November 4, 2003

Rep. Edward J. Markey
2108 Rayburn HOB
Washington, DC 20515-2107

Dear Representative Markey,

As a graduate student in computer science who has studied computer security, I worry deeply that the trust we are placing in electronic voting machines is unwarranted. I urge you to cosponsor the Voter Confidence and Increased Accessibility Act of 2003 (VCIAA, HR 2239). As touchscreen voting (e-voting) technology is adopted across America, it's absolutely vital that these new systems meet basic standards of accountability and openness. I am particularly concerned about the glaring security lapses found by multiple researchers in Diebold's voting machine software, and the callous and lax attitude toward security evidence by their internal memos, which have been leaked to the press. Diebold is currently threatening legal action against me personally for publishing details of these lapses, for instance:

a) the use of uncertified software to run and count elections. The secretary of state of California has halted certification of Diebold machines after discovering this has occured in California; the memos indicate that it has happened in MN, FL, and elsewhere as well, and was in fact a very common situation.
http://www.wired.com/news/politics/0,1283,61068,00.html
http://www.scoop.co.nz/mason/stories/HL0309/S00150.htm

b) Massive unreliability of the election machines and vote counting software, including memory card corruption and unexplained large *negative* vote counts for certain candidates (for instance, -16,022 votes for Gore in FL in 2000).
http://cscott.net/Activism/Diebold/FairUse/lists/support.w3archive/200101/msg00068.html
http://www.scoop.co.nz/mason/stories/HL0310/S00211.htm

c) Exploitable security flaws in the software. The memos reveal that inserting a blank smart card into an election machine *during an election* would grant the voter "manager" rights to alter the ballot and counts. The "audit log" meant to protect the authenticity of the votes was actually editable by *anyone*, just by double-clicking on the file.
http://cscott.net/Activism/Diebold/FairUse/msg00025.html
http://cscott.net/Activism/Diebold/FairUse/lists/support.w3archive/200110/msg00122.html

d) Other documented voting regulation violations; for example, transmitting and viewing vote counts before the election is complete.
http://www.scoop.co.nz/mason/stories/WO0309/S00054.htm
http://cscott.net/Activism/Diebold/FairUse/lists/rcr.w3archive/200202/msg00051.html

Unfortunately, these problems are likely not unique to Diebold. I am particularly concerned that many systems do not use openly reviewed software and cannot provide a voter verifiable paper audit trail. Unless a paper record is generated by publicly reviewed software, verified by the voter and retained for potential recounts, I believe that this technology is unacceptable for use in our elections. With Diebold's current touch-screen systems (and many other vendors' systems), voting irregularities can not be verified or corrected. For example, some elections on touchscreen machines have shown suspiciously high numbers of undercounts --- voters who apparently took the trouble to come to the polling place and enter the machine, only to leave without registering a single vote for any candidate. This seems highly irregular, but with touchscreen machines there is no record to turn to to elucidate the matter. The voting machines provide no record of voter intent.

Further, the public should be allowed to review the software that runs these machines in order to confirm that they act in the way that the manufacturer claims. Right now, however, the leading technologies are not only proprietary, they are covered by trade secret claims. This kind of closed source, or "black box," software lacks sufficient quality assurance. The Diebold flaws illustrate that current testing is radically insufficient. Open source software would allow every patriotic American to participate in the review and increase the confidence of our elections. Australia, inventor of the secret ballot, is already leading the way on this front as well, so the requirement is not impossible. HR 2239 would require voting machines to use publicly reviewed software.

Open source software is not enough, because it is actually extremely difficult to reliably ascertain that the software running on a hardware system is actually the software reviewed. This is perhaps surprising, but the universality of computer software ensures that it is almost always possible to "emulate" the authorized software even when true control of the system resides elsewhere. HR 2239 would also mandate voter verifiable paper audit trails for all new e-voting machines, a prerequisite for accountability and accuracy. The 2000 presidential election was a painful lesson in the failings of current voting technology, but at least there was a back-up system that allowed a manual recount when evidence emerged that the regular voting process was flawed. Without a paper audit trail, a compromised e-voting system could not provide even the cold comfort of Florida's manual recount. With a paper audit trail, no malicious or simply buggy software could prevent true voter intent from being determined. Luckily, adding this protection to the machines is not hard and does not have to add a significant amount to the cost of each unit.

I strongly urge you to cosponsor HR 2239 to ensure that all new e-voting machine purchases provide a voter-verifiable paper audit trail and use publicly reviewed software. This issue is vital to the very heart of our democratic process. Thank you for your time.

Sincerely,

C. Scott Ananian
57 Mystic Street
Arlington, MA 02474