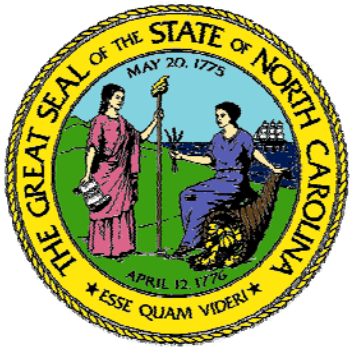
End-to-End Voting Systems
A State Perspective



Presented for
State of North Carolina
By
Stephen Berger

Introduction

This presentation offers the perspective of a state election official on end-to-end (E2E) voting systems. To evaluate any proposed improvement to the election system it is important to properly frame the issue, identifying the criteria by which it is to be evaluated. Any proposal must be evaluated for both its positive attributes but also its own vulnerabilities and limitations. Nothing is perfect and with every improvement there are associated security risks and potential problems. It is important to have a balanced evaluation. Further, elections are resource limited, resources applied to one area are generally withdrawn from another. It is therefore important to understand both sides of the equation, the positive contribution made by the improvement and the degradation that will occur as a result of decreased resources.

With any change there are transition issues and some degree, perhaps a large degree, of disruption. A proposed innovation may offer good improvement after it is established but transition issues may be so formidable as to block its deployment. It would simply be irresponsible to have several confused and error filled elections on the way to bringing about a change, even if potentially offers long term benefit.

Any proposed innovation must compete against other proposed innovations. Only those that bring the most improvement to the complete election process should win the competition for implementation. In this area it is important to observe that there is objective improvement and perceived improvement. With elections making improvements and having the public perceive that there is improvement are both very important. Generally a new proposal must bring a benefit both objectively and in the public perception.

The paper next explores an area that clearly calls for further work. That area is the use of mutually supportive and reinforcing processes. In engineering it is well established that reinforcing structures can multiply the strength of an assembly. Similarly security defense-in-depth, detection mechanisms and redundancy appear to have the potential to similarly multiple the effectiveness of elections.

The paper concludes with a presentation of recent innovations introduced by the State of North Carolina. These innovations, while not directly introducing an E2E voting system, introduce some features in common with E2E voting systems. Notably the North Carolina statewide election reporting system provides a public accounting of every vote from the total back to the precinct from which it came. Using precinct records every vote can be trace further back to the machine or ballot box. Thus any interested party has the ability to deconstruct an election and spot any anomalous inputs.

Contents

Framing the Issue

In evaluating End-to-End (E2E) voting systems, or any other innovations in elections it is important to first establish the context and criteria to be used. From a state election official's perspective that context includes:

1. Understanding the consequence for the complete elections process, not just the voting system
2. Understanding the impact on election satisfaction, of which confidence is a sub-topic
3. Evaluating the resources required
    a. Both the quantity of resource and the type of resource must be understood
    b. Both the resource required directly by the innovation but also the typically greater resources required to introduce an innovation
    c. Finally the areas that will receive fewer resources and the consequential impact of that must be understood
4. How does this innovation compare with alternative solutions

Complete Election Process v Voting System

From the state's perspective it is important that the complete election process be secure, reliable, accurate, user friendly and accessible. In addition to the election process having those attributes voters must perceive that elections are accurate, secure and accessible to them. From this perspective the voting system, meaning the equipment used to support elections, is a component of the election process, albeit an important component.

Ultimately it is the complete election process that must be improved. Proposed improvements of any single component must prove that they also result in improvement to the total process.

Public Satisfaction v Public Confidence

With elections public satisfaction must be treated as a separate issue. An election process and the voting system it uses may be entirely accurate, secure, reliable and very easy to use. However, that does not insure that the public will perceive it that way. Conversely it is entirely possible to have a flawed or even corrupted election process that the public believes was accurate and fair.

Public confidence is a sub-topic of public satisfaction with the election process. There are many issues that people would like to see improved. An election official is responsible to continually work to increase public satisfaction. That means that scarce resources used to address one issue are not available for another issue. The challenge for an election official is to identify the issues where there is the most dissatisfaction that can also be improved and then apply resources to implement that improvement. Sometimes public confidence is the largest issue but sometimes resources are better applied to address other issues, like time spent in line to vote, speed of reporting results or accessibility of voting for people with disabilities.

Election officials must ask if public confidence is the limiting factor for public satisfaction with elections? It may well be and at times is true that long lines at the polling place or slow reporting of results are more important issues for most people.

Public Confidence – The Trust Issue

When it is decided that public confidence is an issue that needs to be addressed, the question must be asked of any innovation, including end-to-end voter verification, "Will it increase public confidence?"

In any security system we must start with something we agree can be trusted and build out from there. The problem with elections is that there is nothing all of us agree can be trusted. Therefore there is no solid foundation from which to build.

Most Americans accept that we must trust our election officials, operating under appropriate checks and balances, under supervision for their superiors. Not everyone would agree with this premise. However, because it is the majority view and because there are not many alternatives the current election process, including the certification and operation of voting systems, is built from that premise. Most people believe that we have good elections and that we can trust our election officials. They further believe that in those cases where that trust is violated there are sufficient checks and balances to identify the breach and remedy it.

While most people trusted their elections, including those using DRE's, some did not. VVPAT was introduced as a method of increasing public confidence. Its proponents would argue that

VVAT has multiple benefits; increased public confidence would be one of the leading benefits in their view. So while most people trusted elections using DRE's presumably a greater percentage would trust elections where there is a VVPAT in conjunction with the DRE.

The question must then be ask, "What percentage of the population still does not trust the election result and why would they trust an end-to-end voting system?" An end-to-end voting system simply replaces one black box for another. The DRE for most voters is a black box and some do not trust it, although most do. The DRE with a VVPAT still is a black box, forwarding its contents into a bigger black box, the accumulation and tally system, and some do not trust it, although most do. ***So why would those voters who do not trust any of the current systems trust an end-to-end system, presumably verifying their vote over the internet?***

There are at least two serious concerns with E2E voting systems. The first is that it is susceptible to coercion, both positive and negative. Negative coercion would be when a boss requires that a worker show that they voted to the companies satisfaction as a condition of employment. In this case the voter, potentially would be opposed to the attempt. With positive coercion, "I will give you a 12 pack if you vote the way I direct.", the voter may be supportive, even enthusiastically support the subversion. E2E voting systems must have a solution for both types of coercion.

A second issue challenging E2E voting systems is the malicious and intentional misuse of the process. In a close race a candidate could have a few voters lie about their vote being accurately reported simply to bring doubt and a recount. This could even be implemented as a long-term, multi-election strategy to gain support for a change of party. Such charges would bring doubt into the minds of other voters as to the integrity of the process. In the face of such an attack, would E2E voting systems increase or decrease public confidence? Hypothetically the answer could go either way. The challenge for proponents is to present objective, compelling evidence that this risk can be effectively mitigated.

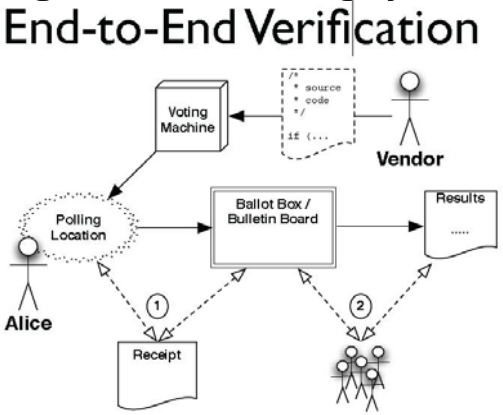
Figure 1 – DRE Voting[1]

Figure 2 – DRE with VVPAT[2]

I don't trust it!

I Still don't trust it!!

Figure 3 – E2E Voting System[3]



Why would I trust it now!!!

[1] Illustration from: http://www.huffingtonpost.com/2008/11/04/amazing-voting-images-pho_n_141136.html
[2] Illustration from: http://porukki.weblogs.us/wp-content/uploads/2009/05/election.jpg
[3] Illustration from a slide in a presentation made by Ben Adida, Harvard University, " (Electronic) Voting Security" presented at the Workshop on Electronic Voting, IDC Herzliya, 17 May 2009.

There have been cryptographic voting schemes proposed for years. The notion of being able to prove that your vote was counted without being able to prove how you voted is very intriguing for mathematicians/cryptographers. Only a miniscule percentage of the population will ever be able to understand the foundations of crypto technologies used. This creates a theoretical limit on how transparent such a system can be. Many people oppose these schemes on this grounds.

The issue is whether or not crypto systems are too complicated for too high a percentage of the population. If people can't get the idea of filling in ovals to express their intent without requiring teams of analysts to interpret their marks, how will voters ever understand how to use a pen that marks with invisible ink or to verify their receipt with a complex mathematical computation?

So the challenge facing proponents of end-to-end voting systems is first to show that public confidence is a leading issue among the range of issues contributing what dissatisfaction exists with elections. Then they must demonstrate that their innovation will significantly improve public confidence. Finally they must show that it will do it for a reasonable expenditure of resources.

Resource Limitations

Elections are highly resource limited. There is virtual unanimity among all parties interested in elections that elections are underfunded and under resources. Election officials, election advocate and voting system vendors uniformly agree that, given their importance, elections should be better resourced. There is agreement on what should be. Election officials, unfortunately, are required to run elections using available resources and this is the source of many differences of opinion. While all agree that election officials should have more resources at their disposal, they do not and must make compromises. It is their responsibility to run the best possible election with available resources.

Resource limitations create a set of zero-sum situations. Time, talent and treasure applied at one point come from another. The question facing election officials is not whether one area or another needs improvement. Rather, the question facing election officials is what area will loose resources if another is improved and is the total election process improved by that trade-off.

Is an Innovation Supportable?

It is important to understand the resources required to support a new innovation. With E2E voting systems there would appear to be a requirement to have increased technical capability in the election process. Additional, specialized expertise would be needed in the vendors, the system certification process and among election officials and works responsible for administering the system. It is important to know what it would take to support an E2E system and where those resources, if not currently available, would come from.

Transition Issues

With every change there are transition issues. Typically implementing a new system requires more time, money and expertise that administering a system that has been in place for some time. New voting systems would have to be purchased and it is unclear where these funds would come from. Election workers, poll workers and voters would have to be educated. Those are not insignificant efforts.

With any change mistakes inevitably happen. People misunderstand their training and make mistakes. Equipment exhibits problems in widespread use that were not foreseen by their designers. A host of potential problems exists.

It is the election officials duty to assure that changes are introduced with minimal disruption. This is a separate analysis from the benefit of the change, after it has been introduced and 'broken in'. Transitional issues can overwhelm the potential long term benefits of an innovation when the transitional disruption is excessive.

Security Domains

The security requirements developed so far have taken something of a "one-size-fits-all" approach, and have failed to recognize that, in voting systems, there are two very different situations. The first situation is when the voter's identity can be linked to the ballot. A second situation exists once the ballot is anonymous and cannot be linked to the voter.

When a voter is voting, a lot of protections cannot be employed out of a need to protect voter privacy. Max Etschmaier, in a paper prepared for NIST, called this the "Voter Privacy Domain".[i]

Figure 4 illustrates where privacy must be maintained, but also the limited functionality required within that domain.

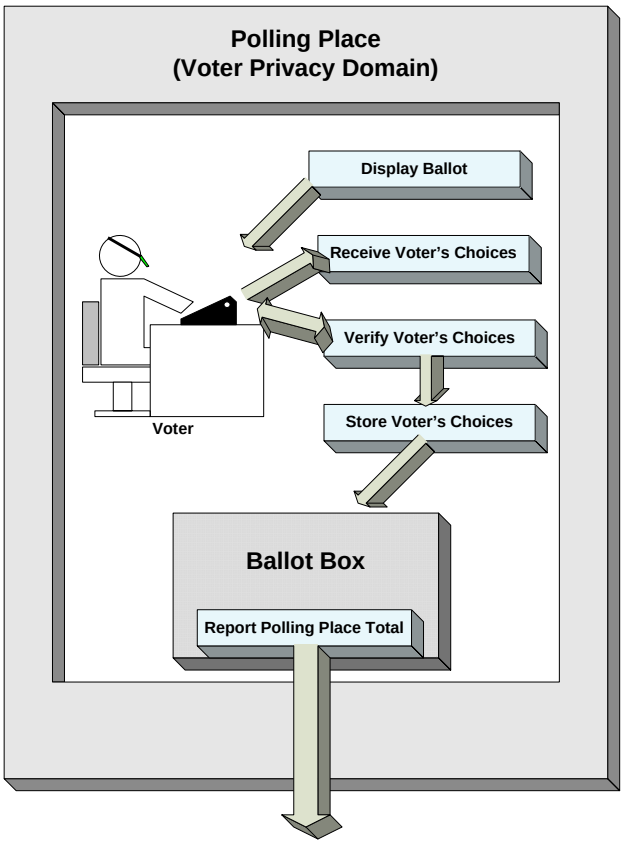


Figure 4: Voter Privacy Domain

Once the ballot is in the ballot box and separated from the identity of the voter, a different situation exists. At the point the ballot is separated from the identity of the voter, all the audit and tracking tools that are used in banking and for electronic commerce can be used. A ballot can be uniquely identified and tracked all the way to the final total. There is no reason not to have a traceable link between every ballot in the final total all the way back to the ballot box. Techniques exist and are well developed that would assure every ballot is included in the final total, and, equally, that no ballots from unknown locations have been added. There is no reason not to have this kind of solid audit data to link ballots from the ballot box to the final total.

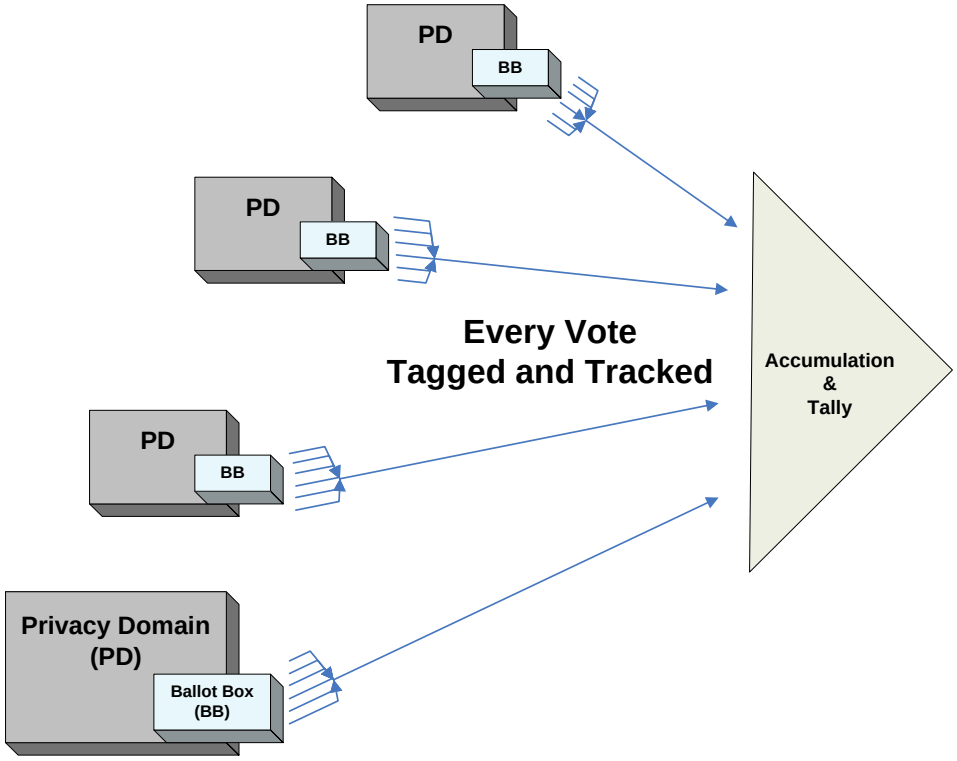


Figure 5 - The Public Domain

Borrowing from Archeology

A missing element in much of the debate about election procedures is a theoretical model building from fundamental principles and causal dynamics. One such principle is that any security system must start with something that is trusted and then build from it. However, in elections there is no universally trusted point. This is a fundamental problem. Most people will agree that, of necessity, we must trust election officials, under the understanding that they act with appropriate checks and balances and under supervision. However, not everyone will accept that premise and hence one of the challenges in designing a security system for elections.

Another fundamental principle is that confidence increases with the number of simultaneous, independent records of an event. Ultimately how a voter votes is a historical event. In archeology and historical research confidence increases with the number of independent, contemporary witnesses to an event. In an election a vote is a record of that historical event, how

the voter voted. Our confidence that we have an accurate record of that event increases with the number of independent witnesses we have and with the reliability of the transmission of the record of those witnesses' testimony.

E2E voting systems add one independent record, the voter's memory. That to be sure is an important record of the vote however it is not flawless. An E2E voting system creates its own, new problems and potential risks. Some voters have faulty memories. More seriously some voter may vote one way and intentionally lie about it to bring doubt and confusion as to the outcome of an election. This could be a strategy for a losing candidate in a close election. If this happens there are two problems. The first is how the election process would adjudicate such a challenge. The second is the damage it would do to public confidence. Such allegations, while in this hypothetical case would be completely false, would bring doubt as to the fairness of the election process.

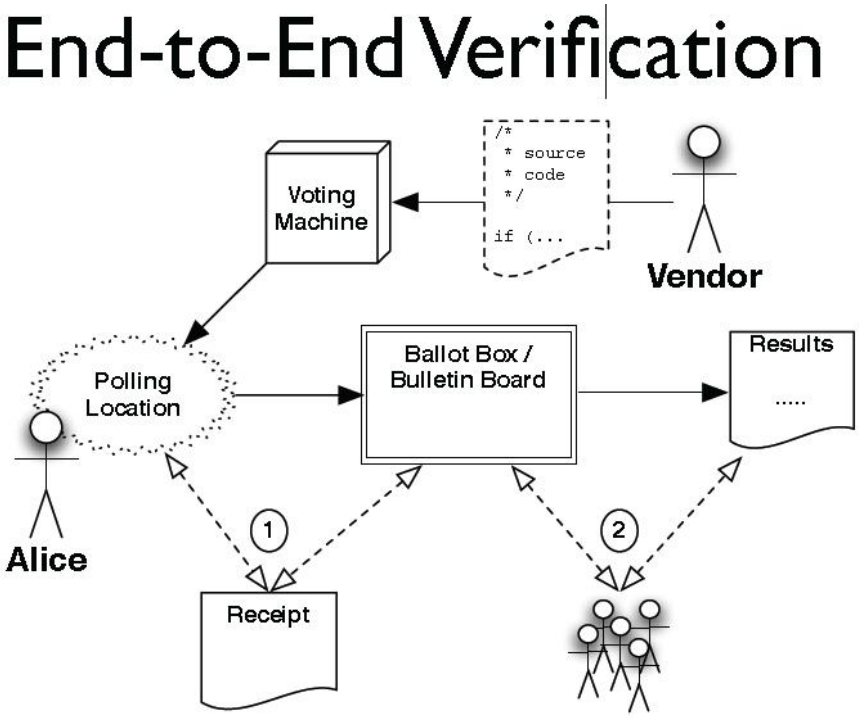


Figure 6 - Diagram of an E2E Voting System

In contrast to this approach it is possible to have multiple totally independent records of a voter's vote. Current systems are required to have multiple memories to record votes. However, all of these records go through the same processor and software. There is no reason that the outputs from the user interface could not be feed to multiple, totally independent processors and memories, provided by different organizations. Figure 7 illustrates an implementation of not only multiple memories or records of the vote, but the recording of those records through totally independent processes, potentially provided by different vendors and using different software.

Also illustrated in Figure 7 is the fact that the principle can be implemented in a variety of ways. If standardized user interface I/O and cast vote record formats were adopted there is no reason why multiple units could not simultaneously record each vote, providing independent accounts of the voter's vote. In one implementation an audit unit would simply monitor the voter's inputs and compare them to the cast vote record recorded by the primary processor. Using digital

certificates a dual-signature system could easily be implemented. The primary process would sign the cast vote record and the audit process would add its own digital certificate to the vote. The audit unit could be and probably should be provided by an entirely different vendor and operate with complete independence from the primary processor.

An alternate embodiment would simply use multiple parallel processors, using different software and separate memories. Here again multiple vendors could provide the units, increasing significantly the chance for intentional or unintentional misreporting of the voter's vote.

These are alternatives or complimentary options to E2E voting systems. They are not mutually exclusive and might be mutually advantageous. However, like E2E systems, would require careful analysis in support of a decision to adopt or abandon it.

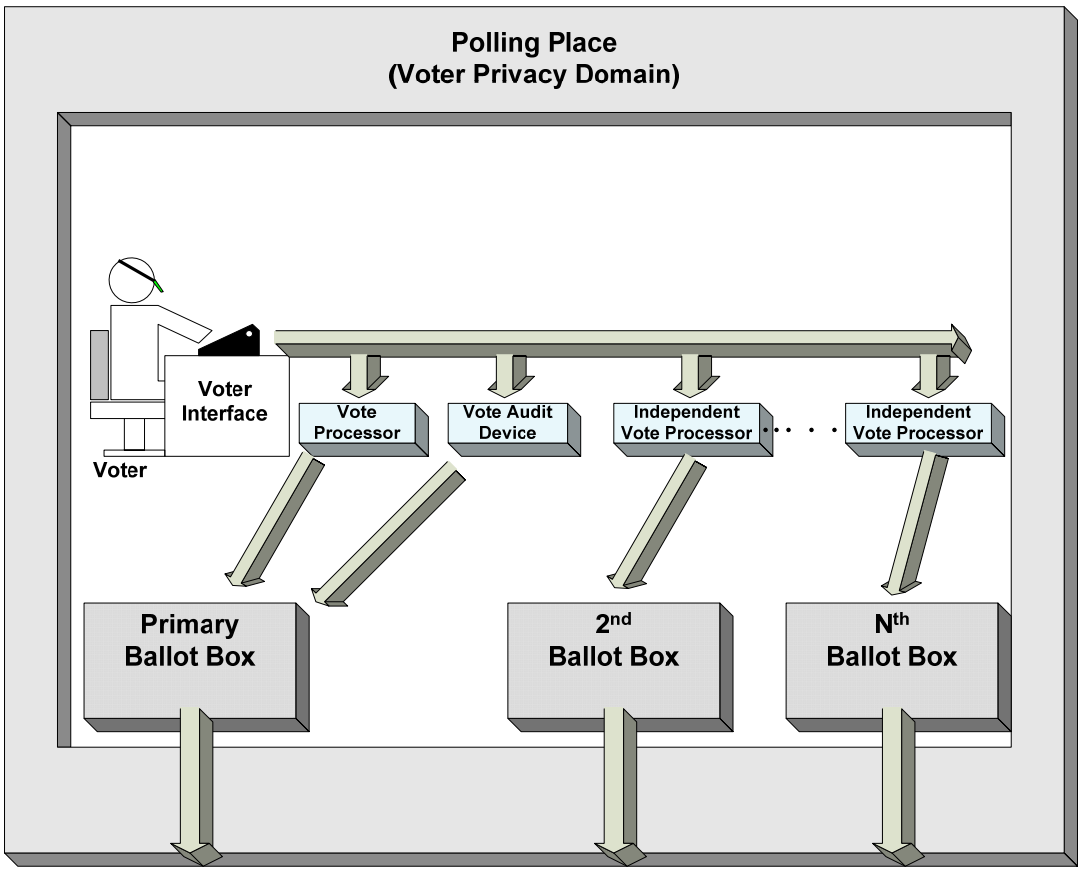


Figure 7 - Implementing Multiple Independent and Contemporary Records

Compounding, Interacting Changes

We now shift from a focus on E2E systems to the current state of the election process. This is done to examine how an E2E voting system contributes to current, not past, election processes. A lot has changed in voting system certification since the 2000 presidential election. The EAC was created. It has established its Voting System Certification Program, which this year certified its first voting systems. NIST National Voluntary Laboratory Accreditation Program (NVLAP) has been given a role in certifying Voting System Test Laboratories (VSTL). The EAC has

published guidance of best practices in election administration. State laws have changed. State and local officials have implemented a wide variety of reforms and improvements.

At this time the full benefit of these changes has yet to be experienced. Certainly their benefit over time remains to be seen. Further, the unintended consequences, both positive and negative, are not yet know. Any further innovations will enter an environment that is very different from the pre-2000 or even the pre-2006 environment. It is completely conceivable that new innovations will either prove to be unnecessary or even counter-productive.

It is entirely conceivable that, given the reforms that have been introduced, doing more of the same will start doing more harm than good. Fundamental and needed changes in how voting systems are tested, certified and safeguarded have been made in the past 8 years. However, further improvements in total election accuracy, security, reliability and usability will possibly require new approaches focused on different issues.

Few systems improve by linearly extending what has been done in the past indefinitely. As the first round of changes made in response to the 2000 presidential election are making their impact, further improvements are seldom obtained by simply 'doing more of the same.' A next generation of improvements will likely come from innovations in new directions.

Mutually Supportive Processes

One clear area for improvement is to align current processes so that they are mutually supportive and reinforcing. Currently most processes operate largely in isolation, and coordinate them so that, in combination, they multiply the total effectiveness. There is potential for significant benefit through enhanced coordination, so as to align efforts from different processes to be mutually supportive and increase the value they make to each other.

EAC-NIST-State Coordination

A principle cooperation exists between NIST NVLAP and the EAC's Certification Program. NVLAP has the responsibility to assess and recommend laboratories to the EAC for accreditation. It then is responsible to monitor those laboratories' ongoing compliance with ISO Guide 17025, General requirements for the competence of testing and calibration laboratories.

In a nutshell, NVLAP is responsible for assuring that voting system test laboratories (VSTLs) have the ability to do a good job. The EAC on the other hand is responsible for reviewing the test plans, test reports and recommendations for system certification coming from the laboratories. The EAC decides whether to certify a voting system, and it relies on the testing at the VSTLs to make that determination. The EAC must examine the work product of the VSTLs and decide if it is up to expectations. Clearly, there is a lot to be gained by assuring that the assessment of a VSTLs ability to do good work, and the ultimate quality of the work it does produce is tightly coupled and using a common set of quality metrics.

Another critical cooperation is between the EAC's Certification Program and state certifications. In general, states have only the most general understanding of what is done at the national level. The result is that state testing is often either redundant or alternately misses the same areas missed in the national program.

Ideally, the national program should test a core set of specifications common to most states. This saves the individual states from dealing with these issues. State certification can then focus on the specific issues and practices of that individual state. National certification intends to

demonstrate the overall capability of a voting system. State certification should seek to identify systems that meet the specific needs of each individual state. There is overlap in these concerns, but there is also a great deal of difference.

The EAC's Director of Certification has held many meetings with state officials to discuss this and related issues. In January 2009 he announced a pilot project to explore implementation of closer EAC-State cooperation.

The ultimate goal of all these efforts is to assure well run, accurate and secure elections. The top priority is that local election officials be able to use the voting system to run good elections, and to create records that prove that they ran a good election. The national and state certification programs could do more, through closer coordination of their efforts, to assure that local officials have the tools they need, and that those tools have been tested and proven to be reliable and effective.

System Reinforcement

What has been relatively unexplored is the potential to extend system reinforcement. A central issue facing elections is analyzing what it is ultimately dependent upon. In the past paper ballots relied on the ability of people to accurately count them. For security, election administration procedures were relied upon to assure that the ballots cast were accurately, counted and included in the vote tallies. Unfortunately, the system of people, paper and procedures had a high rate of inaccuracy, human error and were susceptible to malicious tampering and fraud.

To reduce human error, automation was introduced. Voting machines dramatically improved the situation by replacing counts by people with machine counting. Security was improved by creating multiple separate electronic records of each vote. Multiple records make it much harder to commit fraud because, to be successful, all copies must be changed. However, computerized voting systems have their own problems and vulnerabilities.

In general, the debate has been framed (largely by the popular media) as a choice between people and paper or computer systems. This is a false dichotomy, and one that has drawn attention and resources away from a much more important exploration. The more productive question is "What is the best combination of people, procedures and electronic system to achieve the best total result?"

What is starting to emerge is a "4–vote" system. Increasingly, the following elements provide checks and balances to assure secure and accurate elections:

- People following election administration procedures;
- Computer-based voting systems;
- Historical trends and polls;
- Independent system audit and computer forensic evidence.

The coordination of people and voting systems following well-develop election administration procedures is relatively solid. It is the last two elements that are less understood, especially the growing role of computer forensic techniques in elections.

An enormous and sophisticated body of expertise has been developed to help candidates running for office. Historical voting trends are maintained, often down to the individual precinct level.

Polls help candidates judge how well their campaign efforts are fairing. We are all familiar with exit polls and other mechanisms for monitoring voters' opinions. What is often unrecognized is the roll this plays in election security. When election results come in that are out of line with historical trends, polls or the expectations of a candidate, calls for an investigation are common. As a trigger for an investigation, this body of information forms a pretty good safeguard. After all, it would be pretty hard to rig an election without the vote totals looking odd, and triggering a call for an investigation from the loosing candidate. Although far from perfect, it is an important safeguard.

The increasing use of computer forensic techniques is creating even more interesting benefits. An array of techniques are available, and state and local officials are starting to employ them.

One growing trend is the use of digital file signatures, commonly called HASH codes, to assure that voting system software has not been modified or tampered with. The Georgia Election Center at Kennesaw State has created a self-booting CD for the state of Georgia. When a system is booted from the CD, every file used by the voting system, including those files the voting applications use in the operating system, is examined and its digital signature is compared to the certified version of the software. The check takes 1.5 to 2 minutes and gives a GO/NO GO result. The check can be made before, after, and even during an election.

Parallel monitor testing is another growing tool being used. In a parallel monitor test, sample voting devices are pulled out of service and brought to a test location. The machines are then voted by people using scripts. Typically cameras record every keystroke made during the test. At the end of the election day, the totals are compared to what is expected from the scripts that were voted. The machines don't know that they are part of a test. If there is any malicious or malfunctioning software, the monitored test will reveal a difference in the total, leading to an investigation of the source of the discrepancy, and how widespread it is in the machines used in the actual election.

Other forensic tools are available but have not yet been applied in elections. One technique that security experts use in other areas is to run a separate monitor program simultaneously with an application. The monitor program, as an example, can monitor all reads and writes to election data files. Because all voting software is source code reviewed as part of national certification, the routines that will legitimately read or write election data are well known. The software that legitimately does this is both source code reviewed and extensively tested to assure it is secure and accurate. A monitor program could then simply confirm that only the expected software read and wrote to the election data files. If any other software accessed these files, a record and trigger for an investigation would be created. If the monitor program is provided by an organization separate from the voting software vendor, they become independent actors.

The North Carolina System

North Carolina Director of Elections, Gary Bartlett, and Keith Long, that state's Voting Systems Director, have introduced an innovative new reporting system for the 2008 primary elections that illustrates how new innovations can simultaneously address multiple issues. A web based election reporting system has been implemented that speeds reporting of election results but also improves the uniformity of election administration and utilizes the difference between the public and private domains. Because the system is web based, results are available to the public as soon

as they are reported to the state. The improvement in speed of reporting has proven very poplar with the media and the general public.

The new system also brings improved uniformity and additional checks to election administration. In a process not seen by the general public all counties must report totals form all machines to be used in an election as part of their election preparation. All results will, of course be zero before the election starts. The new process confirms that all machines, statewide are starting the election with a zero total. In the past the zero total check was only done at the local level and occasionally mistakes were made. The new process adds another check that all machines have been properly initialized and are functioning properly.

A very significant aspect of the system is how it makes use of the fundamental difference public and private domains in the election process. In the North Carolina system, election results are reported through the North Carolina State Board of Elections website. Voters are able to monitor results as they are reported to the state, and the results in the total can be traced back to individual precincts.

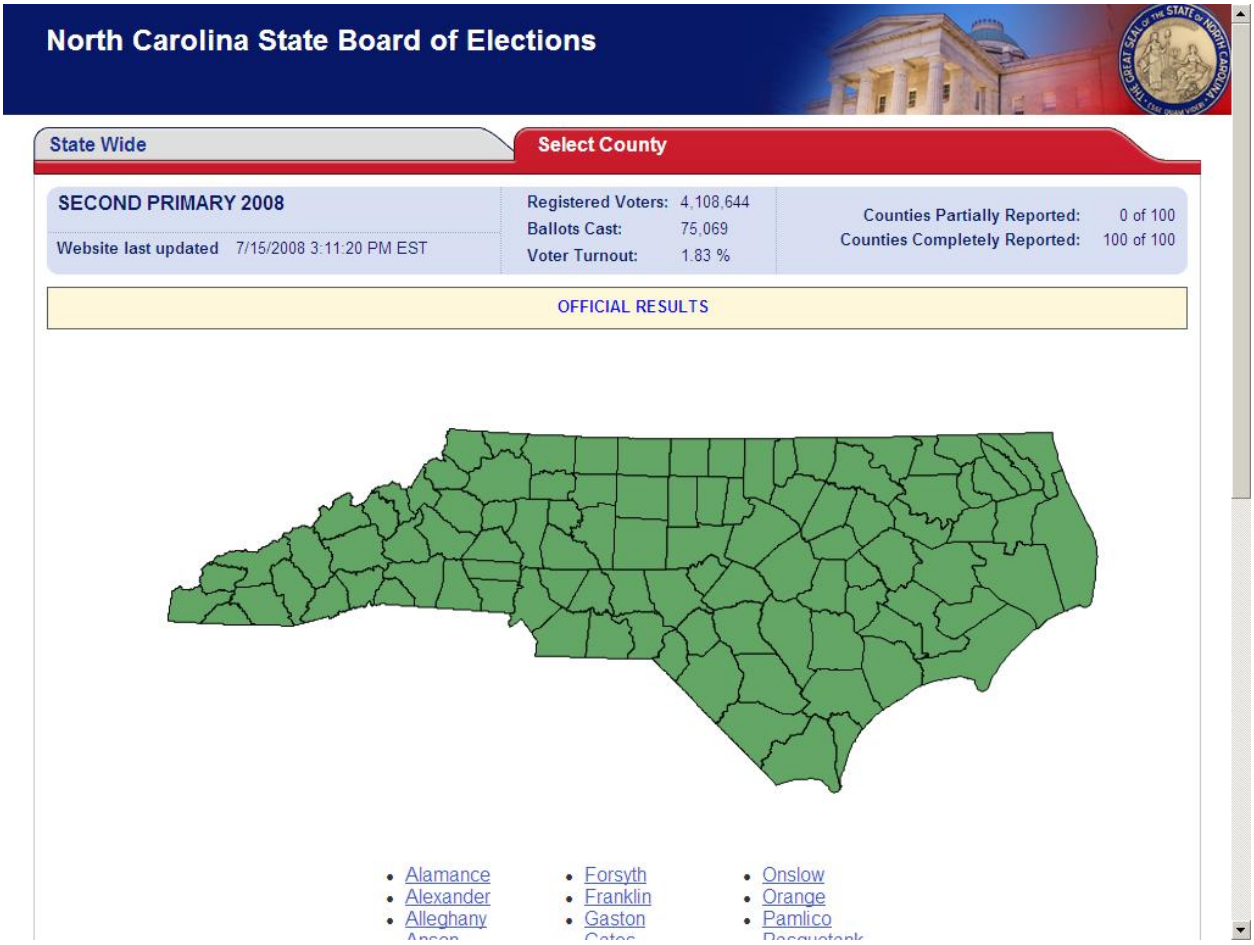


Figure 8: North Carolina's innovated election reporting service

In the North Carolina system, any voter, candidate, party or interest group can go to the state elections reporting site and view the state map with counties showing and get the statewide totals. Clicking on either the county name, listed below the map or on the county in the map

opens up a page with the county map, showing precincts, as shown in Figure 8. Precincts are also listed. Clicking on a precinct brings up precinct totals, illustrated in Figure 9. If access to precinct records is available the precinct totals can be traced back to individual machines or ballot boxes. Hence, every vote in the state can be traced back to a specific machine or ballot box. Equally if any votes are inserted from some other source, that can be identified by not only election officials but by any citizen or group that cares to analyze the results.

Once the vote has exited the privacy domain it can be tagged, traced and made public. In North Carolina's system all that information is fully public and available for analysis. With this process it is hard to imagine how a malicious attack could occur undetected between the ballot box and the state total. That then leaves two issues. The accurate and verified placement of the voter's vote into the ballot box must be assured. Then the integrity of the ballot box must be protected until its contents are tallied and reported into the statewide total.

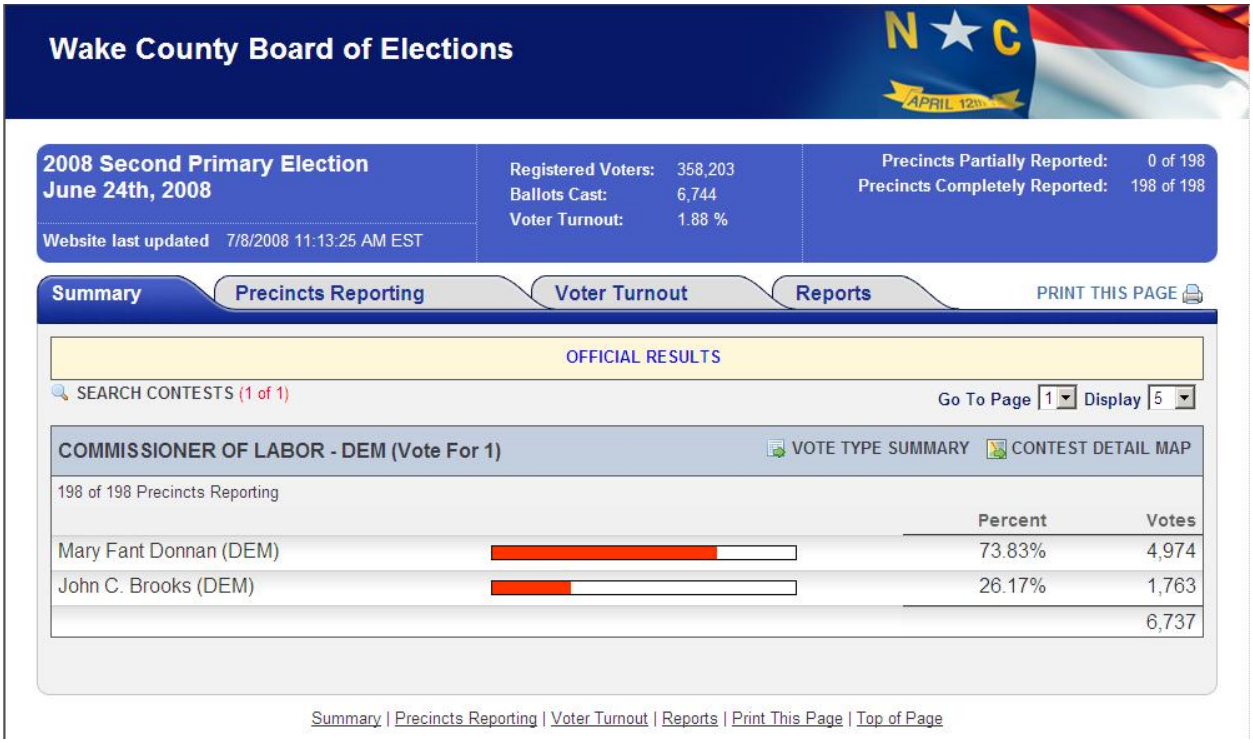


Figure 9: North Carolina's system provide reports down to the individual precinct, allowing analysis of voting trends and tracking of votes back to the precincts.

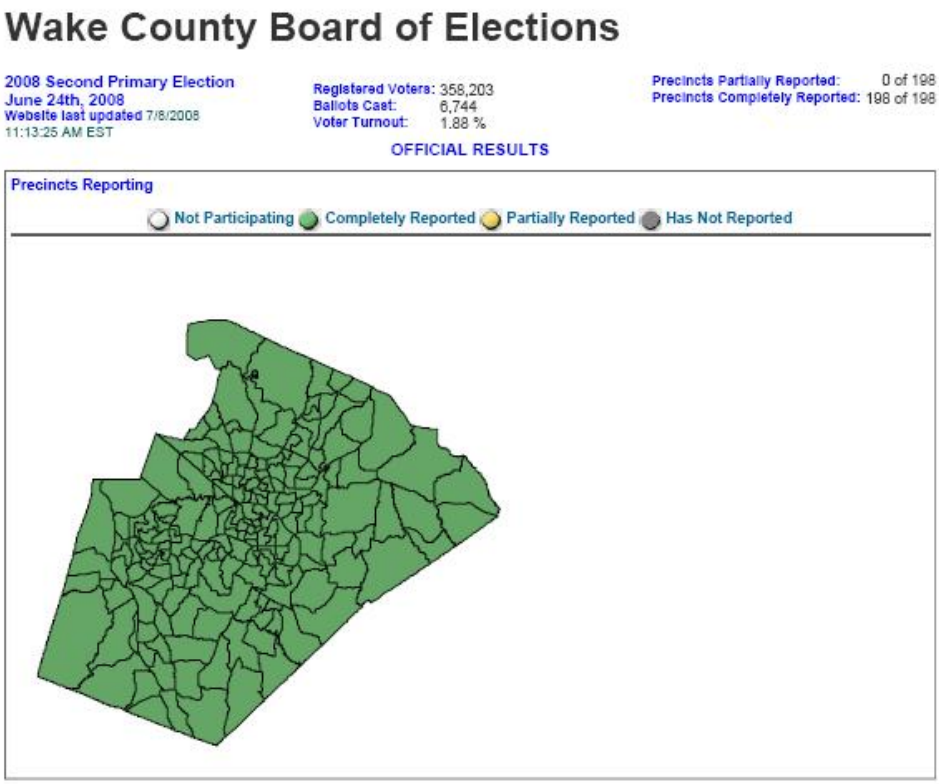


Figure 10: Precinct map of Wake Country, North Carolina

A very different situation exists when the voter is in the voting booth and the ballot and voter's identify can be connected. In this situation, a lot of security measures cannot be used because they would violate the privacy of the voter. However, the voting situation is much simpler than that facing the total voting system. In the voting booth, the following actions must be accomplished:

- The ballot must be presented to the voter;
- The voter's choices must be recorded;
- The voter must be given a chance to confirm the ballot choices and cast the ballot.

Considering the relative simplicity of the task, a number of measures can be conceived that would secure this situation. One of the interesting features of voting systems is the relative lack of using write-once media. There is little reason for not having one piece of software present the ballot to the voter and record the voter's choices on a write-once CD or other media. A second software package, potentially provided by a trusted 3rd party, could then read the recorded ballot and have the voter confirm the choice. If the voter confirms the ballot, the second software would sign the ballot on the media. If the voter chooses to recast the vote the process would be restarted and the validation software would spoil the ballot instead of signing it. Such a system essentially puts two independent witnesses into the voting booth, and creates an indelible record of the ballot.

Crafting security requirements that are situation sensitive would greatly increase the total security of the election system. Today, powerful security practices are being denied the election system because they would violate voter privacy. There is no reason to deny these practices to the entire system. They only need to be denied in the voter privacy domain, where the voter's identify and ballot can be linked. Conversely, other techniques are currently not used in the voter privacy domain because they would be too complex to use in the entire voting system. However, the situation when the voter is in the voting booth is a much simpler situation. A great deal can be done to protect the voting booth situation that would be impractical to do in the entire voting system.

---

[i] Maximilian M. Etschmaier, "Voting Machines: Reliability Requirements, Metrics, and Certification", September 2006.