Even a Remote Chance?

by Pokey Anderson

July 2006

Imagine sitting in your favorite easy chair with a remote control, and being able to just push EJECT and get George Bush out of office. Or, let's say you're on your laptop, and you can dial up a regime change.

"Hmm," you say, "I'm feeling like blue today. Blue is a nice color. I think I'd rather have Kerry for president." Let's say you're up late, it's November 2nd, you see that Kerry is losing in Ohio, and you say, "the HELL with that!" So, with your laptop, you dial into the tabulator for, let's just say, 41 of 88 counties in Ohio. And, you switch 14 votes per precinct from Bush to Kerry. Voila. Kerry wins.

Could that happen?

Or, um, the other way around—Kerry is winning, and someone dials in and changes a dozen or so votes in each of roughly half the precincts in Ohio, and VOILA, Bush wins Ohio. (A flip of a dozen votes in 5,000 precincts would result in a net change of 120,000 votes in Ohio, more than the tallied margin that separated the two candidates.)

Remote control of elections? Science fiction, right? Start playing the Twilight Zone music? Not exactly.

DIEBOLD—Hack Testers Waltz In

Let's look at a test that was done for the State of Maryland on the Diebold electronic voting equipment. The testers used actual Diebold election equipment and, after a week's study, attempted to hack and manipulate it. The newspaper report said they were nearly "giddy" with their success.[1]

---

[1] "Md. computer testers cast a vote: Election boxes easy to mess with," by Stephanie Desmon, January 30, 2004, Sun, http://www.sunspot.net/news/local/balte.md.machine30jan30,0,4050694.story?coll=bal-local-headlines.

"One guy picked the locks protecting the internal printers and memory cards. Another figured out how to vote more than once—and get away with it. Still another launched a dial-up attack, using his modem to slither through an electronic hole in the State Board of Elections software."

The team was able to remotely upload, download, and execute files with full system administrator privileges. Results could be modified at will, including changing votes from precincts.

"My guess is we've only scratched the surface," said Michael A. Wertheimer, who spent 21 years as a cryptologic mathematician and code breaker at the National Security Agency.

As a bonus, the team of test hackers from RABA Technologies was able to change votes and exit the system without a trace of their visit. Slick! Wertheimer said, "If you believe, as I do, that voting is one of our critical infrastructures, then you have to defend it like you do your power grid, your water supply."[2]

The State of Maryland head of elections read the testers' report and promptly issued a press release.[3,4]

I couldn't make this stuff up; here is what Linda Lamone said, "To this date, there has never been an election compromised. The findings in the SAIC and RABA reports both confirm the accuracy and security of Maryland's voting system and procedures as they exist today." And, Maryland bought the Diebold electronic voting machines.

DIEBOLD—A Dedicated Line

Not only is the software of major voting machine companies secret, but so are their contracts with

[2]"The Vexations Of Voting Machines," by Viveca Novak, Time, April 26, 2004, http://www.time.com/time/magazine/printout/0,8816,1101040503629410,00.html.

[3] "Trusted Agent Report: Diebold AccuVote-TS Voting System," Michael A. Wertheimer, January 20, 2004, RABA Technologies, http://www.raba.com/press/TA_Report_AccuVote.pdf.

[4] http://electionline.org/site/docs/pdf/MD.SBE.RABA.Response.01.29.04.pdf.

counties. A curious Diebold contract stipulation came to light, though, in a public hearing of the Voting Systems and Procedures Panel that advises the California Secretary of State.[5]

Panel member TONY MILLER read aloud a portion of Diebold's contract with Kern County:

> 'The vendor, Diebold, must provide one dedicated voice-grade line in the server room for exclusive use by DESI (Diebold Election Systems Inc.) as a modem support line directly connected to server. Line must be a number that does not go through a switchboard so that after-hours work can be conducted whenever necessary.'
>
> TONY MILLER: "It sounds pretty scary from a lay person's point of view. ...It sounds like you're giving the keys to the kingdom to a vendor, which even though you're not doing it, you say right now —"
>
> ANN BARNETT (Auditor-Controller-County Clerk of Kern County, CA.): "That would only be true if we were to hook it up, and we have not."

So, a dedicated line between Diebold and the county's election system that would be connected 24 hours a day? This gives new meaning to Diebold's company motto, "We Won't Rest."

Earlier, Miller had asked Bob Urosevich, then president of Diebold Election Systems, about the contract provision, called Rider O.

> TONY MILLER: Would that be a customary provision in your contracts?
> BOB UROSEVICH: I'm not—I don't understand the question, I guess. ...I apologize, I guess, for the delay. I guess I can't answer the question, because I have no knowledge of it.

While Diebold is one of the largest voting machine companies in the nation, it only counted votes in two of Ohio's counties for the November 2004 election. Most Ohio counties were counted by ES&S or Triad.

---

[5] California Voting Systems and Procedures Panel, http://www.ss.ca.gov/elections/vsptranscript0421.pdf, April 21, 2004, p. 68 and p. 106

But, before we take a closer look at Triad, let's take a look at a different company that brags about its wireless capabilities.

Advanced Voting Solutions (AVS)—So Proud of our Wireless Touchscreens, It's in the Name

One voting machine company has installed wireless local area network (LAN) in its computers and uses that as a selling point. It even put "wireless" in the name of its touchscreens.

Advanced Voting Solutions (AVS) sells touchscreen voting machines called WINvote™. The "WIN" means "Wireless Information Network," the company explains.

AVS is a small voting machine company in Texas. (See Endnote 2 for a look at its family tree.) One of the jurisdictions AVS has sold its touchscreens to is Fairfax County, Virginia, just across the Potomac from the nation's capital. The rollout in Fairfax for the November 2003 election was studded with problems. Faulty direct-recording electronic voting machines (DREs) were removed from precincts for repair on election day, then placed back in service. Despite persistent claims by proponents of touchscreen voting that computer elections count votes accurately, a subsequent test by the Fairfax board of elections showed that one candidate was losing one vote for every 100 votes cast.

Chris Craig, general counsel for the Fairfax County Republican Committee, told me:

> "I could probably give you a list as long as your arm of the problems. We've gotten anecdotal stories, many, many, very consistent. People trying to use the touchscreen machines, and either not getting their vote to appear, or in some cases, some very unusual cases, punching in one name and having their opponent's name appear. That's bizarre to me. There was difficulty throughout the county."[6]

Reports of onscreen vote-hopping (voter attempts to vote for one candidate but the screen shows a different one selected), as well as machine breakdowns, have plagued other brands of touchscreen voting equipment as well.

[6] Chris Craig, phone interview, November 19, 2003.

What is unusual about Advanced Voting Solutions' WINvote™ equipment is that they brag about their equipment's wireless capability. They cite the ease of one person programming over a thousand machines at a time. This is from the Web site of Fairfax County, educating voters about their new equipment:

> *Will the touchscreen machines save the taxpayers money?*
>
> Absolutely! ... Another huge saving will be hundreds of hours in labor costs. The wireless LAN used by the touchscreen machines enables the technicians to program 1,000+ machines simultaneously. There no longer will be the need to produce individual ballot faces, a process which took over 150 hours for the 2002 general election.[7]

And, what about security? No need to worry, they say. It's encrypted!

> "The wireless LAN complies with IEEE 802.11b standards for wireless systems and utilizes a 128-bit encryption Wired Equivalent Privacy (WEP) protocol which was thoroughly tested by the ITAs during the certification process. The wireless LAN is used to simplify the process of opening the polls on election morning and closing the machines and accumulating the results after the poll close. It is not used while ballots are being cast by voters."[8]

Let's ask a nationally-known expert on elections and computer security about the encrypted Wired Equivalent Privacy (WEP). Dr. Avi Rubin is a professor of computer science and technical director of the information security institute at Johns Hopkins University. He co-authored the first independent analysis of electronic voting software. He writes:

> **"There are tools on the Internet to break WEP in seconds. We were the first to do it when I was at AT&T. I think that as bad as some of the voting machines are in terms of security, having wireless capability is a total disaster. I can't think of a worse idea."**[9]

[7, 8] From the Web site of Fairfax County, Virginia, Voting Machine Replacement—Frequently Asked Questions, 6/26/2003, http://www.co.fairfax.va.us/eb/faq%5Fvotingmachine%5Frepl.pdf.

[9] Dr. Avi Rubin, Personal Correspondence, June 30, 2006.

AVS—You Can Change the Ballot on a Thousand Voting Machines, at the Last Minute

The AVS company Web site extols the virtues of its speed and convenience:

> "Last minute corrections or changes to a ballot can be made quickly and simply by regenerating and redownloading the edited database to multiple units through AVS exclusive Wireless Information Network (WIN)."[10]

Reassuring, isn't it? Over a thousand machines could be reprogrammed at once, at the "last minute," but not during the election. And the barrier for a malicious hacker would be what?

Who is checking those "last minute changes" anyway? In a vulnerability not at all limited to one vendor, programming for ballot positions could be switched, or partially siphoned off, so that Major Party A votes go to A, but Major Party B votes go to Third Party C in some precincts, or to A.

Or, what if a candidate's contest is simply left off the ballot in some precincts—that *would* tend to dampen their vote totals. (Senator Barbara Mikulski was completely left off the ballot in her 2004 primary contest for a fourth term for U.S. Senate, according to voter complaints in at least three Maryland counties. Maryland uses Diebold electronic voting.[11])

According to the nonpartisan group Voters Unite, faulty ballot definition programming can thwart accurate electronic vote tabulation of DREs *and* optical scanners. "Every voting system includes a key component, called the ballot definition file, which is never subjected to an outside review. Given that ballot definition files determine the way votes are recorded and counted, the lack of independent oversight of these files is a major security vulnerability." (Hypothetical? No. For a list of 51 elections marred by this problem, see Endnote 3.)

---

[10] Advanced Voting Solutions company Web site, as seen on June 8, 2006, http://www.advancedvoting.com/index.php?p=electionwarehouse.

[11] "The Vexations Of Voting Machines," By Viveca Novak, Time, April 26, 2004, http://www.time.com/time/magazine/printout/0,8816,1101040503-629410,00.html.

Advanced Voting Solutions wrote: "The WINvote™ system possesses features and functionality that will potentially revolutionize the Election Equipment and Solutions Industry."

But, are we revolutionizing elections for the convenience of election workers? Is convenience really the measure by which to judge elections, like getting a drive-through hamburger? Or have we just made hacking an entire jurisdiction really fast, easy, and nearly impossible to detect? And, even if the warehouse before and after the election has airtight security, and all election officials, vendor contractors, custodians, transporters, and other staff are 100 percent incorruptible, how do we know that the wireless capability is disabled during the election?

Do other vendors have invisible connectivity before, after, or during elections? Finding out is not as easy a task as it might seem. Dr. David Dill, professor of computer science at Stanford and founder of VerifiedVoting.org, told me that even somebody with good technical skills examining the inside of a voting machine might not discern wireless capability, especially if it was maliciously installed to avoid detection.[12]

Dr. Dill advised the Election Assistance Commission, a federal agency that advises on elections: "Wireless networking is unnecessary and inherently unsafe, and should be banned outright" for elections.[13]

The chair of the Election Assistance Commission (EAC) is not heeding Dill's recommendation, and seems unaware that AVS wireless voting equipment can *receive* transmissions. Chair Paul Degregorio defends voting systems, even wireless ones, as being secure. He said that the ones with wireless capabilities are able to transmit results but cannot receive transmissions, thus making them impervious to manipulation.[14]

---

[12] Phone call, June 23, 2006. See additionally Endnote 4 on Built-In Wireless Infrared Data Transfer Ports.

[13] Testimony before the Election Assistance Commission, Dr. David Dill, July 28, 2005 Hearing, California Institute of Technology, Pasadena, California, http://www.verifiedvotingfoundation.org/downloads/eactestimony.pdf.

[14] "Study: Fed 'Guidelines' Imperil E-Voting Security," by Michael Hickins, Internet News, June 28, 2006, http://www.internetnews.com/security/article.php/3616656.

After reviewing more than 120 potential threats to voting systems, one of the top recommendations of a 2006 Brennan Center report is to ban wireless components on voting machines.

> RECOMMENDATION #3:
> BAN WIRELESS COMPONENTS ON ALL VOTING MACHINES.
> Our analysis shows that machines with wireless components are particularly vulnerable to attack. We conclude that this vulnerability applies to all three voting systems (DREs, DREs with a voter verified paper audit trail, and precinct count optical scans). **Only two states, New York and Minnesota, ban wireless components on all machines.** California also bans wireless components, but only for DRE machines**. Wireless components should not be permitted on any voting machine.** [Brennan Center footnote: Two other states, West Virginia and Maine, ban networking of machines without banning wireless components themselves. Banning the use of wireless components (even when that involves disabling them), rather than requiring removal of these components, still leaves voting systems unnecessarily insecure. Among other reasons, a software attack program could be designed to re-activate any disabling of the wireless component.][15] (emphasis added)

However, even a 50-state ban of wireless components in elections could be problematic to verify, as technological innovation accelerates. Imagine a memory device about the size of a grain of rice or a freckle, with its own antenna built in, that could be embedded in a sheet of paper or stuck to any surface. Imagine that the device could contain 4 MB of memory which could be accessed or altered wirelessly by a nearby cell phone. Although it sounds like science fiction, this tiny wireless memory chip, called a Memory Spot, was announced July 17, 2006 by Hewlett Packard.

Whether or not this particular innovation leaps to the top of the election thief's shopping list, a sober assessment of the ability of groups that are disproportionately attorneys—state legislators, members of Congress and federal agencies like the EAC—to write laws, regulations, and procedures for elections that can comprehend and stay ahead of technological innovation and developments in computer security is not at all reassuring.

---

[15] "The Machinery of Democracy: Protecting Elections in an Electronic World," executive summary, Brennan Center for Justice at NYU School of Law, June 27, 2006, http://www.brennancenter.org/programs/downloads/Executive%20Summary.pdf.

HART INTERCIVIC and DIEBOLD—Your democracy is safe—under your bed!

In 2005 and 2006, computer experts Harri Hursti and Dr. Herbert Thompson demonstrated fatal security flaws in Florida and Utah in front of election officials. The equipment was actual Diebold optical scan and Diebold DRE voting systems. The device Hursti used to take control of a voting machine and change the results of a test election in Leon County, Florida, was not rocket science but farm science; it cost about $200, and is normally used to record moisture levels in corn. Despite the demonstrations, and the previous hack by RABA scientists, vendors insist that the concerns are theoretical, and it is election "procedures" that keep elections safe.

"It just isn't the piece of equipment," David Bear, a spokesperson for Diebold told the *Washington Post*. "It's all the elements of an election environment that make for a secure election."[16]

Winning elections gives those elected the control of local, state, and federal treasuries and resources. But vendors and many election officials fail to treat electronic voting machines with the care they would treat a truckload of signed blank checks drawn on the U.S. Treasury. They also seem more likely to attack the messengers exposing security problems, such as election supervisors Ion Sancho in Florida and Bruce Funk in Utah, rather than attack the problems.

A one-day election utilizing paper ballots, hand-counted publically in each precinct, can dramatically shrink the time frame of vulnerability to tampering. By contrast, elections to be tabulated by software present a long chain of custody requiring protection that begins many months before election day. Targets for corrupt insiders or outsiders would include software from design to testing to completion, and hardware from manufacture to assembly to transportation. Warehouse storage and software upgrades could also be opportunities for malicious intrusions. Specific programming of the ballot and transmission of election day results must also be protected from errors or fraud.

---

[16] "A Single Person Could Swing an Election," by Zachary A. Goldfarb, June 28, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/27/AR2006062701451.html?referrer=emailarticle.

For one of Harri Hursti's hacks in Leon County, Florida, he required access of only 90 seconds to perform a switch that changed the result of a test election. It was estimated that to accomplish total and complete contamination of the software he checked in Utah would take a thief two to five minutes of access.

Yet, there have been persistent reports that voting machines are unprotected not for just a few minutes, but for days or weeks.

Sleepovers and Unchaperoned DREs

California 2004: "One of the poll workers had the machines in his car for a week because his apartment was too small to store them."[17]

California 2006 (U.S. Congress, district 50): Pamela Smith, Nationwide Coordinator for *VerifiedVoting.org*, reported that Diebold DREs were taken home by election workers prior to the 2006 special election. She wrote, "Depending when they have training, the machines could be at their homes for more than a week or two."

Patti Newton, a San Diego County poll worker, also reported to Brad Friedman:

> "I was an assistant precinct inspector in charge of equipment during this election (I'm in the 50th). I had my two Diebold machines for seven full days before the election (I was dumbfounded). The chain of custody is abysmal. There is a seal on the machines (which are locked) but I am the one who sets up/breaks down the equipment and breaks the seal at the end of the day."[18]

Georgia 2003: Randy Evans, a well-connected Georgia attorney who has represented two Republican Speakers of the House, wrote to Georgia Secretary of State Cathy Cox, stating his

[17] Jim Hamilton of San Diego County told the California Secretary of State panel on Voting Systems and Procedures, April 22, 2004, p. 94 of testimony.

[18] Bradblog.com, http://www.bradblog.com/?p=2932. Also, Newton's experience is cited in a VoterAction.org lawsuit attempting to enjoin the use of Diebold DREs in California in November 2006.

concern that some of the Diebold DREs were being stored in unsecured locations around the state, including "stairwells, hallways, and trunks of cars." He also attempted to throw cold water on the levity of the staff, adding: "please consider conferring with members of your staff in attendance at the meeting as the reports of unsecured storage of the DRE's were widespread, and the subject of some humor at the meeting." (September 18, 2003)

Texas 2006: An election judge in Harris County, Texas, Sarah Gonzales, told me that precinct election equipment is typically in possession of an election worker for days, up to a week, before an election. At the class they attended for election judges, "they basically gave us some guidelines, that the machines needed to be kept securely—don't leave them in the car, don't leave them in the hallway, don't leave them in your office. Don't allow your children to play with them. Store 'em under the bed, or put them in a room. And that's it." She added that at the end of election day, her precinct convention was in a separate room, across a campus, forcing her to leave her equipment unguarded. "There's a lot of times when they are left alone, and I don't know how else to say that." [19]

A second election judge in Harris County, which uses Hart InterCivic electronic voting equipment, told me that the judge picks up the precinct's master controller equipment on the Saturday or Sunday before a Tuesday election. Thus, the equipment can be in their car or home for a three-night sleepover. She says the class before the election is "a joke; we typically already know what the Open Polls password will be. It's been the same since they started. The Close Polls password is the same for all of the judge booth controllers." At her class, they were prompted by the person running the meeting, **"Where will you all be storing your election machines before the election?" The election workers answered, in a chorus, "Under our beds!"**

(This raises several questions. Will the dust bunnies be kind to electronic equipment? Could amorous activities by a precinct judge affect the accuracy of your election, requiring electronic recalibration?)

Michael Wertheimer recommended that we should defend our election systems as a critical infrastructure. It sounds more like we're setting the equivalent of the gold of Fort Knox (control

[19] Phone conversation with Sarah Gonzales, June 30, 2006.

of the state and U.S. treasuries) out on the sidewalk, attaching it to a sapling with a bicycle lock, and assuming that nobody will take it.

TRIAD—Just Phone It In

Let's go back to Ohio and take a look at tiny Triad. Triad is a family-owned operation based in Xenia, Ohio. Triad ran the tabulation software that counted 41 of Ohio's 88 counties in November 2004. Standard punch-card readers read the ballots, then the Triad software kicked in to tabulate the counties. Triad also ran voter registration in 53 Ohio counties.

After the November 2, 2004 election, and before the recount in Ohio demanded by the Green and Libertarian parties, Triad made some changes, adjustments, or reprogramming—whatever you want to call it.

Triad's Brett Rapp says the company did this to all of its 41 counties.

> Prior to the recount, when the secretary of state announced that the recounts should commence, they also gave all of the counties guidelines of how the recounts needed to be conducted, and what should be included on the reports for the recount elections. All of the reports that are produced for this recount only show the presidential race. So in order for the machine to show that, **there has to be a change made to the tabulation reporting**, to tell this reporting system: only report the presidential totals. Okay? That is why we went to Hocking County. Because they were going to prepare—they were going to conduct the recount all by themselves—and we wanted to make sure—and **we did this not just in Hocking County, this is in all of our counties**. We helped them prepare the recount to make sure that the counties had the recounts set up properly. ...The computer system? Has a report file that shows all of the offices and issues that are programmed in for the election. And we had to make a change to the report file to show that it would only display the presidential race.[20] (emphasis added)

[20] December 2004 interview with Triad President Brett Rapp and Triad Vice President Dwayne Rapp, by Evan Davis and Terri Taylor.

Green Party Observers Add Some Information for Two Counties

> *Fulton County, Ohio*
> "The Director for Fulton told me that **Triad is able to reprogram the computer to count only the Presidential ballots by remote dial-up**."

> *Van Wert County, Ohio*
> "When asked if Triad had serviced the machine, the deputy director and a board member stated that **they had serviced the machine over the phone via modem on December 9th.**"[21]

Okay, let's see what one of Triad's vice presidents has been working on.

Cheryl Bellucci, a VP at Triad, posted memos online seeking technical assistance.

> I have my connection set up in my Project, but how do I access the Remote View?
> From: Cheryl Bellucci <> Date: Tue 01/25/2000 at 08:44AMPST

> Can anyone point me to a good ODBC [Open Database Connectivity] example? Specifically, I want to retrieve data from an Access database through VFP6.0.
> From: Cheryl Bellucci <> Date: Friday 01/21/2000 at 14:03PM PST

> I have a VFP6 [Visual Fox Pro 6] application that reads/updates a series of Access MDBs through Remote Views stored in DBCs [Database Connectivities].
> From: Cheryl Bellucci <> Date: Sunday 03/18/2004 <> Xenia, US Version: Visual FoxPro 6

So, Triad made changes to the vote counting software for its counties (nearly half the counties in Ohio) in preparation for the recount. Observers in two counties report that they were told Triad made the changes remotely, by modem. A Triad VP uses an application that "reads/updates" databases through "remote views." The database software appears to be Microsoft Access.

---

[21] 2004 Ballot Recount: Observer Report, December 21, 2004: Report by Green Party Observer, http://www.votecobb.org/recount/ohio_reports/counties/vanwert.php.

Dr. Dan Wallach is an associate professor of computer science at Rice University. He co-authored "Analysis of a Voting System," the first independent look by computer scientists at the software of electronic voting, specifically Diebold DREs, in July 2003. He spoke with me about Microsoft Access in the context of its use in the central tabulating system, called GEMS, for Diebold.

> Microsoft Access is Microsoft's weakest database product ... something you might use to keep track of your recipes, and even then I wouldn't trust it. ... You want to make it be robust against people trying to mess with the computer. **If that computer was accessible from the Internet, anyone could connect to the computer and edit the results as they're written to this database.** If this computer were connected to the Internet, it would be vulnerable to—insert your favorite Internet hacker attack. But even if it's not, **that computer needs to be guarded its entire lifetime from the moment it's shipped from the factory. All it takes is a couple of minutes alone with the computer to install your own software on that machine that might give you back door access, or let your own software could go in and edit the database to flip votes from one candidate to another**.[22]

But—don't worry. Triad says no one should worry about technicians changing anything in the software for elections, because the tech will leave a note inside the computer as to what was done.

That sounds a little like David Beirne, public relations officer for the County Clerk for Harris County, Texas, one of the nation's biggest counties. At a meeting of the local chapter of the League of Women Voters, Beirne was cornered by skeptical citizens. The citizens said they weren't satisfied with "faith-based" elections or paperless electronic voting; they wanted verifiability and authentic recountability. "Well. It's ALWAYS been faith-based elections," Beirne sniffed.

After working as a software technical writer for twenty years, Ellen Theisen co-founded the nonpartisan group, Voters Unite. For the November 2004 election, her group campaigned for paper ballots for at least the presidential and congressional contests as an emergency measure to try to prevent an unverifiable election.

[22] Dr. Dan Wallach, in-person interview, November 20, 2003.

This realm of remote, unsupervised connection in elections greatly concerns Ms. Theisen. "People don't understand how much you can do with software, computers, connectivity—it's not controllable."

So, did someone sit back with a laptop and a modem and make remote changes to election computers in Ohio, before the election, during the election, before the recount, or during the recount? Did they access tabulators run by Triad? Diebold? ES&S? Was it an insider? An outsider? Or were the everything-but-the-kitchen-sink obstacles thrown at the Ohio voters enough to throw the election without any remote electronic piracy?

Did we have a mock election in Ohio? Elsewhere? How about the next election? And the one after that?

It's only control of the most powerful country on the planet that we are talking about. Would someone really try to STEAL that? What if it was easy, remote, and there was almost no likelihood of discovery or punishment?

Do you think we should find out?

ADDENDUM

A little over a year after the initial version of this article was published, a new security flaw was found to be built in to the equipment of one electronic voting vendor. The magnitude of this flaw stunned computer scientists across the country.

The investigation of Diebold DREs in Utah, by Harri Hursti,[23] found what computer scientists are calling the worst security hole yet in computer equipment for elections. The problem is fundamental to the architecture of the software, and would allow someone with a common computer component and knowledge of Diebold to load almost any software without a password or proof of authenticity. Hursti found that it would be easy to install malicious code permanently on the machine in a way that could defeat any attempt to secure the machine afterward. The malicious code could protect itself from forensic investigation, and defeat any security measures added. A hack today, by someone with a few minutes of physical access, might unlock a door allowing election thefts for a number of election cycles into the future.

> "This one is worse than any of the others I've seen. It's more fundamental," said Douglas Jones, a University of Iowa computer scientist and veteran voting system examiner for the state of Iowa. "In the other ones, we've been arguing about the security of the locks on the front door," Jones said. "Now we find that there's no back door. This is the kind of thing where if the states don't get out in front of the hackers, there's a real threat."[24]
>
> **"It's the most serious security breach that's ever been discovered in a voting system. On this one, the probability of success is extremely high because there's no residue.... Any kind of cursory inspection of the machine would not reveal it,"** said Michael Shamos, a Carnegie Mellon University computer science professor and veteran voting systems examiner for the state of Pennsylvania.[25]

---

[23] Hursti's report is at Black Box Voting, http://www.blackboxvoting.org/BBVtsxstudy.pdf.

[24] "New security glitch found in Diebold system," by Ian Hoffman, May 10, 2006, http://www.insidebayarea.com/portlet/article/html/fragments/print_article.jsp?article=3805089.

[25] "Scientists Call Diebold Security Flaw 'Worst Ever,'" by Ian Hoffman, Inside Bay Area, May 11, 2006, http://www.truthout.org/docs_2006/051206F.shtml.

> **"I think it's the most serious thing I've heard to date ... Even describing why I think it's serious is dangerous,"** Johns Hopkins University computer science professor Avi Rubin told Ian Hoffman.[26]

Three of the nation's leading experts on computer security in elections followed up with the discovery that the RABA investigation of January 2004 had uncovered this:

> "Even more shockingly, we learned recently that Diebold and the State of Maryland had been aware of these vulnerabilities for at least two years," wrote David Dill, Doug Jones and Barbara Simons. [27]

David Bear, speaking for Diebold Election Systems, said the company's technicians had intentionally built the machines in such a way that election officials would be able to update their systems in years ahead.

> "For there to be a problem here, you're basically assuming a premise where you have some evil and nefarious election officials who would sneak in and introduce a piece of software. I don't believe these evil elections people exist."[28]

There are no evil people in the world Mr. Bear lives in? Presumably, he leaves his car unlocked, with his credit cards and wallet on the dashboard.

The evil people would not have to be election officials. They could be contractors, delivery people, warehouse people, software developers, manufacturing plant workers, technicians, foreign governments, and so on. In fact, an evil person anywhere could hire or persuade honest people to "update" elections software, and the updaters could believe the update was authentic.

---

[26] Ibid.

[27] " The Diebold Bombshell," by David Dill, Doug Jones and Barbara Simons, OpEd News, July 23, 2006, http://www.opednews.com/articles/opedne_david_di_060723_the_diebold_bombshel.htm. The fundamental problems discovered by RABA are discussed in this article, pp. 1-2, as they were in the earlier version of this article, "Even a Remote Chance," published in January 2005.

[28] "New Fears of Security Risks in Electronic Voting Systems," by Monica Davey, May 12, 2006, New York Times, http://www.nytimes.com/2006/05/12/us/12vote.html?_r=3&oref=slogin&pagewanted=print.

Perhaps Bear should ask his parent company, Diebold, a leading Automated Teller Machine (ATM) company, how effectively evil people are deterred in that sector. The ATM industry sustained $3 billion in losses last year through a criminal practice called "skimming."[29]

Well, but that's ATMs and this is elections. Oops, what about that fellow who used to be a vice president who programmed software for elections for Diebold's predecessor company, Global Election Systems, and was then a consultant for Diebold? Before his election industry employment, Jeffrey Dean served four years in prison for 23 counts of embezzlement. Records state that "the crimes and their cover-up involved a high degree of sophistication and planning in the use and alteration of records in the computerized accounting system."[30]

Dr. Dan Wallach of Rice University said of the gaping security hole which Hursti uncovered, "This is serious. Nobody is dismissing this as a minor issue. It's a major vulnerability." He said that the party line from Diebold is (a) it's not very serious, and (b) it's never been done.

As for the allegation that "it's never been done," Wallach said, "No one knows. If somebody has done this, they aren't saying."[31]

I asked Dr. Wallach, "Based on what you know, with Diebold DREs being locked down in several states and procedures on deck to try to get this stuff clean and ready for elections, do you have confidence that these things will work?"

His answer: "If the attack has already been done, then it's too late."

---

[29] "Automated Thievery," by Sid Kirchheimer, AARP Bulletin, January 2006. See also Endnote 5.

[30] "Election Pros Are Cons," by George Howland Jr., February 11, 2004, Seattle Weekly, http://www.seattleweekly.com/features/0406/040211_news_election.php.

[31] Phone conversation with Dr. Dan Wallach, May 12, 2006.

Endnote 1: An earlier version of this article was originally published in January 2005 at *OnlineJournal.com* and *VotersUnite.org*.

Endnote 2: Election companies are notorious for frequent name changes, and their family trees are also interbred; one could say that Diebold and Advanced Voting Solutions have the same father. Howard Van Pelt sold his previous election business, Global Election Systems. That became Diebold Election Systems. Then Van Pelt became CEO of Advanced Voting Solutions. The two companies, AVS and the Diebold election division, are located just a few miles down the road from each other in the McKinney, Texas area.

Endnote 3: The possibility of hacking an election by changing the ballot definition has been publicly known since at least the January 2004 report of RABA Technologies for the State of Maryland, which stated:

> "[T]he database files that contain the election definition (and results) are neither encrypted nor authentication protected. Results can be modified at will. In addition, ballot definitions can be altered so that the mapping between candidates and their "ordinal numbers" can be changed. A sophisticated user can automate this procedure requiring only a few minutes access to the server." ("Trusted Agent Report: Diebold AccuVote-TS Voting System," pg. 21, http://www.raba.com/press/TA_Report_AccuVote.pdf.)

For examples of election foul-ups related to ballot definition, see "51 Ballot Programming Flaws Reported in the News," http://www.votersunite.org/info/mapVoteSwitch.pdf. For discussion of this seriously-overlooked vulnerability, see "Key Component of Voting System Undergoes No Review," by *VotersUnite.org*, June 18, 2006, http://www.votersunite.org/info/BallotProgramming.pdf.

Endnote 4: For a discussion of Infrared Data Transfer Ports and Diebold touchscreen machines, see Brad Friedman's article, "Why Do Diebold's Touchscreen Voting Machines Have Built-In Wireless Infrared Data Transfer Ports? IrDA Protocol Can 'Totally Compromise System' Without Detection, Warns Federal Voting Standards Website," Bradblog.com, February 22, 2006, http://www.bradblog.com/archives/00002458.htm.

Endnote 5: Crime committed by electronic means is growing. Its scope is global, and law enforcement is struggling to combat it. Identity theft, often involving use of computers, is the nation's fastest growing crime, with financial losses estimated by the Federal Trade Commission at $50 billion per year. **In six months, "IBM's global security intelligence team detected more**

than 237 million security attacks worldwide ... including 54 million against governments, 36 million against manufacturers and 34 million against financial services" ("Hackers' attacks bewilder VeriSign; Key overseer of the Internet says online world now a 'war zone,'" Washington Post, August 6, 2005, http://www.chron.com/cs/CDA/printstory.mpl/business/3298942).

In less than 18 months, thefts due to hackers, lost laptops and dishonest insiders totaled nearly 89 million records containing sensitive personal information involved in security. (As of July 1, 2006. A constantly updated list of these may be found at: http://www.privacyrights.org/ar/ChronDataBreaches.htm.)

One must ask the question: Could the identity of a state or an entire nation be stolen by the thievery of its elections?

Pokey Anderson is an investigative journalist who has been reporting on election transparency issues since 2003. She co-produces a weekly news and analysis radio program, The Monitor, on KPFT-Pacifica (www.kpft.org) in Houston. Some of her research was included in "How They Could Steal the Election This Time," a cover story by Ronnie Dugger, August 16, 2004, in The Nation, *http://www.thenation.com/doc.mhtml?i=20040816&s=dugger. Before that, she was researcher for a major book on the Enron collapse. Her email address is Pokey at kpft.org.*