Requirements for Voting System Security

From: Deutsch, Herb
Sent: Tuesday, September 21, 2004 12:18 PM
To: 'Ronald L. Rivest'
Subject: RE: Thanks for testifying today

Dear Ron,

Thanks for allowing me to have the opportunity to participate.

Since I believe that "perception is reality", I really feel that public misconception of the use of voting machines in elections and therefore their distrust of elections is as big a problem as attempting to improve the standards to improve voting system security. The hue and cry raised by the voting activists and conspiracy theorists as reinforced by the publication of the Diebold Source code analysis and taken up by the press has precipitated a lot of this distrust. This has created a misimpression of how elections are really run and what exposures that they have in practice.

Since elections are now under a microscope, the occasional mishap, virtually always due to human error (and then detected and corrected) is used by these nay sayers and the press to keep the pot stirred and reinforcing the public distrust. Anything reported in the press is accepted as fact and this doesn't only relate to elections. Quotes from voting system "experts" are always printed without the verification of what is quoted. It seems like the press takes the attitude that if they are only reporting what someone else claims, they are absolved of having to verify it. There is also no concerted efforts to refute these claims and, even if attempted, it's old news and doesn't make the papers.

Somehow we need to reverse this public perception to reflect the reality that elections are conducted correctly but do have occasional human error issues and restore confidence in the elections process. Making the ITA process more transparent may help this process. Of course this doesn't mean that voting system standards and voting systems themselves can't or shouldn't be improved. The IEEE effort is providing part of the vehicle for doing this especially in the Usability arena. Dovetailing in the procedures for use in a security evaluation would also assist this.

It was stated in one presentation at the hearing that "anyone" should able to review source code, not just the ITAs. I don't know about "anyone", but maybe consideration should be given to a registry of qualified individuals who sign non-disclosure agreements to have the right of source code review and audit under secure conditions. They could point out flaws to the vendor or ITA so issues can be corrected. I really don't believe it is in anyone’s best interest to have source code out there for hackers to try to find ways of subverting the code or to further stir up public mistrust even though the likelihood of successful tampering within the context of procedures used is remote.

I will include some of these points in the "Recommendations". Feel free to use any of the above "officially".

Sincerely,
Herb

0. Bio

Hi. I'm Herb Deutsch. I'm a Product Development Manager for Election Systems & Software and also Chair of the IEEE P1583 Working Group for development of a Voting System Standard. I was asked to give a self-bio as part of introducing myself so here goes. I'm a graduate elections engineer and have been with ES&S or its predecessor companies for 28 years. I've been working in election product development for thirty years and have been involved in the development of virtually every type of voting and tabulation system as well as every facet of the associated peripheral software. This includes almost all ES&S and its predecessor BRC tabulators and software. It includes punch card systems, both precinct based and central count, optical scan tabulators, both precinct based and central count and Direct Recording Electronic systems both full faced and page based systems. The page based systems include touch screens as well as what was probably the first DRE called the Video Voter. More about that later.

The associated software that I've worked in development of includes front end software, such as election definition and database setup including ballot style creation, ballot layout software for producing camera ready artwork for optical scan ballots and punch card ballot pages and tabulator preparation software for converting election definition and ballot style data to various tabulator formats and transferring it to the tabulator media. It also includes back end software for reading tabulator media or accepting transmitted results from the tabulators or regional sites, storing and aggregating these results and printing reports and exporting data. I even developed a Voter Registration system for small to medium size counties using an assembler-based program running on a microprocessor system that preceded the existence of the IBM PC.

My career has spanned over 43 years and includes 8 years at IBM and 6 years at Terminal Communications Inc., an IBM spin-off, in addition to the 28 years in my current position. During this time I've received 11 patents, including several on a voting system, and an IBM Outstanding Invention Award.

Requirements for Voting System Security

1. Security Overview

Security in voting systems is based on many things. The type of system, the hardware design of the system, the software used in the system and its structure and how the system itself is prepared, used and deployed. This latter point includes not only the Election Day use but the pre and post election process as well. With security considerations you virtually have to view the entire process like a detective would if investigating allegations of vote fraud or wrongdoing. Handling of these considerations requires the dovetailing of security considerations in the equipment design and the processes and procedures followed by the election jurisdiction using the equipment. There must be a chain of custody that shows that the equipment and all associated data is secure from the time the equipment is deemed ready for an election and the time results of the election are officially certified.

Even after the certification of results, a lot of the material associated with the conduction of the election must be kept secure for a period of 22 months after a Federal Election although this period is shorter after local elections and varies state by state. These materials include ballots, whether paper or electronic, all official results reports both from the precinct as well as the central site in the results aggregation process, all audit logs both from the precinct in the use of the equipment as well as those from the central site process. Also required are all electronic files used in setting up the tabulators for voting and the central site system for accumulating and reporting these results, the results themselves and the associated unit event logs where they exist. These event logs should not only include the machine created ones but all the human created records in this process. This encompasses the warehouse process and any serial numbers from seals put on machines and the delivery schedule of units to polling places including serial numbers of units delivered. It includes the activity at the polling place from logging and counting of voters and who have appeared at the polling place and whether there was any exceptions such as challenged or provisional ballots. It includes all forms created from this process as well as all signed zero and results reports from the tabulators and any affidavits that may have been created from any anomaly if one was noted. If the precinct uses paper ballots, it would also include reconciliation forms of ballots received, ballots spoiled and ballots voted. The machine tabulation of ballots should reconcile with the ballots voted and all unused and spoiled ballots should be returned with the election materials. All transported materials needs to be sealed with numbered seals and the seal number recorded and independently communicated to the central site. All of these measures are done in keeping with the concept of chain of custody to ensure that there was no tampering along the way and all information balances.

As you can see, security is a process concern and not just the concern of the voting system tabulation and voting units and voting system software but of the users of the voting system as well. There are things the system must do, since they can't be done by the users of the system, there are things that the users of the system must do since they can't be done by the equipment or the software and there are areas that either the users or the system can do. If possible, the latter is best done by the system since one would assume that it would be less subject to error.

2. Technology Evolution and System Security – Real and Perceived

The evolution of technology and the migration of computers into the home have had a major impact on the voting system security both in actuality and as perceived by the general public.

The first voting system I was heavily involved in the designing was something called the Video Voter. It was probably the first DRE, being first used in an official election in 1975 and having a rear projection screen and filmstrip projector for candidate and contest display with embedded buttons and LEDs for candidate selection and display. This was a time the microprocessor was first being utilized in equipment design but the low function device, the Intel 4004, was inadequate for the job. Since I saw the power of programmability, I created my own instruction set geared to the systems data flow design and created a symbolic language so that the hand program listings could be manually interpreted into binary sequences for manually burning the Programmable Read-Only Memory (PROM). The entire program was stored in less than 1000 bytes which was the capacity of the PROM. Looking at it in today's world, the idea that a virus could be implanted or that there could be back doors implanted in the code is unrealistic.

The first and second generation of electronic voting machines, both DREs and paper ballot tabulators (I would consider the Video Voter generation 0), were built with embedded microprocessors; many using the Zilog Z80. These units are limited to 64k bytes for all program, election definition and results storage use. They have no operating system and programs are written in Z80 assembler. It is not very likely that these would be subject to viruses or back doors in the sense of today's implications.

The units of today are in a different category. Many contain Pentium class or above microprocessors that are more powerful than the mainframes of 20 years ago as well as the same commercial operating systems that are used in our desktop and laptop PCs that we have in our homes and offices. Now, from a theoretic standpoint, the potential is there for these issues to come into play. The question is whether the equipment design, methodology of use and physical access permit these security issues to come into play.

As far as public perception, this technology advancement has made virtually everyone an expert on security. The cost of computers and the power of these computers has put into a major percentage of households computers that are more powerful than the racks and racks of mainframe computer hardware that were used in commerce and industry in the 1960s and 70s that cost hundreds of millions of dollars. The explosive development of the Internet exacerbated the situation. These powerful computers sitting in our homes and offices and being on-line exposed them to the multitudes of viruses and worms that evildoers anywhere in the world can and have unleashed. Since many of us have actually been exposed to these and virtually everyone has read or heard about these attacks in the media, it is assumed that voting systems are subject to the same conditions. The notion of tampering with the voting machine software is also re-enforced by the fact that these computer owners and users have installed and modified software and know how easy it is to do so. They also have had computer crashes and the numerous reboots that are required and translated that into equivalent happenings on voting systems. Therefore

many people equate the use of their computer at home and in the office to the use of voting machines in the polling place and that voting machines contain a program that is downloaded onto each machine for each election.

There are several things that are not commonly understood about voting units. They are not general purpose PCs and do not connect to the Internet. Any modems that may be used are only used for transmission of unofficial results to the jurisdiction central site computer, are only active after the polls are closed and the programs that support them can only perform this function. The programs used in tabulation and voting equipment are not election specific. They are unit specific and, as part of the Independent Test Authority (ITA) certification testing by an approved ITA, have their source code reviewed for structure, both for maintainability and for improper execution, and for the existence of surreptitious code. The compilation of this reviewed code, which is version identified, is witnessed by the ITA and both source code and the compiled executable code is archived. In many cases this code is sent directly to the State, who also must certify the equipment, by the ITA where it is archived for purposes of auditing against what is installed in units shipped by the vendor.

To make the generic tabulator or voting machine work for a specific election requires election definition data to be loaded into the tabulator via some storage media such as a PCMCIA card, Compact Flash, or vendor proprietary memory device. This is true whether the unit is a scanner for voted paper ballots or a DRE for actually voting as well as tabulation. The program or firmware does not have any special recognition of any one voting position over another or knows in advance what party or candidate the voting position will be used for. All knowledge and association is derived from the election definition tables or data structures that are contained in the memory device whether downloaded to the unit or directly used by it. Therefore the idea that the certified program can favor one candidate over another is not palatable.

This favoritism can only occur if the program is actually changed for the specific election, is changed in each unit used in the jurisdiction and goes undetected. This possibility requires a unit that is of a later technology which has the power and memory capacity to afford these surreptitious modifications. Changing the program for a specific election requires access to the source code, knowledge about how the program works so the change will work as intended, access to the machines and implementation in such a fashion that it will go undetected. When considering the normal machine preparation, and when using recommended procedures, it would be difficult if not impossible to achieve, unless there are flaws in the machine design which should be caught during the security evaluation in the ITA certification testing. Normal unit preparation involves transferring the election definition to the tabulator media, placing the media in the tabulator permanently or until the information is transferred, performing a public logic and accuracy test of the tabulator or voting device by voting a specific ballot set and verifying the results, zeroing or clearing these test results and then sealing the unit and/or the memory device so that any tampering will be detectable. It should also be noted that the firmware/software versions used in the test is auditable to ensure that it is the same as the version that was certified for used in the state.

When considering all of these elements, it is hard to fathom how the firmware/software can be surreptitiously modified without detection. I do recognize how the software audit becomes more complex when COTS operating systems and/or application software is involved although I believe it can be achieved.

3. Tabulator Considerations as Relates to Security

To me, voting security boils down to ensuring that the voting system has maximum protection against failure, maximum protection against misuse either intentionally (most likely by a voter with intentions to disrupt) or unintentionally by the pollworker or the election administrator and the methodology to recover from any of the above situations if they do occur. It should be noted that all election issues that I've seen that make the paper are virtually always caused by a chain of events involving improper human procedures, that may or may not include an equipment issue, but resulted in erroneous results being initially published election night. It should also be noted that in general the public is not aware that election night results are unofficial and may not include absentee and overseas ballots (depending on state rules). Official results must be released by an authorized canvassing board from the jurisdiction after authenticating them using methods such as verifying the central site results reports again the tapes or reports printed at the polling place by the tabulators as well as persons voting against ballots tabulated.

Every voting system type has its advantages and disadvantages. In my eyes there is no ideal voting system. Paper based systems have the advantage that the ballots are easily human auditable. They have the disadvantage that votes can be erroneously cast and, even though to satisfy HAVA compliance, the tabulator is required to screen the ballot and give the voter the option to correct the error or accept the ballot as is, correction is a complex process. Correction involves voiding the ballot, placing it into a spoiled ballot container and issuing the voter a new ballot to vote on. They also have the disadvantage that the ballot can be incorrectly voted in a manner the scanner cannot detect such as inadequately marking the target area, circling the name instead of marking the target area or crossing out an unintended vote on an optical scan ballot. If a ballot like this is accepted, it takes a human review to interpret voter intent and correct the tabulated results.

DREs, on the hand, prevent the voter from selecting an invalid vote, show on the screen or panel, candidates that are selected, provide a summary of selections so that the voter can see what is not selected and, under HAVA requires a voting method accessible without assistance by unsighted voters which is usually achieved by an audio ballot capability. The perceived disadvantage of these machines is that it doesn't directly provide a human auditable ballot. In my option adding a paper ballot printout to these units adds a dimension of complexity in use and administration and potential of conflict that defeats the advantage of the DRE in the first place. DREs of today redundantly store ballot records in nonvolatile memories in at least triplicate. It should be noted that the old lever machines and the early full face DREs did not store any ballot records at all. All that existed was the totals from the ballot selections. Even the Video Voter that I

discussed early on added an independent ballot record storage capability after the units were initially deployed.

A new class of voting device is now appearing on the scene that bridges the DRE vote selection advantage, both for the sighted and unsighted voter, but produces a paper record of ballot selections, either from scratch or by marking the same ballot that is printed for voting without benefit of this device, that is then tabulated by a separate optical scan tabulator. The impact of this type of configuration on voting system deployment is yet to be seen.

Security considerations for these different system types vary depending on both type and hardware and software structure. However, many of these are in common. Event log content may differ between DREs and paper tabulators but they must exist with sufficient detail to audit and reconstruct the sequence of happenings in case the process is challenged. For the DRE this usually includes logging of each ballot cast which is not normally done with paper tabulators. Both system types require the assurance that there is a method of securing the election definition. This may require physical security through the use of numbered seals or key locks and/or the use of encryption of the election definition data stored in the media. The use of data formats that are non textual is a consideration in reducing security as does the type of media used for storage, whether it is commercially available at your local electronics store or in a vendor proprietary package. Proprietary media has the advantage of enhanced security due to availability only from the voting system vendor as well as requiring proprietary devices for transferring election data to and from the media. The disadvantage is the potential for increased cost due to the used of limited production media and media access devices as well as potential unavailability of quick replacements of failed media.

DREs have different considerations from paper-based systems in balloting control. Paper based systems use the issuance of the ballot for control of voting. DREs, as with the old lever machines, use machine activation for control of voting. Both systems however are required to have a public counter visible to the pollworker that can be used to continuously ensure that the number of persons voting matches the number of ballots cast.

Once the voting process is completed and the polls are closed, the security issues of getting results at the polling place and getting these results to the central site for storage, accumulation and reporting are virtually the same. This includes the chain of custody of results media and ballots whether paper or electronic. There is more of a difference in central site security required by small rural jurisdictions and large urban jurisdictions. Both of these require protection against unauthorized access. However, the large urban jurisdiction may dual password access, one password for each primary political party and probably is using a large networked infrastructure which would have additional security issues. The small rural jurisdiction may very well be a one-person office operating on a single PC for central site functions where dual password access wouldn’t apply.

There are many other design considerations that determine whether additional security measures must be taken to get equivalent system protection. Some of these relate to the use of COTS hardware with its additional access points versus proprietary hardware with the access control designed in or the use of a COTS operating system with its potential for viruses or the presence of other unauthorized software versus no operating system and total unit control residing in the application. However, these discussion can go on endlessly and I will end this discussion here.

Certifications and Upgrades

The complexity of the certification process at both the ITA and state level has increased dramatically of the last several years especially as relates to software that supports the tabulators and voting units themselves (also referred to as hardware, a misnomer in my eyes). All testing under the FEC 2002 Standards requires a full end-to-end test including a "hardware" and software regardless of whether it is new system or and upgrade to an existing system. At this time, many states only certify tabulators or tabulators and the reporting system but have adopted the 2002 standards thinking that they were just substituting the 2002 for the 1990 and not realizing that the method of certification has changed as well.

Due to this evolution, upgrades of deployed systems are a major concern. As was brought out in testimony, no software is perfect. Even if perfect in design and execution, it can have limitations that are encountered in the continuing evolution of content of elections and utilizations in new customer environments with new conditions that expose the system to limitations not previously encountered. These mostly relate to the supporting software and are not usually exposed until the start of the elections setup process. Even if there is a limitation in the tabulator's handling of a condition, it can usually be "worked around" in the manner of use of the supporting software (tabulator definitions in conjunction with the reporting system definitions). However, if these limitations are in the front-end software, these workarounds are not usually available. The back end software may be exposed to these new requirements as well; not in the core requirement of results storage and aggregation, but in the reporting requirements which many times are unique to a specific state or jurisdiction.

Under the 1990 Standards, each system component was independently certified albeit tested as part of a system. Most states in the 90's only certified tabulators and not the supporting software. Some exceptions to this were Florida, who certified the entire system as a unit, New York and Texas who certified each deployed application and Indiana who certified the accumulation software. With the adoption of the 2002 Standards, the system is certified as an entity with one certification number identifying it. This creates an issue for upgrades especially those that relate to the ballot layout and election definition software and the report generation sections of the back end software. This is exacerbated by more and more states requiring the products that they certify meet the 2002 standards as a baseline for certification and upgrades even though they may not have changed what products require certification. Many did not understand the system implications of the 2002 Standards when adopting them.

To upgrade any piece of the system requires a full ITA testing event with all associated documentation and source code analysis. This is true even if the only change is in an output report or export file format in the results reporting subsystem. This is also true if the change only affects the presentation on an optical scan ballot to meet statute. Both of these are easily auditable in the application environment yet cannot be deployed in today's context due to certification requirements. Many states do not have emergency certification processes. Even if they do, with the scrutiny that election officials are under today, they don't want to do anything that puts them at risk. Thus upgrades become a virtual impossibility.

Summary and Recommendations

1. Security is a function of the type of system used and the procedures controlling their use. Security standards must encompass the procedures associated with end-to-end use of the voting system under test and evaluation and cannot be separated from them.
2. The security evaluation of a voting system should be consistent with the voting system's design and capability. This not only includes type (i.e. DRE vs ballot scanners) but also the architecture (i.e. limited capability, COTS hardware, COTS operating systems, etc.). There shouldn't be a cookie cutter approach where one size fits all. This should be recognized by requirements definitions.
3. Mount a public relations effort to attempt to turn around public perception regarding the certification process and the voting systems that are certified through the process. This may include such things as:
   - Making certification reports available to the public. This may require a redacted version that eliminates sections that compromise vendor proprietary information. Possibly generic sections can be substituted for the redacted ones.
   - Create a registry of qualified individuals (i.e. computer scientists) who would like to right to review source code. They should be required to sign non-disclosure agreements and only have the right of review under secure conditions (maybe at ITA sites). They could point out flaws to the ITA or the vendor for agreement and correction.

   These actions might add transparency to process and defuse some of the activist and computer scientist allegations.
4. For upgrades of existing systems:
   - If a single subsystem is affected, consider testing means that restrict evaluation to that subsystem and provide a means of "certifying" that subsystem.
   - Consider methods for special handling or excluding upgrades to functions such as external reports or ballot layout format that in many cases are state and jurisdiction specific and are innocuous to the system overview functionality. All of these variations especially state specific ones, are not ITA tested today (although included in the source code analysis) and are really left to state certification for verification.

This concludes my presentation. Thank your for your attention and the opportunity to participate.