Subject: [ACCURATE] FULL Summary of my comments
Date: Tuesday, March 30, 2004 4:27 PM
From: R. Mercuri <notable@mindspring.com>
To: <accurate@csl.sri.com>
Cc: "Peter G. Neumann" <neumann@csl.sri.com>, Drew Dean <ddean@csl.sri.com>, Mercuri Rebecca <mercuri@acm.org>

The following is the summary of my comments on the current draft version. Peter and Drew are working on making revisions, if others have any thoughts along the lines of what I've indicated here, in how to clear up these problems with the draft, please pitch in your thoughts (to Peter and Drew).

Peter/Drew -- my comment still stands on page 0 -- it's too much of an analysis of what is wrong and too little of a what we are going to do to fix things. Same is still true of page 1. Nothing else new in the below from what I sent you before (but I cleaned it up a tad for general distribution).

I am writing an additional section on Incident Reporting now and will peruse prior emails from folks to check to see if there's anything left that I need to provide input on.

Sorry if it sounds a bit harsh, that's my style (for what it's worth),
Rebecca Mercuri.

PAGE 0:

My overall suggestion is to have a brief statement of
the problem and to devote MOST of section B to
a CONCRETE LIST OF DELIVERABLES.
This is the FIRST PAGE that the reviewers will see.
Tell them WHAT WE PLAN TO DO, not what is wrong.

PAGE 1:

C1 Call to arms: Most of the information we want to exchange IS secret (not, is NOT secret).

Recent history:

Start with --
Problems with election integrity and auditability were well known by technologists and government officials as far back as 1984 (cite Roy Saltman's NIST treatise here) but these issues were revealed to the general public by the events of Election 2000....

Optical and mark-sense ballot scanners are NOT new equipment. Nor are the DREs new Instead say that:
HAVA accelerated the already-begun replacement of aging lever voting machines and some flawed forms of punch card systems with direct-recording electronic (DRE) and optical mark-sense balloting equipment. (DRE voting systems are generally of two forms, touch-screen and full-face.)

In the "adequacy of the FEC standards" part, please add the footnote to my submission to the FEC (along with the one marked [32] as follows:

"The FEC Proposed Voting Systems Standard Update," a detailed comment by Dr. Rebecca Mercuri, submitted to the Federal Election Commission on September 10, 2001 in accordance with Federal Register FEC Notice 2001-9, Vol. 66, No. 132. http://www.notablesoftware.com/Papers/FECRM.html

General comment -- much of the content of this page is also about what people have already done and said, and it does not STRONGLY ENOUGH indicate what NEEDS TO BE DONE nor what WILL BE DONE. Maybe you eventually get to that, but it is not (yet) obvious to the reader what is going on here, and you want to slam them with it up front.

Page 2:

"has not ensured that voting systems meet any useful security standards."
should be MUCH stronger:
"has not ensured that voting systems meet the level of security standards that

are commonplace to critical computer equipment deployment, such as that used by the Department of Defense, the health care and avionics industries, and banking."

Give the date/year of the audit of the 17 counties in California's equipment (to show that this is CURRENTLY going on).

Add a sentence after the Diebold assertion about checks and balances to explain that:
There is NO configuration control and management practices, even the most minimum suggested by NIST, currently used or required by the FEC/NASED process to ensure that the voting systems being deployed are identical in construction to those that were certified. This a serious and dangerous omission by election authorities.

Human factors and usability was actually added to the FEC/NASED standards. They paid an outside consulting firm to come up with some. You are working with an old document.

Note that the IEEE Voting System Standard effort also entirely omits the equipment and software used to tally the votes and report the vote totals. Their current effort only pertains to the balloting systems.

Omit the sentence about the standards development process not producing surprises. That's wrong (and rude to boot).

C2. Accuracy and integrity are BOTH essential to the voting system. If it produces only accurate reports based on the data it has but that data lacks integrity, it is moot. Reference Saltman's report again here.

Trusting groups with diverse interests may be untrustworthy as well, because it is generally understood that there may be collusion among the political parties, particularly in regions of the country where a certain party is dominant.

You say "in addition to the question of trust" yet your prior paragraph speaks of ACCURACY, not TRUST.

Page 3:

Do you really mean OPEN standards? Or just agreed-upon standards?

Open means something rather different.

Page 4:

You should be able to find a place to insert the following reference in the statistics and audit section:

[*?*] Rebecca T. Mercuri, “On Auditing Audit Trails,” Security Watch, Communications of the ACM, Vol. 46, No. 1, January 2003.

Canvassing and reporting -- at the end of this part, you need to say something about "we will provide...." and then say what we will provide -- like guidelines for canvassing and reporting? and/or ways of ensuring that the canvassing and reporting is being performed correctly...etc....

Operations and procedures --

ONLY use "voter verified paper audit trail" throughout the document (not "verifiable").

Get rid of the "we believes..." that sounds wishy-washy. Tighten that up with "it is well known" or something MUCH stronger.

I thought Avi had recanted on his assertion that the Diebold smartcard protocol allowed voters to vote as many times as they wanted -- after he worked as a pollworker. You MUST remove that. It's wrong.

The sentence about the preference to paper ballots and (hopefully) verified about the voter should be changed to:
Our research will indicate the level of assurance that is applied when paper ballots are available for voter verification.

Section C4

"Paperless DRE Systems" should be renamed to "Fully-Electronic DRE Systems" Use voter verified (decide on whether you want it hyphenated or not and be consistent throughout the document).

Decomposition of the voting machine must be able to PROVE that there is no collusion among the components and that data is transferred correctly. Each transmission points has a data transfer vulnerability. How to mitigate this?

Attesting to the software it is running is OK but the DATA must have full integrity. The folks at SRI should have some references on this....

Security Analysis of Proposed Voting Systems -- what you have said in those 2 paragraphs is not a security analysis, it is a RISKS analysis, since you are dealing with attacks, not necessarily mitigation. Probably you want to change the title of that section to "Risks Analysis of ...."

Design for Audit -- fine, except change verifiable to verified.

Cryptographic Protocols --

Actually mix nets do not allow "anyone" to validate the election. There is considerable obfuscation of the process, and unless you have a Ph.D. in cryptography you probably will not be able to understand that the process was applied correctly to produce the vote totals. We need to change the sentence to reflect who can ensure that it is being done correctly, and also indicate that it is inappropriate for a bunch of propellor-headed geeks to be the only ones who can verify that the process correctly generated true election results.

Software Engineering Tools -- OK, but include the application of NIST certificate protocols for allowing the end-users (in this case the local election officials) to be able to procedurally ensure that the code on the machine was the certified set. It's all very well and good to get it through the certification, but there has to be a way to follow this through to the endpoint where the systems are actually being used, or it's moot. (Remember some NIST folks will probably be vetting this proposal, so you should plug their good stuf in there as much as you can.)

Trusted Hardware Platforms -- the question of TCPA must also be mitigated against whether this provides sufficient "trust" and assurance for the GENERAL PUBLIC (citizens) for non-techies to believe that it's not just a fancier name for a "black-box". You should plan to assess this as well, in this section.

Internet Voting -- wait a second -- where is the Rubin/Wagner/Simons report putting the kibosh on the SERVE project??? You MUST footnote this. AND YOU HAVE COMPLETELY LEFT OUT THE SOCIOLOGICAL FACTORS HERE. Say something like the following: "The bottom line regarding Internet (remote) voting must be its high vulnerability for coercion and vote-selling. Any solution, no matter how secure, must also address and mitigate against these sociological factors." This section should also include some discussion about other forms of networking: Vulnerabilities of dedicated networks and wireless transmissions, also now being introduced in increasing numbers into election systems (for tasks ranging from ballot face programming through end-of-night reporting), must be considered and mitigated.

Remote and Absentee Voting -- Add a sentence explaining that: Traditional forms of bioidentification may be unacceptable for the election setting, because many voters fear governmental collection of such data, and they may self-disenfranchise if such are required to use the systems.

C5 Usability and Accessibility - I see you reference the UMD study, but they did receive a fairly SUBSTANTIAL NSF grant recently and you might want to at least mention that we will be coordinating with them to ensure that we are not duplicating efforts. Have someone check their website ASAP to be sure that the components you have identified here are not ALREADY being done by the UMD team (Ben Bederson et al). If you overlap their currently funded work, it will look like we are out of touch with what they are doing.

I think that a retrospective analysis of the Florida 2000 election is akin to beating a dead horse. PULEASE delete that unless you really think that there is some way to analyze the voting systems and data now that they have ALL been DESTROYED. It is an impossible and absurd task and do not put it into the proposal. We want to move FORWARD, NOT BACKWARD.

C6 Legal and Policy Issues -- REGISTRATION PROCESS? NO!!! THIS IS A PROPOSAL ABOUT VOTING SYSTEMS!!! You do not even want to go there with voter registration. That is a HUGE political hotbed that you will be totally criticized for venturing into. TAKE THAT OUT OF THE PROPOSAL ASAP! We have our hands full with the

state requirements (all of which are different) for dealing with the voting systems themselves, recounts, ballot layouts, and so on. COMPLETELY
TAKE OUT BOTH OF THOSE PARAGRAPHS. You can start with the one that says "the second stage is voting itself" but leave out that sentence and just start with "One key area of research will focus on the interaction between new voting technologies and ...." Then the vote tabulation and canvassing part is really the SECOND stage of the process, but just really "another aspect of the process...." Leave out the 4th stage because there is NO WAY to deal with that. If you MUST put something in about lawsuits -- you want to say something about "providing information that would be useful to plaintiffs, defendants and judges regarding the appropriate setup, operation and deployment of voting systems and the conduct of recounts and canvasses." You want to go on here somewhat about the difficulty in understanding the technology, and that our group could be a useful resource to the legal community in providing information that would allow technical understanding of the equipment that was used, its flaws and problems, etc.

C7 Education and Outreach Plan -- Fine.

C8 Technology Transfer Plan -- This section is on TECHNOLOGY TRANSFER yet you start by downgrading this entire proposal by saying that you don't expect to get any cooperation from the major vendors. THIS IS BUNK. Instead say: "The major vendors have participated with many of us on the IEEE voting standards development team, and have a vested interest in having improved accuracy, integrity, reliability, usability, auditability, blah blah, in their products. We expect that they will engage in ongoing discussion with our research group, and potentially offer products for testing and evaluation."
(Look, maybe they won't but why tell the NSF this???)

C9 Management Plan -- I think that the sentence about Jones, though highly complementary (and true) would be disputed by other folks (Shamos) who have also bridged various disciplines effectively in this field. I think you might want to play up Jones' qualifications (having served as a machine inspector for his state, creating the premiere body of research on optically scanned voting systems, etc.) rather than the vague complements you wrote. ;-)

C10 Evaluation Plan -- Add to the list of evaluation methods --
* Adoption of ACCURATE results and suggestions by vendors, members of the election community, and reflection in legislation.
I think you sort of said that in the paragraph below the bullets, but you can firm it up more.

You might want to note somewhere that ACCURATE does not (??) plan to patent or profit from its developments, so that they can be used by all. Is this correct? Or is that just implied by govt. funding, or do people have problems with this. But you might want to say something about it somewhere.

Footnotes/References

The format is inconsistent. Sometimes you use initials, sometimes you have last name first, sometimes you have first name first. Decide on a style for all of the citations and edit them all to be the same.

For the ones you currently have for me, both are somewhat wrong. They should be as follows:

[38] Rebecca T. Mercuri. Electronic Vote Tabulation: Checks and Balances. Ph.D. thesis, School of Engineering and Applied Science, Department of Computer and Information Systems, University of Pennsylvania, 2001. University Microfilms #3003665. http://www.notablesoftware.com/Papers/thesdefabs.html

[39] Rebecca Mercuri. A Better Ballot Box? IEEE Spectrum, Vol. 39, No. 10, October 2002.
http://www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html