NYSTEC

New York State Technology Enterprise Corporation

NYSTEC Response to SysTest Request For Interpretation of VVSG Vol 1 Requirement 7.4.6.d

For

New York State Board of Elections

Submitted to:

New York State Board of Elections
40 Steuben Place, Albany NY 12207

May 28, 2008
Version 1

Table of Contents

1. BACKGROUND

NYSBOE has requested that NYSTEC respond to the SysTest RFI on the an interpretation of the following VVSG requirement:

7.4.6 Software Setup Validation

> *d. The verification process shall be able to be performed using COTS software and hardware available from sources other than the voting system vendor.*
>
> *i. If the process uses hashes or digital signatures, then the verification software shall use a FIPS 140-2 level 1 or higher validated cryptographic module.*
>
> *ii. The verification process shall either (a) use reference information on unalterable storage media received from the repository or (b) verify the digital signature of the reference information on any other media.*

In particular SysTest is asking for clarification of the term "verification process" and believes that it is ambiguous. In their RFI request SysTest has stated the following facts supporting ambiguity:

- *This is a <u>verification process</u> using COTS software and/or hardware.*
- *Purchasing and using COTS software/hardware to extract modules/binaries poses a security risk and the possibility of opening the voting system to vulnerabilities.*
- *Modifying the COTS software/hardware to meet security risk will make the COTS software/hardware non-COTS.*

SysTest, in their RFI goes on to suggest the following proposed interpretation:

The requirement states the verification process shall be able to be performed using COTS software and hardware available from sources other than the voting system vendor. SysTest Labs interpretation is as follows:

- *Vendor supplies the code to SysTest Labs for a software application tool to extract binaries from the voting system*
- *SysTest Labs executes a full source code review, as well as verifying that all modules/binaries are being pulled to create the hash values*
- *SysTest Labs creates and install the build*
- *SysTest Labs extracts the binary/modules*
- *A COTS software/hardware tool is executed to verify the hash values (this is the verification process as stated in the VVSG 7.4.6d requirement)*

Currently, this is how SysTest Labs is meeting this requirement for our VSTL clients.

2. Executive Summary

NYSTEC does not agree with the SysTest interpretation of the requirement or with their proposed interpretation. We believe that SysTest is interpreting "verification process" too narrowly in believing that it is only referring to the hash verification process. NYSTEC believes that the verification process must refer to the entire software setup validation process as the process as a whole must be trusted and seek to minimize risk. The SysTest interpretation places trust in the voting system vendor to develop and execute properly a key component of the verification process. NYSTEC believes this is not a correct interpretation and does not reflect the intent of the requirement or result in the most secure software setup validation process.

3. NYSTEC Detailed Response

NYSTEC believes that the "verification process" refers to the entire process of verifying that only authorized software is present on the voting systems. NYSTEC believes this interpretation reflects the intent of VVSG 7.4.6 and is supported by the following:

- The interpretation of "verification process" is clearly defined and understood when considering other parts of VVSG 7.4.6.

  7.4.6b defines the process clearly as a process that:

  - Verifies that the correct software is loaded;
  - Verifies that no unauthorized software is present;
  - Verifies that the voting system software on the voting equipment has not been modified;
  - Uses reference information from the NSRL or from a Stated designated repository;

  7.4.6.bi goes on to require that:
  - The process used to verify software **shall** (NYSBOE should to shall) be possible to perform without using software installed on the voting system.

  7.4.6.d goes on to require that:
  - The verification process **shall** (NYSBOE should to shall) be able to be performed using COTS software and hardware from sources other than the voting system vendor.

The SysTest interpretation allows and trusts the voting system vendor to develop and execute the program that is extracting the modules from the voting system to be hash checked. Not only is the module extract program developed by the vendor, it is running on a system developed by the vendor. This is a clear violation of 7.4.6.b and 7.4.6.d. Obviously the problem here is that an insider could easily defeat this security as SysTest is trusting the vendor to check themselves. All the insider would need to do is to insert malicious code in the extract program or within the underlying system to impact the way the extract program operates and defeat the hash check. VVSG 7.4.6 attempts to make this entire process external as a means to mitigate this risk.

NYSBOE modified VVSG 7.4.6 in two places replacing “should” with “shall” as this would ensure that vendors designed systems that would support software setup validation by a 3rd party and not rely on the voting system itself or software developed by the system vendor to participate in the verification process. The requirements that COTS software and hardware be used (7.4.6.d) as well as the requirement that the process must not rely on software installed on the voting system (7.4.6.bi) makes it very clear that the intent of NYSBOE was to trust a COTS hardware and software based verification process.

The NYSTEC interpretation represents a more secure approach where the entire verification process can be run on COTS hardware and using COTS software with read only access to the voting system filesystem and modules. While neither approach is 100% secure, NYSTEC believes that the verification process relying on a COTS tool is more secure than relying on a process that allows the vendor system running vendor software to validate itself.

SysTest is arguing that using COTS software and hardware to extract modules and binaries poses a security risk and NYSTEC agrees. However the security risk posed by a purely COTS based hardware and software process is less than the risks posed when vendor supplied software and hardware are used. VVSG requirement 7.4.6.e adds provisions to help ensure that a COTS solution does not introduce additional risks through the use of a read only and tamper evident port. With this approach and the use of a read only access port an attacker would need to compromise both the voting system and the COTS validation tool to avoid detection.

SysTest is also arguing that COTS software and hardware would need to be modified to meet this requirement and thus making it no longer COTS. NYSTEC disagrees and cites one voting system vendor who implemented a solution that would appear to meet all the requirements in 7.4.6. The design featured a removable PROM chip that is then placed in a COTS read only chip reader for hash checking. Other similar solution designs are certainly possible.

In the RFI, SysTest includes a proposed interpretation. NYSTEC believes the SysTest proposed interpretation should be rejected as it is based on an inaccurate interpretation of “verification process” which ignores the fact that a vendor supplied program running on the vendor system is in violation of VVSG 7.4.6.b.i. Additionally SysTest states that this is how they currently meet the requirement for other VSTL clients. This fact is not relevant for NYS as NYSBOE has modified VVSG 7.4.6 to require the use of COTS software and hardware that does not rely on using software installed on the voting system.

4. Conclusion

NYSTEC believes that SysTest may not be considering VVSG 7.4.6 in full and understand what it is attempting to accomplish. The SysTest interpretation of 7.4.6.d permits additional and unmitigated risk to be added by relying on a vendor supplied program running on the vendor machine to produce the modules which are then hash checked. The NYSTEC interpretation of VVSG 7.4.6 will require a voting system design that allows a pure COTS solution to validate the software setup of voting systems. We believe this is the preferred solution and accurately reflects VVSG requirement section 7.4.6 with the modifications made by NYSBOE. Vendors are likely to complain that implementing VVSG 7.4.6 according to the NYSBOE modifications is difficult but that should not be justification for weakening the requirement.

It should also be noted that NYSTEC realizes and appreciates the fact that vendors may have systems currently under review that do not meet all requirements in VVSG 7.4.6. This fact however should also not be a reason to alter the requirements or interpret them differently.