+ iBeta Software Quality Assurance

Pima County Final Report

Created For:	
Program Name	PIMA
Final Version	N/A
Client	Pima County, Arizona
Project Lead	Kathleen Kempley

Created By:	
Project Lead	William Miller
Test Lead	William Miller
Date	July 2007

Table of Contents:

Executive Summary

iBeta was approached to perform a quantitative investigation for Pima County, Arizona of a specific Diebold GEMS electronic voting system version and associated hard drive data with regard to alleged vote tampering.

The investigation took place at iBeta's certified testing facility in Aurora Colorado.

iBeta received a sealed Seagate Barracuda 7200, ST3250820A, 250 gigabyte hard drive (s/n 6QEoNTQZ) from Pima County which contained four drive images in Symantec Ghost format.

iBeta staged the images for investigation and analysis using an external IDE to firewire converter. Of these images it was discovered that only two, "Item 1" and "Item 2" contained useable data and "Item 1" was 10.2 gigabytes in size while the "Item 2" image was 204 gigabytes in size.

The target file of the investigation was a Diebold GEMS database backup file called "pima consolidated 051606 EARLY DAY1.gbf" which, according to the audit log of the GEMS software was initially created 05/10/06 at 12:27:27, and then overwritten 05/11/06 at 09:56:30.

The focus of the investigation was to determine the validity of the target file and to look for evidence of tampering. The investigation consisted of several tests:

1. R-Studio scans of the two hard drive images "Item 1" and "Item 2" to look for partial, ghost, or deleted evidence of a different version of the DAY1 file, which came back negative.
2. Date and timestamp checks on all of the available copies of the DAY1 file. This showed some irregularities, but these were later explained away by the troublesome installation and backup of the new GEMS systems on July 20th 2006 and the normal copy and cleanup process on July 27, 2006 in preparation for the next election.
3. CRC comparisons on the five available copies of the DAY1 file, which showed all of the files to be identical across the two systems.
4. CRC comparisons of the Preference tables in the 051606 databases which show that the programming was not altered from the initial "L and A" run for the 051606 event.
5. Backing out the deck data in the DAY1 database to uncover any discrepancies in votes coming in and votes total which would pinpoint the addition of votes. This showed no variation in vote totals.

During testing it was discovered that the GEMS software exhibits fundamental security flaws that make definitive validation of data impossible due to the ease of data and log manipulation from outside the GEMS software itself.

Ultimately, it is the determination of iBeta that the overwriting of the target file can be attributed to human error. iBeta arrives at the "human error" conclusion for two reasons:

- iBeta was unable to detect any manipulation of the 051606 event data across the multiple copies of the data discovered.
- The basis of the investigation is that there are log entries that point to tampering - but it is far easier to remove evidence of tampering from the logs than to actually tamper with the vote totals in the Microsoft Access database that the GEMS software uses. So it does not follow that someone with the knowledge to manipulate the GEMS data would neglect to alter the log file to remove the evidence of the manipulation.

Summary of Testing

Setup & Planning

The focus of the investigation was to determine the validity of the target file and to look for evidence of tampering.

Test Execution

The investigation consisted of several tests:

1. R-Studio scans of the two hard drive images “Item 1” and “Item 2” to look for partial, ghost, or deleted evidence of a different version of the DAY1 file, which came back negative.
2. Date and timestamp checks on all of the available copies of the DAY1 file. This showed some irregularities, but these were later explained away by the troublesome installation and backup of the new GEMS systems on July 20th 2006.
3. CRC comparisons on the five available copies of the DAY1 file, which showed all of the files to be identical across the two systems.
4. CRC comparisons of the Preference tables in the 051606 databases which show that the programming was not altered from the initial “L and A” run for the 051606 event.
5. Backing out the deck data in the DAY1 database to uncover any discrepancies in votes coming in and votes total which would pinpoint the addition of votes. This showed no variation in vote totals.

Test Specifics

Test 1 – R-Studio was used to perform a drive-wide scan for deleted, partial, and ghost copy data. While R-Studio did find and recover a great deal of interesting data, none of it was relevant to the investigation at hand.

- This test can be defeated by repeated loading, deleting, and defragmentation of the hard drive, which repeatedly overwrites the deleted data with parts of other files and makes recovery very difficult. Based on iBeta's observations of the drive images this defeat was not performed.

Test 2 – The date and time stamp checks of the files did turn up what appeared to be evidence of tampering as the files pertinent to the investigation showed a pattern of irregularities in either the date/time created or modified. John Moffatt did some investigation on his end and discovered that there were some issues in the backup, installation, and recovery of data during a July 20th 2006 GEMS system update followed by the normal copy and cleanup process on July 27th. This explained the oddities discovered in the file timestamps.

- This test can be defeated by altering the date/time stamp data for the files. There are utilities which will do this, but it appears that this was not done because the files still exhibit non-uniform dates/times. It is unlikely that that defeat was performed because if one of these utilities would have been used, there would have been no alert as all of the date/time stamps would have been sequential to the event - leaving no clue that the files had been altered or replaced.

Test 3 – Ultimately five copies of the target file were discovered or recovered. These five versions were run through a CRC32 process which is used to determine file changes at a bit level. The CRC check returned that all five of the files were identical. The CRC32 value of the target files was "FAD8C70E".

- It is possible to defeat this test by replacing all of the copies of the target file with a prepared version. It is unlikely that the defeat was employed due to the various modification date/time stamps on the target file – if this defeat had been deployed all of the replacements would have the same create/modify timestamp. Additionally the file residing in multiple locations on multiple computers makes this defeat very difficult as access to the various machines and knowledge of the locations would be required.

Test 4 – John Moffatt proposed a test to determine if the programming used in the 051606 event which compared the "preference" table of the initial L and A test to the various saves of the 051606 event. The compare showed that the programming never changed from the initial L and A event.

- It is possible to defeat this test by way of replacing the preference table in all of the 051606 event data sets after the event was over. This defeat being used is unlikely due to the modify date/time stamps of the original L and A data being from the day preceding the event and every copy of the L and A data exhibiting the same date time stamp. A blanket replace of the entire 051606 event dataset would have had to take place to defeat this test, which encounters the same issues as Test 3.

Test 5 – John Moffatt also proposed a test to determine if any votes were added to the vote totals from an external source. This test used the GEMS software to list the decks for each segment of the 051606 event and when backing those decks out, a total of zero votes remained. This means that all of the votes seen came from the central count scanners or precinct voting machines and not some other source.

- As with other tests it is possible to defeat this test by ensuring that any vote modification keeps the vote totals the same. This means that if you add 1000 votes to one candidate, you subtract a total of 1000 votes from one or more other candidates. This defeat has a low probability of being deployed based on the fact that it only works for the total number of votes. Any report run that shows the votes at a precinct level, when compared to a total votes report, will show the data modification.