Merle S. King
Center for Election Systems
Kennesaw State University
August 26, 2009

COTS Products and Certification of Voting Systems

The State of Georgia utilizes a uniform voting system, in place since 2002. This system is built around Premier Election Solutions GEMS 1.18.22G running on a Windows 2000 server and R6 and TSx touchscreen units running BallotStation 4.5.2. As the Executive Director of the Center for Election Systems at Kennesaw State University, my role is to provide advice and technical support to the Secretary of State in regards to the maintenance and use of this system.

If properly selected, unit-tested, integrated and then system-tested, COTS components can reduce the development time and overall cost of a voting system and they can create a more flexible array of hardware and software options for a jurisdiction. The COTS technologies used in the voting system may be relatively mature and less prone to failure than custom developed options. COTS manufacturers and users may have existing support organizations that can aid the jurisdiction in the overall maintenance of the voting system.

The downside to the integration of COTS components can be considerable. Chief among those negative factors is the lack of control, by the voting system vendor, the jurisdiction, or the system integrator, over the upgrades and maintenance issues related to the hardware, firmware and software. The impact of the volatility of COTS components on the federal and state certification of systems is a major concern. I will not address the COTS issues of security, intellectual property, and licensing, which are non-trivial, but beyond the scope of this document.

Depending upon the extent to which the voting system has integrated COTS components into its initial configuration and the type of COTS component used, the replacement, reconfiguration and recertification issues can begin immediately upon deployment of the voting system. This places an unusual burden on the jurisdiction. It must begin negotiating a system change before it has collected data on the initial deployment of the system. It must explain to its funding source(s) that the new system has to have improvements and upgrades immediately. The effort to upgrade the system and retest it at the state level may exceed the capabilities of the jurisdiction.

Selected COTS Issues

Georgia requires the use of a uniform voting system throughout the state. Although there are many advantages to this requirement, it prevents localized changes to the deployment of a system and presents a threshold of change measured in the millions of dollars. Counties cannot change out a voting system that contains obsolete components. The entire state must change in unison. This requirement for uniformity places many constraints on the management of the system. Virtually every issue with the voting system is a statewide issue.

The voting system used in Georgia is built around the Premier Election Solutions (PES) GEMS 1.18.22G election management system. This proprietary software sits on top of a Windows 2000 server configuration. GEMS 1.18.22G will only run in a Windows 2000 environment – it cannot be migrated to run in a Windows 2003/8 environment. Over the first seven years of deployment of this system in Georgia, we were able to preserve its deployment configuration by not applying Service Packs (SPs) as released by Microsoft, and by purchasing replacement servers from Dell that were capable of being downgraded to run Windows 2000. In this same time period, Microsoft announced the end-of-life (EOL) of Windows 2000 (March 31, 2004) and in 2008 we discovered that Dell would no longer be producing a server that could be downgraded to run Windows 2000. Support for software products is phased out over a multi-year schedule. Mainstream Support for Windows 2000 was retired in 2005 and Extended Support will be retired in 2010.

In addition to an outdated version of the operating system, the servers were also utilizing an expiring Secure Socket Layer (SSL) certificate that had to be changed by early 2009 in order for the system to maintain its current level of security.

The State of Georgia mitigated these COTS issues by taking the following steps:

- acquired the new SSL certificate from the vendor and began our own testing of the voting system with the newly installed SSL certificates on both the clients (touchscreen units) and server
- researched and acquired a Dell server capable of being downgraded to run Windows 2000
- applied all current Service Packs to a Windows 2000 installation on our test server
- installed GEMS 1.18.22G on the newly configured Dell 1900 (including Windows 2000 SP4 and the new SSL certificate) and applied the state certification protocol to test this system to ensure that there was full functionality in the system and no anomalies in performance
- contracted with Wyle Labs to review the server configuration in the context of the 1990 VSS under which the system was initially certified
- repeated all state certification tests on the server and affirmed Wyle Labs' results as well as our own prior test results

Once the testing of the system was complete, we ordered 80 Dell servers to stockpile and deploy as our current inventory of servers succumb to age. We continue to look for an additional source for servers. We do not anticipate any additional SPs being issued for Windows 2000.

The second COTS issue relates to batteries used in the ExpressPoll 4000. These batteries are custom built for the COTS tablet that was integrated into the ExpressPoll application and are available from only one manufacturer. The manufacturer discontinued production of the batteries in 2008. Premier Election Solutions has negotiated an agreement with the manufacturer that they will produce limited runs of the battery for future needs.

The last example is a firmware "recall" notice issued by Seagate for a series of hard drives, one of which is used in some of our Dell servers. This recall was issued in the early spring of 2009. Without the application of the firmware upgrade, there is a potential for a catastrophic, unrecoverable hard drive failure. This is not an acceptable risk on an election management system server. The upgrade has been applied to all affected servers and the servers retested.

I chose these examples because they illustrate hardware (batteries and servers), firmware (the Seagate hard drive upgrade) and software (the SSL certificate). The number of jurisdictions that can conduct this kind of testing is limited. The ability of a jurisdiction to stockpile EOL'd hardware is also limited. Jurisdictions that are completely dependent upon the manufacturer and VSTLs for testing would be challenged to mitigate these, or similar, COTS issues.

Non-Georgia Systems

Some contemporary voting systems have included complex COTS products such as Personal Computers (PCs), laptops, and printers, integrated into the voting system's configuration. The motivation to use these components is driven by cost containment and rapid development of the voting system.

PCs are complex products consisting of multiple subsystems, all linked together by an even more complex operating system. A brief discussion of two Microsoft operating systems will illustrate the challenges of using PCs as an integral part of a voting system.

Windows XP is the longest running PC operating system to date. It was released in 2001 with Service Packs 1, 2, 2b, 2c and 3 released in 2002, 2004, 2006, 2007 and 2008, respectively. It has been EOL'd and mainstream support was retired in April of 2009.

Windows Vista was released in early 2007. By February 2008, Service Pack 1 was released to improve system reliability and provide increased administrative control of the PC running Vista. Service Pack 2 was released in April of 2009. Windows Vista has been EOL'd and replaced in the Microsoft marketing mix by Windows 7, which is scheduled for release this year (2009). Mainstream support for Vista will be retired in 2012.

Voting systems built around either of these components could have a very short life cycle indeed. Their inclusion in a system would force jurisdictions to avoid normal maintenance operations and administer elections in the hope that the PCs would run, without maintenance or replacement, for an acceptable period of time. It may also require the jurisdiction to stockpile hardware capable of running these operating systems.

Certification Issues

There are numerous issues related to the certification and recertification of voting systems that have been modified, upgraded, updated, or in some way touched by COTS issues.

1. The EAC Voting System Testing and Certification Program Manual provides for De Minimis Changes. These changes may only impact the hardware of the system and have no impact on the functionality of the system.

   The first criteria for De Minimis changes is problematic. Most changes in hardware in a voting system are driven by the lack of availability or a systemic failure of a component. The likelihood that a substitute hardware component will contain the precise firmware components as its predecessor seems unlikely and unrealistic. The second criteria, "retains unaltered, the reliability, functionality, capability and operability of a system", should be the operative criteria, regardless whether the media of the change is hardware, firmware, or software.

2. Warranty work by component suppliers may be contractually required in the jurisdiction. Many jurisdictions are required or (at least) encouraged to maintain warranties on information technology (IT) components. These maintenance contracts may oblige the jurisdiction to apply upgrades and service packs to the COTS components as directed by the manufacturer of the COTS component. The application of upgrades is considered an IT "best practice". Ideally, the certification criteria should not only accommodate, but should enable these activities.

3. The EAC's COTS conformance strategy should not assume the manufacturer as the sole agent of change in the system. It is easy to visualize a scenario in which a manufacturer might refuse or delay the integration of a COTS-drive change into an existing system so that they might sell a new or different system to a jurisdiction. Additionally, the manufacturer may not be able to address a large number of simultaneous changes occurring across a broad spectrum of jurisdictions. And finally, a voting system may outlive the organization that sold it.

4. COTS components are transitioning from equipment to supplies. Many IT organizations no longer track monitors, printers, PDAs, and in some cases, even laptops. They are considered to be disposable supplies. A COTS conformance policy should address this evolving distinction in COTS components.

5. The speed and environmental conditions that mandate a change in a COTS component are not synchronized with anything other than the market and the manufacturing plan of COTS vendor. These timetables are short and not concerned with the voting system's manufacturer's schedules, the election calendar, or the certification timetable.

6. Voting system manufacturers should disclose, in plain text, the major COTS components and their lifecycle status in the technical and marketing documentation of a voting system. This would permit prospective customers to evaluate the impact of purchasing a system that contains EOL'd components and promulgate an ongoing support strategy.

7. VSTLs should develop methods for testing COTS components with a known propensity for volatility (PCs, operating systems, disk drive controller firmware, etc.) and be able to test a modified system for conformance, quickly and efficiently.

8. Manufacturers must seek a balance between using mature and stable COTS technology and attempting to select components at the early stages of their life cycles.

9. Manufacturers should have an ongoing process of identifying and testing functional equivalents for COTS components.

Conclusion

If we want to benefit from the use of COTS components in our voting systems, we would be better served to see them as interchangeable components rather than integral to the system. Their known attributes and ready availability, clear strengths in the design and deployment of the voting system, should also be leveraged into the ongoing maintenance of the system. If we can formalize and validate a method of utilizing COTS components for both development and maintenance of systems, we will be closer to accomplishing two laudable goals: Decrease the development and operational costs of the voting system and extend the usable life of the voting system beyond the life of its shortest-lived component.

Given the volatility of change in COTS components, it seems prudent not to design the architecture of the voting system around them. A voting system that places a conventional PC or laptop with a conventional operating system at its core will have a very short service life. Manufacturers should attempt to place volatile COTS components at the periphery of the architecture, not the core.