Testimony of Tadayoshi Kohno
Before the Committee on House Administration
U.S. House of Representatives
Hearing on Electronic Voting System Security
July 7, 2004

Thank you Chairman Ney, Ranking Member Larson, and members of the Committee on House Administration for holding today's hearing, and for inviting me to speak on the topic of electronic voting security.

My name is Tadayoshi Kohno,[1] and I am a computer security expert with the Department of Computer Science and Engineering at the University of California at San Diego. I am also a Department of Defense NDSEG Fellow and an IBM PhD Fellow. Before joining the University of California for doctoral studies, I was a cryptography and computer security expert with two of the nation's top computer security firms, Counterpane Labs and Cigital. I have conducted security analyses for and provided guidance to a wide variety of organizations, ranging from billion-dollar corporations like American Express and VISA, to innovative new technology startups.

Last summer I was one of four computer security experts to analyze the design of Diebold's AccuVote-TS paperless electronic voting system.[2] As a consultant, I was accustomed to analyzing computer systems with poorly designed security mechanisms. But, since Diebold's machines had already been used in actual elections, I was initially expecting to find the AccuVote-TS system employing at least somewhat effective security mechanisms. I was mistaken. In our analysis we found that the implementers of the AccuVote-TS system ignored basic security best practices, and we found that the AccuVote-TS system was vulnerable to a number of simple and easy-to-mount integrity- and privacy-compromising attacks (details in our paper).

Although uncovering security problems with Diebold's machines was certainly important, I believe that the most important contribution of our work was highlighting the following two issues of great concern: (1) Because Diebold's machines had been certified, our discoveries show that *the current "logic and accuracy" testing and certification processes for electronic voting machines cannot be trusted to uncover even the most elementary security problems*. This means that there is no reason to assume that other vendors' certified electronic voting machines are any more secure. (2) *Since the machines do not produce a voter-verifiable paper ballot*, if an attack is mounted or if something goes wrong with the voting machines, *there will be no way to confidently perform a recount of the voters' original intents*.

[1] URL: http://www-cse.ucsd.edu/users/tkohno. Email: tkohno@cs.ucsd.edu.

[2] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach. Analysis of an Electronic Voting System. In *2004 IEEE Symposium on Security and Privacy*, pages 27-40, May 2004. Originally published as Johns Hopkins University Information Security Institute Technical Report TR-2003-19, July 23, 2003. Available online at http://www.cse.ucsd.edu/users/tkohno/papers/eVoting/.

Our work catalyzed a national debate on electronic voting security. I come here to explain why I, as a computer security expert, am opposed to the use of existing paperless electronic voting machines in government elections. I will also discuss proposed strategies for improving the security of electronic voting machines. Although not part of my testimony, in the question-and-answer period I would be more than happy to address some of the unsound arguments about the security of existing electronic voting machines and certification processes that you may have heard in the past, such as the assumption that logic and accuracy tests can identify security problems, or the claim that because there have been no documented attacks against electronic voting machines in the past, the concerns of computer security experts must be exaggerated.

Classifying electronic voting machines: Existing systems versus the future/potential

The first thing that we must do is clarify *what types of electronic voting machines we are talking about*. Are we talking about existing, conventional paperless electronic voting machines, like Diebold's AccuVote-TS, and their near-future descendents? Or are we talking about currently hypothetical, conventional-style paperless electronic voting machines of the (probably distant) future? (Or are we talking about non-conventional, cryptography-based voting machines?) Many people don't make a distinction, and lump all electronic voting machines into the same pile, but that is a mistake.

I am going to talk about current electronic voting machines, and their near-future descendents, because I believe that it is those machines that are most relevant to this hearing. I am not ruling out the possibility of having "secure enough" and "transparent enough" conventional-style paperless electronic voting machines in the far future (I say "secure enough" because there is no such thing as absolute security), but creating such machines will require an immense investment in terms of time and money and research, not to mention the challenge of defining what "secure enough" means. We don't have such machines now. And we won't have them by November.

We cannot expect to have secure paperless electronic voting machines by November

Let me elaborate. We know that the AccuVote-TS system has many security problems. And because of the flaws with the current certification processes, we have no reason to believe that other existing electronic voting machines are any better. Although one might try to address all known security problems, either by patching the software or instituting new procedures, this is not sufficient to guarantee that the resulting system is actually secure enough for use in an actual election. There are several reasons why this is true.

First, *spot-treating security problems in electronic voting machines is like spot-treating termites, you can never be sure that you've gotten rid of them all*. This is especially true since those analyzing the security of a system are often contracted only for a limited period of time, and in that time the security analysts may only be able to uncover the most obvious security problems. Fixing those problems may "raise the bar" for an attack, but does not mean that there aren't other serious attack vectors for an attacker to exploit. (Of course, I should stress that security problems in voting machines are much worse than termites in houses; this is because security problems can be exploited by intelligent, coordinated, and malicious adversaries, whereas termites are simply hungry.)

Second, *unless all components of the revised system, including the software and revised procedures, are open to the public for public scrutiny and review, the public will have no reason to believe that the spot-treatment actually succeeded in addressing the security problems*. This is illustrated beautifully by the evolution of the Diebold AccuVote-TS system. After my colleagues and I released our original analysis of the AccuVote-TS system, the state of Maryland hired SAIC,[3] and then later RABA,[4] to perform independent analyses of recent versions of the AccuVote-TS system. We and SAIC identified problems with the way that the AccuVote-TS voting terminals communicate with the back-end tabulation system. Diebold tried to fix those problems by incorporating cryptographic mechanisms into their system. But RABA found that Diebold's revised system had its own security problems (in their attempted fix, Diebold used the SSL cryptographic protocol, but without host authentication). *If Maryland had not commissioned RABA to conduct a subsequent analysis of Diebold's purported fixes to ours and SAIC's reports, no one, except for maybe an attacker, would have uncovered Diebold's insufficient fix to the problems we identified.* This begs the question: for systems that the public cannot openly inspect, when can the public be satisfied that security problems have been successfully addressed?

One popular recommendation is to institute new election procedures in an effort to fix technical problems with the security of paperless electronic voting machines. The above points also apply here since there may be additional security problems not addressed by the new procedures, and since there is no guarantee that the new procedures will be appropriately designed. But there is another problem with relying too heavily on procedures. In security we desire what is called defense-in-depth, which means that a system should remain secure even if one of its components fails. Unfortunately, procedures may not always be implemented correctly – i.e., they may fail. They may fail because the people implementing those procedures are malicious. And they may fail because someone implementing the procedures accidentally makes a mistake. At a recent off-the-record KSG/NSF symposium on electronic voting, an election official made the following observation: At a company, it is natural for new employees to make mistakes on their first day of work. This is problematic since, for elections, every election day is the first (and only) day of work for many, many people.

What can be done between now and November

Since spot-treating security problems cannot be expected to yield a secure enough and transparent enough system, what can we do with existing paperless electronic voting machines? Computer security experts, including myself, advocate adding a voter-verifiable paper ballot to existing paperless electronic voting machines. That is, retrofit

[3] Science Applications International Corporation. Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes, September 2003. Available online at http://www.dbm.maryland.gov/SBE.

[4] RABA Innovative Solution Cell. Trusted Agent Report: Diebold AccuVote-TS Voting System, January 2004. Available online at http://www.raba.com/press/TA_Report_AccuVote.pdf.

existing paperless electronic voting machines with printers, and have the machines print a paper ballot when a voter casts his or her votes. The voter verifies that his or her votes on the paper ballot are correct and, if they are, deposits the ballot in a ballot box. The paper ballot is what becomes the official record in the case of a recount. Of course, another option might be to avoid these new paperless electronic voting machines completely, and use, for example, optical scan voting machines.

One response to this might be that the use of paper ballots in this way is not perfectly secure either – it just defers the problem of election integrity to the counting of the paper ballots, and paper ballot boxes can always be stuffed or destroyed. I would like to advocate the following principle: *any new voting mechanism should be no less secure than (i.e., at least as secure as) the system that it is replacing*. Since the risks with electronic voting machines that produce paper ballots are effectively the same risks that traditional paper ballots have, *paper-based electronic voting machines will be at least as secure as the traditional voting mechanisms*; i.e., by using electronic voting machines with voter-verifiable paper ballots, we have not made security worse than before. As a computer security expert, *I cannot confidently say the same thing about existing* paperless *electronic voting machines, or their near-future descendants*.

To summarize, from a security perspective, my specific recommendation between now and November is to retrofit existing paperless electronic voting machines with the ability to print a voter-verifiable paper ballot, or to revert to existing paper-based voting methods like optical scan systems. If that is impossible, LCCR[5] has suggested that jurisdictions that have paperless electronic voting machines should hire independent security analysts and follow those analysts' advice. Based on my previous remarks, it should be clear that this is not a sufficient solution and that it is no substitute for the use of a voter-verifiable paper ballot. Furthermore, although it will be obvious if a jurisdiction decides to use paper ballots, it will be much less clear if and to what extent a jurisdiction follows the LCCR recommendations.

Long-term

For the long-term, the most important general principle is to involve all relevant experts in all decisions. By relevant experts, I mean not only computer security experts, but also election officials, experts on human-computer interaction, experts on the needs of those with disabilities, and so on. Elections are too important to not involve members of all of these groups. This hearing is a sign that we are moving in the right direction, and I would like to thank the committee for its focus on this important issue. I believe that the dialog that we are having today will help bring us closer to an acceptable solution with respect to the security of electronic voting machines.

[5] Recommendations of the Brennan Center for Justice and the Leadership Conference on Civil Rights for Improving Reliability of Direct Recording Electronic Voting Systems. Available online at http://www.civilrights.org/issues/voting/lccr_brennan_report.pdf.