On the Issue of Source Code Escrow and/or Disclosure

(By AVANTE International Technology, Inc. Rev B May 28, 2007)

Source code disclosure and escrow has become critical because of the pending Federal bills on the Election System and, for this discussion, the current New York State Election Code. One may say that the usefulness of escrow and disclosure of source code in pursuit of improvement in the integrity of our nation's voting systems is at best unclear. Key reasons for this is the use and for most part the needed use of "third party software" available commercially-off-the-shelf (COTS).

AVANTE has nothing ingenious to offer beyond what has been superbly discoursed in several Internet blogs[1] and websites. We offer our comments below with perspective as a manufacturer possibly offering somewhat different insight

AVANTE generally agrees with the approach taken in the EAC 2005 VVSG in terms of reviewing and escrowing of source codes. The following are some of the key aspects:

- Voting system manufacturers must submit all internally developed source code to authorized independent testing agencies for source code review and certification.
- Final certified source code is compiled to produce a "witness build" that serves as the "gold" standard of the voting system.
- All certified source code and execution code is escrowed with NIST (almost all vendors comply with this voluntary requirement).
- All source code and execution code incorporates "hash" codes to ensure authenticity that can be independently verified.
- Most states require additional escrowing of the voting system's source code and execution code that may or may not have variations that are certified by other states.
- The EAC 2005 VVSG specifically exempts reviewing or certifying commercial-off-the-shelf (COTS) third party source code such as operating systems, database, and firmware embedded in ancillary devices.
- Most states require the submission of at least a set of certified hardware and software used in their state for hard evidence and reference.
- The current New York State Election Code on escrowing can be and is now interpreted to include:
    - Vendor developed software modules.
    - Third party operating systems.
    - Third party software functional modules.
    - All drivers for components such as printers, touch-screens, etc.
    - All firmware (software inside hardware components) that may include:
        - Bios
        - Microprocessor codes
        - Graphic chip
        - Compilers, etc.

[1] http://avi-rubin.blogspot.com/2007/02/hr-811-new-holt-bill.html; http://www.votetrustusa.org/index.php?option=com_content&task=view&id=2276&Itemid=26;

Other system information may be more important than source code to those seeking system integrity. Compiler and execution code is discussed below.

Source Codes (High level programming language):

- Human Readable representation of the instruction that the computer is to use for operations. This is the recipe for all operations.
- FEC 2002 VSS and EAC 2005 VVSG all require detailed explanations of source codes (within the source codes) written by all voting system vendors.
- Standard computers are loaded with different software execution codes so that it can perform different functions between different components (microprocessor, memories, graphic display, etc.) of the computer as well as other functions. All of these sub-components involve firmware (machine-based software) and execution codes of different functional modules.
- The voting systems use third party operating systems to develop functions and provide complicated functions (such as those required for many accessibility features such as foreign languages, speech engines, etc.)
- Most election systems use some established software modules or packages for special functions such as databases and drivers for printer and/or touch-screen displays.
- Some vendors historically developed simple voting systems (commonly found in 1970-2000) for "touch-button" direct electronic recording using simpler processor such as the Z80, etc. The vendor developed all the required functions and interfaces and thus had available to themselves all software source codes and execution codes.
- Most functional voting systems providing accessibility features use Microsoft based operating systems because of the abundant availability of functional modules and additional software from third parties (including Microsoft themselves).

Compilers (Converting high level language to machine level language):

- The Compiler is a software package that converts human-readable source code into machine-readable execution codes.
- Most compilers are historically pieced together. Full availability may be unlikely.
- Some compilers are developed by the developers such as Microsoft themselves. Z80 may have compiler developed by the chipmaker, etc.
- Having source code without compiler source code is almost as good as only having execution codes.

Execution Codes (Machine level or assembler programming language):

- Computer instructions (machine language) that have been converted (compiled) from the source codes.
- Vendor developed source codes, and all of the execution codes of the operating system, database, speech-engines, drivers, etc. are all "bound" (hashed) with SHA1 and escrowed.
- Execution codes can be escrowed in Federal, State, and County with proper authorities.
- Expert programmers can make additions and modifications to execution codes directly without using the compiler or language converters and thus source codes.

Very Important Notes:

1. Having execution codes that are hashed and verified to be the same as those loaded into voting machines confirm no "tampering" to the system. This is a key process in auditing (along with the system event audit log) any voting system. ***This is key in ensuring system security***.
2. Having source code from vendor developed software helps software experts that are familiar with that programming language to find and resolve any errors (unintentional or intentional) that may have been made by the vendors. ***Having source codes does not contribute directly to the system security.***
3. Having third party source codes may help experts "understand" (not easy) potential errors due to communications between different functional modules. ***They do not directly contribute to the security of the system.***

4. Modifications to the vendor source codes and then recompiled for testing is the normal diagnostic means for eliminating and confirming source errors.
5. **No one, even those that use Z-80 processors, can provide all source codes.**
6. **No one can yet provide the compiler source codes.**
7. Requiring the escrowing of all source codes as defined is unreasonable in the search to ensure voting system security.

AVANTE believes the current approach used by EAC with the assistance of NIST is wise and practical. May the following aspects can be made more specific.

- Require that COTS software and firmware be defined as those that have established commercial applications other than that of a voting system.
- Require that no modification on such firmware and software be made to meet the specific needs of the voting systems incorporating them.
- If any modification of such firmware and software is done on the voting system application, that firmware and software should be certified and source code placed into escrow in NIST and other state agencies that require escrowing of the specific voting machine source code.
- Incorporate election codes (Federal, State or EAC requirements) that all source code placed in escrow can be reviewed by court appointed experts. Expert opinions can be rendered on any aspect of the source codes as long as the actual source codes are not disclosed.

AVANTE agrees with ACCURATE-VOTING and their position on disclosure[2] of source code developed by the voting system manufacturers. Our rational has been stated earlier[3]. The following offers additional clarification.

- The fact that voting systems are managed independently by more than 100,000 independent jurisdictions with different State election codes requiring different degrees of security protections makes it unwise to have total open source to the public.
- Very light penalties have been imposed against offenders that changed the source codes for elections. This legal precedent provides very little deterrent to those that are willing to commit such offenses having access to available public source codes.
- AVANTE agrees that source codes should be made available for qualified independent reviews.
- Currently, experts appointed by the State (in some but not all states) can review and examine the source codes used in the voting systems.
- AVANTE understands the desire of the voting integrity community to have a more transparent voting process. The process should be open for qualified public review and examination. We suggest qualifications of such public experts include at least the following:

[2] http://accurate-voting.org/wp-content/uploads/2007/02/AR.2007.pdf
[3] http://www.vote-trakker.com/IS%20OPEN%20SOURCE%20OR%20SOFTWARE%20ELECTRONIC%20VERIFICATION%20A%20SOLUTION%20FOR%20SECURED%20E-VOTING.pdf

- Such experts must be US citizens that are endorsed by publicly registered citizen groups (e.g. 501C, etc.), universities, or other public institutions as stipulated by a court of proper jurisdiction.
- Such examination must be done in environments that are controlled by the Court to prevent any form of copying.
- All experts must sign an agreement of non-disclosure on the actual source codes and be allowed to make comments to the manufacturers but not the public unless sanctioned and allowed by the Court of proper jurisdiction.
- All experts having the desire to provide the source code review services on behalf of the public must sign an agreement that they will be barred from working on or consulting for any voting systems manufacturers including those of not-for-profit institutions.

AVANTE believes there is an implicit public responsibility for all voting system manufacturers to include proper and adequate transparency. However, the public's right to know must not damage the business interests of the entities that provide such commercial systems and services. We hope the above ideas may be modified to satisfy both the public and commercial interests.