Chapter 4
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris

with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar

4
Can These Things Be Rigged?

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

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

The Fine Old Tradition of Vote-Rigging[1]

How to rig paper ballots

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

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

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

How to rig the Australian Paper Ballot system:

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

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

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

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

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

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

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

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

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

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

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

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

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

Rigging the lever machines

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

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

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

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

Rigging Punch Cards

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

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

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

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

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

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

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

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

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

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

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

Who might want to tamper with elections?

Political candidates:

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

True believers:

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

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

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

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

Gambling interests:

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

Hackers:

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

Dan Spillane, a test engineer for touch-screen machines at VoteHere, told me that in 2001, one of the software engineers working on voting machine software for his company hacked the code to make the touch screen register one vote, while inside the machine, the ballot image and tabulator recorded the opposite. "Look what I can do!" the engineer announced. And herein lies the problem: Programmers who like to hack also like to talk about it, which can make them a target for bribery or extortion.

Profiteers:

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

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

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

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

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

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

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

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

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

How would you find someone to bribe?

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

I know. I did this.

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

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

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

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

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

How would you choose someone to approach?

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

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

• What tampering methods are most likely?

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

Tampering opportunities unique to Internet voting

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

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

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

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

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

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

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

Tampering opportunities unique to optical-scan machines

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

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

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

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

Tampering with computerized voting systems

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

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

A total of 453 technologists have endorsed the *Resolution on Electronic Voting* so far, and no comparable group of computer scientists — in fact, no technology group at all — has embraced the opposite side.

Resolution on Electronic Voting

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

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

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

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

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

David L. Dill
Professor of Computer Science
Stanford University

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

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

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

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

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

Lack of Trust: A Dangerous Thing

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

A sampling of opinions from online forums...

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

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

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

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

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

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

"They've created this whole UFO effect," said Jesse Durazo,[10] a registrar of voters for the county who is not versed in computer science. He was not persuaded by 453 of the nation's top computer scientists, choosing instead to follow advice from voting-machine vendors (who make millions with every sale) and NASS (which is sponsored by voting-machine company money).

"They've created this whole UFO effect," said a registrar of voters who is not versed in computer science. He was not persuaded by 453 of the nation's top computer scientists, choosing instead to follow advice from voting-machine vendors ..."

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

Rigging elections through "back doors"

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

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

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

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

10 Approaches to tampering with a voting machine

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

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

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

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

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

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

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

nonpartiskan
FreeRepublic.com

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

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

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

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

BlackCopterControl
slashdot.com

"Guard with jealous attention the public liberty. Suspect every one who approaches that jewel.
— Patrick Henry
June 5, 1778

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

No, no, don't stop me now…

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

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

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

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

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

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

LiberalProgressiveDemInTexas
DemocraticUnderground.com

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

bimbo
FreeRepublic.com

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

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

alizard.
slashdot.com

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

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

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

15. Compromise the binary code, below the level of the source code, which will not be detectable even with a line-by-line examination of the source code and won't be solved by using a digital signature.
16. Make your ROM eraseable; The firmware is supposed to be sealed into a non-eraseable ROM, but some voting machines can "flash" the ROM when you boot them up with an updated card, and this means the ROM is rewriteable.
17. Accidentally put a few bugs in the software. Software engineering is like writing music or creating a painting. It is inspired, sometimes in the middle of the night, and in the wee hours things slip past the best of them. Sometimes engineers just don't catch bugs in the code. Or perhaps, a programmer plays with bugs for a hobby…

Bugs in the Code

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

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

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

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

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

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

Found on Internet voting source code, called votation

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

Found these comments in Diebold source code files:

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

Fix problem with race stats results not being sent correctly.

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

Revert improvement in detection of invalid smart cards

Fixed minor bug when internal keyboard did not work properly.

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

Fix problem with transfer sending wrong precinct id

Fix problem with not closing election after setting for election.

Fixed problem that caused an error when view ballot results.

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

Fixed problem in PollBook for Closed Primary Elections.

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

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

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

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

Fix bug uploading candidate totals

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

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

Fixed bug that did not accumulate write-in votes.

Handle failure of some files during upload.

Fix bug in validating ResultFile

Ballot station remembers opened election (again)

Truly fixed the bug in LanSelView

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

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

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

Chapter 4 footnotes

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

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

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

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

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

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

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

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

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

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

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

12 – Bartcop.com, by "Barney Gumble."

13 – slashdot.com, by Effugas

14 – slashdot.com, by "ccmay"

15 – DemocraticUnderground.com, by "BurtWorm"

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