SECURITY TESTING REVIEW

COLORADO EVOTING SYSTEMS

Mike Weber
Office of Cyber Security
17 Dec 2007
Version 1.8

EXECUTIVE SUMMARY 3
BACKGROUND 4
THREAT AGENTS 4
Adversaries 5
Adversaries not evaluated 6
Usage Scenarios 6
VULNERABILITIES 7
RISK ASSESSMENT 7
Premier Election Solutions (formerly Diebold) 7
ES&S 8
Sequoia 8
HART 8
CONCLUSION 9

EXECUTIVE SUMMARY

The Office of Cyber Security received a request in late November to assist the Secretary of State by providing a review of the security specific test results as recorded by the Voting Systems Certification Program Testing Board (Testing Board). The work effort was scheduled to begin on December 4, 2007 and be completed on December 12, 2007. Due to the abbreviated nature of this review, it was understood among all parties that the results would not be comprehensive enough to serve as a determining factor in certification or decertification.

A meeting was held on December 4 to identify the purpose and goals of the engagement as established by the Secretary of State. We met with the Testing Board on December 5 and began reviewing the Restrictions documented in each project overview report generated by the Testing Board. December 6 and 7 were spent reviewing each Condition documented in the Testing Board reports and we analyzed the risks imposed by the failed security tests on December 10 and 11.

The only impact addressed by this report is that of *altering votes*. Other risks were identified that could be realized, such as an increase in public distrust of the system, forcing an audit or recount, frivolous litigation, denial of service, and privacy compromise, but are not explored in this report.

The following table outlines the number of findings by Vendor that indicate the risk of internal users exploiting system vulnerabilities to alter recorded votes.

Vendor System	**Risk Findings (total)**
Premier Election Solutions (formerly Diebold)	4
ES&S	6
Sequoia	5
Hart	4

The common thread between each risk is the *insider threat*. All high risk scenarios that could result in altered votes involve improper use of the system by county or state personnel. Thus, if the Secretary of State believes this risk is sufficiently mitigated within each county through their internal security plans or through audit of their personnel practices, the risks would be mitigated since the “external only” field would apply and there are no external Risk Findings.

BACKGROUND

This document contains summary data for the review project. It is detailed in the following categories:

- Threats (Threat Agents)
- Vulnerabilities
- Risk Assessment
- Mitigating Factors
- Conclusion
- Recommendations

These categories are liberally derived from the best practice framework for Risk Assessment in accordance with NIST SP 800-30. This framework identifies Risk as a function of the probability of a given threat agent exercising a vulnerability and the resulting impact of the adverse event, while taking into account the existing controls already in place. For the purpose of this assessment:

- Probability was identified as “high” if a particular threat agent had direct access to exploit a specific vulnerability and would likely go undetected.
- “Altering votes” was selected by the Secretary of State to be the evaluated impact. The impact of altered votes was set as “high”.
- Vulnerabilities identified are specific results of failed test criteria, thus all of them have been verified to be present.
- Control mechanisms in place include the documented Conditions in the overview reports, along with the following assumptions:
  - The Usage Scenario within the counties follows the best-case example provided by the Testing Board
  - The Election Judges are trustworthy
  - The state Testing Board is comprised of highly capable individuals

For each system, the specific vulnerabilities were examined to identify which threat agent might be able to exploit it, at what phase it could be exploited, and whether the impact had a high likelihood of occurring.

THREAT AGENTS

A threat agent is the person, group, or occurrence that could potentially exploit one or more vulnerabilities present on a given system. The threat agents identified through this engagement were used for all systems.

Typically, risk assessments take into account the statistical probability that a threat agent may exploit a vulnerability based on motive, means, and opportunity. Since the systems that were assessed have “cyclical” usage patterns with reasonably distinct phases of use during which specific tasks occur, we found it necessary to evaluate each threat agent acting at a specific phase of usage instead of as an aggregate. For example, while the threat of citizens (voters) exploiting a specific vulnerability during an election provides 100% opportunity, averaging that threat over the course of two years (or 25 months) would dilute the level of exposure (1 day / 730 days).

Adversaries

Political Activists:
This group is composed of organizations that are opposed to electronic voting in general or are specifically targeting an elected official to either discredit them or to have them removed from office. This group is external to the voting process and their actions are deemed to be external and organizational. An example might include calling for a recount or audit or filing some sort of litigation regarding the integrity of the voting system.

Vandals:
This group is comprised of individuals that act alone, for no other reason than causing damage or mischief. Their motivation is to cause chaos.

Disgruntled County Employees:
This group is comprised of county employees that have access to the County Clerk's office. It is assumed for the purpose of this assessment that these individuals have access to all components and are part of the election process.

Disgruntled State Employees:
This group is comprised of employees or contractors in the Secretary of State's Elections Division office. A disgruntled state employee may include those that have been bribed or otherwise coerced and who's motive is revenge or personal gain.

Insufficiently Trained County Personnel:
This group is comprised of county employees or contractors that are part of the election process. These people would be responsible for storing, maintaining, and programming the voting systems in use by their respective county. They have no motive in particular and the actions that were evaluated here are "mistakes".

Insufficiently Trained Election Judges:
This group is comprised of the volunteer election judges. They have no motive in particular and the actions that were evaluated here are "mistakes".

Unknown or Remote Groups or Individuals:
This group is included in the event there are systems that can be accessed over a telecommunications network outside the boundaries of the immediate building.

Voting System Vendor:
This group includes the specific vendor's employees and contractors. Generally, this group's motives are of a business-preservation nature.

Citizens (voter):
This group includes regular citizen voters that have no malicious intent.

Adversaries not evaluated

Disgruntled (Malicious) Election Judges:

Because this group is a trusted insider group that can significantly alter the course of an election, they were not included in the evaluation. If the integrity of this group were in question, the accuracy of every election, including those that use only paper ballots, would be suspect.

Insufficiently Trained State Personnel:

This group is comprised of state employees or contractors that are part of the election process. These people would be responsible for certifying the voting systems and installing trusted build software and firmware. They have no motive in particular and their actions would be classified as “mistakes”. This group is not being evaluated due to the trusted and highly skilled nature of the group. If members of this group are not fully trained subject matter experts regarding the systems being tested or installed, there would be no controls that would prevent significant mistakes from occurring.

Usage Scenarios

The usage scenarios below were relayed to the team during the assessment. These are “best-case”. Since the team had no method of determining if any counties can uphold the operational and/or environmental procedures required by the State, the only scenario that was taken into account was this “best case”.

Phase I: Storage

Phase II: 60 days before election, ballot preparation

Phase III: 40 days before election, verify paper ballots and program memory cards

Phase IV: 14 days before election, conduct accuracy tests

Phase V: Early voting (14 days prior for General election, seven days prior for Primary).

Phase VI: Day before election:

Polling Place Election: Election Judge takes system(s) to his home, to be transported to the polling place the day of election.

Voting Center Election: Contractor or County delivers palletized and shrink-wrapped voting systems to the Voting Center,

Mail-in Ballot Election: Contractor or County delivers voting systems to the County Clerk’s Office.

Phase VII: Election day, open and close polls, collect memory cards and send to county clerk’s office by courier.

Phase VIII: One or more days after election, contractor or county retrieves systems and delivers them to storage.

Phase IX: Within 17 days of the election (14 days for a Primary election), Counties will conduct post-election audit and report security incidents to the Secretary of State for review.

Phase X: County performs maintenance and repairs while in storage.

VULNERABILITIES

A complete list of vulnerabilities identified by the testing team and evaluated as significant is detailed in a separate document and maintained by the Secretary of State.

RISK ASSESSMENT

The following list, broken down by individual vendor, describes what threat agent can act on a vulnerability during one or more usage scenario phases. The following impacts were recognized as a result of the failed security controls:

1. Alter vote totals
2. Promote public distrust
3. Force an audit or recount
4. Litigation
5. Denial of Service
6. Compromise of voter privacy

Due to the compressed timeframe during which this assessment was performed and aligning with the Secretary of State's goals, the only Risk scenarios described here are those that result in a high risk of changing vote totals. Note that for each system and based solely on the results of the Testing Board's evaluation of the security controls, there were a greater number of high risk scenarios identified for risks other than the *alteration of vote* totals.

Premier Election Solutions (formerly Diebold)

1. Disgruntled county employees can change vote totals by altering the database directly, outside of the application, during an election.
2. Disgruntled county employees can change vote totals within the application and go undetected during an election.
3. Insufficiently trained county employees can change vote totals within the application and go undetected during an election.
4. Disgruntled county employees can load corrupt firmware both after accuracy testing and before the end of the election.

ES&S

1. Disgruntled county employees can use the reporting module and alter votes during an election.
2. Disgruntled county employees can upload votes to the system for counting multiple times on purpose.
3. Disgruntled county employees can alter votes processed by the central count scanner (due to the requirement for the system to remain logged in as the local administrator) at any time between accuracy testing and the end of the election.
4. Disgruntled county employees can load compromised software / firmware at virtually any time without being detected due to the system not having the ability to verify the trusted build.
5. Disgruntled state employees can load compromised software / firmware without detection due to the lack of the system to provide trusted build verification in the field.
6. Disgruntled county employees can reprogram the Direct Reporting Electronic (DRE) voting machine without detection after the accuracy tests and before the election.

Sequoia

1. Disgruntled county employees can alter the database undetected at any time during an election due to the requirement for the system to run as administrator.
2. Disgruntled county employees can reload the software and set the database access credentials at any time due to the requirement for the system to run as administrator and the inability to verify trusted build.
3. Disgruntled county employees can change vote totals or otherwise alter the database without detection at any time during an election due to the lack of comprehensive logging in the application.
4. Disgruntled county employees can alter any data processed (including vote totals) during an election through WinETP due to the requirement for the system to operate under administrative credentials without a password.
5. Disgruntled state employees can load compromised software / firmware without detection due to the lack of the system to provide trusted build verification in the field.

HART

1. Disgruntled county employees may have* the ability to alter the database, thereby altering vote totals by accessing the database directly at any time during an election.
2. Insufficiently trained county personnel may have* the ability to inadvertently alter vote totals by accessing the database directly at any time during an election.
3. Disgruntled county employees can load uncertified, untrusted software / firmware provided by the vendor due to the inability of the system components to produce a trusted build verification and the lack of adherence to the trusted build methodology shown by the vendor.

4. Disgruntled county employees can zero out the database within the application and from the operating system during an election and go undetected due to incomplete logging.

* - the proprietary nature of the system precluded testing certain conditions; therefore these conditions were assumed to be true and are reflected here as a possible condition.

CONCLUSION

All of the identified risk situations that have a direct result of altered votes rely on disgruntled employees taking action (15 scenarios involving disgruntled county employees and two scenarios involving disgruntled state employees). The remaining two risk scenarios presume specific mistakes will be made by county personnel.

If the Secretary of State is comfortable with the existing training provided to county and state personnel or if there is a significant work-around developed by the Testing Board that would provide a “detective control”, these risk scenarios could be considered mitigated.