

Proposal for special demonstration of alleged security vulnerabilities in the Diebold AccuVote-OS system claimed by Black Box Voting

In recent months, Black Box Voting has made many public allegations regarding security vulnerabilities of the Diebold AccuVote-OS (AV-OS) equipment. Several of these have centered around the AccuVote-OS system, in particular around the memory cards used to store the election definition and results. (blend w/ original)

In May 2005, election officials in the Leon County, Florida, provided Mr. Hari Hursti access to Diebold equipment in order to demonstrate potential vectors of attack on the AV-OS system. The exploits from Mr. Hursti's testing were detailed in the document entitled Black Box Report: Critical Security Issues with Diebold Optical Scan Design, dated July 4, 2005.

It is recognized that the memory cards used by the voting system contain sensitive information. As such they must be protected with the same care with which physical ballots must be, and are, protected. This protection is implemented through a combination of software and use procedures, and any examination of the system without considering both is necessarily inaccurate.

To alleviate potential concern with the Diebold AccuVote-OS (model D) firmware version 1.96.6, of which the vendor has applied for state certification, the Secretary of State's office is proposing the demonstration and testing described below. The purpose of this test is to identify security vulnerabilities that may exist that are not effectively mitigated by proposed Use Procedures, to identify security vulnerabilities that cannot be mitigated, if any; and to identify additional security measures that can be taken to enhance the security of the Diebold OS voting system. This test will be strictly limited in scope to the real-life conditions imposed on the operation of this system in the proposed California Uses Procedures for the proposed Diebold system. Representatives will be asked to demonstrate how the Diebold OS system can be attacked and official vote results can be altered without detection via their proposed manipulation of OS memory card.

Proposed Testing Protocol

Pre-Test Equipment Verification

1. Diebold representatives will present a GEMS server and AccuVote-OS v. 1.96.6 equipment, configured in accordance with the system specifications currently pending California certification for use, and in accordance with the proposed Official Use Procedures submitted for certification of this system. The system will be configured for the standard test General election used for California certification testing.
2. After the GEMS server and the OS reader have generated zero reports, a standard logic and accuracy test deck will be processed through the AV-OS reader and the tabulated vote results will be printed out on the AV-OS. The vote results will then be uploaded to the GEMS server and vote results will be printed from GEMS. The vote reports from both GEMS and the AV-OS will be verified.
3. The election will be zeroed and reset on the GEMS server and the AV-OS card will be re-downloaded.

Pre-Election Setup & Testing

4. Black Box Voting representatives will be asked to explain and demonstrate how their proposed attack on the system would be conducted undetected.
5. Black Box Voting representatives will then be provided with a freshly-downloaded memory card and allowed a maximum time of (time limit) to manipulate the data on the card, while under observation by Secretary of State and Diebold personnel.
6. The memory card will be sealed in the AV-OS unit using appropriate tamper-evident seals and Secretary of State personnel will set the unit for election.

7. A zero report will be printed from the AV-OS.
8. The standard logic and accuracy test deck will be run through the AV-OS once again. After “closing the polls”, a poll closing summary report will be printed from the AV-OS and compared to the results from the previous test.
9. Vote totals from the altered memory card will be uploaded to the GEMS server. Vote results reports will be printed from GEMS and compared to the report from the AV-OS, as well as the reports from step two, above.

Election & Post-Election

10. Integrity of the tamper-evident seals on the AV-OS unit will be verified.
11. A zero report will be printed from the AV-OS.
12. A set of ballots will be run through the AV-OS machine under supervision. After “closing the polls”, a poll closing summary report will be printed from the AV-OS unit and compared to the actual ballots that were cast.
13. Vote totals from the AV-OS unit will be uploaded to the GEMS server. Vote results reports will be printed from GEMS and compared to the report from the AV-OS.

Detection of tampering at any point by election officials during the test will be considered failure of the attack.

Proposed Test Conditions

1. Prior to the test, Black Box Voting will identify all the attacks they intend to demonstrate.
2. The tests will be private and held on the Secretary of State premises at a time mutually agreeable to Secretary of State and Diebold. The Secretary of State will provide security.
3. Black Box Voting will be limited to three participants at the test. Diebold will be limited to four participants at the test.
4. The test and its results will remain confidential for thirty days or until the Secretary of State publishes its report on the test, whichever event comes first. All participants in the test will sign a confidentiality agreement to that effect.
5. Secretary of State personnel will record the entire test on videotape. One camera will be positioned to record the overall test. A second camera will be used to provide close up recording of Black Box Voting’s actions to read and alter the memory card, as well as any anomalies that occur during the test. Additionally, the Secretary of State may use still photography to document the test and any problems encountered. Black Box Voting may make no other recordings of the test.
6. Black Box Voting personnel may observe the operation of all Diebold equipment, but (with the exception of step 4 above) may not touch or operate the Diebold equipment during any of the testing. Violation of this provision will immediately terminate the test.
7. All test reports, as well as all recordings of the test will remain the physical property of the Secretary of State. Copies of the reports and the recordings will be provided free of charge to Black Box Voting upon publication of the Secretary of State’s official report of the test, or upon the thirtieth day following the test, whichever comes first. The altered memory card will remain the property of the Secretary of State as well.
8. Upon Secretary of State request, Black Box Voting will provide documentation of any programs or utilities used to alter the memory card for the test, as well documentation of the steps taken to alter the card.