"Free and fair elections"? The GAO report on voting machines

Submitted by lambert on Mon, 12/05/2005 - 9:23am
Departments:
Department of No! They Would Never to Do That! [1]
Thread:
Election Fraud [2]

DBK's blogswarm on verified voting [3] inspired me to read the GAO report [4] on electronic voting machines, which I found on a Kos thread here [5]. [NOTE: Serious election researchers would be more than welcome here. Contact the blog [6].]

The GAO report does *not* prove that the Republicans stole Ohio 2004. However, it does make a *prima facie* case that ample means to steal Ohio 2004 existed, and ample opportunities as well.

What follows is long, a much much longer excerpt than is usual here. But the detail is essential to understand if you care about maintaining a functioning democracy. If there are any technical people reading, you will immediately understand what shit software, and what shit systems, the (Republican) corporations selling into the electronic voting market have foisted on us.

> **Product Development** Multiple recent reports, including several state-commissioned technical reviews and security assessments, voiced concerns about the development of secure and reliable electronic voting systems by system vendors. Three major areas of concern are weak security controls, audit trail design flaws, and weak security management practices.
>
> **Weak system security controls.** Some electronic voting systems provided weak system security controls over key components (including electronic storage for votes and ballots, remote system access equipment, and system event and audit logs), access to the systems, and the physical system hardware.
>
> *Regarding key software components*, several evaluations demonstrated that election management systems did not encrypt the data files containing cast votes (to protect them from being viewed or modified). Evaluations also showed that, in some cases, other computer programs could access these cast vote files and alter them without the system recording this action in its audit logs. Two reports documented how it might be possible to alter the ballot definition files on one model of DRE so that the votes shown on the touch screen for one candidate would actually be recorded and counted for a different candidate. In addition, one of these reports found that it was possible to gain full control of a regional vote tabulation computerâ€?including the

ability to modify the voting softwareâ€?via a modem connection. More recently, computer security experts working with a local elections supervisor in Florida demonstrated that someone with physical access to an optical scan voting system could falsify election results without leaving any record of this action in the systemâ€?s audit logs by using altered memory cards. If exploited, these weaknesses could damage the integrity of ballots, votes, and voting system software by allowing unauthorized modifications.

Regarding access controls, many security examinations reported flaws in how controls were implemented in some DRE systems. For example, one model failed to password-protect the supervisor functions controlling key system capabilities; another relied on an easily guessed password to access these functions. In another case, the same personal identification number was programmed into all supervisor cards nationwideâ€?meaning that the number was likely to be widely known. Reviewers also found that values used to encrypt election data (called encryption keys) were defined in the source code. Several reviews reported that smart cards (used to activate the touch screen on DRE systems) and memory cards (used to program the terminals of optical scan systems) were not secured by some voting systems. Reviewers exploited this weakness by altering such cards and using them to improperly access administrator functions, vote multiple times, change vote totals, and produce false election reports in a test environment. Some election officials and security experts felt that physical and procedural controls would detect anyone attempting to vote multiple times during an actual election. Nevertheless, in the event of lax supervision, the privileges available through these access control flaws could allow unauthorized personnel to disrupt operations or modify data and programs that are crucial to the accuracy and integrity of the voting process.

Regarding physical hardware controls, several recent reports found that many of the DRE models under examination contained weaknesses in controls designed to protect the system. For instance, one report noted that all the locks on a particular DRE model were easily picked, and were all controlled by the same keysâ€?keys that the reportsâ€? authors were able to copy at a local store. However, the affected election officials felt that this risk would be mitigated by typical polling-place supervisors, who would be able to detect anyone picking the lock on a DRE terminal. In another report, reviewers were concerned that a particular model of DRE was linked together with others to form a rudimentary network. If one of these machines were accidentally or intentionally unplugged from the others, voting functions on the other machines in the network would be disrupted. In addition, reviewers found that the switches used to turn a DRE system on or off, as well as those used to close the polls on a particular DRE terminal, were not protected.

Design flaws in the voter-verified paper audit trail systems. Voter- verified paper audit trail systems involve adding a paper printout to a DRE system that a voter can review and verify. Some citizen advocacy groups, security experts, and elections officials advocate these systems as a protection against potential DRE flaws. However, other election officials and researchers have raised concerns about

potential reliability and security flaws in the design of such systems. Critics of the systems argue that adding printers increases the chance of mechanical failure and disruption to the polling place. Critics also point out that these systems introduce security risks involving the paper audit trail itself. Election officials would need to safeguard the paper ballots. If voting system mechanisms for protecting the paper audit trail were inadequate, an insider could associate voters with their individual paper ballots and votes, particularly if the system stored voter-verified ballots sequentially on a continuous roll of paper. If not protected, such information could breach voter confidentiality.

Weak security management practices. Selected state elections officials, computer security experts, and election experts view the reported instances of weak controls as an indication that the voting system vendors lack strong security management and development practices. Security experts and local election officials cite the position of trust that vendors occupy in the overall election process, and say that to ensure the security and reliability of electronic voting systemsâ€?as well as improve votersâ€? confidence in the electoral processâ€?vendorsâ€? practices need to be above reproach. Specific concerns have been expressed about (1) the personnel security policies used by vendors, including whether vendors conduct background checks on programmers and systems developers; (2) whether vendors have established strict internal security protocols and have adhered to them during software development; and (3) whether vendors have established clear chain of custody procedures for handling and transporting their software securely. A committee of election system vendors generally disagrees with these concerns and asserts that their security management practices are sound.

Election operations Several reports raised concerns about the operational practices of local jurisdictions and the performance of their electronic voting systems during elections. These include incorrect system configurations, poor implementation of security procedures, and operational failures during an election.

Incorrect system configuration. Some state and local election reviews have documented cases in which local governments did not configure their voting systems properly for an election. For instance, a county in California presented some voters with an incorrect electronic ballot in the March 2004 primary. As a result, these voters were unable to vote on certain races. In another case, a county in Pennsylvania made a ballot programming error on its DRE system. This error contributed to many votes not being captured correctly by the voting system, evidenced by that countyâ€?s undervote percentage, which reached 80 percent in some precincts. .

Poor implementation of security procedures. Several reports indicated that state and local officials did not always follow security procedures. Reports from Maryland found that a regional vote tabulation computer was connected to the Internet, and that local officials had not updated it with several security patches, thus exposing the system to general security threats. In another example, election monitors in Florida described how certain precincts did not ensure that the number of votes matched the

number of signatures on the precinct sign-in sheets, thus raising questions as to whether the voting systems captured the correct number of votes. A report from California cited a number of counties that failed to follow mandatory security measures set forth by the Secretary of Stateâ€?s office that were designed to compensate for potential security weaknesses in their electronic voting systems.

System failures during elections. Several state and local jurisdictions have documented instances when their electronic voting systems exhibited operational problems during elections. For example, California officials documented how a failure in a key component of their system led to polling place disruptions and an unknown number of disenfranchised voters. In another instance, DRE voting machines in one county in North Carolina continued to accept votes after their memories were full, effectively causing over 4,000 votes to be lost. The same system was used in Pennsylvania, where the stateâ€?s designated voting system examiner noted several other problems, including the systemâ€?s failure to accurately capture write-in or straight ticket votes, screen freezes, and difficulties sensing votersâ€? touches. A Florida county experienced several problems with its DRE system, including instances where each touch screen took up to 1 hour to activate and had to be activated separately and sequentially, causing delays at the polling place. In addition, election monitors discovered that the system contained a flaw that allowed one DRE systemâ€?s ballots to be added to the canvass totals multiple times without being detected. In another instance, a malfunction in a DRE system in Ohio caused the system to record approximately 3,900 votes too many for one presidential candidate in the 2004 general election. While each of these problems was noted in an operational environment, the root cause was not known in all cases.

Well.

Means, opportunity.... What else does any crime need? Motive! And a suspect! And maybe a suspect with a past pattern of behavior... Hmm, let me think...

NOTE Representative Rush Holt is doing good work on this issue. Sign his petition [7].

No votes yet

Source URL (modified on 12/05/2005 - 12:46pm):
http://www.correntewire.com/free_and_fair_elections_the_gao_report_on_voting_machines

Links
[1] http://www.correntewire.com/departments/department_of_no_they_would_never_to_do_that
[2] http://www.correntewire.com/thread/election_fraud
[3] http://frogsdong.blogspot.com/2005/11/support-hr-550-verified-voting-is.html
[4] http://www.gao.gov/new.items/d05956.pdf
[5] http://www.dailykos.com/comments/2005/12/2/181553/157/322#322
[6] http://www.correntewire.com/feedback

[7] http://www.rushholt.com/petition.html