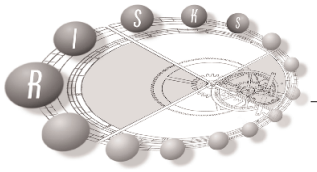

Risks of E-voting

Electronic voting has spread throughout the U.S. and the world without sufficient attention to reliability, security, or transparency. Today's e-voting systems use proprietary code, and vendors have often asserted the confidentiality of this code when independent reviews of certified systems were requested. This confidentiality conflicts with the transparency required for public elections.

In order to provide an independent assessment of the voting systems certified for use in California, Secretary of State Debra Bowen initiated a top-to-bottom review of those e-voting systems. She asked us to recruit a team of experts and gave us access to all the equipment, source code, and technical information that the Secretary of State's office had.

The results showed that the systems appeared not to be designed or implemented with security in mind. The design and implementation ignored basic security principles, and we found serious security vulnerabilities in all three vendors' systems. The security flaws were systemic and surprisingly similar across the three systems.

For example, malicious code could exploit vulnerabilities in the voting software to spread virally from machine to machine. As a result, when the voting machines return results to election central to count the votes, a virus could infect the county's election management systems. At the next election, the infected election management systems could then infect every voting machine in the county.

This virus could be introduced at several points in the process. An attacker could tamper with an e-voting machine while it is stored unattended overnight in a polling place. For some of the systems, a voter could introduce malicious code in under a minute, while voting.

Many flaws resulted from elementary mistakes such as straightforward buffer overrun vulnerabilities and flawed cryptography. One piece of voting software appends a three-letter suffix to a password and sends this "encrypted" result over the network. Another has encryption keys hard-coded in the source code, meaning the keys are the same for all machines using that software—an obvious security flaw. One of the manufacturers used its own name as a hard-wired password. Our public reports had to be written carefully to convey the depth of the problem without providing a "road map" for attackers.

We drew several lessons from this exercise.

First, the national regulatory system has not worked well. Federal testing repeatedly failed to detect flaws in voting systems. Election officials relied in good faith upon these certifications when they purchased, deployed, and used these voting systems. They, and voters, deserve better.

This should provide a strong impetus to reform the oversight system so that states do not have to bear the cost of securing voting systems one state at a time. Vendors will build whatever the regulatory system allows and the marketplace demands. So far these forces have failed to weed out flawed voting systems.

Fortunately, the results of the top-to-bottom review give us an opportunity to change the regulatory process to make it effective. Federal officials are currently preparing a major revision of the federal voting standards, and we encourage the computing community to become more involved in these issues.

Secondly, applying technology to solve one problem may introduce other problems. E-voting systems were introduced to eliminate paper and problems such as hanging chads. However, without paper, voters cannot check that their vote is correctly recorded and cannot independently validate vote totals. Thus the solution to one problem introduced another: the violation of a fundamental tenet, that there must be an independent means for verifying results.

This problem can be mitigated with voter-verified paper records that election officials audit after each election. However, only 16 states currently require this. The security vulnerabilities we found highlight the importance of election auditing: without audits, there may be no way to rebut suspicion of tampering.

Electronic voting systems form a critical part of the election process. We have far to go to ensure they are a transparent and secure part of that process. C

PAUL WATSON

Matt Bishop (bishop@cs.ucdavis.edu) is a professor in the Department of Computer Science at the University of California at Davis. He teaches and does research in computer security and information assurance. **David Wagner** (daw@cs.berkeley.edu) is a professor in the computer science division at the University of California at Berkeley, a cofounder of the ACCURATE center on voting, and a member of the federal advisory committee charged with helping draft the next-generation voting standard.