and John Elder took over Diebold's national printing division.

Six weeks later, Diebold landed the biggest voting-machine order in history: The $54 million conversion of the state of Georgia to touch-screen voting.

9
The First Public Look – Ever –
into a secret voting system

Author and historian Thom Hartmann writes:[1]

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

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

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

For example, you can't ask any questions.

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

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

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

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

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

"It is frustrating because claims are made about these systems, how they are designed, how they work, that, frankly, I don't believe," says Dill. "In some cases, I don't believe it because the claims they are making are impossible. I am limited in my ability to refute these impossible claims because all the data is hidden behind a veil of secrecy." [5]

When members of the California Task Force on Electronic Voting asked how the machines were tested, Wyle and Ciber declined to answer.

"We wanted to know what these ITAs do," said Dill. "So we invited them to speak to us. ... They refused to come visit us. They were also too busy to join us in a phone conference. Finally, out of frustration, I wrote up 10 or 15 questions and sent it to them via the Secretary of State's office. They didn't feel like answering those questions, either."

"What testing do the manufacturers do?" asks Dill. "If you go to their Web pages, it says 'if you'd like to know something about us, please go to hell' in the nicest possible way."

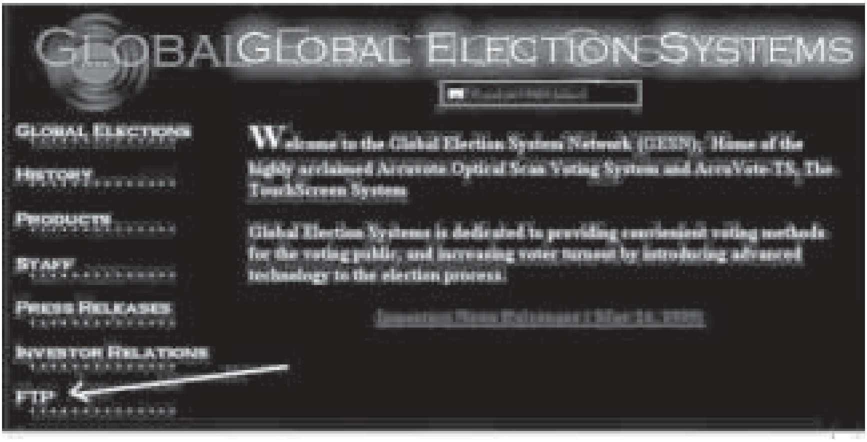
You can't examine a machine or even look at a manual. David Allen, who published an Internet version of this book, wanted me to find out how the machines work.

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

He didn't have that information, and neither did anyone else. I decided to find some programmers for the vendors. I was most interested in ES&S — at that time, I hadn't done much work at all on Diebold Election Systems. I entered "@essvote.com" into the Google search engine, looking for e-mails that might give me names I could contact, and found a few dozen employees who work for ES&S.

I postponed calling them. What would I say? So I stalled by convincing myself that I should find as many names as possible. I got some from Sequoia. I entered "Global Election Systems" and found some old documents with e-mails ending in "gesn.com."

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



Welcome to the Global Election System Network (GESN), Home of the highly acclaimed Accuvote Optical Scan Voting System and AccuVote-TS, The TouchScreen System

Global Election Systems is dedicated to providing convenient voting methods for the voting public, and increasing voter turnout by introducing advanced technology to the election process.

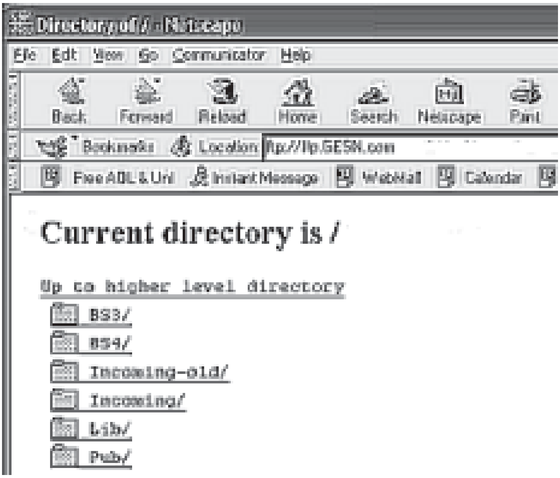
[illegible]

Old Global Election Systems Web page: GESN.com

I clicked all the links, including the link called “FTP,” which took me to a page full of files.

I called David Allen. “What am I looking at?”

Allen admitted that the file names, like “BS4” and “GA-062802” meant nothing to him, but we both knew that this was an online file stash. He snorted and offered a comment: “Incredible stupidity.”


Directory of / - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print
Bookmarks Location: ftp://ftp.GESN.com
Free AOL & Unl Instant Message WebMail Calendar

Current directory is /

Up to higher level directory
- BS3/
- BS4/
- Incoming-old/
- Incoming/
- Lib/
- Pub/

I’d found the crown jewels for Diebold Election Systems. What follows is the first detailed look — ever — into a secret voting system.

rob-georgia.zip

(Noun or verb?)

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

What if you knew that the devil went down to Georgia on November 5, 2002, and handed that state an election with six upsets, tossing triple-amputee war veteran Max Cleland out of the U.S. Senate in favor of a candidate who ran ads calling Cleland unpatriotic?

Suppose you knew that in Georgia, the first Republican governor in 134 years had been elected despite trailing in every poll, and that African American candidates fared poorly even in their own districts?

If you learned that these machines had been installed just prior to an election — and then you saw a folder called "rob-georgia," looked inside, and found instructions to replace the files in the new Georgia voting system with something unknown, what would you do?

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

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

"No."

"Why not?"

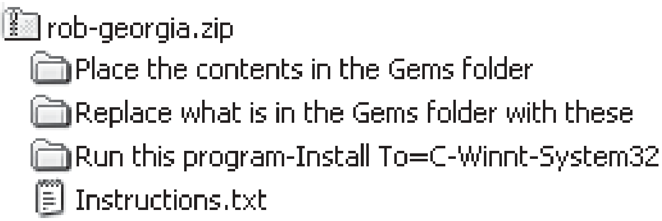
"Because I don't think 'rob-georgia' could possibly mean rob Georgia," he said.

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

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

Why in the world would an ATM manufacturer like Diebold leave sensitive files hanging out there on an unprotected Internet site? I made a few phone calls, which confirmed that Diebold *knew* the site was unprotected, and learned that the site had been there for years.

I kept asking if anyone knew who Rob was. Everyone told me there was no employee named Rob in Georgia. Perhaps rob was a verb?



rob-georgia.zip
Place the contents in the Gems folder
Replace what is in the Gems folder with these
Run this program-Install To=C-Winnt-System32
Instructions.txt

"rob-georgia" is a compressed folder with three more folders, containing 3,794 more files, inside it. It contains uncertified program modifications, a way to slip any damn thing you want into a voting machine.

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

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

A program modification was needed because the touch-screens were freezing up, crashing the machines. Makes sense. The problem must be a big one to justify modifying the progam on all 22,000 machines in Georgia. But wait a minute — This is in the Media Backgrounder put out by the Georgia Secretary of State Press Office. [7]

> "Before being considered for acquisition in Georgia ... software is examined for reliability and hardware is subjected to a variety of 'torture tests.' The state testing examines both hardware and software for accuracy and reliability, and mock elections are conducted on the equipment, witnessed by county election officials."

The document names Wyle Laboratories and Ciber, Inc., citing their "extensive experience in NASA-related testing." So how did these NASA-testing labs miss something so obvious that all 22,000 voting machines required a modifications to keep them from crashing?

Here is what Diebold wrote to certifier Wyle Laboratories in its latest touch-screen certification documents:

> "It is Diebold Election Systems, Inc. policy that the only acceptable level of conformance is Zero Defects."[8]

Okay, we all know that "zero defects" is one of those terms that sounds good and doesn't happen. But we ought to at least hold Diebold to this promise:

> "The manufacturing test location, test date, and inspector initials will be recorded on a label on every voting machine."

Whose initials are on the Georgia machines? Anyone's?

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

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

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

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

If each touch screen was tested before leaving the factory, why did every single machine need modifications, in order not to crash, *after* they reached Georgia? The machines were shipped to Georgia in June 2002. And once they arrived, we are told, there was more testing:

> "Upon arrival at Diebold's central warehouse in Atlanta, each unit was put through a diagnostic sequence to test a variety of functions, including the card reader, serial port, printer, the internal clock and the calibration of the touch screen itself. These tests were audited by experts from Kennesaw State University's Center for Election Systems."

The following statement, on Georgia Secretary of State letterhead, remains posted on the state's Web site as of the writing of this book.

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

Was this testing rigorous? Yes, rigorous, they promised. According to the Media Backgrounder:

> "Georgia's multi-tiered election equipment testing program [is] among the most rigorous in the nation."

Could someone take a moment to do the math with me? If this testing is "rigorous," might we expect them to invest, say, 10 minutes per machine? The testing just described adds up to every touch-screen unit being tested three times before it gets to the "logic and accuracy" test. You can check the footnotes for my calculations: All this testing would take 17 people working 40 hours per week for four months doing nothing but rigorous testing.[10]

Call me a skeptic, but I want to see the payroll records on that.

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

And what exactly was in rob-georgia.zip?

* * * * *

With so many unanswered questions, I decided to ask the public officials responsible for voting systems in the state of Georgia about these program modifications. Here are excerpts from a February 11, 2003, interview with Michael Barnes, Assistant Director of Elections for the state of Georgia: [11]

Harris: "I want to ask you about the program update that was done on all the machines shortly before the election."

Barnes: "All right."

Harris: "Was that patch certified?"

Barnes: "Yes."

Harris: "By whom?"

Barnes: "Before we put anything on our equipment we run through state certification labs, and then, in addition to that, we forwarded the patch to Wyle labs in Huntsville. ... Wyle said it did not affect the certification elements. So it did not need to be certified."

Harris: "Where's the written report from Wyle on that? Can I have a copy?"

Barnes: "I'd have to look for it. I don't know if there was ever a written report by Wyle. It might have been by phone. Also, in Georgia we test independently at Kennesaw University — a state university."

Harris: "Can I see that report?"

Barnes: "You'd have to talk to Dr. Williams, and he's out of town ... Dr. Williams is on the National Association of State Election Directors (NASED) certification, and I think he's also at Kennesaw University. He does the certification for the state of Georgia."

Harris: "Was this new patch tested with a Logic and Accuracy test, or was it tested by looking at the code line by line?"

Barnes: "Logic and Accuracy, and also they verify that our version is identical and also any software is tested through Ciber and Wyle."

Harris: "But Wyle decided not to test the patch, you say. Was this patch put on all the machines or just some of the machines?"

Barnes: "All the machines."

Harris: "So every machine in Georgia got this program update."

Barnes: "Yes, every one of the machines used on election day in November. If it had been sent out to counties prior already, Diebold and their technicians went out and manually touched every machine. Some of the machines were still at the manufacturer, they did the patches on those."

Harris: "How long did it take to do patches on — what was it, around 22,000 machines?"

Barnes: "It took about a month to go back out and touch the systems."

Harris: "Can you tell me about the procedure used?"

Barnes: "The actual installation was a matter of putting in a new memory card. ... They take the PCMCIA card, install it, and in the booting-up process the upgrade is installed."

OK, let's regroup. So far, we have thousands of defective voting systems that somehow made it through Wyle's hardware testing, Ciber's software testing, Diebold's factory testing, rigorous testing on arrival at the Georgia warehouse and more testing when delivered to each of Georgia's 159 counties. But the machines didn't work.

Then we have a set of file replacements called "rob-georgia," and a Georgia state elections official telling us they replaced files on all 22,000 machines in Georgia. In an act of computer science clairvoyance, it was determined by telephone that nothing was on the modifications that anyone needed to look at. We know from a memo dated September 16 that there were plans to install program modifications; we know that the Georgia general election was held November 5, 2003, and we've been told that it took about a month to go out and "touch" every machine.

What we have here is a group of Georgia election officials running around the state replacing the computer commands in the voting system *right before the election* without anyone examining what the new commands actually do. Who ordered this? Let's find out where the buck stops.

Harris: "Where did the actual cards come from?"

Barnes: "Diebold gave a physical card — one card that activates each machine. There were about 20 teams of technicians. They line the machines up, install the card, turn on, boot up, take that card out, move on, then test the machine."

Harris: "Were people driving around the state putting the patches on the machines?"

Barnes: "Yes."

The order came from Diebold and was implemented by Georgia election officials and Diebold employees.

Harris: "What comment do you have on the unprotected FTP site?"

Barnes: "That FTP site did not affect us in any way, shape or form because we did not do any file transferring from it. None of the servers ever connected so no one could have transferred files from it. No files were transferred relating to state elections."

When someone issues that many denials in a single answer, it makes me wonder if the truth lies somewhere in the opposite direction.

Harris: "How do you know that no one pulled files from the FTP site?"

Barnes: “One voting machine calls the servers and uploads the info. We don’t allow the counties to hook up their servers to a network line.”

Harris: “I notice that one of the things the network builder put on the [county] machines was a modem.”

Barnes: “The only time you use the modem is on election night. That is the only time the unit was used, was election night when they plug it into the phone.”

Harris: “Having the screens freeze up is a pretty severe error — how did 5 percent of the machines get out of the factory with that? How did they get through Wyle testing labs?”

Barnes: “All I know is that the machines were repaired.”

Harris: “How do you know that the software in the machines is what was certified at the labs?”

Barnes: “There is a build date and a version number that you can verify. Kennesaw University did an extensive audit of the signature feature — Dr. Williams and his team went out and tested every machine afterwards to make sure nothing was installed on them that shouldn’t have been.”

Harris: “They tested every one of 22,000 machines?”

Barnes: “They did a random sampling.”

So the FTP site, which contained 40,000 files, placed there over a period of six years, was never used and no one transferred files from it, no one could transfer files from it, no files were transferred. And the modems which James Rellinger (the contractor who installed the Georgia servers for 159 counties) was instructed to put into every county voting system were never used except for once.

(When questioned on August 22, 2003, Dr. Britain Williams claimed that most counties did not use these modems *at all*. “Some counties don’t have phone lines. Some don’t even have bathrooms,” he told a group of people that included computer programmer Roxanne Jekot and *Atlanta Journal-Constitution* reporter Jim Galloway.)

On February 12, 2003, I interviewed Dr. Williams, Kennesaw Election Center, an organization funded by the Georgia Secretary of State.[12]

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

Dr. Williams: “For the state of Georgia — I don’t do certification.

The law gives the Secretary of State the authority to say what systems are certified and what are not. What I do is an evaluation of the system."

Harris: "What was your involvement in certifying the program patch that was put on? Did you actually certify the patch, or did you determine that it was not necessary?"

Dr. Williams: "Part of our testing program is when these machines are delivered, we look at the machines and see that they comply. And in the process of doing that — representatives of Kennesaw University did this — we found about 4-5 percent of the machines were rejected, not all because of screen freezes, but that was one of the problems."

Harris: "It was the screen freezes that caused them to issue a program patch?"

Dr. Williams: "Yes. The vendor [Diebold] created a patch addressing the screen freezing. It made it better but didn't completely alleviate the problem."

Harris: "Did you do a line-by-line examination of the original source code?"

Dr. Williams: "For the original — no. We don't look at the source code anyway; that's something done by the federal ITAs."

Harris: "Did you do a line-by-line examination of the patch?"

Dr. Williams: "The patch was to the operating system, not to the program *per se*."

Harris: "It only changed Windows files? Do you know that it didn't change anything in the other program? Did you examine that?"

Dr. Williams: "We were assured by the vendor that the patch did not impact any of the things that we had previously tested on the machine."

(The evaluator was assured by the vendor? Who's in charge?)

Harris: "Did anyone look at what was contained in the replacement files?"

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

Harris: "Did you issue a written report to the Secretary of State indicating that it was not necessary to look at the patch?"

Dr. Williams: "It was informal — not a report — we were in the heat of trying to get an election off the ground. A lot was done by e-mails."

So Barnes points to the ITAs but admits they never examined the program modifications, and then he points to Williams, who in turn points to the ITAs and then points to the vendor. No one writes a report about any of this. Dr. Williams implies that this program replacement was put on when they took delivery, but that was in June. The program modifications were done in October.

Harris: "What month did you install that program patch?"

Dr. Williams: "When we took delivery, we were seeing that the patch was on there."

Harris: "I have a memo from the Secretary of State's office that is dated in August [Sept. 16, actually], and it says that due to a problem with the screens freezing, a patch was going to be put on all the machines in Georgia. ... Apparently, someone had already taken delivery on these machines and they had already been shipped out around the state before the patch was applied, is that right?"

Dr. Williams: "The patches were done while we were doing acceptance testing. One of the things we looked for during acceptance testing was to make sure the patch was put in."

Harris: "But as I understand it, a team of people went around the state putting these patches on."

Dr. Williams: "By the time they put the patches in, the majority of the machines had been delivered. Actually, it was going on at the same time. When they started putting the patches in around the state, we tested the machines where they did that [put the patches in] at the factory."

Harris: "When I spoke with Michael Barnes, he said that you tested all the machines, or a random sampling of the machines, after the patch was put on."

Dr. Williams: "We had five or six teams of people with a test script that they ran on each machine — "

Harris: "The test script did what?"

Dr. Williams: "The test script was generic. It was in two parts. One part tested the functionality of the machine. It was a hardware diagnostic; it primarily tested that the printer worked, that the serial port worked, that the card reader worked, tested the date and time in the machine, and to an extent checked calibration of the machine. Then if it passed all of those, it tested the election. We loaded a small sample election in, the same as the one used during certification testing, and we ran a pattern of votes on there."

This is good, but he's telling me about testing printers and things. Barnes had told me that "Dr. Williams and his team went out and tested every machine afterwards to make sure nothing was installed on them that shouldn't have been." I wanted to know if anything had been put in the software that might affect our votes.

Harris: "Can you tell me about the digital signature?" [A digital signature is used to show that no changes in the software were done.]

Dr. Williams: "That's part of the test that involves looking at the software — putting the patch on wouldn't change the digital signature."

Harris: "But if you put in a program patch, wouldn't that show that a change has been made?"

Dr. Williams: "No, because the patch was only in the Windows portion — there was no digital signature check on the operating system … "

I'm sorry to subject you to this excruciating interview, and I apologize for throwing terms like "digital signature" around. I had heard that this "checksum" or "digital signature" was a way to determine that no unauthorized code was put into our voting system, so I was trying to find out how it worked — or if they used it at all.

But Dr. Williams, the official voting machine examiner for Maryland, Virginia and Georgia, was indicating that he did not check things if they involved the Windows operating system. That would open up a security hole the size of British Columbia. All you'd have to do is mess with Windows, upload your handiwork into the Georgia voting system, and you'd have direct access to a million votes at once.

Dr. Williams was interested in the non-Windows code and the ITA labs; I wanted to know about the Windows modifications and the other security problems associated with sticking program modifications on voting machines using PCMCIA cards.

Dr. Williams: "They write the source code and the source code is submitted to the federal lab. When it passes the lab they freeze the source code; at that point it's archived. Any change after that is subject to retesting."

That's nice, but he just said they changed the frozen source code without retesting it. And why stop at replacing the Windows operating system — maybe the whole program could be replaced by substituting unauthorized cards during this process of "patching" the voting software.

Harris: "What was the security around the creation of the cards used to implement the patch?"

Dr. Williams: "That's a real good question. Like I say, we were in the heat of the election. Some of the things we did, we probably compromised security a little bit. Let me emphasize, we've gone back since the election and done extensive testing on all this."

Harris: "Based on your knowledge of what that patch did, would it have been needed for all the machines of same make, model and program? Including machines sold to Maryland and Kansas that were built and shipped around the same time?"

Dr. Williams: "Yeah, but now the key phrase is 'with the same system.' Maryland ran a similar version with a different version of Windows and did not have this problem."

Harris: "So the program was certified by the federal labs even when it ran on different versions of the operating system?"

Dr. Williams: "Yes, they don't go into the operating system."

Maybe the federal labs don't, and Williams said that he didn't, but someone was going into the operating system: Talbot Iredale, senior vice president of research and development for Diebold Election Systems, one of the two original programmers hired during the Vancouver Manuever era, modified the Windows CE operating system used in Georgia.[13] One man. One million votes.

Talbot Iredale could be as honest as a church pastor — actually, one of the pastors at my church once ran off with $16,000 — but even if Iredale has absolute integrity, allowing one person unchecked access to a million votes at once has got to be the biggest security breach in the history of the U.S. electoral system. (Now if one man got his own uncertified software into Diebold's optical-scan system, that would be bigger: In 2002, those machines counted about seven million votes.[14] More on that later.)

Harris: "There was an unprotected FTP site which contained software and hardware specifications, some source code and lots of files. One file on that site was called "rob-georgia," and this file contained files with instructions to 'replace GEMS files with these' and 'replace Windows files with these and run program.' Does this concern you?"

Dr. Williams: "I'm not familiar with that FTP site."

Harris: "Is there a utility which reports the signature? Who checks this, and how close to Election Day?"

Dr. Williams: "We do that when we do acceptance testing. That would be before election testing."

Harris: "What way would there be to make sure nothing had changed between the time that you took delivery and the election?"

Dr. Williams: "Well there wouldn't — there's no way that you can be absolutely sure that nothing has changed."

Harris: "Wouldn't it help to check that digital signature, or checksum, or whatever, right before the election?"

Dr. Williams: "Well, that is outside of the scope of what some of the people there can do. I can't think of any way anyone could come in and replace those files before the election — "

Harris: "Since no one at the state level looks at the source code, if the federal lab doesn't examine the source code line by line, we have a problem, wouldn't you agree?"

Dr. Williams: "Yes. But wait a minute — I feel you are going to write a conspiracy article."

Harris: "What I'm looking at is the security of the system itself — specifically, what procedures are in place to make sure an insider cannot insert malicious code into the system."

Dr. Williams: "There are external procedures involved that prevent that."

Harris: "This is exactly what I want to know. If you know what procedures would prevent that, could you explain them to me?"

Dr. Williams: "We have the source code. How can they prevent us from reviewing it? I have copies of source code that I've certified."

Harris: “But you said you do not examine the source code.”

Dr. Williams: “Yes, but the ITA did it. The ITA, when they finish certifying the system, I get it from the ITA — someone would have to tamper with the source code before it goes to the ITA and the ITA would have to not catch it.”

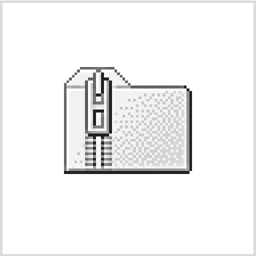
Of course, both Williams and Barnes just told us that the ITA never examined the modifications made to 22,000 machines in Georgia. Let's consider a few points here:

Tiny programs can be added to any program modification. The file “Setup.exe” launches many of these, some of which are “.dll” files, which stands for “dynamic link library.” These are small files that hide inside executable programs and can launch various functions (whatever the programmer tells them to do). They can be set up to delay their launch until a triggering event occurs. There is nothing wrong with .dll files, but there is something very wrong with putting new .dll files into a voting machine if no one has examined them.

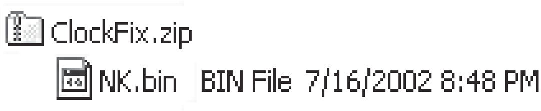
Other files, such as “nk.bin,” also contain executables that can literally rewrite the way the system works. The nk.bin file is like a mini-Windows operating system. If a programmer modifies the nk.bin file and these unexamined files are put on the voting machine, the truth is, we have no idea what that machine is doing.

Any time you do a program modification, you can introduce a small trojan horse or virus that can corrupt the election.

The rob-georgia.zip folder includes a file called “setup.exe” that was never examined by certifiers. It contains many .dll files. The “clockfix” zip file is an nk.bin file. Someone should have looked at these.



ClockFix.zip



ClockFix.zip

NK.bin BIN File 7/16/2002 8:48 PM

(Hey! What’s this?
I found it on the
Diebold FTP site.)

Now, about the Windows operating system: In order to use "COTS" software (Commercial Off-The-Shelf) without having certifiers examine it, the commercial software must be used "as is," with no modifications. If the patches that Barnes and Williams referred to were Windows patches, the moment Diebold modified them they became subject to certification. They did not come from Microsoft. They came directly from Diebold. Therefore, they were not "as is, off the shelf." Someone should have looked at these, too.

The rob-georgia.zip file includes one folder containing replacements for the Windows operating system and two folders with replacement files that are *not* for Windows. You don't need to be a computer scientist to see this: Just look at the file names, which instruct the user to alter the GEMS program. GEMS is not part of the Windows operating system. Someone should have looked at these.

Someone should have looked at all these files, but no one did. In fact, no one has any idea what was on those Georgia voting machines on Nov. 5, 2002. Georgia certified an illegal election. Now what?

* * * * *

As word spread about voting system files found on an open FTP site, it became a favorite topic of conversation on Internet discussion forums.

> *"This could make Watergate look like a game of tiddlywinks... Get a good seat. This could be quite a long ride!"*
>
> — *"TruthIsAll"*

Public examination of the files is the best thing that could have happened. It's the only way we can engage in an informed debate about voting machines. I'm glad we got a look inside, but what we found should divest you once and for all of the idea that we can "trust" secret voting systems created by for-profit corporations.

There is no reason to believe that other manufacturers, such as ES&S and Sequoia, are any better than Diebold — in fact, one of the founders of the original ES&S system, Bob Urosevich, also oversaw development of original software now used by Diebold Election

Systems. Because voting systems (except AccuPoll,[15] which is open-source) are kept secret, I am focusing on Diebold only because we can't find out anything about the other vendors' systems.

We do know that ES&S filed a patent infringement lawsuit against Global Election Systems at one time, [16] indicating that some part of the system was alleged to be identical. Also, Chapter 2 shows that Diebold, Sequoia and ES&S have all miscounted elections many times.

Some advocates confuse what happened with Diebold's unprotected FTP site with "open source." Very reputable programs, such as the Linux operating system, have been developed through open source, letting the whole world examine the system and suggest improvements. What Diebold did, though, is quite different.

If you never obtain public feedback to improve your software, what you have is horrific security, not an open-source system. People have by now examined the Diebold files, but it's still not open source because no one has the slightest idea what Diebold has done to correct the flaws, if anything.

If the Diebold system had allowed everyone with expertise to critique the software during development and then showed how it corrected the flaws, that would be open source. Such a procedure would no doubt arrive at a very simple and secure program with a voter-verified paper ballot to back it up.

Instead, Diebold allowed only a small handful of programmers to look at its software. Then they put all the software (along with passwords and encryption keys) on an open Web site and left it there for six years, where crackers could download it and people interested in elections could find it, but respectable experts and citizens' groups were not told of its existence or allowed to examine anything.

Putting that kind of material on an unprotected Web site was "a major security stuff-up by anyone's reckoning."[17] That's how Thomas C. Greene of *The Register* describes what Diebold did, and he's right. Diebold's entire secret election system was available to any hacker with a laptop.

Our certification system is fundamentally broken. The system is secret, relies on a few cronies and is accountable to no one. Worse, the certifiers have clearly given a passing grade to software so flawed that it miscounts, loses votes and invites people to come in the back door to make illicit changes. But even this inadequate certification system would be better than what we discovered is really happening:

Diebold has used software directly off its FTP site without submitting it for certification at all. Quite literally, this software went from a programmer's desk directly into our voting machines.

The Diebold FTP site and election-tampering:

If you want to tamper with an election through electronic voting machines, you want to play with:

Ballot configuration — Switch the position of candidates. A vote for one candidate goes to the other.

Vote recording — Record votes electronically for the wrong candidate, or stuff the electronic ballot box.

Vote tallying — Incorrectly add up the votes, or substitute a bogus vote tally for the real one, or change the vote tally while it is being counted.

You'd want to find out as much as you could about procedures. No problem — the Diebold open FTP site contained the "Ballot Station User Manual," the "Poll Worker Training Guide" and at least two versions of the "GEMS User Manual," along with the "Voter Card Programming Manual" and hardware configuration manuals for the AccuVote touch-screen system.

It would be helpful to play with elections in the comfort of your own home. Not a problem — full installation versions of the Diebold voting programs were on the Web site.

*BallotStation.ex*e (vote recording and precinct tallying for the touch-screen machines)

GEMS.exe (county-level tallying of all the precincts, found in the GEMS folders)

VCProgrammer.exe (programs to sign in and validate voter cards)

Just about every version of the Diebold programs ever certified, and hundreds that were never certified, were available.

It might be helpful also to know what kind of testing the voting system goes through, especially the details on the "Logic and Accuracy" testing done right before and after the election. After all, you'd want to make sure that whatever hacking you do doesn't get caught. Testing procedures, sample testing results and instructions on how to do the testing were also on the Diebold FTP site.

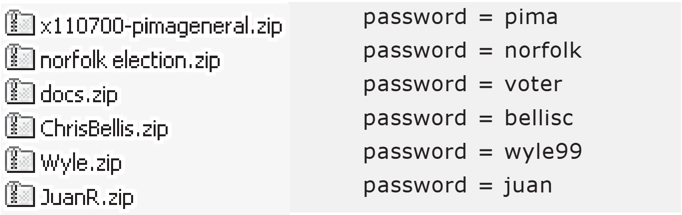
You'd want to see some typical ballot configurations — or, better yet, get the data files created for actual elections. That way you'd know the positioning of the candidates on the ballot, and you could even get the candidate I.D. number used by the computers to assign votes. You could do test runs using real election files.

No problem: On the FTP site were files designated for counties in California, Maryland, Arizona, Kentucky, Colorado, Texas, Georgia, North Carolina, Kansas and Virginia. Some files, like one for San Luis Obispo County, California, were date-stamped on an election day (curiously, five hours before the polls closed).

By now you may have heard about a report by Johns Hopkins and Rice University scientists, which used these files. What you may not realize is that these scientists studied less than 5 percent of the information on the FTP site. They studied the source code of one of the voting-system components, the touch screen. The FTP files also included source code for many other components of the voting system, and compiled files, databases and technical documentation and drawings.

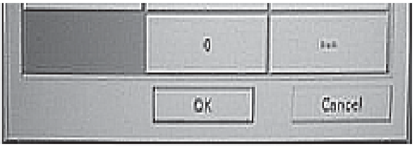
The site also contained information on how to set up remote access, and passwords.

Guessing many of the passwords is easy because files are named for Diebold employees, and many passwords are simply the name of the location using the software.



x110700-pimageneral.zip	password = pima
norfolk election.zip	password = norfolk
docs.zip	password = voter
ChrisBellis.zip	password = bellisc
Wyle.zip	password = wyle99
JuanR.zip	password = juan

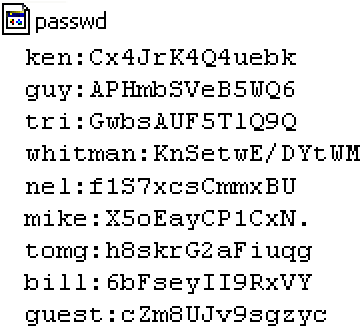
The supervisor password for voting machines at the polling place was "1111." When I saw this in the manual, it reminded me of buying a new briefcase. It comes with a "default" combination, but of course you change the combination as soon as you start using the briefcase.



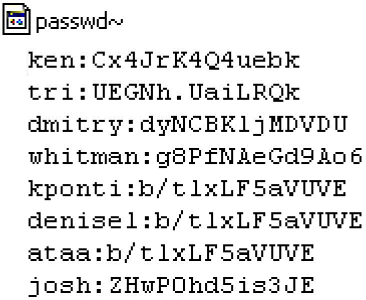
1. Insert the Manager card into the card reader.
2. Enter the password 1,1,1,1,and touch "OK".
3. Remove card when instructed.
4. When the screen below appears, press the "End Election" button.

For some reason, Diebold's voting machines were less secure than your briefcase. That's because programmers hard-wired the password into the source code. That way, no one could change the password, and anyone inside the polling place (the janitor, a crooked politician) could pretend to be a supervisor by entering "1111."

In case you need a fancy password, the files called "passwd" might come in handy. I don't know if anyone found a use for the Diebold programmer passwords, but these were sitting there.



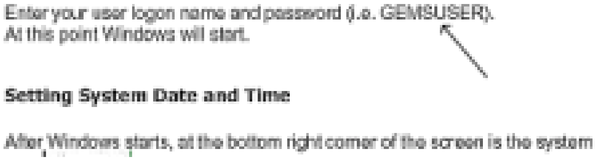
```
ken:Cx4JrK4Q4uebk
guy:APHmbSVeB5WQ6
tri:GwbsAUF5T1Q9Q
whitman:KnSetwE/DYtWM
nel:f1S7xcsCmmxBU
mike:X5oEayCP1CxN.
tomg:h8skrG2aFiuqg
bill:6bFseyII9RxVY
guest:cZm8UJv9sgzyc
```



```
ken:Cx4JrK4Q4uebk
tri:UEGNh.UaiLRQk
dmitry:dyNCBKljMDVDU
whitman:g8PfNAeGd9Ao6
kponti:b/tlxLF5aVUVE
denisel:b/tlxLF5aVUVE
ataa:b/tlxLF5aVUVE
josh:ZHwPOhd5is3JE
```

At the county election supervisor's office, the results from all the polling places are tabulated using a program called GEMS, and the password, "GEMSUSER," was in the user manual. The election supervisor can change "GEMSUSER," but later I'll show you how a 10-year-old could change it right back.

A cracker who wants to pretend he is the elections supervisor might start by installing one of the GEMS vote-tallying programs on his home computer. There were over 100 versions of this program on the FTP site, many of which were never certified but were used anyway.



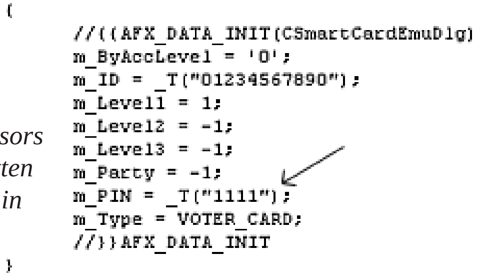
Enter your user logon name and password (i.e. GEMSUSER).
At this point Windows will start.

Setting System Date and Time

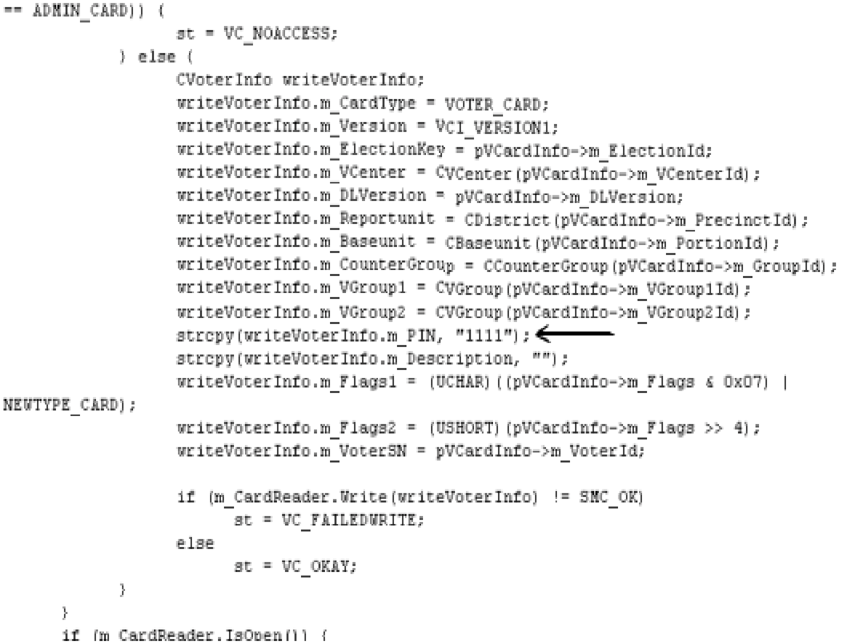
After Windows starts, at the bottom right corner of the screen is the system

The password for the GEMS program is "GEMSUSER"

Supervisor access at the polling place is granted by the password 1111. Instead of allowing supervisors to control the password, it is written into the source code and printed in the manuals.



```
{
    //{{AFX_DATA_INIT(CSmartCardEmuDlg)
    m_ByAccLevel = '0';
    m_ID = _T("01234567890");
    m_Level1 = 1;
    m_Level2 = -1;
    m_Level3 = -1;
    m_Party = -1;
    m_PIN = _T("1111");
    m_Type = VOTER_CARD;
    //}}AFX_DATA_INIT
}
```



```
== ADMIN_CARD)) {
                        st = VC_NOACCESS;
                } else {
                        CVoterInfo writeVoterInfo;
                        writeVoterInfo.m_CardType = VOTER_CARD;
                        writeVoterInfo.m_Version = VCI_VERSION1;
                        writeVoterInfo.m_ElectionKey = pVCardInfo->m_ElectionId;
                        writeVoterInfo.m_VCenter = CVCenter(pVCardInfo->m_VCenterId);
                        writeVoterInfo.m_DLVersion = pVCardInfo->m_DLVersion;
                        writeVoterInfo.m_Reportunit = CDistrict(pVCardInfo->m_PrecinctId);
                        writeVoterInfo.m_Baseunit = CBaseunit(pVCardInfo->m_PortionId);
                        writeVoterInfo.m_CounterGroup = CCounterGroup(pVCardInfo->m_GroupId);
                        writeVoterInfo.m_VGroup1 = CVGroup(pVCardInfo->m_VGroup1Id);
                        writeVoterInfo.m_VGroup2 = CVGroup(pVCardInfo->m_VGroup2Id);
                        strcpy(writeVoterInfo.m_PIN, "1111");
                        strcpy(writeVoterInfo.m_Description, "");
                        writeVoterInfo.m_Flags1 = (UCHAR)((pVCardInfo->m_Flags & 0x07) |
NEWTYPE_CARD);
                        writeVoterInfo.m_Flags2 = (USHORT)(pVCardInfo->m_Flags >> 4);
                        writeVoterInfo.m_VoterSN = pVCardInfo->m_VoterId;

                        if (m_CardReader.Write(writeVoterInfo) != SMC_OK)
                                st = VC_FAILEDWRITE;
                        else
                                st = VC_OKAY;
                }
        }
        if (m_CardReader.IsOpen()) {
```

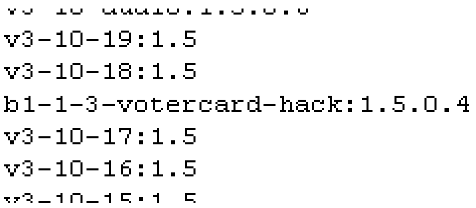
GEMS is on the central computer at the county elections office. This is the software that creates the ballots before the election, and it also accumulates the incoming votes from the polling place and creates election reports. The same GEMS program handles both touch screens and optical-scan machines. There were many vote databases tagged to cities and counties, so a cracker could practice tampering with real software and real votes.

Any computer that has Windows seems to work, but meticulous people would follow the instructions left on the FTP site and put the GEMS program on a Dell PC with Windows NT 2k installed. Diebold support techs have also helped counties set up GEMS on Windows XP and Windows 2000.

So many versions of the GEMS program, so little time. A good version to start with would be GEMS 1.17.17 — according to NASED documents, that was an officially certified version of GEMS during the general election in November 2002.

A folder called "Pima Upgrade" might be a good choice for a hacker living in Tucson, and the new 1.18 series was also available. An even newer program, version 1.19, was put on the FTP site on January 26, 2003, just three days before it was taken down.

Suppose you wanted to simulate an actual touch-screen voting machine. You need to activate those with a smart card, and the average desktop computer isn't set up for that. Put the word "votercard" into a text search on the Diebold files, and this pops up in a file called "votercard.cpp,v"



```
v3-10-audio:1.5.0.6
v3-10-19:1.5
v3-10-18:1.5
b1-1-3-votercard-hack:1.5.0.4
v3-10-17:1.5
v3-10-16:1.5
v3-10-15:1.5
```

Now, if I'm a cracker and I get the "Votercard.cpp,v" file, and I'm running a computer that really isn't a voting machine but want to figure out how it works, here it is: a neat little program that can cancel out the card reader entirely. Diebold handed me the road map and helped me find it by naming it "votercard-hack." A moderately skilled programmer will know how to paste it into the latest touch-screen source code, recompile, install, and start playing around.

The suffix "cpp" stands for "C++," and these files are source code. "Source code" contains the commands given to the computer that tell it how to execute the program. Many people are surprised to learn that source-code files consist of English-like programming commands that people can read. After software engineers write the program, it is compiled to make it machine-readable.

The cvs.tar file that Diebold left on its Web site was a source code "tree" for the program used to cast votes on touch screens. The tree contains the history of Diebold's software development process, going all the way back to Bob Urosevich's original company, I-Mark Systems, through Global Election Systems, and including 2002 programming under Diebold Election Systems.

Leaving other people's pants unzipped

It's bad enough when you leave your own sensitive stuff on the Web. But Diebold exposed other people's confidential information, also. Diebold left 15,900 of Microsoft's proprietary Windows CE source- code files on its public Web site, ready to assemble like a set of Legos.

The Microsoft Windows CE Platform Builder is a set of development tools for building a Windows CE operating system into customized gadgets. You are supposed to have a license to use it, and, according to Bill Cullinan of Venturcom Inc., a Waltham, Massachussetts-based Windows CE distributor and developer, the kit is not free.

"The Platform Builder development kit for the new Windows CE .net runs about $995," he told me. "Earlier, the cost was up over $2,000."

Any cracker in the world could access the pricey Microsoft developer's platforms through the Diebold FTP site.

Despite a notice that says, "You may not copy the [Hewlett Packard] Software onto any public network,"copies of Hewlett Packard software were on the public FTP site hosted by Diebold.

A document marked "Intel Confidential" pertaining to microprocessor development for personal PCs was on the FTP site, along with the Merlin PPC Sourcekit for personal PCs and the Intel Cotulla development kit and board support packages for Microsoft Windows CE .NET and PocketPC 2002.

So Diebold expects us to trust them with our vote, yet they are quite cavalier with other people's intellectual property and, as we will see in the next section, with people's personal information.

On the Diebold FTP site: Private info on 310,000 Texans

During the writing of this chapter, I tried to take a more complete inventory of what was on that site and was surprised to find personal information for 310,000 Texans.

Identity thieves can work anonymously from anywhere in the world and, armed with your Social Security number and a few other details, can quite literally ruin your life. And all they need is your name, address and birthday to get your Social Security number. [18]

In this file were birthdays. First, middle and last names. Street addresses. Apartment numbers. School districts. Political affiliations. Voting habits. I assume they will say it was some kind of voter registration file, but it sure has a lot of information. Each kind of information (name, zip code, etc.) is called a “field,” and this file had 167 fields, which included data from about three dozen elections, logged in over several years by many different people. Ninety-five thousand people from Plano are in this file, and a couple hundred thousand more from Richardson, McKinney, Wylie, Dallas and surrounding areas.

People have a right to privacy, even in the Internet age. Any woman who has an abusive ex-boyfriend will tell you that she doesn't want her apartment number published on a Web site. Child custody cases can get nasty. Thieves who find a database like the one left in the open by Diebold may try to sell the information.

Because of this file I know that Bob L. of Plano is a Republican and likes to do absentee voting, and that he and his wife are the same age. But does Bob know that Diebold hung his undies out the window for all to see?

Someone will explain to me that you can buy voter registration files for a nominal fee. But that doesn’t mean you can buy those lists and stick them on the Internet, and what was Diebold doing with this information anyway?

I wondered if any reporters had their personal information posted. Yep — two reporters for the *Dallas Morning News*, the publisher for the *Plano Star-Courier* and the managing editor of the *Herald & Times Newspapers*.

And does Bob Urosevich, the president of Diebold Election Systems, know that his wife and daughter had their private information on that FTP site?

What do Diebold and the other guardians of our vote have to say about this?

> "We protect the Bill of Rights, the Constitution and the Declaration of Independence. We protect the Hope Diamond. Now, we protect the most sacred treasure we have, our secret ballot."[19]
>
> — Diebold CEO Wally O'Dell

> "Sometimes our customers use the FTP site to transfer their own files. It has been up quite some years. People go there from counties, cities, sometimes there is stuff there for state certification boards, federal certification, a lot of test material gets passed around."[20]
>
> — Guy Lancaster
> Diebold contractor

> "...the current group of computer 'wizards' who are so shrilly attacking ... are no longer behaving like constructive critics but rather as irresponsible alarmists and it's getting a little old."
>
> — Dan Burk
> Registrar of Voters
> Washoe County, NV
> (from Diebold web site)

> "They're talking about what they could do if they had access to the [computer program] code...But they're not going to get access to that code. Even if they did, we'd detect it." [21]
>
> — Dr. Britain Williams

"For 144 years, Diebold has been synonymous with security, and we take security very seriously in all of our products and services."

— Diebold Web site

"It is all fine and well to upload results over the Internet, but we don't exactly have a lot of experience in Internet security in this company, and government computers are crackers favorite targets."

Barry Herron
Diebold Regional Manager
Diebold internal E-mail - 2/3/99

Joe Richardson, official spokesman for Diebold, in response to a question from the author: "Our ongoing investigation has found no merit to the insinuations of security breaches in our election solutions."

Harris: "So if there were 20,000 files including hardware, software specs, testing protocols, source code, you do not feel that is a security breach?"

Richardson [shuffling papers]: "Our ongoing investigation has found no merit to the insinuations of security breaches in our election solutions." [22]

"The scientists are undermining people's confidence in democracy. None of the critics is giving any credence to the extensive system of checks and balances that we employ internally."

Mischelle Townsend
Registrar of Voters
Riverside County, CA
Associated Press 8/17/03

Townsend's county uses Sequoia machines. She made this statement in August 2003; in September, Sequoia's secret voting software was found on an unprotected Web site. It had been sitting there for a year and a half.