Computerized Voting Machines: A View from the Trenches

Barbara Simons

simons@acm.org

As a result of Florida 2000, some Americans concluded that paper ballots simply couldn't be counted, even though businesses, banks, racetracks, lottery systems, and others count and deal with paper all the time. Instead, paperless computerized voting systems (Direct Recording Electronic or DREs) were touted as the solution to "the Florida problem".

Election officials in the U.S. were told that DREs in the long run would be cheaper than alternative voting systems. They also were told that DREs had been extensively tested and that the certification process guaranteed that the machines were reliable and secure. No mention was made of the costs ballot design, of pre-election testing, and of secure storage of DREs; nothing was said about the threat of hidden malicious code; no mention was made of the inadequacy of the testing and certification processes, to say nothing of the difficulty of creating bug-free software.

Why were independent computer security experts not consulted about such a major and fundamental change in how elections are held? Why were some election officials and policy makers hostile when computer security experts warned of the risks of computerized voting to the point of accusing computer scientists of being "fear mongers" and Luddites? How could Harris Miller, the President of the Information Technology Association of America, a lobbying organization that has received compensation from voting machine vendors, claim on Election Day 2004 that, "Electronic voting machine issues that have been cited are related to human error, process missteps or unsubstantiated reports"? How would he know? Why would anyone listen to him?

Why do many election officials and politicians believe that internet voting would increase voter turnout in the U.S., even though no rigorous testing has occurred? And, even if internet voting would increase turnout, how can these same people who have been reading about internet viruses for years not understand that internet voting is a very very risky proposition?

In short, why have DRE vendors and many election officials succeeded at challenging the expertise of computer scientists and computer security experts?

The refusal of policy makers to listen to the computing community hardly began with the introduction of poorly engineered and insecure voting machines. Many computer scientists and computer security experts became involved with policy debates over crypto policy, copyright, patents, and computerized surveillance – to name some of the major issues.

The disconnect between the computing community and policy makers is perhaps best illustrated by the Digital Millennium Copyright Act (DMCA),

S. De Capitani di Vimercati et al. (Eds.): ESORICS 2005, LNCS 3679, pp. 1–2, 2005.

which became part of US law in 1998. It was only by chance that I learned why implementation of the most controversial aspects of the DMCA, the anti-circumvention and anti-dissemination provisions, was postponed until 2000. The delay was written into the DMCA because lawmakers knew, or someone they trusted told them, that aspects of the DMCA might criminalize work on securing software against Y2K problems. Yet, the fact that Y2K was hardly the only software security issue that would require the kinds of reverse engineering that was done to fix Y2K bugs was either unknown to the lawmakers or a matter of indifference to them.

A discussion of the DMCA brings us full circle back to the issue of computerized voting systems. In the U.S. the software that is deployed in these systems is secret, as is the testing – paid for by the software vendors – and the test results. Because of the anti-circumvention provisions of the DMCA, computer security experts risk violating U.S. Federal law if they wish to reverse engineer voting machine software to search for bugs or malicious code. Consequently, a law that was crafted by the movie and record industries to prevent unauthorized copying is assisting voting machine vendors with concealing their software from meaningful independent review.

Clearly, we computing professionals have been failing at explaining the risks of inappropriate, careless, or poorly designed software to the general public and especially to policy makers, at least in the U.S. (At this conference I hope to learn more about what is happening in Europe). While perhaps not enough of us have become involved with efforts to educate policy makers, there are some fundamental reasons why our expertise is frequently ignored:

1. People who have never done much programming do not understand how difficult it is to find bugs in software.
2. Because people don't understand point 1, they certainly don't understand that last minute software patches are very dangerous.
3. Consequently, most people have a hard time believing computer security experts when they say that it's possible to write malicious code and conceal it in a large program. They just don't understand why it can be very difficult to determine that malware is present, let alone locate it in a large body of code.

In addition, we are a relatively young profession, and many of us have an independent streak and a casual mode of dress that, taken together, make some politicians view us as potential trouble makers, rather than as people whose views the politicians should take seriously.

Yet, we must make our voices heard. The issues are too critical to allow us to be shut out of the debate.

I'll give an overview of some of the technological and policy issues relating to computerized voting machines, and perhaps touch on how we might do a better job of getting our message across. I also look forward to hearing ideas that others might have of how we might better explain software-related risks to non-technical decision makers.