

Hack the Vote: How to Steal a Presidential Election

11/10/2004

Chuck Herrin, CISSP, CISA, MCSE, CEH

<http://www.chuckherrin.com>

Author's Note – Before we begin, I'd like to say that it has been amazing to see how different initial reactions have been to this information. When I showed people drafts of this document, their response depended almost 100% on their party affiliation. If they are Democratic or Independent, they express shock, sorrow, and resignation that our country is out of control. If Republican, they immediately assume that I'm a liberal Democrat expressing "sour grapes" since the election "obviously didn't go my way", even though I am, in fact, a Southern White Republican. Since this information may stir the same feelings in you as you read this as a result of your personal political ideology, I would like to get something out of the way up front:

For the purposes of this document, who won the recent election is irrelevant.

Let me say that again – the winning and losing candidates and parties are irrelevant to the issue that I am trying to bring to your attention. What IS relevant is that there is mounting evidence that the election did not reflect the will of the people, and this document will demonstrate how poor design, planning, implementation, execution, monitoring, and auditing may have result in widespread fraud being perpetrated against the American public. We all know that this was the most heavily contested election in recent memory, with the country deeply divided and over \$1 Billion spent on trying to gain or maintain power of our country, the most powerful nation the world has ever known. Given the stakes, I feel that dismissing this information as a "conspiracy theory" or "sour grapes" is a mistake. If your candidate wins an election through fraud, does the end justify the means? If your candidate loses, and there is evidence that the election was stolen rather than won, can you really put that behind you and support the winner? Is this the way a Democracy works?

I am going to show you, step by step and with screenshots, how a theoretical attack against our election system could very easily steal a Statewide or even a National election. This attack would be easy to carry out, difficult to detect, and exert enormous influence on the results, leaving the humble voter coldly left out of the decision-making process.

First, a few facts before we get started:

- 1) Tens of millions of American citizens voted on touch screen terminals in the 2004 election, even though **EVERY** information security expert ever engaged to

review the security of electronic voting systems has given them failing grades, calling the security lapses “Stunning”, “blinding”, and “horrifying”. However, I feel that it is unlikely that these individual touch screen machines would be targeted. At greater risk than the individual touch screens are the Central Voting Tabulation computers, which compile the results from many other systems, such as touch screens and optically scanned cards. From a hacker’s standpoint, there are a couple of reasons why these central computers are better targets:

- a. It is extremely labor intensive to compromise a large number of systems, and the chance of failure or being detected increases every time an attack is attempted. Also, the controversy surrounding the touch screen terminals ensures that their results will be closely watched, and this theory has been born out in recent days.
- b. If one were to compromise the individual terminals, they would only be able to influence a few hundred to maybe a couple of thousand votes. These factors create a very poor risk/reward ratio, which is a key factor in determining which systems it makes sense to attack.
- c. On the other hand, the Central Vote Tabulation systems are a very inviting target – by simply compromising one Windows desktop, you could potentially influence tens or hundreds of thousands of votes, with only one attack to execute and only one attack to erase your tracks after. This makes for an extremely attractive target, particularly when one realizes that by compromising these machines you can affect the votes that people cast not only by the new touch screen systems, but also voters using **traditional** methods, such as optical scanning systems since the tallies from all of these systems are brought together for Centralized Tabulation. This further helps an attacker stay under the radar and avoid detection, since scrutiny will not be as focused on the older systems, even though the vote data is still very much at risk since it is all brought together at a few critical points. This also has been born out by early investigations, where the touch screen results seem to be fairly in line with expectations, while some very strange results are being reported in precincts still using some of the older methods.

This is not to say that the touch screens don’t have their problems, which are well documented on the web and the news. My point here is that if you want to steal an election, targeting the individual touch screen machines is not the easiest way to do it.

- 2) Three companies manufacture the vast majority of the electronic voting systems in the US. The big 2, Diebold and ES&S, control 80% of the market. These companies have been very secretive about their systems, and have repeatedly refused to allow their security to be tested. Fortunately (?), they left a wide open FTP server on the web, and Hackers and other curious parties were able to download a great deal of their software to experiment on. Hackers, both amateur and pro, have had these packages available for some time to practice their Hacking techniques on. This familiarity is key to quickly exploiting the design

flaws and covering your tracks, as I will show using detailed screenshots and steps later in this document.

- 3) In 2003, the President of Diebold wrote a letter pledging his commitment "to helping Ohio deliver its electoral votes to the President." His brother is president of ES&S, the #2 company in the marketplace. Diebold's CEO is a Republican Pioneer, meaning that he has raised over \$100,000 for the GOP. It's actually well over \$100,000, and is quite clear that the leaders of these companies are very partisan. While this does not indicate wrongdoing, it is troubling for anyone with so much potential influence over our votes to express strong partisan feelings one way or the other. We want them to count our votes impartially, not help their side win. (<http://www.onlinejournal.com/evoting/042804Landes/042804landes.html>)

- 4) Exit polls and other indicators predicting election results have traditionally never been THAT wrong. Karen Hughes sat the President down and told him that he had lost the race around 10:30 pm, based on the exit poll data, which is generally accurate. So many bellwethers were wrong that night, from approval rating forecasts to traditional expectations that high turnout favors the challenger that there is still wide speculation as to how all of these usually reliable indicators were so consistently wrong. Everyone agrees that something strange happened election night – some claim that the exit polls were sabotaged, but I think of the 2 options for foul play, the exit polls or the vote, it was the actual vote that was sabotaged. Fox's conservative Dick Morris, in an article for The Hill, (<http://www.thehill.com/morris/110404.aspx>), says that he suspects foul play and that the exit polls were altered in a massive conspiracy to keep voters on the west coast home. I tend to agree that either the exit polls or the vote counts were wrong, but I think it would be much easier and more beneficial to any conspirator to interfere with the actual vote tally than to conspire with a large, geographically diverse group of pollsters to try and sway voters on the west coast to stay home and not vote for Bush (where all three states were expected to go to Kerry anyway). In fact, there is growing evidence that the central vote tabulation machines were manipulated, either from the inside or the outside, and our votes did not count. **For example, in one county in Ohio, vote tallies give Bush 4,258 votes in a precinct where only 638 ballots were cast.** (<http://www.cnn.com/2004/ALLPOLITICS/11/05/voting.problems.ap/>) The FBI is currently investigating another instance at the behest of a Congressional candidate, and the State of NC may have to have another statewide election as a result of e-voting malfunctions (4500 votes completely disappeared in one instance in Cartaret County – see <http://www.charlotte.com/mld/charlotte/10133265.htm?1c>). Many more examples are continually being reported on the web. Blackboxvoting.org is currently organizing a massive Freedom of Information Act request to try to find out what happened, but as I will show you in a few pages, this may not tell us much, since it is as easy to erase your tracks as it is to change votes. Please see www.blackboxvoting.org, <http://www.commondreams.org/views04/1106-30.htm>, and www.votergate.tv for more details, and watch the 30 minute movie

from the Votergate.tv site. I will post more links at the end of this document, and I'm sure that by the time you read this, much more information will be on the web. Please check Google or your favorite search engine for more up-to-date information than this document can provide.

- 5) As an Information Security professional, for years I have been telling everyone who would listen (and plenty who wouldn't), from Senators to family members to friends and coworkers that electronic voting completely undermines the reliability and accountability of our Electoral Process, and that someday a National Election would be stolen as a result. My family and friends can attest to this, and I am by no means alone in my opinion among security professionals. Anyone with a basic knowledge of computer security will attest that a Windows machine, complete with hanging modems and closed-source software, is not a secure platform to be trusted with anything sensitive or important, let alone something as critical as our votes.
- 6) On the following pages are screenshots and commentary as I walk you through exactly how to steal an election from a Central Vote Tabulation Computer running Diebold's GEMS software. These machines used for this vote tabulation are just regular PCs running standard versions of Microsoft Windows, and are usually connected by modem to upload results. Often, these modems are left plugged in and may be available to dial into remotely, and I have heard reports of these machines being connected to the Internet to allow queries to be run to check results using a Java client called Jresult (included in the GEMS application from Diebold). For those of you not versed in Information Security, the average time for an unprotected Windows-based PC to be compromised after being connected to the Internet is between 20-40 minutes. As I am fond of saying, hacking a default Windows machine is like hunting a dairy cow with a rifle and scope, and unfortunately, this is where our votes are stored and counted. Well, in theory, they are counted. More on that later.
- 7) This demonstration is being performed using Microsoft Windows 2000, Diebold's GEMS software version 1.18.15.0 and Microsoft Access 2000. Nothing else. I obtained the GEMS software and the sample voter database (coloradospringscityelection.mdb) from www.blackboxvoting.org. I encourage anyone curious to download these utilities and try this yourself – these step by step instructions will serve to show that only moderate skill is needed to pull off an attack of this type and potentially cost the American public tens or hundreds of thousand of votes.

****Important** - I would like to stress that this demonstration was performed locally on a system totally under my control, and no unauthorized access to any computer system occurred. The voting database used was the sample obtained from www.blackboxvoting.org, and this election does not reflect data for**

any election currently taking place. I want to be very clear that this is only a proof-of-concept demonstration, and at no time was actual voter fraud committed in order to prove a point. THIS IS A DEMONSTRATION ONLY, very similar to the well-documented demonstration Bev Harris performed for Governor Howard Dean recently on National television. Also, GEMS software is a trademark of Diebold, and Windows and Access are both copyrights of Microsoft, Inc.**

With all that out of the way – OK! Let’s get started!

Step One: The Before Picture.

This is the summary report run based on our sample election from Colorado Springs, CO. This is what the actual, official results looked like before I decided to cast “my vote”.

Election Summary Report		Date:11/09/04
City of Colorado Springs		Time:23:59:07
Official Election		Page:1 of 2
Summary For Jurisdiction Wide, All Counters, All Races		
Registered Voters 222605 - Cards Cast 50950 22.89%		Num. Report Precinct 266 - Num. Reporting 266 100.00%
District 1		
	Total	
Number of Precincts	78	
Precincts Reporting	78	100.0 %
Times Counted	16386/61577	26.6 %
Total Votes	11663	
Jim Null	11663	100.00%
District 2		
	Total	
Number of Precincts	60	
Precincts Reporting	60	100.0 %
Times Counted	12918/61152	21.1 %
Total Votes	11301	
Leon Kirk	2374	21.01%
Kevin Butcher	4251	37.62%
Charles E. Wingate	4676	41.38%
District 3		
	Total	
Number of Precincts	69	
Precincts Reporting	69	100.0 %
Times Counted	13026/54717	23.8 %
Total Votes	12500	
Linda Barley	4209	33.67%
Sallie Clark	8291	66.33%

Figure 1: Election summary report – before.

Pay attention to **District 3**. Here we have Sallie Clark in District 3 winning by a 2/3 majority. But let’s say that for this scenario, Sallie’s daughter is my ex, or she supports gay marriage, or maybe she’s against deficit spending. Whatever – let’s say maybe she’s a Pinko Commie and must be stopped, so let’s have some fun.....

Note – I do not actually know Sallie Clark or any of these election participants, and therefore cannot speak to her character. Again, this is just a demonstration.

Since in this example I'm a Hacker, I may or may not have a copy of the GEMS software. Actually, I probably do, since everybody who wants one can find it, but to their credit, the GEMS software isn't really that insecure. It's a good thing there are a bunch of backdoors and other ways in....

Step 2: Getting in.

The biggest part of step two is getting into the Windows PC in question, either locally or over a network. As anyone confronted with the continuing barrage of viruses, worm, and Hackers can attest, this is not really a problem. In fact, let's run through a few sample ways in, just off the top of my head:

- 1) Wander into the building, and quietly put a wireless access point on the same network segment as the Tabulation PC, maybe behind a copier somewhere, and then casually come in from across the street using a laptop and wireless card.
- 2) Find the telephone number of the office the PC is located in, and use a "war-dialing" program such as ToneLoc to dial all of the numbers in that exchange looking for a hanging modem. This technique was made famous by the 1983 movie "Wargames" and it still works today. These machines typically have hanging modems installed, so this should be a fairly easy way in.
- 3) If you're an insider, you already have the phone numbers and any usernames and passwords you may need. Dial into the machine, authenticate normally, and then manipulate the data as explained below.
- 4) Come in through the Internet. It is reported that many of these machines are connected to the Internet to enable results to be queried using Jresult to pull data from the central PCs. Windows PCs on the Internet are inherently vulnerable, particularly if they're not behind a firewall. Since a firewall would prevent the legitimate Jresult queries from being made, these machines are likely at extreme risk for being compromised through their Internet connection.
- 5) Again, if you're an insider - walk up to the machine and use the keyboard and mouse. Most poll workers, despite being good, caring people, tend to be political enough to motivate them to volunteer. It's just human nature to use the tools at your disposal to your advantage, and people have a remarkable knack for justifying even the worst acts if they can convince themselves that the cause is worthwhile.

With a little time and creativity, dozens more ways in are possible. You have probably already thought of a couple more, haven't you? As a note for non-technical folks - did you know that in Windows, C: drives are shared out by default? No? Well, they are. But there's a super-secret Hacker trick to connect to them. You have to call it C\$ instead

of just C. The \$ means it's a "hidden" drive, but it is still accessible via the network. In the screenshots in step two, once network access is gained, we simply browse to the C: drive of the server and go to the C:\program files\GEMS\localDB directory. Here we will find an Access database for each election named <NameOfElection>.mdb. With a copy of Microsoft Access, we open it and find that no, it is not even password protected. The directory it's in isn't protected or restricted in any way. The data is not encrypted or even encoded. It is as open as an email message, and this is where all of our voting data is stored. From here, you could add candidates, drop them from the ballots, or delete entire precincts, but all of that is too obvious. A very simple trick would be to switch candidate IDs (see Figure 3 to see what candidate IDs look like), which would cause the vote tallies to simply reverse. This would be unlikely to raise much suspicion, since the total number of votes cast and turnout numbers would not change. Since Hacking rule #1 is to not get caught, rather than add a candidate or do something wild, we'll be "subtle" and just change the results.

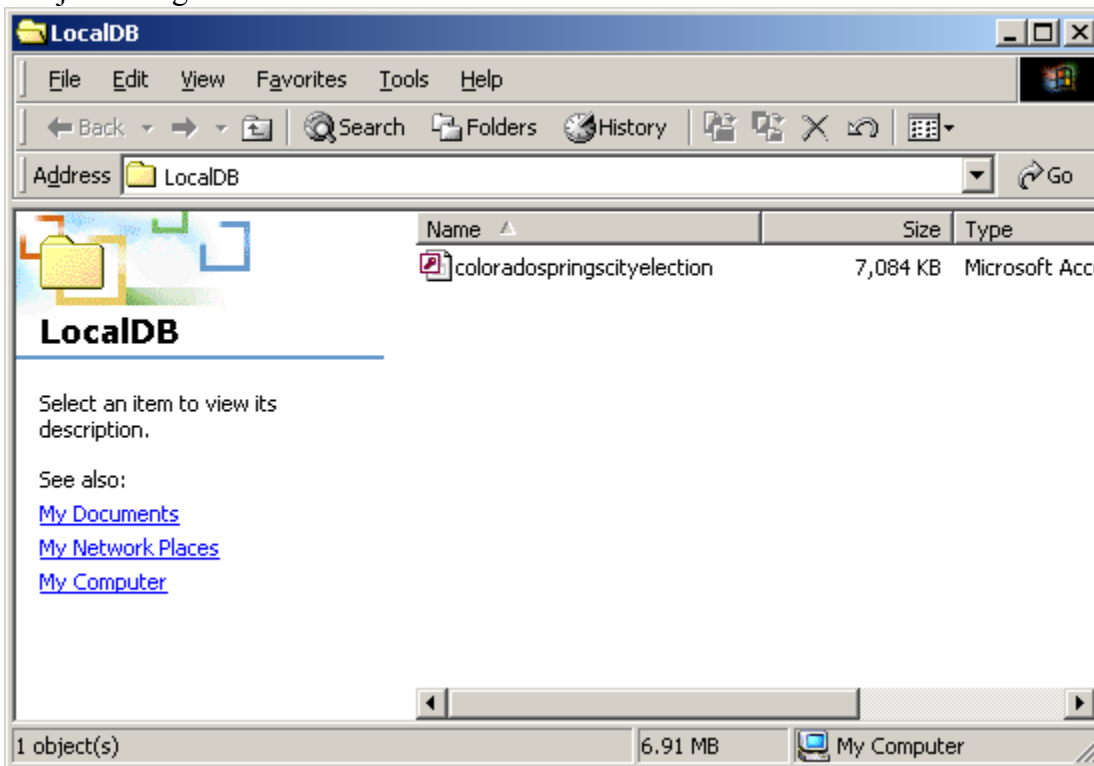


Figure 2: The c:\program files\GEMS\localDB folder where all of our valuable data is stored.

This is the Access database that is the back end for the entire system. Potentially hundreds of thousands of votes could be stored here on a central computer with no access control, no passwords, etc. When we open the database and view the Candidate table inside, we see:

KeyId	Label	RaceId	CandidateType	SortSeq	NumCandVGrou	ExportId
500	YES		0	10		
501	NO		0	20		
502	YES		0	10		
503	NO		0	20		
538	YES		0	10		
539	NO		0	20		
540	YES		0	10		
541	NO		0	20		
543	Candidate 70		0	70		
545	Jim Null		0	20		
546	Kevin Butcher		0	20		
547	Leon Kirk		0	10		
548	Keith Monschke		0	30		
549	Charles E. Wing		0	40		
550	Linda Barley		0	10		
551	Sallie Clark		0	20		
552	Kendell Kretzsc		0	10		
553	Margaret Radfor		0	30		
554	Luis "Joe" Yban		0	20		
555	Tom Gallagher		0	30		
556	Judy Noyes		0	10		
557	Tim Pleasant		0	20		

Figure 3: The Candidate table

Ah ha! Sallie’s opponent, Linda Barley, was assigned 550 as a candidate number, and Sallie is candidate number 551.

From another table in the same database, we see that the Race ID is 221 (CandVGroup Table), meaning that their Key IDs are 541(Linda) and 542 (Sallie). Remember that the original vote results were 4209 to 8291, Linda to Sallie.

Step 3: Changing the Votes

I located the ID, #541 in the CandidateCounter table and simply by clicking on the cell and typing with my number keys, I gave Linda 111 votes for every reporting unit. There were 71 reporting units, so she should have 7881 votes now, an increase of over 3600 votes. I finally found a way to make my vote count! We’ll come back and check the math later to make sure there are no surprises.

CounterBatchId	ReportUnitId	CounterGroupId	CandVGroupId	TotalVotes
19	1073741892	0	541	111
126	1073741913	0	541	111
45	1073741921	0	541	111
358	1073741923	0	541	111
151	1073741945	0	541	111
76	1073741946	0	541	111
136	1073741948	0	541	111
729	1073741950	0	541	111
551	1073741951	0	541	111
25	1073741953	0	541	111
17	1073741957	0	541	111
17	1073741958	0	541	111
147	1073741966	0	541	111
358	1073741967	0	541	111
109	1073741986	0	541	111
28	1073742004	0	541	111
126	1073742012	0	541	111
16	1073742022	0	541	111
109	1073742027	0	541	111
27	1073742043	0	541	111
45	1073742056	0	541	111
110	1073742072	0	541	111
129	1073742081	0	541	111
60	1073742096	0	541	111
78	1073742099	0	541	111
109	1073742100	0	541	111
27	1073742101	0	541	111
3	1073742130	0	541	111
27	1073742135	0	541	111
110	1073742141	0	541	111
123	1073742170	0	541	111
1281	1073742816	14	541	111
1170	1073742816	15	541	111
1285	1073742816	15	541	111

Figure 4: Changing the votes inside the CandidateCounter table. This is repeated in the CandidateSummary table, since some records are cross-linked, and I want to know exactly how many votes I'm changing.

Once I was done adding 3672 votes to Linda's tally, I blanked all of Sallie's votes, making her total 0. Hopefully she was so over-confident that she didn't bother to vote ;-). A real attacker would likely be more subtle to avoid suspicion, but again, this is a demonstration. Unfortunately, since many of the new machines do not produce a paper ballot, a manual recount would be very difficult, if not altogether impossible. This is a clear violation of many state election laws, but elections officials put them in place anyway. I wouldn't withdraw \$20 from an ATM without a receipt, but I guess my vote isn't worth that much trouble.

Anyway, now that our results are changed, we save the database, and viola!

Step 4: Run the new summary report and declare my candidate the winner!

Election Summary Report				Date:11/10/04
City of Colorado Springs				Time:00:43:08
Official Election				Page:1 of 2
Summary For Jurisdiction Wide, All Counters, All Races				
Registered Voters 222605 - Cards Cast 50950		22.89%	Num. Report Precinct 266 - Num. Reporting 266 100.00%	
District 1				
			Total	
Number of Precincts			78	
Precincts Reporting			78	100.0 %
Times Counted			16386/61577	26.6 %
Total Votes			11663	
Jim Null			11663	100.00%
District 2				
			Total	
Number of Precincts			60	
Precincts Reporting			60	100.0 %
Times Counted			12918/61152	21.1 %
Total Votes			11301	
Leon Kirk			2374	21.01%
Kevin Butcher			4251	37.62%
Charles E. Wingate			4676	41.38%
District 3				
			Total	
Number of Precincts			69	
Precincts Reporting			69	100.0 %
Times Counted			13026/54717	23.8 %
Total Votes			7881	
Linda Barley			7881	100.00%
Sallie Clark			0	0.00%

Figure 5: The new summary report with the results the way I wanted them.

Note the final numbers for **District 3 – 7881 to 0**. **Just as I expected, I was able to override the wishes of 11,963 voters and replace their ballots with my own.**

My candidate wins in a landslide, although the voters actually voted 2-to-1 for her opponent. This took me about 5 minutes and a moderate exercise of skill. There were no passwords to crack, and all I had to do was figure out the way things were stored in an unprotected, clear text Access database, which fortunately, has been available on the web for quite some time for Hacker-types to practice on. In fact, with the widespread availability of the GEMS software, you can go in and create your own elections to practice on before ever venturing out to touch the real thing.

Now that my work here is done, all that remains is clearing up the audit trail. Diebold insists that this cannot be done, but this has repeatedly been shown to be false. In fact, in a memo by Diebold principal engineer Ken Clark in 2001, he says **“Being able to end-run the database has admittedly got people out of a bind though. Jane (I think it was Jane) did some fancy footwork on the .mdb file in Gaston recently. I know our dealers do it. King County is famous for it. That's why we've never put a password on the file before.”** (<http://www.blackboxvoting.org/Oct2001msg00122.html>)

In a particularly humorous and distressing response to Diebold's assertion that "Generated entries on the audit log cannot be terminated or interfered with by program control or by human intervention", the folks at www.blackboxvoting.org actually trained a chimpanzee to delete the audit logs from an election database. You read that right – a chimp. Well, since it wasn't a human or computer, I guess they're technically correct. Here's a link. <http://blackboxvoting.org/baxter/baxterVPR.mov>

Another audit log incident occurred during the Washington State primary **just six weeks ago**. Two interesting events took place here:

1) all entries are absent from the audit log between 9:52 pm and 1:31 am. This includes records of summary reports being printed during that time frame, which is something that is always logged by the system, and shows up when they are printed before and after that block of time. Here is the audit log: <http://www.blackboxvoting.org/auditlog.PDF>

2) Here are copies of the 5 sets of summary reports printed off during that missing time period, complete with timestamps showing that they were printed during that block of time and signed by the elections chief, Dean Logan. <http://www.blackboxvoting.org/resultspages.PDF>

Anyone with knowledge of Information Security can tell you what it means when you are missing audit logs for a specific block of time, and known events took place that should be reflected in the logs.

It means you were Hacked.

Conclusions:

I don't pretend to know the full extent of what's happening here, so please, draw your own conclusions. I personally have no hard evidence that voter fraud was perpetrated in the recent election, but I do know that it was not only possible, but apparently very easy, potentially undetectable, and highly rewarding for the perpetrator(s).

We all know that this last race was extremely close and extremely hard fought. The country is still bitterly divided over it. Over \$1.2 Billion was spent trying to get the candidates elected. In such a tight race, which was repeatedly referred to as "**The Most Important Election in Recent History**", would you trust an election process where you went behind a curtain and whispered through a hole in the wall to tell a stranger who you wanted to vote for, then left without a receipt, trusting that the invisible stranger would do the right thing and pass your vote along? With electronic voting using these insecure and untrustworthy systems, that's almost exactly what's taking place. Worse, there is no reliable audit trail or accountability in the event that impropriety does take place.

Knowing what you know now, do you trust the results? Do you think your vote counted? Fellow Republicans – this time, the election went in our favor. Does that make this a non-issue, where the ends justify the means? What about next time, when your candidate

doesn't win? Knowing these vulnerabilities exist, if Hillary Clinton is elected in 2008, will you trust that the results are dependable? Is this the democracy we are exporting to the rest of the world?

Was the will of the people done? Were our voices heard? I don't know, but I'd really like to find out. Unfortunately, Bev Harris, who has been working tirelessly to raise awareness of this issue, was recently told by 2 different news producers that they had been prohibited from covering the issue and would **not** run stories about it. Many Republicans are quickly dismissing these questions, calling the results "sour grapes" and "liberal whining". This is incredibly short-sighted and stupid, particularly coming from a party in which we pride ourselves on being "Values Voters" who are known for doing the right thing. Remember, **we are Americans first, Republicans and Democrats (or independents) second**. This is not a partisan issue; this is an issue of who controls our country!

Here are more links for your reference:

<http://www.blackboxvoting.org>
<http://www.blackboxvoting.com>
http://ustogether.org/Florida_Election.htm
<http://ustogether.org/election04/FloridaDataStats.htm>
<http://www.rubberbug.com/temp/Florida2004chart.htm>
http://ustogether.org/election04/PA_vote_patt.htm
<http://www.thehill.com/morris/110404.aspx>
<http://www.blackboxvoting.org/>
<http://www.votergate.tv/>
<http://www.thomhartmann.com/>

Please help get the word out so maybe we can fix this stupid, stupid system and get our country back on track. If our voices are heard, if our officials and our newspapers, our radio and TV stations hear from us, we can get to the bottom of this and fix these issues so our votes will once again matter and power can be returned to us, the American people. Please, don't assume someone else will do it for you – just take a minute and send a note to your Senator, your local paper, or anyone who loves our democracy and wants to safeguard the basic principles our great country was founded upon – a Government founded **of the people, for the people, and by the people**.

Thanks for your time and attention, and God Bless America. You are free to distribute this document in its entirety to help get the word out, and I thank you for your assistance in doing so.

Chuck Herrin, CISSP, CISA, MCSE, CEH
CISSP – Certified Information Systems Security Professional
CISA – Certified Information Systems Auditor
MCSE – Microsoft Certified Systems Engineer
CEH – Certified Ethical Hacker
www.chuckherrin.com