

Attn:

Ms. Brianna Lierman
Ms. Dawn Mehlhaff
Mr. John Mott-Smith
S.D.S. Elections
California Secretary of State

Hand Delivered 9/19/03

Ms. Lierman,

Allow me to recap the Diebold controversy in brief:

Jan. 2003: Writer Bev Harris discovers that Diebold Election Systems has an FTP site ("File Transfer Protocol") area up and live on the internet, with no passwords, public access allowed. She facilitated a mass copy of the contents, and began raising concerns as to the security of DES products.

July/August 2003: the materials copied by Harris have been spread rather widely. The complete source code for one of the areas of greatest concern was in there – the touchscreen voting terminals. This software is analyzed in detail by the John Hopkins team, which finds serious security flaws but no evidence of deliberate vote manipulation.

Meanwhile, Harris leads a second team studying GEMS, the central vote-count system in use at county offices. While the members of her team are possessed of less serious academic credentials and the final report less scholarly, they are able to establish a pattern of flaws that DO appear to deliberately facilitate vote fraud.

Harris writes up her team's findings here:

<http://www.scoop.co.nz/mason/stories/HL0307/S00065.htm>

Her allegations are explosive:

- Should anyone load MS-Access on the central vote-count system running GEMS, or otherwise look at the data on the GEMS via a remote connection with MS-Access on the remote machine, there is NO security whatsoever. Zip, nada, none. Unauthorized users with no password can alter voting data, audit trails, passwords and anything else.
- The database was internally set up to defeat the normal precinct spot-checking: the GEMS console user is unaware that voting data is stored in three separate tables, none of which have to match (by default they do, but they're subject to tampering). We don't know what the 3rd one does, but the first two are understood: one provides precinct-by-precinct data, while the other is cited for countywide figures. If the table feeding countywide data is altered, you get altered results – but a spot-check of

individual precincts will come up accurate. Only printing out totals from each precinct and adding them up on a hand calculator and then comparing it to the countywide total would tell the tale – and nobody would think to DO that, because the data all appears to be coming from the same source.

- Nowhere in the GEMS documentation is this multiple-table issue addressed, nor is MS-Access ever revealed as a “hack tool”.

In the last two weeks, a set of Diebold Election Systems internal Emails were leaked by an insider, along with additional company documentation that was NOT for review by anyone outside the company. The most explosive is an exchange of Emails between central support staffer Ken Clark (title of “Principle Engineer”) and somebody communicating with the Federal Independent Testing Authority named Metamor (now Ciber Inc) in October of 2001:

To: "support"
Subject: alteration of Audit Log in Access
From: "Nel Finberg"
Date: Tue, 16 Oct 2001 23:31:30 -0700
Importance: Normal

Jennifer Price at Metamor (about to be Ciber) has indicated that she can access the GEMS Access database and alter the Audit log without entering a password. What is the position of our development staff on this issue? Can we justify this? Or should this be anathema?
Nel

Clark's reply:

Subject: RE: alteration of Audit Log in Access
From: "Ken Clark"
Date: Thu, 18 Oct 2001 09:55:02 -0700
Importance: Normal
In-reply-to:

Its a tough question, and it has a lot to do with perception. Of course everyone knows perception is reality.

Right now you can open GEMS' .mdb file with MS-Access, and alter its contents. That includes the audit log. This isn't anything new. In VTS, you can open the database with progress and do the same. The same would go for anyone else's system using whatever database they are using. Hard drives are read-write entities. You can change their contents.

Now, where the perception comes in is that its right now very *easy* to change the contents. Double click the .mdb file. Even technical wizards at Metamor (or Ciber, or whatever) can figure that one out.

It is possible to put a secret password on the .mdb file to prevent Metamor from opening it with Access. I've threatened to put a password on the .mdb before when dealers/customers/support have done stupid things with the GEMS database structure using Access. Being able to end-run the database has admittedly got people out of a bind though. Jane (I think it was Jane) did some fancy footwork on the .mdb file in Gaston recently. I know our dealers do it. King County is famous for it. That's why we've never put a password on the file before.

Note however that even if we put a password on the file, it doesn't really prove much. Someone has to know the password, else how would GEMS open it. So this technically brings us back to square one: the audit log is modifiable by that person at least (read, me). Back to perception though, if you don't bring this up you might skate through Metamor.

There might be some clever crypto techniques to make it even harder to change the log (for me, they guy with the password that is). We're talking big changes here though, and at the moment largely theoretical ones. I'd doubt that any of our competitors are that clever.

By the way, all of this is why Texas gets its sh*t in a knot over the log printer. Log printers are not read-write, so you don't have the problem. Of course if I were Texas I would be more worried about modifications to our electronic ballots than to our electron logs, but that is another story I guess.

Bottom line on Metamor is to find out what it is going to take to make them happy. You can try the old standard of the NT password gains access to the operating system, and that after that point all bets are off. You have to trust the person with the NT password at least. This is all about Florida, and we have had VTS certified in Florida under the status quo for nearly ten years.

I sense a loosing battle here though. The changes to put a password on the .mdb file are not trivial and probably not even backward compatible, but we'll do it if that is what it is going to take.

Ken

And the final response back from Metamor:

Subject: RE: alteration of Audit Log in Access
From: "Nel Finberg"
Date: Wed, 17 Oct 2001 14:48:16 -0700
Importance: Normal

Thanks for the response, Ken. For now Metamor accepts the requirement to restrict the server password to authorized staff in the jurisdiction, and that it

should be the responsibility of the jurisdiction to restrict knowledge of this password. So no action is necessary in this matter, at this time. Nel

It gets worse. Clark knew he was a liar regarding NT security – if anything, after the recent flood of worm attacks against WindowsXP (the current descendent of NT) the whole world knows Windows security sucks.

But worse, Clark knew that security procedures in WindowsNT weren't even being used, as his response to this query shows:

To: <support@gesn.com>
Subject: RE: GEMS administration
From: "Larry Dix" <ljdglobal@gesn.com>
Date: Tue, 5 Sep 2000 15:17:55 -0500
Importance: Normal
In-reply-to: <020201c01459\$11774d50\$0a04a8c0@gesn.com>

Please explain in further detail the access with non admin user ID's? Also have you heard from anyone in Florida?

Larry J. Dix

Global Election Systems

(972)-542-6000

Clark's response, about a year BEFORE instructing somebody to lie to the Federal testing lab (Metamor):

To: <support@gesn.com>
Subject: RE: GEMS administration
From: "Ken Clark" <ken@gesn.com>
Date: Tue, 5 Sep 2000 15:17:35 -0500
Importance: Normal
In-reply-to: <NDBBJBKEHMHBEPMMLKOLAEPBCGAA.ljdglobal@gesn.com>

GEMS has normal users and admin users. Admin users are allowed to change the election status (and thus remove the locks on the database), normal users are not.

Looks good in an RFP response, but everyone just logs in as user admin password global...

Ken

Not that this was their only adventure in things that "look good in an RFP response":

To: "Support Team (E-mail)"
Subject: RE: AVTS - Diagnostics & Installation
From: "Ken Clark"
Date: Tue, 6 Jul 1999 16:41:56 -0500
Importance: Normal

> Quoting an earlier message from Juan Rivera:

> I do not feel that it is necessary or desired to do
> this on each and every election. We, the manufacturer,
> are supposed to set the > procedures to follow for this
> equipment since we build it.

Clark:

I hate more than anyone else in the company to bring up a certification issue with this, but a number of jurisdictions require a "system test" before every election. I just helped Knecht yesterday with an RFP from Riverside that required this. That is why the AccuVote displays the silly ***System Test Passed*** message on boot up instead of "memory test passed", which is all it actually tests.

No argument from me that it is pointless. You could probably get away with a batch file that prints "system test passed" for all I know. We will do something along those lines with the new unit after a memory test or whatever.

Ken

These messages confirming the accuracy of Harris' findings AND Diebold's deliberate cover-up of this zero-security nightmare are enough to cause the California Secretary of State's office to yank Diebold's certification.

Adding insult to injury is a Diebold file, marked "internal use ONLY", containing the actual elections-day procedures for Diebold's Canada-based technical staff. The file is named "ElectionSupportGuide.PDF". Some hilarious and disturbing excerpts:

1. Overview

This document is intended for Diebold Election Systems, Inc. staff attending elections, and attempts to address the majority of representative situations that may be encountered at an election. The document aims primarily at educating novice election support staff, and is in no way intended to provide an authoritative basis of product information.

Please note that this document is intended strictly for the consumption of Diebold Election Systems, Inc. staff, and is not intended for customers or other election-related authorities.

2.1. Border crossing

Indicate that you are attending an election when questioned by US customs. Provide a terse explanation of what your job is as well as the business the company you work for is in. Under no circumstances should you indicate that you intend on working in the US. If requested, give Tab's name and work telephone number as reference.

3. General issues

As representative of Diebold on election day, you will be considered the paragon of knowledge and authority with respect to the jurisdiction's election, even though you may in fact be the least qualified person on site. In light of this, present yourself in as diplomatic, reassuring, and professional a manner as possible.

3.2. Communication

You will generally be considered to be a high-ranking election specialist and a paragon of knowledge and solutions, which may be disconcerting when things go wrong. Do not promote your ignorance - in case of doubt, call a designated contact who may be more knowledgeable than you.

Ideally, you should not remain all day at election central, but spend at least several hours visiting polling places in order to view the voting process itself.

Be observant throughout the election, making notes of any anomalies or issues you believe the company could/should be aware of.

Be aware of the fact that pollworkers are often quite aged, and that technological issues that to you are utterly banal may be quite daunting to the pollworkers.

Do not flaunt your knowledge, particularly if it is technical only, and not election specific. Not only may your audience be less than receptive, you may be called to task where you least expect it, and can least make a difference.

Carry with you a list of telephone numbers of Diebold Election Systems, Inc. contact people. Carry a cell phone with you if possible - if you don't already have one, attempt to procure one from the jurisdiction.

Remember to take along the Excel spreadsheet containing all employee phone numbers.

Be aware of any senior technical staff that will be present at the election other than yourself. Be aware of their strengths and limitations as far as product and election knowledge is concerned. Just because someone has been working for our organization for years does not mean they will be aware of every facet of election management requirements.

Defer to more experienced staff where possible. Do not offer answers if you are not perfectly comfortable with doing so - an incorrect answer may well have more serious consequences than no answer at all. It is acceptable to indicate that you are not aware of the answer requested, and that you will contact another company representative who will be equipped with the answer.

Offer the minimum amount of information necessary. Consider the nature of information being discussed, your familiarity with the subject being discussed, the position of the individual you are discussing the issue with, as well as any individuals or press who may be present who you are not familiar with.

Under no circumstances should you discuss anything to do with the election with the press, or appear on press cameras. The same applies generally to any individuals outside of the immediate election environment. You cannot be familiar with the partisan politics that may be rife in the jurisdiction, and possible oppositional sentiments towards our product or company.

Do not offer damaging opinions of our systems, even when their failings become obvious.

Contact Tab or Ken at the Vancouver office once the election has been deemed to have been closed.

3.3. Attendance

Expect to be onsite on election day between 6am and 7am. Depending on how well the election goes, you may be able to leave the site as early as 10pm or 11pm. If things go badly, you could be there until the next morning.

6.2. AccuFeed

The jurisdiction may be using the AccuFeed in order to process absentee ballots in batch mode. The AccuFeed is often sensitive to the orientation, size, and print quality of the ballot. AccuFeed units tend to reflect varying behavior in terms of speed and quality of processing. Familiarize yourself with the functioning of the AccuFeed before the election if it will be used in the election. Do not offer information as to the AccuFeed's shortcomings to the jurisdiction, even where obvious.

In conclusion:

Diebold Election Systems has pulled off a monumental, Worldcom/Enron-class fraud against its entire customer base, the California Secretary of State's office, the Federal Elections Commission and more.

At a minimum, their certification status in California must be immediately reviewed.

The more disturbing question is, how did this garbage get past ANY prior inspection? That query calls into question the entire idea of elections software that is sealed from public review, and the idea of not having a paper trail.

You may consider these remarks to be a written prelude to the questions and comments I intend to raise publicly at your offices on the meeting of October 9, 2003 1:00pm at 1500 11th Street, 1st Floor Auditorium.

Jim March

Email: jmarch@prodigy.net

<http://www.equalccw.com/voteprar.html>

Phone: 916-xxx-xxxx / Fax: 707-221-7152