Voting System Examination
AccuPoll, Inc

Prepared for the
Secretary of State of Texas

James Sneeringer, Ph.D.
Designee of the Attorney General

This report conveys the findings of the Attorney General's designee from an examination of the equipment listed, pursuant to Title 9, Chapter 122 of the Texas Election Code, section 122.036(b).

Examination Date	May 27, 2004
Report Date	June 19, 2004

Component	**Version**	**NASED Number**
AccuPoll Voting Station (AVS)	2.3.14	N-2-13-11-11-001
Voting Administration Workstation (VAW)	2.3.14	N-2-13-11-11-001
Central Count Server	2.3.14	N-2-13-11-11-001
Central Vote Consolidator	2.3.14	N-2-13-11-11-001
Election Management System (EMS)	2.3.14	N-2-13-11-11-001

Notes

- All components are Unix-based and implemented in Java.
- The hardware, except for the clamshell, is off the shelf.

DRE System: AccuPoll Voting Station and Voting Administration Workstation

Election Setup	The election definition is loaded into the VAW laptop from a CD-ROM created with the Election Management System (EMS). The entire election definition is stored in each VAW and downloaded from the VAW to the voting stations as needed. Software to operate the VAW and voting stations is also loaded into the VAW via CD-ROM. There is permanently resident software that performs this loading, and it refuses to load any software that has not been digitally signed by AccuPoll.
Zero-total report	On the ink-jet printer in any one of the voting stations.

Authorization to vote / Ballot selection	A poll worker initializes a GoVote card on the VAW laptop to authorize voting and specify the precinct. This card can only be used to vote once, until it is re-activated by a poll worker for another voter.
View / Vote	LCD display / touch screen
Vote Storage	On a system with one VAW laptop in the precinct, four or five copies of each vote record are stored as follows: (1) MySQL database on the hard drive of the voting station, (2) the optional paper proof of vote, (3) a postscript record stored as a BLOB in the same database, (4) a compact flash memory in the voting station, and (5) in a MySQL database on the VAW laptop. Two of these are on the same physical device, but the data is still on a minimum of three different physical devices, not counting the paper. Each additional VAW laptop in the precinct adds one additional copy.
Provisional Ballots	If a provisional ballot is requested, the VAW laptop automatically prints out a ballot retrieval number, which can later be used to accept the ballot.
Connectivity	All precinct equipment is connected using Ethernet. There should be no connections to other equipment or to the Internet. Transmissions are check-summed with a private protocol.
Precinct Consolidation	Precinct results are continuously consolidated on the VAW laptop in the precinct. If there is more than one VAW laptop, the consolidated results are stored on all of them.
Transfer Results	Results are written on an encrypted CD for transfer to the Central Vote Consolidator and the Central Count Server. A re-writable CD cannot be used. Modem transfers are also supported, but AccuPoll did not request certification of modem transfers.
Print precinct results	On the ink-jet printer in any one of the voting stations.
Straight party / crossover	Yes. Any straight-party voting must be done before any votes are cast in individual races. This means that straight-party voting cannot override votes in individual races, but it also means that straight-party votes cannot be changed, except by voiding the entire ballot and starting over.
ADA	Yes, but ADA capability is verified separately by the Secretary of State's office, so it was not demonstrated to the examiners.

Setup & Tabulation: Election Management System, Central Vote Consolidator, Central Count Server

Tamper Resistance	Operating system access is prohibited at all times (not just when the system is running) and data is protected by Unix and MySQL passwords. Other data is protected by other passwords. The system boots directly to the AccuVote application, and AccuVote asserts that operating system access is not possible without opening the machine, but admits that access can be achieved by an expert if the machine is opened.
OS access	Not permitted. See previous item for details.
Real-Time Audit Log	No.
Data Integrity	We did not discuss how they maintain data consistency between tables in the event of a power failure or other similar event.

Transmission	Although AccuPoll supports modem transmission, they asked that it not be certified at this exam.

Concerns

1. If a voter tries to change a straight-party vote, it will first give a warning and then clear the entire ballot.
   Recommendation: This behavior is unusual and inconvenient for those affected, but acceptable in my opinion, because I believe straight-party votes are rarely changed.
2. In the exam, it was not possible to change a straight-party vote at all, but this is a configuration option.
   Recommendation: In Texas, the system should be configured to allow straight-party votes to be changed, and this should be a requirement for certification.
3. Access to the entire machine is controlled by passwords (such as the BIOS password) that are known only to AccuVote. This security measure can be broken (as AccuVote admits) by someone who can take the machine apart, and (in my opinion) can likely be broken without disassembling the machine, because BIOS security is only designed and intended to provide protection against casual access attempts. For example, many manufacturers have master BIOS passwords that can be easily found on the Internet.

   The machine most vulnerable to attack is the VAW laptop, since it controls the others in the precinct. We should assume that attackers can gain access to the machines if they have physical access, which means that other safeguards are needed. For example, databases should be protected by encryption or hash codes, such as a CRC. Otherwise, fraud could be perpetrated by tampering with tables.

   For example, a single county employee with physical access could switch the candidate names in the Candidates table (page 11 of the *AccuPoll EMS Hardware / Software Specification*) in some precinct laptops, and the result would be that the vote totals for those two candidates would be reversed in those precincts. Only data would be changed, so this would be undetected by the checksum AccuPoll computes on the code, or any other safeguard I know of. It could be done directly without accessing the file system or database, so one would only need to either get past the BIOS password, or take the machine apart and directly access the hard drive.
   Recommendation: Certification should be denied until AccuPoll either provides additional database protection or explains how existing safeguards are adequate.
4. Passwords are stored in a password vault. AccuVote would not say how the vault password (or master password) is stored or protected, although they offered to let us try to break it.
   Recommendation: Although we could attempt to break it by hacking, it would be time consuming. I recommend that the system not be certified until AccuVote reveals how it works.
5. The Central Count Server does not have a real-time audit log.
   Recommendation: Since this is required, the system should not be certified until the problem is fixed.

6. We do not know what steps AccuPoll has taken to guarantee database integrity in the event of a system failure, such as a power failure. The system must guarantee that a precinct can never be double-counted or omitted. For example, if a failure occurs at central count, all internal table must be consistent – either the precinct data must be recorded both in the totals table and in the table of precincts received, or it must be recorded neither place. One method is to use a commit/rollback feature of the database, but there are others. Similar precautions should be taken with the precinct equipment.
   Recommendation: This should be discussed at the next exam.
7. The GoVote card is difficult to insert into the voting station. It must be pressed in with some force, and when this is not done the station doesn't work and it isn't clear what is wrong, so the voter may not be able to recover without help. It does not help to press hard on the card after it is inserted; it must be removed and re-inserted.
   Recommendation: AccuPoll should solve this problem, possibly by finding more tolerant hardware.
   Note: I think it is better to authorize voting by printing a slip of paper with a numeric authorization code, and have the voter enter the number at the voting station. This eliminates problems inserting the card, saves the expense of the cards and card readers, and makes it unnecessary to retrieve the cards from voters. The codes should be 4 to 5 digits and should automatically expire if not used in a short time – say 30 minutes. This is merely a comment, with no effect on certification.
8. Although the card reader is labeled with a picture, it is not completely clear which way the card should be inserted.
   Recommendation: AccuPoll should solve this problem. In my opinion, the very best solution is to label one side of the card with arrows and words to indicate which end to insert, and then orient the card reader so that the card is inserted with the label facing up, rather than left or right. Experience with retail readers indicates that users are almost never confused if the label faces up, but frequently confused (even with extensive labeling) by any other orientation.

Conclusion.

Although there are some problems, AccuPoll has done an excellent job overall and the system has a lot of potential. I encourage them to address the problems and bring the system back for re-examination.