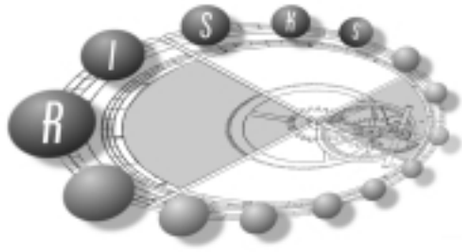

Rebecca Mercuri

Voting Automation (Early and Often?)

Computerization of manual processes often creates opportunities for social risks, despite decades of experience. This is clear to everyone who has waded through deeply nested telephone menus and then been disconnected. Electronic voting is an area where automation seems highly desirable but fails to offer significant improvements over existing systems, as illustrated by the following examples.

Back in 1992, when I wrote here [5] about computerized vote tabulation, a $60 million election system intended for purchase by New York City had come under scrutiny. Although the system had been custom-designed to meet New York's stringent and extensive criteria, numerous major flaws (particularly those related to secure operations) were noted during acceptance testing and review by independent examiners. New York withheld its final purchase approval and legal wranglings ensued. This summer, the contract was finally cancelled, with New York agreeing to pay for equipment and services it had received; all lawsuits were dropped, thus ending a long and costly process without replacing New York's bulky arsenal of mechanical lever machines.

Given New York's lack of success in obtaining a secure, accurate, reliable voting system, built from the ground up, operating in a closed network environment, despite considerable time, resources, expertise and expenditures, it might seem preposterous to propose the creation of a system that would enable "the casting of a secure and secret electronic ballot transmitted to election officials using the Internet" [3]. Internet security features are largely add-ons (firewalls, encryption), and problems are numerous (denial-of-service attacks, spoofing, monitoring). (See [2, 6].) Yet this does not seem to dissuade well-intentioned officials from promoting the belief that online voting is around the corner, and that it will resolve a wide range of problems from low voter turnout to access for the disabled.

The recent California Task Force report suggested e-voting could be helpful to "the occasional voter who neglects to participate due to a busy schedule and tight time constraints" [3]. Convenient access is a vacuous promise, in that the described authorization process requires pre-election submission of a signed e-voting request, subsequent receipt of a password, instructions, and access software. Clearly, it would be far easier to mail out a conventional absentee ballot that could be quickly marked and returned, rather than requiring each voter to reboot a computer in order to install "a clean, uncorrupted operating system and/or a clean Internet browser" [3].

Countless e-voting dot-coms have materialized recently, each hoping to land lucrative contracts in various aspects of election automation. Purportedly an academic project at Rensselaer Polytechnic Institute, voteauction.com was shut down following threats of legal action for violating New York state election laws [1]. It has since been sold and reopened at an off-shore location where prosecution may be circumventable. Vote-selling combined with Internet balloting provides a powerful way to throw an election to the highest bidder, but this is probably not what election boards have in mind for their modernized systems. The tried-and-true method of showing up to vote where your neighbors can verify your existence is still best used at least until biometric identification is reliable and commonplace.

While jurisdictions rush to obtain new voting systems, protective laws have lagged behind. Neither the Federal Election Commission nor any state agencies have required that computerized election equipment and software comply with existing government standards for secure systems. The best of these, the ISO Common Criteria, addresses matters important to voting such as privacy and anonymity; although it fails to delineate areas in which satisfaction of some requirements would preclude implementation of others, its components should not be ignored by those who are establishing minimum certification benchmarks [4].

Computerization of voting systems can have costly consequences, not only in time and money, but also in the much grander sense of further eroding confidence in the democratic process. "If it ain't broke, don't fix it" might be a Luddite's battle cry, but it may also be prudent where the benefits of automation are still outweighed by the risks. C

PAUL WATSON

References

1. Anderson, M.K. Close vote? You can bid on it (Aug. 17, 2000), and Voteauction bids the dust (Aug. 22, 2000), *Wired News*.
2. Blaze, M.A. and Bellovin, S.M. Tapping on my network door. *Commun ACM 43*, 10 (Oct. 2000).
3. California Internet Voting Task Force. A report on the feasibility of Internet voting. January 2000; www.ss.ca.gov/executive/ivote/home.htm.
4. Mercuri, R. Ph.D. dissertation; www.seas.upenn.edu/~mercuri.
5. Mercuri, R. Voting-machine risks. *Commun. ACM 35*, 11 (Nov. 1992).
6. Weinstein, L. Risks of Internet voting. *Commun ACM 43*, 6 (Jun. 2000).

Rebecca Mercuri (mercuri@acm.org) is a member of the computer science faculty at Bryn Mawr College.