black box voting
CONSUMER PROTECTION FOR ELECTIONS
www.BlackBoxVoting.Org
330 SW 43rd St Suite K PMB 547 Renton WA 98055
425-793-1030 http://www.blackboxvoting.org

Diebold TSx Evaluation

SECURITY ALERT: May 22, 2006
Supplemental report, additional observations

Unredacted on July 2, 2006 by Black Box Voting

A Black Box Voting Project
Prepared by: Harri Hursti

On behalf of Black Box Voting, Inc.

Purpose of this document

This document captures some miscellaneous supplementary observations for further study. These items should be considered either not properly studied, or just starting points without any real study done and without known significance, if any. In some cases it is unknown if the item discussed has been only existed in the development phase and been disabled or removed before release version.

1. Flash memory erasure:

There seems to be a memory card-triggered feature to erase the contents of flash memory. This destructive function was started in the TS6 with the file EraseFFX.bsq, and was carried over to the TSx when the file ErasePSM.stl is found on the memory card. This feature was not tested in Emery County and should be examined further.

2. Further study needed on macros:

TS6 and TSx machines have as build-in feature new kind of macro capabilities. This capability is simplistic Windows Window Manager Message recording and play function. Presumably the feature has been designed for automation of volume testing, if this is the case it is important to understand that this approach bypasses part of the system and therefore is by no means equal to end-to-end testing. There are number of concerns, including but not limited, around this feature functionality warranting further studies.

- The files are stored on the removable memory card as unprotected plain-text files. There are no protection mechanisms against modifications to these files
- Are the WM_message filters adequate
- Is the processing function secure against buffer overflow / boundary overflow attacks
- the message parameters passed back to windows checked, is there proper exception handling in place

Creation and access to the macros is available on poll worker level access, under circumstances even without any smart card authentification.

On the preliminary testing following issues were identified :

- macro is not contained in the user interface logic. Because of this macro can access settings changing the telephone number / ip address and initiate call
- Two machines, with completely identical software release numbers had different behavior with the same macro. Machine A just had a software crash and become unstable, while machine B produced an error message on the system log and contained the error while still ending to experience loss of software functionalities. There were other examples of different, but reproducible, software behaviors between machines with both modified and unmodified macros.

- File handle processing seems to be flawed and interrupted by exception macro processing produced open file handles
- There seems to be user interface race conditions, which can not be triggered by human interaction with the machine, but are revealed by no delay playback of the human actions

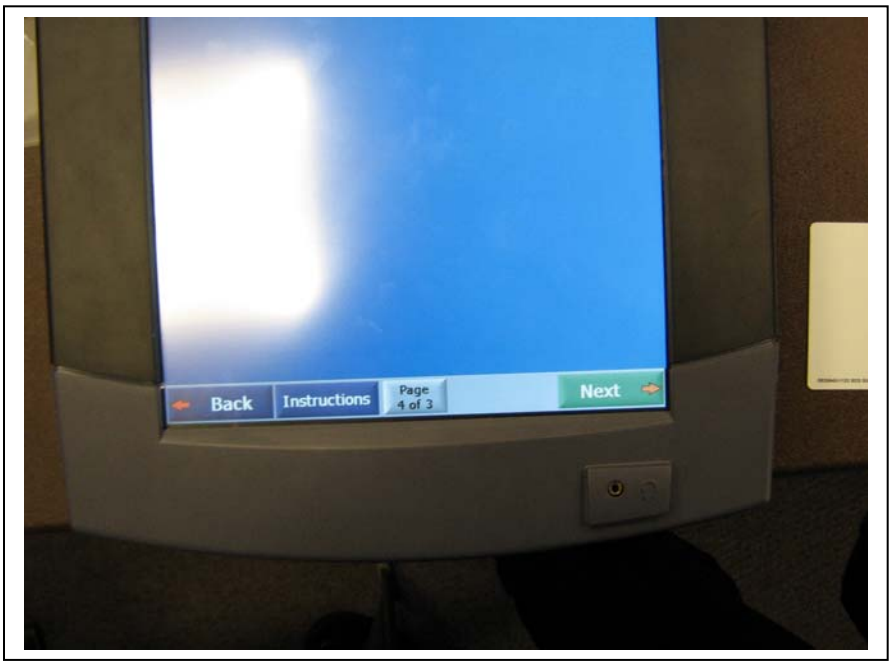

Fig. 8 – Macro skips to "Page 4 of 3" of 3 page ballot and stops without error message while macro is still active

3. Back door

The TS6 is likely to have an additional back door for accessing windows, though this could not tested in Emery County – also it is unknown if any of this in any form has been carried over to TSx. Further source code analysis of the well-known "CVS.TAR" file[2], which contains source code for the TS6 and has been widely used in touch-screen system security studies, has revealed this feature.

The fact that this backdoor has not been published before underlines the fact that source code reviews performed this far have been not conclusive.

The start-up program for the ballot station is looking for existence of file Explorer.glb on the

memory card. The file itself can be empty, because the found file based on the name alone is a trigger for alternative execution of general purpose file management utility program instead of the ballot station, therefore enabling access to Operating System. This back door has also been documented in the publicly available memos:

> Re: Tippacanoe, IN - Upgrading AVTS
>
> * To: <support@dieboldes.com>
> * Subject: Re: Tippacanoe, IN - Upgrading AVTS
> * From: "Talbot Iredale" <tiredale@dieboldes.com>
> * Date: Tue, 8 Oct 2002 10:38:37 -0700
> * References:
>
> <GOEFLGCGEKJOLBNCMPEIOELOCCAA.jeffhintz@dieboldes.com>
>
> To access the OS in WinCE 3.0 create a file called "Explorer.glb" on the pcmica card, insert the card into the unit and turn the unit on. The unit will then display the desktop rather than run Ballot Station. You can then go to the windows directory and select "control" and then "network" to set the ip address.
>
> The other option is the setup a DHCP server on the Windows machine which will automatically configure the network card.
>
> Tab

4. Automatic deletion of files, including election file-extension files:

In case the memory card is full, the system will, without any interaction with user start to delete files from the card to free up memory. This deletion will also take out files with election file extensions from the election subdirectory. There is no way to verify which logic the system follows when choosing for the files to be deleted.

5. Memory card test file merits further study:

From the publicly available documentation there is reference to memory card testing with 16-bit "gray-code algorith" using file:

COUNTUP.DAT

This functionality should be studied,. Vulnerabilities are unknown.

6. Other file names should be examined:

The following references were found from the publicly available documentation :

DIAG.BIN
DIAG.NB0

No testing was done with these files, it is unknown what, if any, functionalities are involved.

7. Outdated OpenSSL version

The OpenSSL used in the TSx BallotStation 4.6.4 software is an outdated version 0.9.7e, dated 25/10 1994, which is known to contain some security vulnerabilities. At the time of the writing, most current versions are 0.9.7j and 0.9.8b.

8. Certificate will expire

The Cyptographic certificate of TSx has an expiration date of 31/1 2009. Installation / replacement process for renewed certificate was not studied.

9. Piggyback connectors under modem

The modem is implemented on the motherboard as piggyback module. However, there are two sets of connectors underneath this modem built for two different kinds of piggybacks. It is unknown what the other piggybacks enable.

11. Memory discrepancies:

Emery County Clerk Bruce Funk noticed that some of his machines, which were marked with a yellow stick-on dot and had serial numbers in the 201000-223000 range, had screen messages indicating critically low available memory storage at the time of the delivery. Whereas machines in the 230000-255000 range had memory storage of 22-27 MB, the machines in the earlier serial number blocks had memory storage of 4-8 MB.

Funk was told by Diebold representatives[1] in a tape recorded meeting Mar. 27, 2006 that there were no differences between the programs installed on the machines, that none of the machines were used, and that there were no extra programs on the machines.

It was noted during this study that some machines contained test election data. Deleting this data did not free up a significant amount of memory. After this study, Diebold has explained that this lack of memory is due to the presence of extra fonts installed on some machines. No study was done to find out the reason for varying free memory sizes.

Serial Number	Available memory	Serial Number	Available memory
201492	7 MB (17% free)	245521	26 MB (59% free)
203638	6 MB (14% free)	244533	24 MB (54% free)
210639	8 MB (17% free)	245397	25 MB (57% free)
211883	7 MB (16% free)	245506	26 MB (60% free)
216349	8 MB (19% free)	248120	26 MB (59% free)
219632	7 MB (17% free)	248250	25 MB (58% free)
220005	4 MB (10% free)	248347	25 MB (57% free)
223158	11 MB (25% free)	248469	26 MB (58% free)
230354	22 MB (51% free)	249309	25 MB (57% free)
232637	24 MB (55% free)	249448	27 MB (62% free)
237382	26 MB (59% free)	251787	27 MB (60% free)
243050	24 MB (55% free)	254449	23 MB (52% free)
244076	26 MB (59% free)	254546	25 MB (56% free)
244282	25 MB (58% free)	254706	25 MB (57% free)
244401	28 MB (63% free)	255073	25 MB (58% free)
244486	26 MB (58% free)		

Fig. 9 – Serial numbers: Variations in memory storage available

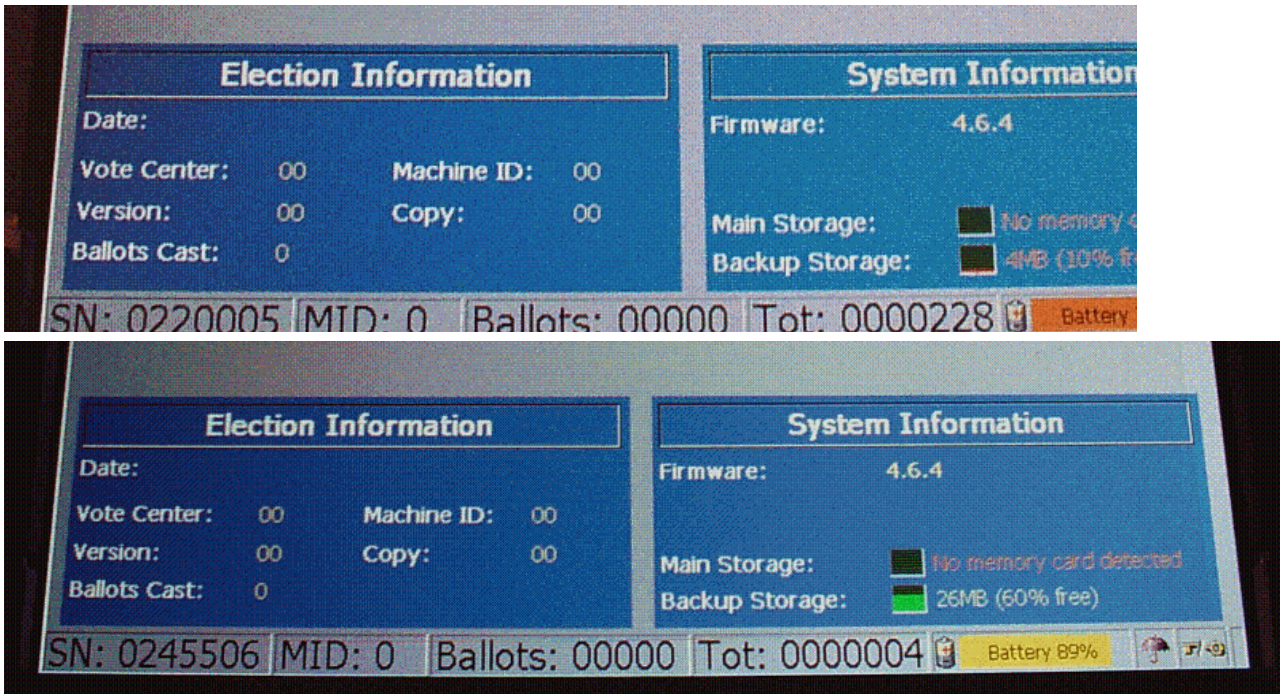

Fig. 10 – Screen shots: Variations in memory storage available

12. Electrical hazards:

The electrical sockets on the TSx are not properly fitted to the case. Every unit examined revealed problems with sockets popping out or falling out, sometimes by simply moving the machine or through light contact with the cord. Because many polling places lack sufficient wall outlets to plug in all the machines, these machines are typically daisy-chained together

(one machine plugged to the next) with a single machine plugged in to the wall. The improperly designed socket design presents potentially an electrical hazard to poll workers and voters.

Fig. 11 – Exposed 110 volt wiring and socket falling out

13. VVPAT – Voter Verifiable Paper Audit Trail: The printer mechanism for the TSx machines examined in Emery County does not sufficiently guide the paper, producing frequent paper jams.

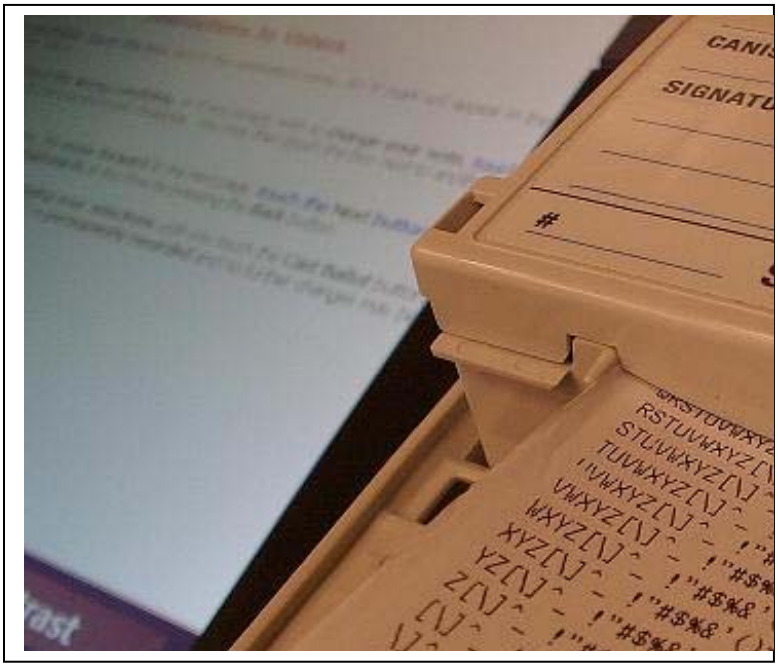

Fig. 12 – Paper jam in progress

In addition, a design decision to place a brown door over the paper which the voter is supposed to verify leads to questions about the usefulness of the VVPAT. Unless the door is

lifted up it obstructs view of the paper representation of the voter's vote. If the system is to be used to verify a paper trail, it should have instructions printed prominently on the casing instructing voters to lift the brown door to see the paper trail.

Fig. 13 – Brown door blocking view of voter verifiable paper trail

The lens used to view the VVPAT tends to obstruct the viewing of the paper representation of the vote.

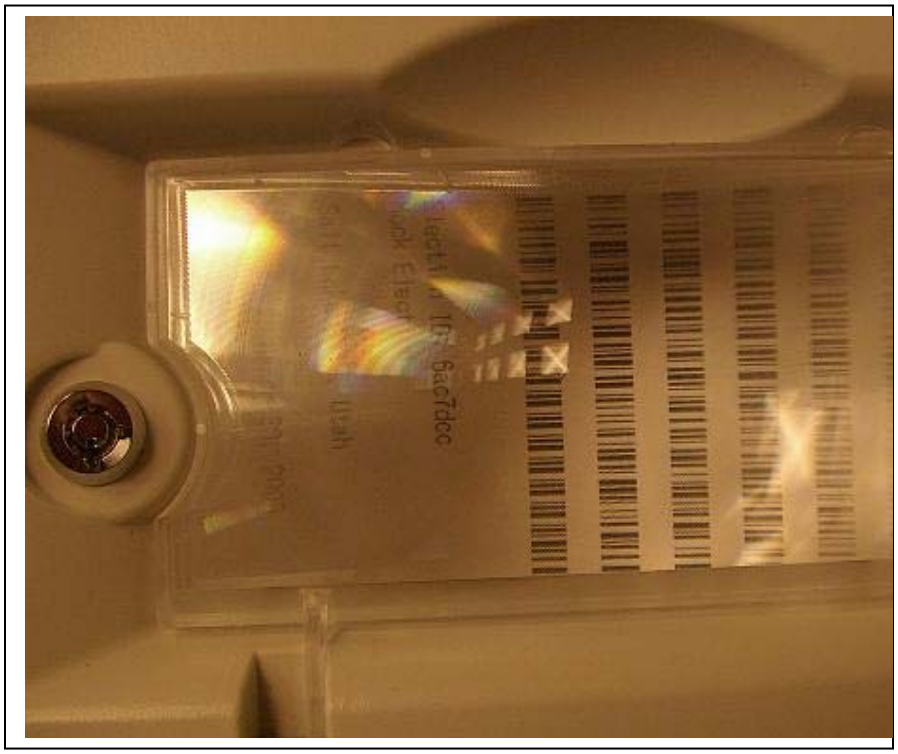

Fig. 14 – Print is too small so magnifying lens is provided but the lens distorts.

The voter can lift the lens, but the print is very small and the bottom of the paper record of the vote does not display fully.

Fig. 15 – Print is small; lower part of paper trail tends not to scroll up into full view.

FOOTNOTES

[1] Tape recorded Emery County meeting with state elections director, county commissioners and Diebold attorneys, March 27, 2006

[2] Files found by Bev Harris on Diebold FTP site Jan. 23, 2003

ACKNOWLEDGEMENTS

The citizenry owes an immense debt of gratitude to Bruce Funk, the Emery County Clerk for Emery County, Utah who, upon noticing anomalies in the Diebold TSx machines delivered to his county, requested an independent evaluation of this voting system.

Appreciation is expressed to Kalle Kaukonen for providing his perspective on this report.

