

Craft, Paul

From: Ronald L. Rivest [rivest@mit.edu]
Sent: Thursday, July 28, 2005 8:21 PM
To: Multiple recipients of list
Subject: {Spam?} FW: Multiple vulnerabilities in Diebold Optical Scan

Dear Barbara --

Thank you for your letter (copied below) bringing to my attention the Hursti report on potential serious vulnerabilities in Diebold op-scan machines, including a summary of the report and links to the full report. While I had seen a report on this material, I had not previously seen this summary you forwarded or the full report it links to. (I had seen the news report at <http://www.scoop.co.nz/stories/HL0505/S00381.htm>.)

I am (hereby) forwarding your letter and associated report to the TGDC and to the EAC Commissioners.

I don't know whether this report accurately describes vulnerabilities in the Diebold systems or not. The report gives quite a bit of detail and seems (unfortunately) very plausible. Of course, independent testing and verification would be required to tell. I have not contacted Diebold for their comments on this report. I have not seen any documentation of the certification exam reports for the relevant Diebold machines. I have not conducted any examination myself.

I agree with your suggestion that this reported vulnerability seems sufficiently serious and egregious that the EAC should consider steps to independently evaluate its validity, and perhaps (if the report is correct) de-certifying the machines found to have such vulnerabilities. If this report is correct, the vulnerability is indeed quite startling and shocking. While the investigation was sponsored by Bev Harris's organization BlackBoxVoting.org, which is itself often controversial, the reported vulnerability is sufficiently clearly described that validating its accuracy should be relatively straightforward for anyone with access to the relevant equipment.

On a somewhat larger perspective, this incident has several morals:

- It supports the position, made in testimony by Dill and others, that evaluating the security of the software within a voting system is exceptionally tricky and difficult.
- It supports the position that current certification procedures may not be up to the task of identifying all the serious vulnerabilities in voting systems submitted for evaluation.
- It supports the resolution, passed by the TGDC but not yet implemented with requirements, requiring open-ended search for vulnerabilities in voting systems submitted for evaluation. (It is however clear, as Hursti states, that any system containing such flaws should not have passed even the earlier voting system standards.)
- It supports the position that voting system evaluation should be much more demanding and rigorous than at present.
- It supports the position that source code for voting systems should be much more generally available for analysis by qualified parties, so that vulnerabilities like this are more likely to be caught before they are exploited. (I was pleased to see that Florida election officials were helpful in facilitating this investigation, such goodwill might be lacking in other cases where investigation requires access to equipment or source code.)

- It supports the position that voting system vendors should, for the purposes of security evaluation, be treated as potential adversaries to the integrity of the election process. (Such a design flaw, if actually present, seems an invitation to fraud.)
- It supports the position that voter-verified paper audit trails provide useful protection against software problems and fraud. (In this case the paper op-scan ballots are this protection.) Of course, this is only true to the extent that recounts are performed; it is very disturbing (as the news article reports) that spontaneous random recounts are often prohibited by state law(!).
- It makes clear the necessity for procedures to handle serious and credible vulnerability reports, the need for an independent process to evaluate such reports, and the need to decertify equipment found to have serious vulnerabilities.

In his report Hursti also makes other recommendations (such as the one to require retention of the memory cards after an election) that are good ones.

Again, I thank you for bringing this to my attention. I am sure that this material will be seriously considered by both the TGDC and the EAC. This incident will, I expect, be an interesting "test case" for the EAC to demonstrate its commitment to the integrity of voting systems in this country when a serious vulnerability is reported.

Please keep me informed if you obtain further relevant information on this matter, particularly relating to the validity of the vulnerability report itself, or other evaluations of this report.

Sincerely,
Ronald L. Rivest

>Date: Thu, 28 Jul 2005 14:23:58 -0700
>Subject: FW: Multiple vulnerabilities in Diebold Optical Scan
>From: Barbara Simons <simons@acm.org>
>To: Ron Rivest <rivest@theory.lcs.mit.edu>

>Hi, Ron. I'm sure you are aware of the Hursti report. I found some of >O'Dell's comments about that report interesting, especially:

>> Based on my experience in the financial services industry, discovery >> of multiple security vulnerabilities of this severity in equipment >> in use by any bank or brokerage house would trigger an immediate >> shutdown of all the affected systems, followed by a full internal >> and external audit, and, in all likelihood, formal investigation by >> regulatory and law enforcement agencies. We should accept no less >> from the election services industry.

>Is there any chance that the TGDC could recommend to the EAC that the >EAC call for all Diebold op scans to be withdrawn from the market until >this security hole is eliminated and that all other op scan systems be >tested for the same security hole?

>Regards,
>Barbara

>----- Forwarded Message

>from comp.risks

>Date: Wed, 13 Jul 2005 13:35:39 -0500
>From: "Bruce O'Dell" <bodell@digitalagility.com>
>Subject: Multiple vulnerabilities in Diebold Optical Scan

>A Technical Report published by BlackBoxVoting.org (4 Jul 2005) details
>multiple critical security vulnerabilities in the Diebold Optical Scan
>voting equipment that was used to tally approximately 25 million votes
>in the 2004 US election.

>
>Overview: <http://www.bbvdocs.org/general/BBVreport-1sheet.pdf> and Full
>technical report: <http://www.blackboxvoting.org/BBVreport.pdf>

>
>Harri Hursti, an independent security consultant - with the consent of
>election officials in Leon County, Florida - was able to take full
>control of the Diebold optical scan device and manipulate vote totals
>and audit reports at will.

>
>The Diebold Precinct-Based Optical Scan 1.94w device accommodates a
>removable memory card. It had been believed that this card contained
>only the electronic "ballot box", the ballot design and the race
>definitions; astonishingly enough, the memory card also contains
>executable code essential to the operation of the optical scan system.
>The presence of executable code on the memory card is not mentioned in
>the official product documentation. This architecture permits multiple
>methods for unauthorized code to be downloaded to the memory cards, and
>is wide open to exploitation by malicious insiders.

>
>The individual cards are programmed by the Diebold GEMS central
>tabulator device via a RS-232 serial port connection or via modem over
>the public phone network. There are no checksum mechanisms to detect or
>prevent tampering with the executable code, and worse yet, there are
>credible exploits which could compromise both the checksum and
>executable. The report notes that this appears to be in violation of
>Chapter 5 of the 1990 Federal Election Commission standards for
>election equipment, and therefore should never have been certified for
>use.

>
>The executable code is written in a proprietary language, Accu-Basic.
>Accu-Basic programs are first compiled into ASCII pseudocode, which is
>then executed by an interpreter residing in the optical scan device.
>Hursti located an inexpensive device capable of reading and updating
>the memory cards advertised on the Internet, and using a
>publicly-available version of the Accu-Basic compiler (found on the
>Internet, along with Diebold source code and other documents, by Bev
>Harris in 2003) was able to exploit these vulnerabilities - and
>publicly demonstrated the ability to modify vote totals and audit
>reports at will.

>
>According to the report:

>
>"Exploits available with this design include, but are not limited to:

>
>"1) Paper trail falsification - Ability to modify the election results
>reports so that they do not match the actual vote data

>
>"1.1) Production of false optical scan reports to facilitate checks and
>balances (matching the optical scan report to the central tabulator
>report), in order to conceal attacks like redistribution of the votes
>or Trojan horse scripts such as those designed by Dr. Herbert
>Thompson. (19)

>
>"1.2) An ingenious exploit presents itself, for a single memory card to
>mimic votes from many precincts at once while transmitting votes to the
>central tabulator. The paper trail falsification methods in this report
>will hide evidence of out-of-place information from the optical scan
>report if that attack is used.

>
>"2) Removal of information about pre-loaded votes

>
>"2.1) Ability to hide pre-loaded votes

>"2.2) Ability to hide a pre-arranged integer overflow

>

>"3) Ability to program conditional behavior based on time/date, number of votes counted, and many other hidden triggers.

>

>"According to public statements by elections officials(20), the paper trail produced by the precinct optical scan has been placed into the role of a vital safeguard mechanism. The paper report from the optical scan machine is the key record used to confirm the integrity of the central tabulator record. The exploits demonstrated in the false optical scan machine reports ("poll tapes") shown on page 16 do not change the votes, only the report of the votes. When combined with the Trojan horse attack demonstrated by Dr. Thompson, this attack vector maintains an illusion of integrity by producing false reports to match the contaminated central tabulator report.

>

>"The [second] exploit demonstrated in the poll tape with a true report containing false votes, shown on page 18, changes the votes but not the report. This example pre-stuffs the ballot box in such a way as to produce an integer overflow. In this exploit, a small number of votes is loaded for one candidate, offset by a large number of votes for the opposing candidate such that the sum of the numbers, because of the overflow, will be zero. The large number is designed to trigger an integer overflow such that after a certain number of votes is received it will flip the vote counter over to begin counting from zero for that candidate... combining the false report method (demonstrated on page 16) with the pre-arranged integer overflow (demonstrated on 18) seems to be an especially efficient exploit because it is a one-step process that takes out both the actual process and its safeguard at the same time, while surviving scrutiny of almost anything short of a full manual recount."

>

>Reportedly, at least 500 jurisdictions used the vulnerable optical scan system in 2004; for example, the Diebold Precinct-Based Optical Scan 1.94w system counted approximately 2.5 million votes in 30 counties, or about one-third of all the votes in Florida, and nationwide, approximately 25 million votes
>(http://www.freddevan.com/blog/archives/00006724.html).

>

>Although the exploits described in the report could be uncovered if a full hand recount was performed, in practice, detection is unlikely. Most jurisdictions limit the time frame for contesting an election. For numerous reasons, both candidates and election administrators are reluctant to question the official tally, while hand recounts are expensive - with costs borne by the contesting party. Few elections tallied by optical scan equipment are ever fully recounted, and automatic recounts legally triggered by a narrow margin of victory will, of course, fail to detect large-scale manipulation that shifts results outside the recount threshold. Finally, there are classic problems with paper ballot chain of custody; the more time passes, and the further a paper artifact travels from its point of origin, the more vulnerable it is to tampering.

>

>Therefore, the mere presence of a paper trail will not deter or detect electronic vote manipulation by malicious insiders unless the voter-verified paper ballot or optical scan ballot is actually randomly audited - preferably, in-precinct, on election night. Yet the cost and time required by a truly effective and random audit protocol undermines the case for electronically-assisted vote tallying. Therefore some analysts now recommend US implementation of the Canadian system - hand-counting of paper ballots in-precinct on Election Night, with accommodation for the visually-impaired - as the best countermeasure to systematic electronic election fraud.

>

>Based on my experience in the financial services industry, discovery of multiple security vulnerabilities of this severity in equipment in use by any bank or brokerage house would trigger an immediate shutdown of

>all the affected systems, followed by a full internal and external
>audit, and, in all likelihood, formal investigation by regulatory and
>law enforcement agencies. We should accept no less from the election
>services industry.

>
>The affected Diebold optical scan equipment should be immediately
>withdrawn from use in any election until independent recertification is
>achieved, or a secure alternative is obtained. All other election
>equipment - manufactured by Diebold or by other vendors - should be
>examined, and if subject to the same vulnerability, should also be
>withdrawn. An investigation to determine how equipment with such
>serious vulnerabilities to insider manipulation could ever have been
>certified should also be launched, and certification and oversight
>procedures enhanced.

>
>Good people died to gain and defend our right to vote. Election
>administration must not be exempt from industry best practices for
>security, audit and control.

>
>Bruce O'Dell, Partner, Digital Agility Incorporated
>www.digitalagility.com Member, ACM SIGSOFT, SIGMETRICS, SIGART
>bodell@digitalagility.com

>-----
> > -----Original Message-----
> > From: Scarl, Ethan [mailto:ethan.scarl@boeing.com]
> > Sent: Wednesday, July 27, 2005 05:36 PM
> > To: vote-wg@lists.cpsr.org
> > Cc: 'Scarl, Ethan'
> > Subject: [vote-wg] FW: Black Box Voting Board Member Arrested in San
> > Diego

>for Viewing Vote-Tallying

> >
> > This seems to escalate the problem of adequate public monitoring of
> > vote tallying to a new level. I'll be interested in knowing whether
> > anyone in the area has additional information, or can let us know
> > how the local media are covering the situation.
> > - Ethan

> > _____
> > From: <http://www.blackboxvoting.org>

> > -----Original Message-----
> > From: Black Box Voting [mailto:crew@blackboxvoting.org]
> > Sent: Wednesday, July 27, 2005 3:51 AM
> > To: Scarl, Ethan
> > Subject: Black Box Voting Board Member Arrested in San Diego for
> > Viewing Vote-Tallying

> > VIEWING THE DIEBOLD VOTE-TALLYING SCREEN PROHIBITED

> >
> > Jim March, a member of the Black Box Voting board of directors, was
> > arrested Tuesday evening for trying to observe the Diebold central
> > tabulator (vote tallying machine) as the votes were being counted in
> > San Diego's mayoral election (July 26).
> > (- online discussion: <http://www.blackboxvoting.org> -)

> >
> > According to Jim Hamilton, an elections integrity advocate from San
> > Diego, he and March visited the office of the registrar of elections
> > earlier in the day. During this visit, March made two requests,
> > which were refused by Mikel Haas, the San Diego Registrar of
> > elections.

> >
> > 1) March asked that the central tabulator, the computer that tallies
> > up the votes from all the precincts, be positioned so that citizens
> > could observe it. According to Hamilton, this would have required

> > simply moving a table a few feet.
> >
> > 2) March also asked for a copy of the ".gbf" files -- the vote tally
> > files collected during the course of tabulation - to be provided for
> > examination after the election.
> >
> > ...
> >
> > The arrest of Jim March underlines a fundamental problem facing
> > Americans today as, increasingly, they lose the ability to monitor,
> > verify, or watch any part of the counting process.
> >
> > <http://www.blackboxvoting.org>.
>
>----- End of Forwarded Message

Ronald L. Rivest
Room 32-G692, Stata Center, MIT, Cambridge MA 02139
Tel 617-253-5880, Email <rivest@mit.edu>

- From Black Box Voting Document Archive