Open letter in response to electronic voting articles in the October Communications of the ACM journal (Volume 51 No.10 10/08)
http://mags.acm.org/communications/200810/?CFID=5384174&CFTOKEN=38021074

The in vogue term "E2E" – End-to-End has reached voting systems, and while this may seem a new concept in fact the principles and concepts are enshrined in the OASIS Election Markup Language (EML) since its inception (http://docs.oasis-open.org/elections). EML provides mechanisms for managing and auditing the entire voting process from declaration of intent to hold an election, the recording of the candidates and issues to be voted on, the registration of voters, the determining of the polling places through to the layout and details of the ballots and then the voting and tabulation with public reporting of the results. It is essential that all of these aspects of the E2E voting process are published and recorded in open public information formats using an open publically specified process that protects voters' rights and provides inspection and transparency both during and following the election. The OASIS EML specification is an internationally accredited standard[1] developed over the past five years to meet these needs.

Unfortunately proponents of E2E voting in the current issue of the Communications of the ACM journal (Volume 51 No.10 10/08) miss this central point. They offer up encryption and crypto-key systems as the means to achieve E2E election processes. Professor David Wagner from UC Berkeley sounds a cautionary note in the article on "Clean Elections" by stating "One of the things about cryptography is that the devil is in the details". Even Hollywood understands, with the making of popular films with computers and encryption as themes and documentaries like "Hacking Democracy" and "Uncounted", that encryption can obfuscate peoples abilities to deduce what has happened in an election and is for many exactly the opposite of what is required.

The problem is that since the invention of democracy in Athens 2,000 years ago the ability to count elections by using simple voting techniques (that started with stones in large earthenware jars) has been outrun by the sheer scale and complexity of society with now tens of millions and even billions of potential voters and topics and agendas that are no longer just a simple yes or no selection. Fundamentally however the problem has not changed. As those founders of democracy understood very clearly you need transparency of the process, open public polling places with oversight and safe private voting, access to all steps of the process for all sides involved, traceability and auditability to perform verification, and above all you need vigilance and inspection to ensure that what should be happening is happening, and what should not be happening is not.

How can computers help in providing a better environment? The fact is that computers are at the heart of the problems surrounding the voting process. They are deeply involved in producing and replicating all the artifacts in the election process such as the ballots and registration forms through to counting and tracking the results. They are also producing opinion polls, online instant ballots, canvassing and tracking of registered voters, running political parties campaigns by organizing supporters calling and visiting with potential voters, tracking donations and running email action lists and every other aspect of what it takes to run a successful election campaign today.

[1] OASIS EML is an approved published standard formally adopted by the European Council of Ministers and also currently under review for adoption as an ISO standard.

One of the most telling references in the ACM Communications Journal "Clean Elections" article is the very short note about the municipal election in Tacoma Park, Maryland. I too have conversed with the good folks there about their voting system needs. Two things stand out, first an aging population with a predominance of retirees with special access and voting needs, and second a very small budget and non-existent IT support infrastructure. This is not untypical of precincts across America. So what is needed is a system that is childishly simple to operate, completely transparent to setup, configure and to verify worked correctly while costing around $500 per voting unit. The solutions touted in "Clean Elections" such as encryption, intangible entry methods, invisible ink, and tear-off receipts can be checked at the door given these prerequisites. You simply cannot have voting infrastructure that only the computing elite can understand and crosscheck. Instead voting systems have to be based on methods and processes that an average election management person or volunteer can fully comprehend and most such people are older and less computer literate. Simply put that means an underpinning that is founded on paper and today a great number of States now recognize that with a legal requirement on their statutes for using paper ballots as the ballot of record.

There are fundamental differences between a solution designed by academics with advanced degrees in mathematics compared to a commercial system built for the workplace and public use. While these e-Voting mathematicians may be well meaning in providing help to the good citizens of Tacoma Park as a test system, this is not the same as building robust trusted solutions for use across the entire country.

While we may scoff at stones in jars, the ancient Greeks thought long and hard about the principles of operation and safeguards in their voting processes using what was available to them and when we look closely those same fundamentals of transparency, inspection and verification apply today.

In the ACM articles there is much talk of cryptography and other mathematical techniques for ensuring voting systems. At the heart of the mathematics the bottom line is that the professors are trying to replicate the same safeguards that paper ballots provide in the real tangible world but in the ephemeral world of physics and electronics inside a computer memory chip. Unfortunately, no matter how clever the mathematics, we cannot directly verify with our tangible senses or sight what has occurred inside a computer chip world. For example they cite how using encryption you can log on in the comfort of your home and check via the internet that your vote was counted, well really?!? Sure the computer will show you that you voted but you still have absolutely no idea if your vote was really counted in the total that it showed as the election result! To perform that trick needs much more than just the computer telling you reassuringly that it counted your vote. There has to be other independent ways of verifying that, and the National Institute of Standards and Technology (NIST) has come to exactly the same conclusion in their reports submitted to the EAC (Elections Administration Commission) on the need for software independence in the voting process.

What exactly is software independence[2]? This is a classic study in simple logic. It is useless to ask the computer that is collecting your vote for details of how it is recording your vote. Quite simply it can change your vote and you will have no way of knowing. Therefore logic theory

[2] "One should strongly prefer any approach where the integrity of the election outcome is not dependent on trusting the correctness of complex software." (from Software Independent report http://vote.nist.gov/SI-in-voting.pdf by Ronald L. Rivest (MIT), John P. Wack (NIST)).

requires that instead a second independent computer is needed, that will also display to you how your vote is being counted. So that if both computers do not agree then you will be able to discern a problem. Also because the first computer is being physically prevented from knowing how the second computer will display your vote to you, it cannot risk changing your vote surreptitiously. Similarly the second computer is prevented from collaborating with the first and only knows the information that you verify and present to it. Figure 1 illustrates this logic concept.

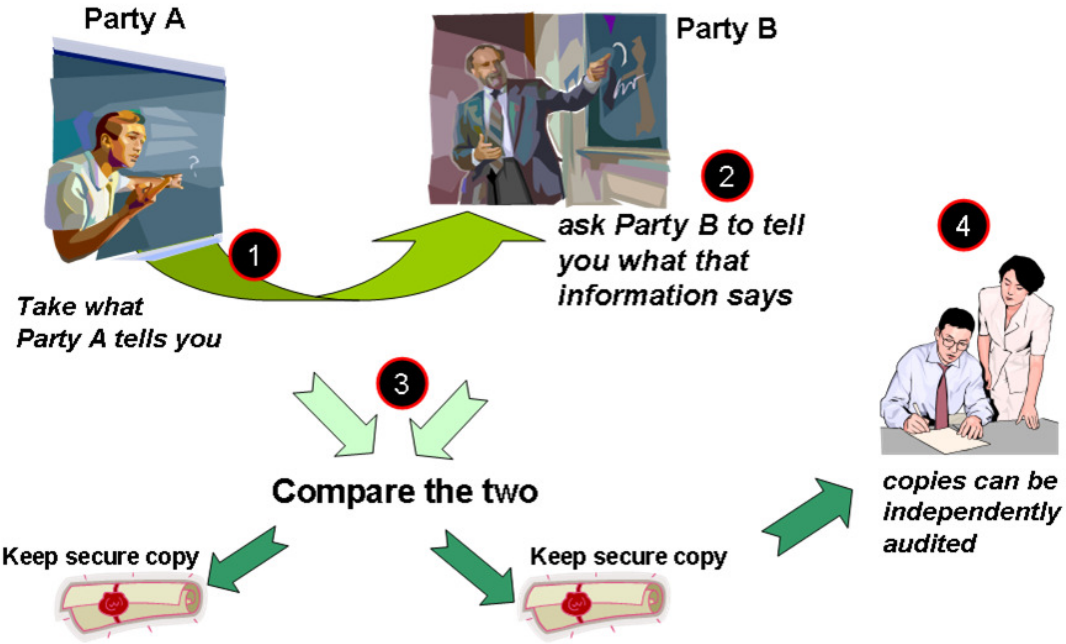


Figure 1 – Logic of independent verification to create trust and auditability

We can see this simple principle at work with a computer aided paper ballot writer and scanning. The idea is that the first computer produces your ballot selections on paper, and then the second computer then independently verifies those. Here the computer and paper are working together, not trying to replace one with the other but instead using the strengths of each to enhance the voting process and we will now step through and illustrate this. Figure 2 below here shows the complete process using software independence techniques and the OASIS EML records.

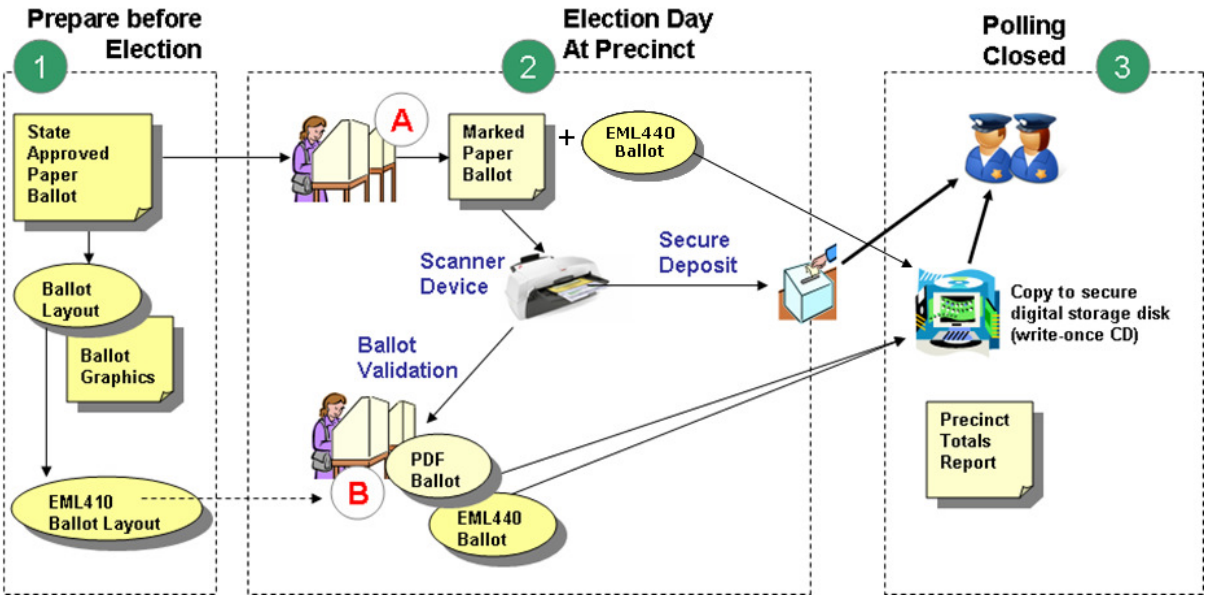


Figure 2 – Software Independence via verified paper ballot voting

In the first instance (Step A – Figure 2) a computer displays to you a scanned digital image copy of the actual official approved paper ballot to be cast. You make selections for your vote by clicking with a pointing device on the appropriate check boxes you wish to select. Notice three things here:

- First because the scanned form is a fixed digital image the computer displaying the ballot cannot interpret the information directly, nor manipulate it, whereas the human can see, read, interpret and verify the choices.
- Second the computer records your choices anonymously based simply on positional coordinates that you click with the pointing device. It has no notion of what those choices represent.
- The logic and programming are simple and consistent, can be precisely verified, and can be reused regardless of the actual ballot and election.

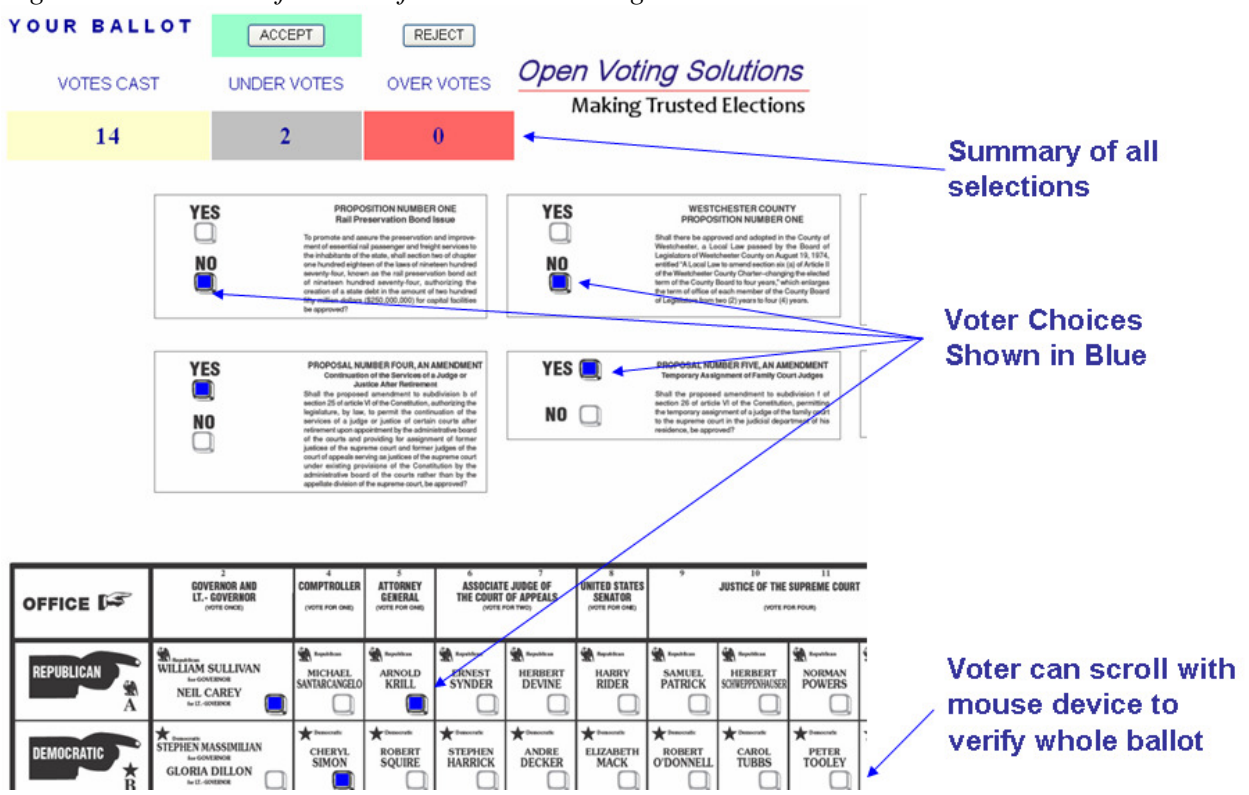
Your selections are recorded by the computer and stored digitally. The computer then prints out a paper ballot with your choices (this can also be made independent so the voting computer cannot directly control the printer itself). This completes Step A in Figure 2, and the results are your paper ballot and its matching digital record (EML 440).

You then physically carry your printed ballot to a second independent computer for scanning and tallying. What you are ensuring is that there is no way for the two computers to covertly signal each other by establishing a physical separation.

Now the second computer scans the paper ballot (Step B – Figure 2), shows you the selections you made visually against the image it made of your ballot and checks for under or over votes and alerts you accordingly. Next you confirm those choices and your scanned paper ballot is then mechanically deposited from the scanner into the secured ballot box as a permanent record of what the computer has also electronically recorded. The recorded information is stored in open public formats that the OASIS EML provides that any computer savvy person can then inspect, compare to the paper ballots and verify as needed (EML 440 and scanned PDF image).

This process is illustrated in Figure 3 below where the voter confirms that the machine really has accepted their ballot as they intended (this example is for an actual New York ballot).

Figure 3 – Voter Verification of Ballot Processing



So now we have a complete chain of custody with three independently generated records of the vote; one from the original computer that printed the paper ballot; one from the second computer that scanned it; and then the paper ballot itself.

Notice this is vastly different from most optical scanning systems in use today that simply scan in the ballot and give an audible "beep" to confirm that your vote was recorded. What vote? How do you know how the computer interpreted the marks on your paper ballot? There is no way for you to know and in fact what we have there is simply the digital equivalent of "hanging chads" because during a later audit how would you know that the second time the computer scans the ballot it is actually making the same determinations as the first time?

However in our example of a software independent process[3] we can see that a later audit can crosscheck from all three sources to verify that the totals obtained actually correspond to the wishes expressed by the voter.

This brings us to a further real safeguard that is in a verifiable auditable process. Kathy Dopp, another mathematician and statistician, understands that very well, and she has been working on algorithms not to hide or encrypt votes but to increase confidence that a true and proper election took place, or at least to know when a certain result looks odd and in need of deeper

[3] White paper "Do Paper Trails fail to secure eVoting?" provides software independence definitions – http://www.openvotingsolutions.net/material/Do%20Paper%20Trails%20fail%20to%20secure%20eVoting.pdf

investigation (see http://electionarchive.org). For the ancient Greeks this was all part of the process, they broke open their jars, counted the stones, and compared the total numbers to the overall number of citizens entitled to vote and of those who actually had voted. Of course those same principles apply today, but the challenge is in metaphorically breaking open the computer and tipping out a pile of counting stones is not so simple!

However there are solutions to this as well. Notice we stopped above at the point where we have three independent records of the votes cast. The next step is to actually tally the votes. So far all we have recorded is the positions selected on the ballot form in an anonymous coordinates set of points. Next we need to take those and total up the counts for each of those "stones". Notice at this point the computer still has no idea what those coordinates represent; they are still anonymous point references. That is very good. This again makes it very simple to write a transparent computer program that only counts like-points and totals them. And that same computer program can be reused unchanged for every election and inspected and tested to make sure that the program steps are doing nothing more and nothing less.

Here we should mention open source software programs. Again the article "Clean Elections" is tellingly silent on this topic. For many it is a fundamental principle that the software used in elections must be open source. This permits independent inspection of the software and also independent verification. Unfortunately those involved in developing exotic art based on cryptography and mathematics see it as their trade secrets and rights to retain all software code and not reveal it publically at all. Instead they want to have "black-box" testing to verify that their software is working correctly and providing accurate results. This is total software dependence and the antithesis of what software independence is all about.

Notice that the sets of computer records that we created previously are completely anonymous, and yet they establish a chain of custody by polling place and voting machine that can be independently crosschecked. The California Secretary of State has taken an important first step towards this by publishing 2006, 2007, and 2008 election results using the OASIS EML 510 formats for reporting elections (http://www.sos.ca.gov/elections/ca_elect_results/result_example.htm). This gives county by county details of all voting totals.

The related OASIS EML 440 records carry the actual ballot level details and those would be the next step in this public accountability of the voting process. Given EML 440 records and open source tabulation software, any citizen with a compatible computer can then potentially follow the instructions to run the software and verify that the totals published in the EML 510 are correct. Also of course these open records can be converted into spreadsheets and then analyzed using the statistical approaches that Dopp and others have developed.

Given all this how far away are we from attaining software independence and open source for public elections? The design described above using OASIS EML has already been implemented in a prototype and demonstrated and the software placed in the public domain at the EML Voting project (http://www.emlvoting.org). A second open source component has been developed by the Open Voting Consortium in collaboration with computer science students and faculty at several campuses of the University of California and it utilizes the pre-scanned techniques(in Figure 2 Step A) to ensure anonymous ballot handling by the ballot writer and scanner component.

However several important barriers exist to moving all this open source work to wider adoption. The largest is the requirement for formal development and certification testing as stipulated by

the EAC for voting systems in the USA. This costs significant resources running into hundreds of thousands of dollars. While the State of New York election board passed a resolution in principle to support funding for open source certification it has not followed through any further on that. It is however only a matter of time before the right combination and opportunity presents itself to formally complete the open source work described and already underway.

In the meantime public election officials and administrators will continue to receive proposals from academic sources because such projects in cryptography provide a perfect outlet for the mathematical skills of doctorial students and associated funding for their tutors. Unfortunately while well intended these projects do not align with the fundamental concepts the ancient Greeks understood for democracy. The democratic process is not one that can be "owned" by any individual, enterprise or corporation that controls and manages it. It must be publicly accountable and transparent.

Creating software independence in solutions is challenging and some universities computer science departments are seeing this and getting involved in the open source challenge notably those from New York University and as noted previously University of California and UC Berkeley. Particularly it is insightful for computer science students to understand the challenges of designing and implementing logically complete yet simple, elegant and intuitive processes that are secure and resistant to corruption. Too often today complexity is the result in computer systems because it is easier to design complexity.

The role of open public standards is also critical here ensuring that voting systems are interoperable and components are interchangeable. This creates a broader and open marketplace where new and better solutions are able to easily fit into the existing infrastructure without election authorities having to discard entirely their systems and purchase over again.

These are not only problems and challenges here in the United States, the effects are felt globally where support for better democratic processes are critically needed to allow people to freely express their political choices.

We can make computer systems that fulfill all the needed criteria but this however does require a systematic public coordinated and collaborative approach to achieve this and these are what have been sadly lacking under the current administration in the White House. Instead it has been continually fixated with allowing private corporations free hand to exploit marketplaces regardless of the consequences.

David RR Webber,
Senior Member of ACM,
Member OASIS EML TC,
CTO Open Voting Solutions, Inc

drrwebber@acm.org