Notes for a Hearing of the California Assembly
Committee on Elections Reapportionment and
Constitutional Amendments

Peter G. Neumann
Principal Scientist, Computer Science Lab
SRI International, Menlo Park, California
333 Ravenswood Ave, Menlo Park CA 94025-3493
Tel 1-650/859-2375; Fax 1-650/859-2844
Neumann@CSL.sri.com; http://www.csl.sri.com/neumann

Wednesday, January 17, 2001

Summary: The election process is inherently subject to errors, manipulation, and fraud. It is a process that demands extraordinary integrity of any computerized systems involved, as well as honesty and experience of the people involved in administering elections. Evidently, it may require considerable sophistication on the part of voters as well.

The Year 2000 U.S. election process has demonstrated many weaknesses and irregularities in the existing processes. As a result of the Florida punched-card experience, there is a huge cry to get rid of old-fashioned systems. In particular, vendors of electronic systems have come out of the woodwork with promises of eliminating spoiled ballots, punched-card anomalies, and recounts, and providing instant results; however, those systems lack adequate assurances of the integrity of the voting process. Because of ubiquitous human errors (which typically occur in all computer systems), software Trojan horses, and trapdoors (especially if inserted during development or maintenance), existing electronic systems have insufficient guarantees that votes that are actually counted are precisely what the voter had intended. Although it is impossible to guarantee the correctness of hardware and software, it is unfortunate that even common standards for system security are typically ignored.

The highest potential risks relate to electronic systems – and worst of all Internet voting, limited by the intrinsic lack of security in Internet systems and a morass of sociological problems. Old-style lever machines and well-managed optical scanning systems are typically more reliable and less subvertible than electronic ballot systems. It is interesting to note that a very large part of the world still uses paper ballots marked with an X for the selected choice; that approach is considered very reliable and surprisingly quick in the counting phase when distributed into precincts with suitable oversight.

Rebecca Mercuri's recent PhD thesis (noted below) at the University of Pennsylvania provides an extensive set of criteria against which electronic voting systems should be evaluated, but also points out that any such criteria are at the same time inherently incomplete and intrinsically difficult if not impossible to satisfy. She also proposes a strategy that would significantly increase the accountability of electronic voting systems (such as direct-recording touch-screen systems), providing an independent paper trail for each ballot that is verified by the voter before the ballot is cast. This would provide an audit trail in the event of disputes.

The bottom line is of course that all voting systems are subject to varying degrees of errors and manipulation. As a technologist, I have a responsibility to seek checks and balances not only on the technology but also on the voting process as a whole. As legislators, you have an obligation to ensure that you do not endorse simplistic solutions that could in actuality make the integrity of the election process much less than it is today, with even greater opportunities for fraud and subversion.

The next two pages provide two brief documents that I have written previously with colleagues:

- The first is a reprint of an article in the Communications of the ACM (Association for Computing Machinery).

- The second is taken from the on-line Risks Forum Digest, 12 December 2000, Volume 21, Issue 14 (which I have moderated since its inception in August 1986). The entire issue is archived at http://catless.ncl.ac.uk/Risks/21.14.html. For subscriptions to the Risks Forum, risks-request@CSL.sri.com with one line text: SUBSCRIBE

My 1995 book (*Computer-Related Risks,* Addison-Wesley) contains extensive material on the lack of integrity in then-existing election systems, and discussion of requirements for improving the process. The situation has not improved appreciably since then, although there have been some advances toward better electronic systems. Rebecca Mercuri's thesis has carried the approach of my book much farther. I strongly recommend that you use her guidelines for any future efforts to shift to automated voting systems. You and your staffers will also find considerable background information on my Web site.

Please feel free to call on me for further information and background.

System Integrity Revisited

Rebecca T. Mercuri and Peter G. Neumann
mercuri@acm.org and pneumann@acm.org **Communications of the ACM vol. 44, no. 1**
January 2001, page 160

Consider a computer product specification with data input, tabulation, reporting, and audit capabilities. The read error must not exceed one in a million, although the input device is allowed to reject any data that it considers to be marginal. Although the system is intended for use in secure applications, only functional (black box) acceptance testing has been performed, and the system does not conform to even the most minimal security criteria.

In addition, the user interface (which changes periodically) is designed without ergonomic considerations. Input error rates are typically around 2%, although experience has indicated errors in excess of 10% under certain conditions. This is not considered problematic because errors are thought to be distributed evenly throughout the data. The interface provides essentially no user feedback as to the content of input selections or to the correctness of the inputs, even though variation from the proper input sequence will void the user data.

Furthermore, multiple reads of the same user data set often produce different results, due to storage media problems. The media contain a physical audit trail of user activity that can be manually perused. There is an expectation that this audit trail should provide full recoverability for all data in order to include information lost through user error. (In practice, the audit trail is often disregarded, even when the user error rate could yield a significant difference in the reported results.)

We have just described the balloting systems used by over a third of the voters in the United States. For decades, voters have been required to use inherently flawed punched-card systems, which are misrepresented as providing 100% accuracy ("every vote counts") – even though this assertion is widely known to be patently untrue. Lest you think that other voting approaches are better, mark-sense systems suffer from many of the same problems described above. Lever-style voting machines offer more security, auditability, and a significantly better user interface, but these devices have other drawbacks – including the fact that no new ones have been manufactured for decades.

Erroneous claims and product failures leading to losses are the basis of many liability suits, yet (up to now) candidates have been dissuaded from contesting election results through the legal system. Those who have lost their vote through faulty equipment also have little or no recourse; there is no recognized monetary or other value for the right of suffrage in any democracy. With consumer product failures, many avenues such as recalls and class action suits are available to ameliorate the situation – but these are not presently applicable to the voting process. As recent events have demonstrated, the right to a properly counted private vote is an ideal rather than a guarantee.

The foreseeable future holds little promise for accurate and secure elections. Earlier columns here [November 1990, 1992, 1993, 2000, and June 2000] and Rebecca Mercuri's doctoral thesis [http://www.notablesoftware.com/evote.html] describe a multitude of problems with direct electronic balloting (where audit trails provide no more security than the fox guarding the henhouse) and Internet voting (which facilitates tampering by anyone on the planet, places trust in the hands of an insider electronic elite, and increases the likelihood of privacy violations). Flawed though they may be, the paper-based and lever methods at least provide a visible auditing mechanism that is absent in fully automated systems.

In their rush to prevent "another Florida" in their own jurisdictions, many legislators and election officials mistakenly believe that more computerization offers the solution. All voting products are vulnerable due to the adversarial nature of the election process, in addition to technical, social, and sociotechnical risks common to all secure systems. Proposals for universal voting machines fail to address the sheer impossibility of creating an ubiquitous system that could conform with each of the varying and often conflicting election laws of the individual states. Paper-based systems are not totally bad; some simple fixes (such as printing the candidates' names directly on the ballot and automated validity checks before ballot deposit) could go a long way in reducing user error and improving auditability.

As the saying goes, "Those who fail to learn from the past are doomed to repeat it." If the computer science community remains mute and allows unauditable and insecure voting systems to be procured by our communities, then we abdicate what may be our only opportunity to ensure the democratic process in elections. Government officials need your help in understanding the serious risks inherent in computer-related election systems. Now is the time for all good computer scientists to come to the aid of the election process.

Internet and Electronic Voting (from the Risks Forum, vol, 21 no 14)
Peter Neumann, Rebecca Mercuri, and Lauren Weinstein, December 14, 2000

A recurring mantra heard from some entities involved in the development and promotion of Internet-based voting systems is that they have conducted "public tests" and thus their systems are secure. If hackers don't break into such systems, the tests are declared a success.

This is of course illogical on its face, because it seems unlikely that people (both U.S. and internationally based) with an interest in subverting the U.S. election process would care to tip their hands by participating in what are essentially publicity stunts. These might attract your average 12-year old hacker, but not the pros who wait for production systems for their carefully mounted attacks.

In fact, using such "tests" as any sort of validation technique runs contrary to long-established computer and engineering verification practices, and makes a mockery of the rigorous design and testing that is required of systems that are to be deemed secure through extensive and methodical processes (e.g., to gain certification under the ISO Common Criteria or its predecessors TCSEC/ITSEC). "I left my Porsche out in the parking lot with the doors unlocked and the key in the ignition and since it doesn't appear to have been stolen this must be a safe neighborhood," would be an equally nonsensical statement of supposed validation. All proposed voting systems should be subjected to rigorous evaluation, public inspection, and *open-source code* license agreements. Some applicable methodologies do exist, but have not been required. For example, Level 4 Common Criteria should be a *minimum* standard, although even that is not enough. (See http://csrc.nist.gov/cc for the CC Web site.)

Security is only as strong as its weakest links. Internet voting (I-voting) will *always* be limited in its integrity by factors beyond the I-voting algorithms. For example, encryption can be an important part of an overall election system. However, although we have strong cryptographic algorithms, we do not have systems with adequate security into which the cryptography can be embedded. Furthermore, voter authentication, vote integrity, voter anonymity, auditability, accountability, recountability, and so on, are all involved, and many of these requirements operate at cross-purposes with one another. The massive vulnerabilities of standard personal-computer operating systems represent very serious concerns, in terms of hidden viruses, worms, Trojan horses, and further surprises unknowingly downloaded by the user with other packages, and waiting to pounce on election day. One proposed solution would be to boot a fresh system from external media in order to vote, but even such an approach does not adequately address these potential vulnerabilities.

Deficient network protocols and the opportunities for insider fraud and accidental misuse abound. In addition to the issues noted above are the weaknesses that result from inadequate operational environments. Neither the client nor the server systems will be adequately secure under foreseeable technology – including Internet Service Providers and Web servers. For example, proposals such as the use of rotating IP numbers and multiple systems to try to defend against denial of service attacks can be rendered impotent by similar attacks on network concentration points.

As always in any election environment, there are many opportunities for fraud, mischief, and manipulation – despite ostensible checks and balances. These problems are exacerbated with electronic and Internet voting, where the lack of any physical ballots makes such manipulations impossible to detect and correct – because there is no meaningful recount capability. Extraordinary vigilance is necessary, but never sufficient.

In the wake of the recent Presidential election problems, the knee-jerk reaction of "gee, can't we modernize and solve all this with electronic and/or Internet voting?" is predictable, but still wrongheaded. The shining lure of these "hype-tech" voting schemes is only a technological fool's gold that will create new problems far more intractable than those they claim to solve.

Peter Neumann moderates the ACM Risks Forum, Chairs the ACM Committee on Computers and Public Policy, and is a cofounder of PFIR – People For Internet Responsibility <http://www.pfir.org>.

Rebecca Mercuri is a Professor of Computer Science at Bryn Mawr College. She has provided expert testimony on voting systems throughout the past decade. For information on her Penn doctoral thesis and other writings on this subject, see http://www.notablesoftware.com/evote.html .

Lauren Weinstein <lauren@vortex.com> and <lauren@pfir.org> moderates the Privacy Forum <http://www.vortex.com> and is a cofounder of PFIR – People For Internet Responsibility <http://www.pfir.org>, and Member of the ACM Committee on Computers and Public Policy. See http://www.pfir.org/statements/voting for an earlier statement on I-voting.