Cleveland State University
Center for Election Integrity

California Top to Bottom Review ("TTBR") of Voting Technology

Background

- Initiated by the California Secretary of State (SOS), Debra Bowen, whose office contracted with the University of California system. Technical assessment research teams (focusing on security, accuracy and reliability issues) were led and staffed by some of the most respected computer scientists in the nation, from California and elsewhere. Documentation assessment teams involved both regulatory specialists and technically trained experts (software engineers or information systems). The Accessibility team focused on physical disability-related issues and involved two noted specialists.

- Three California voting systems ("VS") were comprehensively assessed: the election management/tabulation software plus the voting devices (optical scanning and DRE touchscreens), from Diebold, Hart, and Sequoia. With minor differences, all of these systems are in use in other States. ES&S systems were not evaluated.

- Researchers had unprecedented access to the voting devices, software source code, testing lab and regulatory system certification reports, and other technical information.

- When focusing on security and accuracy, teams considered activities that might be conducted by insiders as well as external intruders; they also considered protection of voting data from operator/election official mistakes.

Summary or Exemplar Findings

Overview: The most troubling security flaws are at the level of baseline, elementary computer security, i.e., they are not concerned with sophisticated or contested security principles on which scientists might disagree.

Election management/tabulation software

- For all VS, the system architecture depends on a commercial operating system known to have security vulnerabilities. All vendors failed to secure this system properly. System architecture had not been designed with either basic or sophisticated security protections. All systems failed to follow standard security design principles.
- All systems were susceptible to viruses that could be introduced from a number of vectors, including from voting device memory cards. (Viruses and other rogue programming can, e.g., "flip" votes among candidates, scramble tabulation data, delete voting data, and cause system programming to fail.)
- Viruses could infect the central computer and then be spread to all the voting devices when their memory cards are prepared for the next election.
- System logs of operator activity ("audit logs") could be overwritten or erased, meaning that insider attackers could manipulate voting data and results, and then erase the logging inventories that would show the access and activity; or, could be used to frame a different employee.
- Systems permitted relatively easy bypassing of passwords, thus permitting broader access than authorized.
- In each VS, many other security holes exist that could compromise the system's ability to report accurate election results -- or any results.

A Partnership of the Cleveland-Marshall College of Law & the Maxine Goodman Levin College of Urban Affairs
Campus Address 1801 Euclid Avenue, LB 229 * *Mailing Address* 2121 Euclid Avenue, LB 138 Cleveland, OH 44115
216.687.2313 *Voice* * 216.687.6881 *Fax* * www.csuohio.edu/cei/

Voting Devices

- All systems failed to follow standard security design principles, and lacked even basic security protections. All systems' devices (DREs and precinct-based optical scanners) were subject to easy, undetectable attacks that could occur during the normal time that a voter would be at a voting machine casting a ballot.
- Some devices permitted the researchers to introduce malicious code onto a voting machine in under a minute, while appearing to be in the process of voting.
- All DRE touchscreen voting units permit a voter to generate and cast multiple ballots during a normal time voting could occur, in ways that would be largely undetectable to poll workers unless they were specially trained and closely supervising the voter's activity at the unit (voter privacy might still be compromised).
- Some DRE devices permitted the researchers to damage the Voter-Verified Paper Audit Trail (VVPAT) covertly, so the voters could verify that their votes were printed correctly, but after the election the VVPAT could not be read.
- Other DRE devices could be modified to store votes incorrectly, but print them on the VVPAT correctly (for example, a voter's choice of John Adams results in the VVPAT printing "John Adams" but the DRE stores the vote as a vote for "Thomas Jefferson").

Documentation Review

- The NASED "qualification" (certification) of all systems was based on testing lab ("ITA") studies that were seriously flawed. While the ITA reports varied significantly, generally it was not possible to ascertain whether the lab had conducted the independent tests needed to determine VS satisfaction of FEC 2002 standards. Often the ITA would test a device but not the voting system as a whole, despite the guidelines' requirements for system testing to determine whether the various components worked accurately and reliably in concert.
- Documentation was uniformly seriously deficient in alerting officials to security vulnerabilities and the management and training strategies so that election officials could protect the voting systems and accuracy of results.
- The VS vendors varied significantly in the adequacy of the documentation they provided to local election officials. Some documentation was clear and well-written for support; other manuals were vague, contradictory and confusing.
- Poor quality in a vendor's documentation for election officials can lead to a series of expensive technical services contracts with the vendors, so that a jurisdiction can run the systems.

Accessibility

- Although some voting systems could be used by some voters with certain disabilities, each of the tested systems has accessibility design limitations that will not allow independent voting by voters with other disabilities.
- Support stands for all the voting systems impeded physical access by most voters in wheelchairs.
- The VVPAT paper trail printouts of the tested systems cannot be directly read and verified by blind voters, and were also found to be difficult or impossible to read and verify for many other voters with disabilities.

Impact

- The California SOS decertified all VS that were reviewed and recertified them with special system-specific requirements. DRE units can be used only for accessibility, and a 100% hand-count audit of the votes.
- The Secretaries of State in several other states have convened experts and election officials to respond to the TTBR findings relevant to their states' VS and to develop operational plans for protecting the integrity of the vote.
- In other states, such as in Kentucky, the Attorney General initiated action: he convened an expert study to review VS reports with an expedited review of Kentucky's VS. Link to the report is below.
- New concerns have arisen over the VS regulatory system for it did not weed out seriously flawed systems. Despite regulatory changes, these studies have raised concerns about the new regulatory system/standards.

Further Reading

All the California TTBR reports, plus the regulatory actions the SOS undertook in response:
http://www.sos.ca.gov/elections/elections_vsr.htm

Kentucky AG's announcement is at http://ag.ky.gov/news/votingsystemreport.htm; expert's report is at http://ag.ky.gov/NR/rdonlyres/1B3F7428-0728-4E83-AADB-51343C13FA29/0/votingexpertletter.pdf.