Inside RISKS

Rebecca T. Mercuri and Peter G. Neumann

System Integrity Revisited

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 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 U.S. 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. 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 (see www.seas.upenn.edu/~mercuri/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. C

Rebecca Mercuri (mercuri@acm.org) is a member of the Computer Science faculty at Bryn Mawr College.
Peter Neumann (neumann@csl.sri.com) moderates the ACM Risks Forum.

PAUL WATSON