Rebecca Mercuri

VOTING-MACHINE RISKS

INSIDE RISKS

On July 23, 1992, New York City Mayor Dinkins announced that seven thousand Direct Recording Electronic (DRE) voting machines would be purchased from Sequoia Pacific, pending the outcome of public hearings. This runs counter to the advice of the N.Y. Bar Association, independent groups of concerned scientists and citizens (such as Election Watch, CPSR and NYPIRG), and SRI International (a consultant to N.Y.C., and the system evaluators), all of whom have indicated that the equipment is not yet fit for use.

Background. At first glance, most DREs appear similar to mechanical 'lever' voting machines. Lacking any visual identification as 'computers' (no monitors or keyboards), voters would be unlikely to assume that one or more (in some cases, as many as nine) microprocessors are housed in the units. The ballot is printed on paper which is mounted over a panel of buttons and LEDs. A thin piece of flexible plastic covers the ballot face, to protect it from damage or removal. The machine is housed in an impact and moisture-resistant case, shielded from EMI, and protected by battery backup in the event of power loss. At the start of the election session, poll workers run through a procedure to make the machine operational, and similarly follow another sequence (which produces a printed result total) to shut the device down at the end of the day. A cartridge which contains the record of votes (scrambled for anonymity) is removed and taken to a central site for vote tallying.

Risks. The astute reader, having been given this description of the system, should already have at least a dozen points of entry in mind for system tampering. Rest assured that all of the obvious ones (and many of the nonobvious ones) have been brought to the attention of the N.Y.C. Board of Elections. Furthermore, in SRI's latest published evaluation (June 19, 1991) the Sequoia Pacific AVC Advantage® systems failed 15 environmental/engineering requirements and 13 functional requirements including resistance to dropping, temperature, humidity and vibration. Under the heading of reliability, the vendor's reply to the testing status report stated: "SP doesn't know how to show that the Electronic Voting Machine and its Programmable Memory Device meets requirement—this depends on poll workers' competence."

The Pennsylvania Board of Elections examined the system on July 11, 1990, and rejected it for a number of reasons, including the fact that it "can be placed inadvertently in a mode in which the voter is unable to vote for certain candidates" and it "reports straight-party votes in a bizarre and inconsistent manner." When this was brought to the attention of NYCBOE, they replied by stating "the vendor has admitted to us that release 2.04 of their software used in the Pennsylvania certification process had just been modified and that it was a mistake to have used it even in a certification demonstration." Needless to say, the machines have not yet received certification in Pennsylvania.

Other problems noted with the system include its lack of a guaranteed audit trail (see "Inside RISKS," *Commun. ACM 33*, 11, Nov. 1990), and the presence of a real-time clock which Pennsylvania examiner Michael Shamos referred to as "a feature that is of potential use to software intruders."

Vaporware. Sequoia Pacific has now had almost four years since they were told they would be awarded the contract (following a competitive evaluation of four systems) if they could bring their machines up to the specifications stated in the Requirements for Purchase. At an August 20 open forum, a SP representative stated publicly that no machine presently existed that could meet those standards. Yet the city intends to award SP the $60 million contract anyway, giving them 18 months to satisfy the RFP and deliver a dozen machines for preliminary testing (the remainder to be phased in over a period of six years).

Conclusions. One might think the election of our government officials would be a matter that should be covered by the Computer Security Act of 1987, but voting machines, being procured by the states and municipalities (not by the federal government) do not fall under the auspices of this law, which needs to be broadened. Additionally, no laws in N.Y. state presently preclude convicted felons or foreign nationals from manufacturing, engineering, programming or servicing voting machines.

This would not be so much of a concern, had computer industry vendors been able to provide fully auditable, tamper-proof, reliable, and secure systems capable of handling anonymous transactions. Such products are needed not only in voting, but in the health field for AIDS test reporting, and in banking for Swiss-style accounts. It is incumbent on us to devise methodologies for designing verifiable systems that meet these stringent criteria, and to demand that they be implemented where necessary. "Trust us" should not be the bottom line for computer scientists. ■

***Rebecca Mercuri** is a research fellow at the University of Pennsylvania's Moore School of Engineering and a computer consultant with Notable Software. She has served on the board of the Princeton ACM chapter since its inception in 1980. Email mercuri@gradient.cis.upenn.edu.*