The CPSR Newsletter

Volume 19, Number 1 | Computer Professionals for Social Responsibility | Winter 2001

Getting the Chad Out: Elections, Technology, and Reform

by Erik Nilsson
erikn@cpsr.org

Finally, the Spotlight Falls on Elections Technology

The 2000 US presidential election was shocking and embarrassing. Americans were shocked to discover that their elections systems are woefully inadequate. The world was surprised to discover that America, one of the worlds oldest and stablest democracies, could have such rotten elections machinery.

And it was embarrassing. In Florida, a close race for president exposed technical and procedural failures. Other states experienced similar incidents, demonstrating that the embarrassment is national. It was embarrassing to have the ensuing squabble engulf all three branches of government.

It's unfortunate that such a debacle was required to focus attention on a thoroughly-researched problem. CPSR's work on election systems began in the 80s with the work of Bob Wilcox, Eva Waskell, myself, and others. Elections experts have been writing since the 70s on the inadequacy of US election systems. Unfortunately, systems that were inadequate in 1970 are still in use today, and are still inadequate.

Citizens and elected officials demand that something be done. We must replace defective systems with new ones; we must pay for these new systems; we must make voting more convenient; we must use the Internet; we must return to simpler, reliable systems; we must act boldly; we must act cautiously--there is agreement that something must be done, but no agreement on what to do.

The world's democracies watch the debate in America, and consider their own actions. Democratic nations all incorporate innovations developed around the globe over the last three centuries. The problem is not uniquely American; all democracies are re-evaluating their democratic machinery to some degree, in light of Florida.

Certainly, something must be done. Hopefully, Americans will be moved to action, not because our pride has been hurt, but because we owe ourselves and the world more trustworthy elections. Hopefully, all the world's democracies will take sensible steps where they are required. But in our headlong rush to do something, it's important to understand what is actually broken and what might be done to fix it.

To assist this critical debate, CPSR's Winter 2001 Newsletter is devoted to elections. In "No Easy Answers," Lorrie Faith Cranor surveys elections technology, evaluates the prospects for Internet voting, and makes recommendations for action. "Why Has Voting Technology Failed Us?" examines the performance of existing systems, and considers the prospects for improvement. In "Sweden to Experiment with E-voting," Anders Olsson reports on Sweden's current electoral experiments.

In "System Integrity Revisited," Rebecca Mercuri and Peter Neumann examine the reasons why current voting systems have failed. They call on computer professionals to contribute their expertise to an informed discussion.

I hope these articles contribute to your understanding and interest in elections technology. This is the third major publication CPSR has devoted to this issue. Roughly every five years, CPSR has devoted a special report or newsletter to voting. Hopefully, in 2005, the topic of elections technology will not warrant such treatment. I hope the next five years bring us elections systems worth trusting.

Erik Nilsson <erikn@cpsr.org> chairs the CPSR Working Group on voting. He has published various articles on voting systems, written elections software, and observed elections. He is based in Seattle.

[top]

What's inside...

- Introduction: Getting the Chad Out: Elections, Technology, and Reform
- Voting After Florida: No Easy Answers
- Why Has Voting Technology Failed Us?
- Sweden to Experiment with E-voting
- System Integrity Revisited
- For Further Reading and Research on Voting

P.O. Box 717
Palo Alto, CA 94302-0717
Tel. (650) 322-3778
Fax (650) 322-4748
webmaster@cpsr.org

Newsletter Index

Voting After Florida: No Easy Answers

by Lorrie Faith Cranor
http://lorrie.cranor.org/

What's inside...

- Introduction: Getting the Chad Out: Elections, Technology, and Reform
- Voting After Florida: No Easy Answers
- Why Has Voting Technology Failed Us?
- Sweden to Experiment with E-voting
- System Integrity Revisited
- For Further Reading and Research on Voting

P.O. Box 717
Palo Alto, CA 94302-0717
Tel. (650) 322-3778
Fax (650) 322-4748
webmaster@cpsr.org

As the world watched the electoral drama unfold in Florida at the end of 2000, my phone started ringing off the hook. "Wouldn't all our problems be solved if they just used Internet voting?" "Was that butterfly ballot really as confusing as they claim?" "And what exactly is the difference between a pregnant and a dimpled chad?" I spoke with numerous reporters, several state officials, and many colleagues and friends. While the actual outcome of the Presidential election remained unknown, it became clear that throughout the United States, people were soon going to be taking a hard look at their voting equipment and procedures, and trying to figure out how to improve them. After they finished scrutinizing and debating the events in Florida, what everyone really wanted to know was what new technology their state could buy that would ensure that in future elections all votes would be fairly counted. But there are no easy answers.

Voting Technology

Mechanical lever voting machines

Mechanical lever voting machines have been in use in parts of the United States since 1892. Voters pull levers that correspond with the candidates and issues they wish to vote for. When a lever is pulled it causes a counter wheel to rotate. At the end of an election, officials open up the back of each machine to read the counter wheels and determine how many votes were cast for each candidate. By the 1960s, these machines were used by about half the voters in the US. These machines were appealing because they allowed election results to be determined quickly, and because they were able to thwart voting fraud schemes that had become widespread using paper ballots.

One of the main disadvantages of lever machines is there is no ability to audit them and to "recount" individual ballots. If the machine malfunctions and a counter wheel fails to turn, no record exists from which a proper tally can be determined. Sometimes levers are mislabeled (either accidentally or deliberately). Lever machines are also difficult to test exhaustively, as a person has to manually enter large numbers of votes into each machine that is to be tested. These machines have also been known to cause confusion when recording and tallying write-in ballots. Because of their size and weight, these machines are expensive to store and transport. Lever machines are still in use in 15% of counties in the US. However, because they are no longer manufactured, it is becoming difficult to obtain spare parts for them. During the 2000 Presidential election, New York City voters reported that levers were broken off of some machines, making it impossible for them to vote for some local offices.

Punch card voting systems

The State of Florida purchased their punch card voting system about 20 years ago to replace the lever machines they were using at the time. The Florida punch card machines are known as *Votomatic* machines. The cards used by these machines are printed with rows of marks where holes can be punched. The names of the candidates are not printed on the cards themselves, but rather on a ballot holder device that looks something like a book with cardboard pages. When the card is properly inserted into the ballot holder, one column of holes is visible through the "spine" of the book. Each hole lines up with the name of a candidate printed on the book's pages. Election officials try to print candidate names only on the left side of each two-page spread, so that the holes are to the right of the candidates names. But sometimes they end up with ballot layouts that use both the left and right sides of the page. Having used this system‹butterfly ballots and all‹when I lived in St. Louis, I can assure anyone who insists that the system shouldn't be *that* difficult to figure out, that indeed it is. Especially when two page "butterfly" layouts are used, the system can be quite confusing even to someone with 20-20 vision and good hand-eye coordination. The Associated Press recently quoted one of the inventors of the Votomatic system as saying that he had never intended it to be used with a butterfly layout.

The 2000 Presidential election was not the first time that there were lawsuits over Votomatic ballot confusion. In 1987, ballots cast in predominantly black wards of St. Louis were more than three times as likely to be improperly punched, and therefore not counted, as those cast in predominantly white wards. A federal judge subsequently ruled

that the punch card system used in St. Louis "denies blacks an equal opportunity with whites to participate in the political process." The judge ordered the city to increase voter education in black wards and count improperly marked ballots by hand.

Another kind of punch card ballot system called *Datavote* reduces voter confusion about which hole to punch by printing the candidate names directly on the ballot. However, Datavote systems can cause problems and added expense because most elections require voters to use multiple ballot cards. In precincts where these systems are used, under votes are common when voters forget to vote in the races listed on the back of the punch cards, or neglect to vote all of the punch cards they are given. Sometimes Datavote systems also have a high rate of over votes for reasons that are not entirely clear. Datavote cards are voted using a special mechanical hole punch device that cleanly removes the chad from each hole a voter punches.

Besides the difficulty in understanding and marking punch card ballots, these ballots have also been known for a long time to be difficult to tally accurately. Votomatic systems suffer from the frequent occurrence of hanging, swinging, pregnant, and dimpled chad. These terms have now become household words in the US and the butts of many jokes. But in early November 2000, most Americans had never heard these terms. The word chad first came to my attention when I read Roy Saltman's 1988 National Bureau of Standards report *Accuracy, Integrity, and Security in Computerized Vote-Tallying* [http://www.nist.gov/itl/lab/specpubs/500-158.htm] while working on my dissertation. Saltman described a large number of problems with punch card ballots, and highlighted the chad problem in particular. Despite these warnings, punch card systems remain in use in 20% of counties in the US.

Optical-scan voting systems

One popular alternative to punch card systems are optical-scan systems, used in 40% of counties in the US. These systems are similar to the systems used to administer college entrance exams and other standardized tests. Voters use a pen or pencil to fill in an oval or connect dots on a paper ballot. A machine scans these ballots to count the votes. Both punch card and optical-scan systems suffer from the problem that voters may improperly mark their ballots, causing the ballot-counting computer to count them incorrectly or not at all. And both kinds of ballots can be tampered with during the counting process. However, in many precincts where optical-scan ballots are used, a scanner is available in each precinct so that voters can feed their ballots into the scanner themselves and check to see if it is accepted by the machine. If the machine reports that the ballot is mismarked, the voter can correct the problem and submit it again. In precincts where such a scanner is available, the percentage of uncounted ballots is often reduced by roughly a factor of five (when no scanner is available, optical-scan and punch card ballots result in similar percentages of uncounted ballots). Similar improvements might be possible if punch card readers were available at precincts as well.

Direct recording electronic systems

In the aftermath of the 2000 Presidential election, people are calling for a voting system in which every vote cast will be counted. They want systems in which it is not possible for a voter to mark a ballot in such a way that it will not be counted. And they want systems that will allow for accurate recounts without the risk of ballot tampering or the need to argue about what constitutes a vote. Vendors of computerized voting systems, often referred to as direct recording electronic (DRE) systems, claim to have an answer. A computerized voting machine that allows voters to register their votes using a touch screen, ATM-machine like terminal, or a panel with buttons and lights, could ensure that voters do not unintentionally vote for too many or too few candidates. Indeed, in the 9% of counties in the US where these machines are already in use, the feedback from voters is generally positive. Voters typically find the machines easy to use, and like the fact that the machines warn them if they fail to vote for a particular office and do not permit overvotes. I used one of these machines in New Jersey this year, and found it quite simple to use, although a carelessly designed ballot could probably render even a DRE machine difficult to use and confusing to voters.

While DRE machines may be easy to use, produce unambiguous results, and don't involve paper ballots that might be tampered with, they are not without problems. DRE machines must be trusted to accurately record each vote as the voter entered it. If the machines do not record a vote accurately, or fail to record it at all, there is no record to go back to for a recount (as with lever machines).

I tend to think that with sufficient review and oversight, we should be able to deploy DRE

machines that have a very low risk of failure (through either accidental error or fraud). I don't think we can build a perfect machine, but we should be able to build a machine with risks lower than the risks associated with a paper ballot system. I do not know enough about existing DRE systems to know whether any of them are good enough today, but have heard about enough problems to be suspicious. Another problem with DRE machines is the amount of time each machine is monopolized by a single voter. When DRE machines are used, each voter must have exclusive access to a terminal for the entire time it takes to mark the ballot. Election officials with experience using DRE machines report that generally about 30 voters per hour can use a single DRE machine. (This is probably similar to the number of voters that can use a lever machine in an hour.) Thus, it takes a large number of machines to serve the voters in each county. The machines are expensive, and each must be configured and tested before every election.

Some vendors are promoting computerized systems that use off-the-shelf PCs as a much less expensive alternative to traditional DRE systems. Besides the significant cost advantage, some vendors claim that there is less of a risk of hardware tampering on such machines since they are not being manufactured for the express purpose of voting. However, because these computers are manufactured as general purpose computers, there are also a lot more areas where things may go wrong and a lot more places where malicious code may be hidden. And conducting an election on them using a general purpose operating system opens them up to a wide range of vulnerabilities. Hand-counted paper ballots

The apparent lack of a perfect voting technology has lead many people to suggest that we just go back to the old hand-counted paper ballots used in the past in the US, and still used throughout most of the world. A well-designed paper ballot would probably use a separate ballot paper for each race, and include large boxes for voters to use to mark their preferences. In most countries where this system is used, ballots can be tallied very quickly, sometimes in a matter of hours, using government employees or citizen panels. But in most of these countries voters are asked to vote in only a few races, often only one race. With the large number of races and other ballot questions on US ballots, a hand counted paper ballot system would be more cumbersome. As suggested by computer-related risks expert Peter Neumann [http://www.csl.sri.com/users/neumann/], it might be practical if used for Presidential voting only, and not for other races. Even if a paper ballot system were practical, problems would remain. Voters could still accidently skip over ballot questions or vote for too many candidates on a ballot. And paper ballots can be tampered with during transport and counting, and are subject to a range of voting fraud schemes that involve vote buying and ballot box stuffing. This option should be considered along with other possible options, but it does not appear to offer a perfect solution either.

Internet Voting: Don't Try This At Home

Perhaps the questions I heard most frequently following this year's election were questions about Internet voting. As the popularity of online shopping and banking increase, so does voter interest in the possibility of voting from home or work over the Internet. The first governmental election to be conducted over the Internet in the US was the 1996 Reform Party Presidential primary, in which Internet voting was offered, along with vote-by-mail and vote-by-phone, as an option to party members who did not attend the party convention. In 2000 the Arizona Democratic Party offered Internet voting as an option in their Presidential primary. And Internet voting was used in the 2000 Alaska Republican Presidential straw poll as well as in a number of non-binding shadow elections. In the November 2000 Presidential election, a few hundred over seas military personal were given the opportunity to cast their absentee ballots via the Internet.

The problems that have actually occurred in online elections to date are relatively minor compared with the types of problems that experts fear might occur if Internet voting was used in contentious governmental elections. At an NSF sponsored e-Voting Workshop in October [http://www.netvoting.org/], security experts discussed a wide range of problems. Most significant were probably the vulnerabilities of the personal computer platform and the vulnerabilities of the Internet infrastructure itself. Individuals don't currently have the ability to shield their personal computers from viruses and trojan horses that might manifest themselves on election day. Furthermore, the ability to prevent denial of service attacks against voting servers or voters' Internet connections is limited. Hackers could design attacks to take out large portions of the Internet, or focus on neighborhoods known to support a particular party. Avi Rubin [http://www.avirubin.com/] wrote a short essay [http://www.avirubin.com/e-voting.security.html] following the NSF workshop that provides a good overview of these and other security concerns.

The conclusions reached by workshop participants about the security risks of remote Internet voting were similar to the conclusions reached by the California Internet Voting Task Force [http://www.ss.ca.gov/executive/ivote/] in January 2000. The taskforce also outline security concerns, and suggested that if Internet voting was to be pursued, it should be introduced in several stages, beginning with Internet voting terminals in neighborhood polling places. This first phase would not really offer any advantage to voters, but it would provide a more controlled environment in which to gain experience with Internet voting.

People often ask me why the security risks associated with Internet voting are different from the risks associated with online banking. Some have even suggested that Automatic Teller Machines [http://www.votebyatm.com/] be employed for voting, in addition to their primary banking functions. Internet voting is very different from banking applications for a number of reasons. One of the most important differences has to do with auditing and secret ballot requirements. When you do a financial transaction, generally you get a receipt. Periodically your bank sends you a statement that summarizes all of your transactions for the past month or quarter. You can compare this summary with the receipts you received, and determine whether your bank made any errors. Furthermore, every financial transaction is recorded in great detail, along with information about who was involved in the transaction. But in secret ballot elections voters do not get receipts (if they did they could sell their votes or be coerced to vote in a particular way). And audit trails are specifically designed not to reveal the voter associated with each ballot. Also, while financial transactions occur every day of the year, major elections occur on just one day. Even if we extended the voting period to several days or even a few weeks there will still be a small window of opportunity that will be the focal point for those wishing to disrupt the election.

One of the primary motivations that has been given for remote Internet voting is the possibility of increased voter turnout. However, little evidence exists to suggest that the availability of remote Internet voting would succeed in bringing substantial increases in voter turnout. And any increase in turnout is likely to impact some voter groups more than others (in particular the people who have Internet connected computers in their homes). Thus, Internet voting could serve to widen the gap that already exists in the way different socioeconomic groups are represented at the polls.

Internet voting may be a good solution for non-governmental elections, especially for organizations that already have experience with vote-by-mail balloting. These elections generally are less interesting targets for hackers, involve smaller numbers of voters, and sometimes have less stringent secret ballot requirements Internet voting has been used successfully in shareholder proxy balloting for several years. Many professional organizations are finding Internet voting to be a cost-effective alternative to vote-by-mail. Is the Will of the People Countable?

The Bottom Line

Assuming we can find a better voting technology, how much would it cost? Cost estimates vary widely. DRE machines cost approximately $5,000 per unit. A system that uses off-the-shelf personal computers might be able to reduce that cost by as much as a factor of 10. Refinements on existing systems, such as putting scanners in every precinct that uses punch card or optical-scan ballots, might be substantially cheaper. Quotes in the media indicate that most states looking into replacing their voting equipment are assuming that they will have to spend upwards of $100 million. In November 2000 when I was interviewed for ABC NightLine I had heard estimates of $20-$50 million for a large county. Replacing voting machines will cost a lot of money. Most of that money will have to come out of state and local budgets. Recently introduced Federal legislation includes $100 million in matching grants for states to upgrade their voting equipment, but this doesn't appear to be anywhere near the actual costs. As I said, there are no easy answers. It is my hope that states will proceed cautiously in adopting new voting technologies, first establishing detailed requirements and certification criteria, and rigorously evaluating each candidate technology to see whether it meets the criteria. The technology development and evaluation necessary to satisfy these goals will be expensive. But by spending the money up front, we are more likely to avoid costly law suits and recounts, as well as to maintain public confidence in our electoral process, something that is very difficult to put a price on.

December 2000, Revised 19 March 2001

Dr. Lorrie Faith Cranor [http://lorrie.cranor.org/] has been studying electronic voting systems since 1994. She maintains the e-lection electronic voting mailing list [http://lorrie.cranor.org/voting/] and in 2000

served on the executive committee of a National Science Foundation sponsored Internet voting taskforce. She is a senior technical staff member at AT&T Labs-Research Shannon Laboratory in Florham Park, New Jersey. Her primary research focus is online privacy. She chairs the Platform for Privacy Preferences Project (P3P) Specification Working Group at the W3C, and last year she served on the Federal Trade Commission Advisory Committee on Online Access and Security. She is also a member of the project team that developed the Publius censorship-resistant publishing system, which was honored by *Index on Censorship* magazine for the "Best Circumvention of Censorship."

[top] Newsletter Index

Why Has Voting Technology Failed Us?

by Erik Nilsson
erikn@cpsr.org

Florida was a wake up call. In the aftermath of the last presidential election, there seems to be general agreement that America's current election systems are inadequate, and something must be done. It seems likely that something will be done. Laws will be passed. Money will be spent on new elections systems. Hopefully, carefully-considered actions will result in elections systems that are markedly more secure and accurate than the systems we use today. But this happy outcome is anything but certain.

Study Undermines Faith In Technology

In December, 2000, the presidents of MIT and Caltech announced a joint "Caltech / MIT Voting Project" to study voting systems and develop a new "voting machine" to prevent future debacles like we saw in Florida. This was one of many announcements around that time promoting various initiatives, technologies, and companies. Each claimed to have the technological fix for our election woes. Many of these announcements, like Caltech / MIT's, assumed that careful application of technology should result in the best election system possible. Some, like the Caltech / MIT announcement, combined this confidence with statements of obvious ignorance of how elections systems work and how they fail. But many of us in the voting community may have been too quick to write off Caltech / MIT's project. On February 1, 2001, the project released its first piece of research: a study on the accuracy of elections systems, nationwide, in the last four presidential elections [1]. The study uses a clever methodology to mine deep results from available election statistics. The results were surprising, even to many elections experts. The study measured the "residual vote": the number of ballots that did not end up having a vote for president counted, either because of undervote, overvote, or some other problem such as a stray mark. The residual vote is an estimate of a voting system's accuracy, probably the best such measure we will ever have on past elections. The average residual votes found were as follows:

machine type	residual vote (%)	margin of error	year of introduction [2]
mechanical lever voting machine	1.6	0.10	1892
hand-counted paper ballot	2.0	0.14	1856 [3]
optically-scanned paper ballot	2.3	0.19	1980s [4]
Vote-O-Matic-type punch card	2.9	0.09	1964
electronic "DRE" voting machine	3.0	0.17	1970s [3]
DataVote-type punch card	3.2	0.33	1968 [5]

With lever voting machines, the voter sets small levers or switches to indicate their choices, then pulls a master lever to make their vote. With optically-scanned ballots, the voter fills in a box or makes some other mark on a paper ballot; an optical scanner then reads the votes. Vote-O-Matic ballots are the type that produce the now-famous chad. With a DRE machine, the voter votes on a computer that usually resembles an ATM, picking candidates from a screen; the votes are recorded in the DRE's computer memory. DataVote punch cards are similar to Vote-O-Matic, except the candidates' names are printed on the ballot, and a different method is used to punch a hole in the ballot. The study does not attempt to identify the causes of residual vote in each system. Rather, the study correctly assumes that any failure to capture voter intent is an inaccuracy in the voting system, or perhaps a fraud. To guard against the possibility that, for example, DRE machines are concentrated in counties where more people tend to have no opinion on the presidential race, the researchers studied counties where the voting system had changed. The above results stand:

What's inside...

- Introduction: Getting the Chad Out: Elections, Technology, and Reform
- Voting After Florida: No Easy Answers
- Why Has Voting Technology Failed Us?
- Sweden to Experiment with E-voting
- System Integrity Revisited
- For Further Reading and Research on Voting

P.O. Box 717
Palo Alto, CA 94302-0717
Tel. (650) 322-3778
Fax (650) 322-4748
webmaster@cpsr.org

> "Levers and paper and scanned ballots appear to offer similar rates of reliability.... Paper ballots, lever machines, and optically scanned ballots produce lower residual vote rates [than] punch card and electronic methods.... Paper might even be an improvement over lever machines."

The startling result is, with the exception of optical, older technologies were significantly more accurate than newer technologies [6].

These results are a stark warning of how difficult it is to implement new voting technologies. People worked hard to develop these new technologies. Election officials carefully evaluated the systems, with increasing attentiveness over the last decade. The result: our best efforts applying computer technology have decreased the accuracy of elections, to the point where the true outcomes of many races are unknowable.

Many technologists and technology enthusiasts will read the above words and refuse to believe them. "There must be some other explanation," they will say. "Nothing has been proven," they will say. "Future technology will be better," they will say.

But there is no other plausible explanation: new technology may have reduced the cost of elections, and certainly has increased counting speed, but the above results show no statistically significant progress in elections accuracy over people counting paper ballots, one at a time, by hand. This data is not a proof, but enthusiasts of punchcard and DRE technologies in particular are not given much solace [7]. Furthermore, accuracy is only part of the problem: we must also worry about the security of voting systems. It's hard to measure security objectively, but there is no reason to think that newer systems are more secure than older ones. On the contrary, there is good reason to suspect that, since newer technologies have a more complex chain of activities between the voter and the outcome, newer technologies present more opportunities for fraud than older systems.

Will Yet More Technology Help?

Some suggest Internet-based voting will solve our problems. Tens of millions of dollars have been poured into Internet-voting startup companies. Some companies have already failed, but several remain. These companies try to create an electronic "ballot" with homomorphic encryption [8] or similar techniques. Their mantra seems to be, "if we can do e-commerce, we should be able to do e-voting." But the problems of e-voting are radically different from e-commerce. For example, you get a balance statement from your bank each month telling you what happened to your money. But, you don't get a statement from your county telling you how you voted, so you can't verify that your vote was correctly handled. You cannot get such a statement, because it could be used to buy votes or pressure voters.

A bank statement provides a real-world check on e-commerce, as well as buying by credit card over the phone, sending checks through the mail, and similar transactions that otherwise wouldn't be sufficiently trustworthy. Without the equivalent of a bank statement, e-voting requires a fantastical technological infrastructure. Ultimately, with or without fancy encryption tricks, e-voting requires a secure networked voting application. As Bruce Schneier points out, "A secure Internet voting system is theoretically possible, but it would be the first secure networked application **ever created** in the history of computers" [9]. Clearly, such a system could not use any current operating systems or browsers, since none of these is secure when used with a network. Thus, it is not even theoretically possible to develop a secure voting system where people vote from home, using their insecure browser on their insecure PC.

The very imperfect security of banking systems is acceptable, because we can catch their mistakes. The same level of security (or even vastly better security) is intolerable in voting systems, because the results can't be checked. E-commerce doesn't provide us with the technology to conduct e-voting. A secure voting system isn't sufficient, anyway. The system also needs to prevent votes from being altered or destroyed, in case of fraud by one or several people. With systems that have a physical ballot, altering a large number of ballots to change an election requires unsupervised access to the ballots, skill, and time to make the alterations. Since electronic records can be changed almost instantly by a surreptitious computer program, an acceptable technology would have to be able to create and manage an electronic ballot that can't be forged or altered. It must be possible to determine that a ballot came from a single voter, but there must be no way to know who that single voter is. If one had such a powerful technology, why apply it first to the small and often unprofitable elections market? Surely, this technology would be applied first to more lucrative ends. For example, a technology that enabled secure electronic ballots might also enable unforgeable electronic cheques, an unbreakable copyright

enforcement scheme, or unforgeable digital cash that requires no trusted third party. These more lucrative applications would provide revenue to develop and prove the new technology. Later, the mature technology would find application in elections.

Thus, unproven technologies should not be applied first to voting. We should not risk democracy on unproven technology. Also, since applying an unproven technology first to voting normally makes no economic sense, there is good reason to suspect both the viability of the technology and the wisdom of the technologists.

Real-World Lessons

Still, there are many proponents of Internet voting. Some of the proponents have a grasp of the preceding issues, yet remain convinced that, for some reason, a good Internet voting system must be possible. Some seem to believe that anything which can be done in the real world can be done analogously on the Internet at a cost that trends toward zero. The battering of dot-com companies over the last year has tempered rhetoric, but many of the plainly ignorant statements by smart people about Internet voting can be attributed to a quasi-religious belief that good java programmers can replace any activity in the real world with a better version on-line. As we've seen, this is just not the case for voting. This suggests there may be other plausible-sounding projects that begin with an "e" and a dash that are also unworkable. Why not vote with paper ballots, counted one at a time? There are disadvantages to hand counting, primarily speed and cost. But it's now clear that much of the cost savings of most newer systems came from their lower accuracy and greater vulnerability to fraud, a tragic false economy. The performance of optical systems give us some hope. They are faster and more economical than hand count, and preserve the option of a hand count to verify machine-count results. Caltech/MIT's results suggest that, today, optical systems are nearly as accurate as hand-counted ballots. With careful work, they can probably be made as accurate as hand-counted ballots. Carefully-designed procedures for random recounts by hand can probably bring the likelihood of fraud in machine ballot counting down to acceptable levels, at least for optical ballots.

Beyond convenience for the news media and our natural desire to know results immediately, speed has an advantage: the longer counting goes on, the more likely errors are. Thirty-six hours is about the longest a person can stay continuously alert. If an election continues for more than 36 hours, either the operation must be stopped then restarted, or all responsibilities must be handed over from one person to the next. Errors thrive in such moments of confusion. Naturally, where there is potential for error, often there is potential for fraud. The ideal vote-counting system is swift as well as accurate.

But while we are waiting for that better system, it would be better to use hand counting in places that currently use punch-card or DRE systems. Optical systems that use the highest-quality optical readers and statistically-meaningful random hand recounts should continue to be used, for the time being. Mechanical voting machines have in inherent weakness, in that each individual's ballot is not recorded, only totals of votes for all people who used the machine, so a meaningful recount down to the level of the individual ballot is not possible. This problem makes mechanical lever machines undesirable. However, it would be a wrenching change for counties using mechanical voting machines to stop using them all at once. Mechanical lever machines should be retired, over time. That said, it would still make me uncomfortable to vote on a mechanical lever machine.

It will take years at a minimum to develop new, better systems. Meanwhile, reliable elections depend on us recognizing that our efforts so far to improve voting with technology have been an almost unmitigated disaster. The money spent on various automated systems to strengthen our democracy has instead weakened it. Voting technology has failed us because we regarded vote counting as a simple problem. We assumed that competent application of commercially-available technology to elections would naturally improve elections. We were wrong.

The author is grateful for the assistance of Dave Bilgray and Lawrence Hecht and the CPSR Working Group on Voting in the preparation of this article.

Erik Nilsson <erikn@cpsr.org> chairs the CPSR Working Group on voting. He has published various articles on voting systems, written elections software, and observed elections. He is based in Seattle.

Notes

[1] The Caltech/MIT Voting Project, "A Preliminary Assessment of the Reliability of Existing Voting Equipment" 2/1/2001
http://www.vote.caltech.edu/Reports/report1.pdf

[2] The "year of introduction" column is my addition and wasn't in the Caltech/MIT report. Source: http://inventors.miningco.com/science/inventors/library/weekly/aa111300b.htm , or as noted.

[3] The modern paper ballot was introduced in Australia in 1856. It gradually displaced an older paper ballot technology.

[4] Eric A. Fischer *Congressional Research Service Report for Congress RL30773: Voting Technologies in the United States.*
cnie@cnie.org

[5] Sequoia Pacific Customer Support, telephone conversation, 3/6/01
http://www.seqpac.com

[6] The study is unable to control for one source of bias that may make DRE and mechanical lever machines look better than they are. Some states allow party-line voting, where a voter can vote for all or at least many races by making a single indication. On lever machines, this is usually done by pulling one large lever for the chosen party. All of the above systems can support party-line voting, but party-line voting has traditionally been used with lever machines. Lever machines users have shown the most interest in DRE machines. Since voting straight-party never creates a residual vote, jurisdictions with party-line voting should have lower residual votes, independent of the technology used. If party-line voting is correlated with lever and DRE machines, the study would overstate their accuracy. Another possible bias is that optically-scanned ballots are used in two different ways. In some areas, the optical ballots are pre-scanned in the polling place, to check for overvotes. If there is an overvote, the ballot is rejected and the voter is given another chance on a new ballot. Some studies have shown this practice significantly reduces overvotes, so optical ballots without precinct pre-scan may by statistically worse than lever or hand-count, but that would seem to make optical with precinct pre-scan statistically better than lever or hand-count.

[7] The Caltech/MIT study ends with a note of optimism regarding DRE machines that is at odds with the rest of the report.

[8] A homomorphic encryption scheme is a public-key cryptosystem with the special property than one can compute an operation on plaintexts, say addition, by manipulating only ciphertext. Therefore, someone without knowledge of the private key can compute simple functions of the encrypted data. (Source: http://www.zurich.ibm.com/~sti/g-kk/mobile/homomorphic.html)

[9] Schneier, Bruce, "Voting and Technology," *Crypto-Gram* 12/15/2000 [http://www.counterpane.com/crypto-gram-0012.html]

[top] Newsletter Index

Sweden to Experiment with E-voting

by Anders Olsson
anders.r.olsson@telia.com

What's inside...

- Introduction: Getting the Chad Out: Elections, Technology, and Reform
- Voting After Florida: No Easy Answers
- Why Has Voting Technology Failed Us?
- Sweden to Experiment with E-voting
- System Integrity Revisited
- For Further Reading and Research on Voting

P.O. Box 717
Palo Alto, CA 94302-0717
Tel. (650) 322-3778
Fax (650) 322-4748
webmaster@cpsr.org

As part of a series of small experiments in e-voting, the Swedish government is funding a project to conduct student elections at Umeå University via the Internet. The elections are to be held between April 27 and May 11. The project will use technology developed by US company Safevote [http://www.safevote.com/], in conjunction with the small Swedish company Vivarto Technologies [http://www.vivarto.com/].

Government Lays Groundwork

Sweden has uncomplicated government elections: a paper ballot in a physical box. Elections are every four years; referendums are rare. Like most older western democracies, Sweden is experiencing a "democratic crisis," and the government is worried, but not so worried that it's prepared to use IT to reengineer the very structure of democracy. Rather, new technology is used to better the facade. However, this is more action than previous governments have taken.

Last year, the government awarded minor sums to all sorts of experiments and projects aimed at renewing or bettering democratic processes. In November, 2000, 66 such projects received grants of between $1,200 and $60,000. The average grant was $15,000. Most of these projects are efforts to make more people interested and active in politics. A couple of funded projects involve e-voting. More such grants will be made this year.

Does this indicate that the Swedish government is determined to do something radical in creating new forms of democracy for the new, IT-based society? In my opinion, probably not. The government hands out small sums to communities, organizations, and companies. Some of these small projects might succeed one way or another, but no big societal player is threatened by any of the experiments and the government has not committed itself to anything radical. A special committee on voting technology (Valtekniska utredningen) appointed by the government published its findings in January, 2001. Among the recommendations was a proposal to try voting via Internet. The committee favored a most cautious approach: small steps and small experiments to begin with and thorough evaluation of each step. Also in January, I authored a report [http://www.itkommissionen.se/extra/document/?id=120] for the government IT commission on e-voting.

The government wants to look sharp, modern, hip, and active, and is therefore willing to put at least minor sums into experiments of the kind we now see in Umeå. The technical skill for the projects won't be found in the government ministries, though. Sweden has rather small government ministries, but big state agencies. The state agencies are where the specialists work.

In January, the national bureau of Statistics (SCB) reported that 55% of Swedes aged 16-64 said they would prefer to vote via the Internet if this was possible. This got some media attention. Although the survey most certainly was made in a reliable way, it was the opinion of a poorly informed citizenry. Also, the opinion of about 1.5 million people of age 65 and older was left out. But the survey is a reminder that Swedes have a strongly IT-positive approach. For example, Sweden has one of the highest number of Internet connections per capita in the world. So far, the question of e-voting hasn't been widely-discussed in Sweden.

Experiment In Umeå

Umeå University [http://www.umu.se/] is a small institution in the far north of Sweden. It prides itself on being "…practical, open and dynamic—not bound by mossy traditions." Markus Hällgren is vice president of the Umeå student union [http://www.us.umu.se/index.asp], and is in charge of the Internet-election in Umeå. According to Hällgren, the government is providing $20,000 for the Umeå experiment. Another $20,000 was provided by a state research-fund called KK-stiftelsen and $6,000 by the city of Umeå.

The student union was interested in Internet voting because of the desire to increase voter participation and reduce cost, said Hällgren, who hopes Internet voting will raise voter participation from 10% to 17%. Some students attend classes on campus as infrequently as

once a month, and live far from campus. Internet voting will be much more convenient for them, Hällgren claimed. Approximately 12,500 students are eligible to vote in the election. Voters have a choice between voting via the Internet, by mail, or in person. According to Safevote president Ed Gerck, each voter will be issued a six-character "Digital Vote Certificate," essentially a password. "A DVC has only six characters, yet provides a fully secure off-line ballot control structure for voting and auditing," said Gerck. "At the same time, it enforces a set of voting rules and allows for human verification that they are followed. The DVC and the voting rules guarantee that only one ballot will be counted per voter, even though a voter may vote several times in different locations and using different methods."

Conclusion

The Umeå experiment will most likely get some media coverage: it's something new, it's easy to describe, and it may cause some conflict that can be exploited journalistically. I recently discussed the Umeå experiment on national television. Consequently, Internet voting may become more widely discussed. However, wider discussion does not guarantee wider support. During my work with the e-voting report, I have spoken to many people working with different aspects of IT and democracy, including government officials, IT experts, companies promoting e-voting solutions, and students. Not one person I talked to claimed that voting via the Internet would in itself contribute to a better democracy. Everyone agrees that the learning and deliberative parts of the democratic process are far more important and that IT should be used to support those parts.

Anders Olsson <anders.r.olsson@telia.com> is a freelance writer specializing in democracy -- especially IT and the legal infrastructure of democracy. He lives in Hasselby, in the Stockholm area.

[top]

Newsletter Index

System Integrity Revisited

by Rebecca T. Mercuri
Peter G. Neumann

(This article first appeared under "Inside Risks" in *Communications of the ACM*.)

Consider a computer product specification with data input, tabulation, reporting, and audit capabilities. The read error must not exceed one in a million, although the input device is allowed to reject any data that it considers to be marginal. Although the system is intended for use in secure applications, only functional (black box) acceptance testing has been performed, and the system does not conform to even the most minimal security criteria.

In addition, the user interface (which changes periodically) is designed without ergonomic considerations. Input error rates are typically around 2%, although experience has indicated errors in excess of 10% under certain conditions. This is not considered problematic because errors are thought to be distributed evenly throughout the data. The interface provides essentially no user feedback as to the content of input selections or to the correctness of the inputs, even though variation from the proper input sequence will void the user data.

Furthermore, multiple reads of the same user data set often produce different results, due to storage media problems. The media contain a physical audit trail of user activity that can be manually perused. There is an expectation that this audit trail should provide full recoverability for all data in order to include information lost through user error. (In practice, the audit trail is often disregarded, even when the user error rate could yield a significant difference in the reported results.)

We have just described the balloting systems used by over a third of the voters in the United States. For decades, voters have been required to use inherently flawed punched-card systems, which are misrepresented as providing 100% accuracy ("every vote counts") -- even though this assertion is widely known to be patently untrue. Lest you think that other voting approaches are better, mark-sense systems suffer from many of the same problems described above. Lever-style voting machines offer more security, auditability, and a significantly better user interface, but these devices have other drawbacks -- including the fact that no new ones have been manufactured for decades.

Erroneous claims and product failures leading to losses are the basis of many liability suits, yet (up to now) candidates have been dissuaded from contesting election results through the legal system. Those who have lost their vote through faulty equipment also have little or no recourse; there is no recognized monetary or other value for the right of suffrage in any democracy. With consumer product failures, many avenues such as recalls and class action suits are available to ameliorate the situation, but these are not presently applicable to the voting process. As recent events have demonstrated, the right to a properly counted private vote is an ideal rather than a guarantee.

The foreseeable future holds little promise for accurate and secure elections. Inside Risks columns by Peter Neumann [http://www.csl.sri.com/users/neumann/insiderisks.html], November 1990, 1992, 1993, 2000, and June 2000) and Rebecca Mercuri's doctoral thesis [http://www.notablesoftware.com/evote.html] describe a multitude of problems with direct electronic balloting (where audit trails provide no more security than the fox guarding the henhouse) and Internet voting (which facilitates tampering by anyone on the planet, places trust in the hands of an insider electronic elite, and increases the likelihood of privacy violations). Flawed though they may be, the paper-based and lever methods at least provide a visible auditing mechanism that is absent in fully automated systems.

In their rush to prevent "another Florida" in their own jurisdictions, many legislators and election officials mistakenly believe that more computerization offers the solution. In addition to technical, social, and sociotechnical risks common to all secure systems, voting products are additionally vulnerable due to the adversarial nature of the election process,. Proposals for universal voting machines fail to address the sheer impossibility of creating an ubiquitous system that could conform with each of the varying and often conflicting election laws of the individual states. Paper-based systems are not totally bad; some simple fixes (such as printing the candidates' names directly on the ballot and automated

What's inside...

- Introduction: Getting the Chad Out: Elections, Technology, and Reform
- Voting After Florida: No Easy Answers
- Why Has Voting Technology Failed Us?
- Sweden to Experiment with E-voting
- System Integrity Revisited
- For Further Reading and Research on Voting

P.O. Box 717
Palo Alto, CA 94302-0717
Tel. (650) 322-3778
Fax (650) 322-4748
webmaster@cpsr.org

validity checks before ballot deposit) could go a long way in reducing user error and improving auditability.

As the saying goes, "Those who fail to learn from the past are doomed to repeat it." If the computer science community remains mute and allows unauditable and insecure voting systems to be procured by our communities, then we abdicate what may be our only opportunity to ensure the democratic process in elections. Government officials need your help in understanding the serious risks inherent in computer-related election systems. Now is the time for all good computer scientists to come to the aid of the election process.

Rebecca Mercuri <mercuri@acm.org> is a member of the Computer Science faculty at Bryn Mawr College and the President of the consulting firm Notable Software, Inc. [http://www.notablesoftware.com]. She has written extensively and testified on the subject of electronic voting systems for the past decade, and her statement on the necessity of a hand recount in the recent Florida election is referenced on the U.S. Supreme Court website. She specializes in interactive programming and forensic computing.

Peter Neumann [neumann@csl.sri.com, http://www.csl.sri.com/users/neumann] is a Norbert Wiener Award recipient and moderates the ACM Risks forum. He is a researcher in the SRI computer Science Lab.

[top]

Newsletter Index

For Further Reading and Research on Voting

by Erik Nilsson
erikn@cpsr.org

What's inside...

- Introduction: Getting the Chad Out: Elections, Technology, and Reform
- Voting After Florida: No Easy Answers
- Why Has Voting Technology Failed Us?
- Sweden to Experiment with E-voting
- System Integrity Revisited
- For Further Reading and Research on Voting

Elections Technology

Roy Saltman's seminal NIST paper on elections systems, probably the most-cited work on electronic vote-counting:
Accuracy, Integrity and Security in Computerized Vote-Tallying
http://www.nist.gov/itl/lab/specpubs/500-158.htm

Two more papers by Roy Saltman:
Adopting Computerized Voting in Developing Countries: Comparisons with the US Experience
http://www.cpsr.org/issues/voting_saltman.html
Assuring Accuracy, Integrity and Security in National Elections: The Role of the US Congress
http://www.cpsr.org/conferences/cpf93/saltman.html

Rebecca Mercuri's encyclopedic and widely-respected elections technology site, with many links
http://mainline.brynmawr.edu/~rmercuri/notable/evote.html
or http://www.notablesoftware.com/evote.html

Lorrie Faith Cranor's voting page, with a link to her popular e-lections mailing list
http://www.research.att.com/~lorrie/voting/

California Task Force Report on Internet Voting
http://www.ss.ca.gov/executive/ivote/final_report.htm#final-1

A brief history of voting equipment
http://inventors.miningco.com/science/inventors/library/weekly/aa111300b.htm

California Internet Voting Initiative
http://www.votesite.com

Caltech/MIT Voting Technology Project
http://www.vote.caltech.edu

Two articles by Bruce Schneier of Counterpane Labs on voting security
http://www.counterpane.com/crypto-gram-0102.html#10
and http://www.counterpane.com/crypto-gram-0012.html#1

Internet Policy Institute's *Report of the National Workshop on Internet Voting: Issues and Research Agenda*
http://www.netvoting.org/Resources/InternetVotingReport.pdf

Some companies with Internet voting products or announced plans

These companies vary greatly in their level of sophistication and funding

Election.com
http://www.election.com (Formerly Votation.com)

iBallot LTD
http://www.iballot.com

Safevote
http://www.safevote.com
and http://www.thebell.net

Validity Systems
http://www.eballot.net

VoteHere.net
http://www.votehere.net

Elections Generally

Resources for elections administrators around the world, and succinct explanations for election tasks ranging from voter education to vote counting:
http://www.aceproject.org

A wealth of elections resources; a worldwide elections calendar; and an extensive, searchable worldwide elections equipment buying guide:
http://www.ifes.org

Paper: *Turnout Decline in the U.S. and other Advanced Industrial Democracies*, by Martin P. Wattenberg
http://www.democ.uci.edu/democ/papers/marty.html

Elections in the US

2000 election
http://www.cnn.com/ELECTION/2000/results/

Electoral college votes by state from 1788 to 1996
http://www.nara.gov/fedreg/elctcoll/ecfront.html

Florida election law
http://www.leg.state.fl.us/statutes/

California Voter Foundation (information of interest to any voter):
http://www.calvoter.org

[top] Newsletter Index