Trust is Our Most Important Product

To benefit the most from our democracy we need to believe the mechanism for choosing our government is equitable. Trust let's us move forward together. Distrust can stop us in our tracks

When the election system is trusted, the battle for winning an office or deciding a question is in the realm of competing ideas, not in the rigging of a system.

Trust in the democratic mechanism for collective decision making, our representative bodies, depends on selecting representatives, and on occasion making laws, through trustworthy elections.

Trust comes in varying degrees. Election managers will best inspire trust when elections are viewed as air-tight by the layperson and the expert alike. Expert opinions alone don't deliver trust.

I've been taking a fresh look at elections after 40 years of supplying election / registration technology. My other credential for speaking to you on trust is my mathematical training at Harvard specializing in optimization through precision and simplicity.

I have been seeing a lot of discussion of security technology for elections that professes to deliver trust. Much of it is not the best choice for elections because it doesn't deliver simplicity.

In particular, I am seeing a lot of security technology and expertise being offered without the offeror or the offeree clearly defining what is being secured. If it's not focused on clear goals, why would we feel more secure? We need to define our terms clearly if we are to have meaningful discussions. We must define the terms that describe our intended election products and our proposed election tools.

I think we agree that the overall goal of elections is delivering voting results with accuracy, and with a continuous and simple presentation of methods and outputs that a lay person can see are trustworthy.

What do Elections Deliver? Let's recognize how brief the list is.

To focus our discussion at the next level, here is a list of what needs to be produced and shown to the public as convincingly trustworthy.

At its most basic, here's what the public wants to find are accurate and trustworthy:

- All votes are recorded and preserved by methods legally sanctioned to produce an official result.
- All votes are counted by methods legally sanctioned to produce an official result.
- All information that qualifies a voter to vote is kept uncorrupted and available in a master database with restorable copies.
- All electors who are entitled to vote are not obstructed / delayed by disruptive actors or events to the point of eliminating some eligible voters' votes.

Several additional efficiencies reassure the public that voters aren't being slow walked:

- All information that qualifies a voter to vote must be kept available at the polls.
- All information that qualifies a voter to vote must be kept available in the elections office.
- All information that an elections office declares essential to reach voters is not obstructed from flowing through its normal channels.

What's Old and What's New?

Don't throw out the baby just because you're offered security bath water.

Elections offices and their support vendors have always had the above responsibilities.

Elections offices have typically done great in delivering no matter what.

- They've proofed every step of the way to presenting a ballot and voter data to each voter.
- They've documented and publicized Plan A – the default plan of operations.
- They've prepared and documented and validated Plan B and Plan C.
- They've recognized when a backup plan needed to be invoked.
- They've offered transparency in the execution of Plan B, Plan C, and extemporaneous acts in the service of keeping the election integral and accurate and verifiable.

Adding computers to election data processing doesn't change the public's needs nor the basic approach.

Data needs to be proofed. Ballot data. Voter data.

Backup plans are still essential to maintain trust as a demonstration of professionalism.

Transparency must be integral in all processes to keep the public trust.

What Categories of Systems Must We Secure? The higher up the data pyramid we can protect with a bold stroke the more convincing we will be.

The rest of this paper will discuss the several data systems used to run an election from beginning to end and the most obvious means for keeping public trust in their data.

The data systems are:

- Voting Equipment to hold cast ballots including their digital counterparts
- Tabulating systems to hold accumulated votes
- Voter and elections master database systems
- Poll place database systems (poll books)
- Elections office information that voters need

We are leading up to some mechanisms for protecting data from loss or corruption. Some are fairly well implemented today. Some need implementing if we want to complete a circle of trust.

What Security Mechanisms Most Inspire Lay Person Trust?

Mechanisms for keeping trust include the following:

- Proofing
- Checking working copies against source documents
- Checking working copies against earlier copies plus change logs for the interval between copies
- Isolating data storage
- Data encryption everywhere with protocols for times that unencrypted data must be used

Documentation for the human checks is required. At a minimum, it should show that any procedures used were planned rather than ad hoc. Documentation should also show how the checks are a part of the chain of custody for data used to build an election and/or record and tabulate and publish results.

Public explanations and verification should be allocated enough time and materials to make the public feel invited rather than that they are intruding.

Back to the data systems.

Cast Ballots including digital counterparts

Voting equipment is almost unique in the realm of security management. Voting equipment's security requirement is to assure that votes are kept uncorrupted and secret until they are tabulated.

Other computer systems in elections and other computer systems in most environments are for delivering and presenting information.

Cast ballots have been shown to be securely managed for several decades. By prohibiting any connection of voting equipment to any network or equipment outside the polling place, voting equipment met a criterion for data protection that the lay public could trust.

Of course, certification is essential for bolstering the assertion that the isolation is real. Certification is also essential for documenting that the product records and preserves votes as cast.

Tabulating systems to hold accumulated votes

Tabulating systems are also certified. The weak link in voting systems introduced in the last five years is the assurance that bar codes specifying votes cast on each individual ballot are true to the voter's intent.

Tabulation systems themselves are verifiable because their results can be repeatedly checked by hand counting or by counting with a different open source mechanism using OCR of the contest names and voter selected choice(s). Also, such repeated auditing can verify or contradict the assertion that the bar codes perfectly match the voters' choices as printed in human readable language.

Master database with restorable copies

The master voter and election database is considered the most likely subject of attack today. Several state databases were breached in 2016. County database managers reported attempts to probe their databases that year. A vendor was reputedly phished.

We all know that security products are not 100% successful at preventing internet-based attacks. They are like most engineered products – aspirational but not perfect.

Here's where the election management community needs to define its own solution if it wants to anoint the master database with the same level of trust as the voting components of elections.

At the cost of some inconvenience and money, this can be done. Voting systems show us the way. The military and intelligence agencies show us the way.

Isolate master database servers and networks and backups from the internet.

This is lay person simple. The market technical “solutions” bring this image to mind: “Sure you can swim safely in an algae covered pond with our germ repellant. It’s 99% effective”.

Database security is a matter of will power to suffer inconvenience and a matter of modest dollars (compared to a voting system) to purchase and install.

Instead of keeping your databases and processes in the middle of a crowd of other technology – isolate it all and you can finally realistically assure your constituents that their election data is safe.

OR

Let the generic security market sell you their latest and greatest which works most of the time.

Voter and elections poll place database systems (electronic pollbooks)

Voter check-in solutions occupy a narrow slice of the computerized universe. When in use, they are constantly being proofed for correct and current information via voter interactions. Most computer systems are used without checking that the user’s personal information is correct and up to date.

Defining security for voter check-in products is simple. When a system produces a result that a voter or poll worker challenges, call downtown and find out if the master database has it right. If so, diagnose the check-in product and fix the situation according to the evidence. Worst case – invoke plan B.

Check-in products are constantly under observation by poll workers and voters. This greatly reduces the likelihood of an unauthorized person getting direct access.

Also, voter check-in computers eliminate almost all hacking vectors by locking in their single application, locking out other programs, and by blocking browsing.

Voter check-in products could be abused but the scope of inconvenience would be very limited – typically to one computer and one or several voters. Since the abuse requires physical access and can lead to jail time, securing against USB sticks or Bluetooth scanning from within the computer is just another symbol of concern - not a needed tool.

Since check-in products serve a broad array of functions that facilitate voting and poll place administration, deploying jurisdictions would do well to concentrate on testing and proofing rather than locking down. This is what we do with almost all software these days including ios, Windows, and Android which you can’t avoid recognizing are products all poll books use. Stating your product or a product you certified in a laboratory is inviolable when it’s based on an operating system with hundred of thousands of documented bugs is not convincing.

Voter check-in system certification that included a binary lockdown component has been a farce from the outset. How can I tell. It costs several million dollars to get voting software certified. It costs just one 1/1000th of that amount to certify voter check-in systems.

Were we to go to voting equipment deep certification, we would be no more secure because we are already secure to the 99.999th percentile. Meanwhile, we would also make these poll place computers much less functional because every added function would cost tens or hundreds of thousands of dollars to certify and would still come with their own risk of uncaught vulnerabilities.

Elections managers and policy setters will do well to emphasize functionality and utilize proofing to ensure that malfunctioning devices are removed from service. Any search for a silver bullet is just going to leave them holding fool's gold.

Information voters need

In this arena we can't have control of the information delivery mechanisms. The best we can do is utilize the most robust web delivery platforms available. Choose a primary repository for your web site for elections and back it up with a separate but also strong platform.

As robust as your state or county or city site may be it would be most reliable to isolate elections information from the other governmental web functions your jurisdiction offers.

Your security job around such a choice is to guarantee configuration parameters are double and triple checked.

One more thought on why isolation – here are screen captures showing functions that share a large jurisdiction's web site that are fairly typical of today's environments.

In conclusion, I'd like to see, and possibly lead, an effort to garner more trust for election computers while working to minimize the inconvenience.

About the Author:

John Medcalf, VOTEC CEO, was born and raised in New Jersey. John missed out on the body to be a lifeguard at the Jersey shore so he enjoyed playing with math. He won several statewide and multi-state competitions showing the Bronx High School of Science what Jersey could do. College years at Harvard because MIT didn't have a computer yet. Ten years consulting on mission critical projects like nuclear sub positioning and cancer radiation for the Saudis. Found elections in 1978 and sensed there were improvements to be made. Loved and love the people who give their all to deliver trust. No regrets.