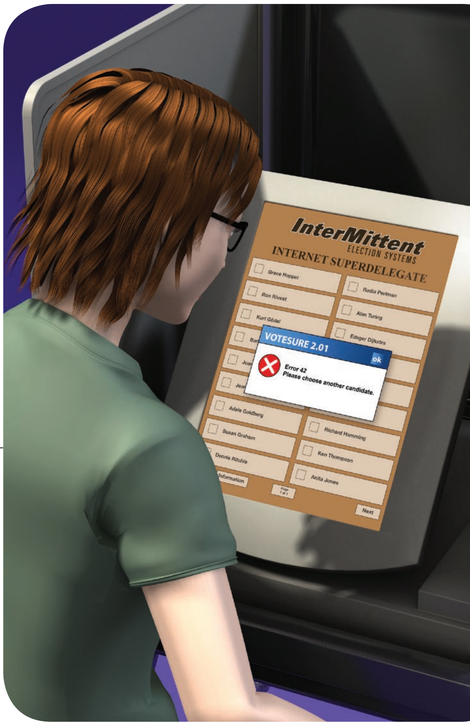
New Research Results for Electronic Voting

David R. Jefferson
Lawrence Livermore National Laboratory

Aviel D. Rubin
Johns Hopkins University

Voting systems have become controversial in the years following the multiple election disasters that occurred in the US during and after 2000. Of particular note were the electronic voting (e-voting) systems that were widely deployed to replace the pre-scored punch-card systems, systems that have been frequently judged to be central to the problem in the 2000 Florida general election. The (premature) deployment of e-voting machines stimulated a new field of security and privacy research around the subject of elections, a subject that has turned out to be more complex and deeper than anyone would have predicted a decade ago. E-voting systems have traditionally been designed to prevent, or at least detect, attacks by voters. But insiders—poll workers, election officials, and vendors—were considered trusted. That standard is no longer satisfactory. The goal now is to create practical systems that can provide trustworthy election results and vote privacy even in the face of insider malfeasance, software error, or maliciousness. It's a tall challenge, but we've been making great progress.



We received many submissions for this special issue of *IEEE Security & Privacy*; we thank all authors of all of the submitted articles for contributing. We're grateful to all of our external reviewers for providing detailed reviews—they helped us identify five excellent articles, and we're pleased to present what represents a sample of some of the finest recent work on election technology from authors on three continents. The articles cover a broad range of topics, including different receipt schemes, analysis and audit, and novel development strategies.

In the paper "A Three-Ballot-based Secure Electronic Voting System," Brazilian authors Regivaldo Costa, Altair Santin, and Carlos Maziero propose a secure electronic implementation of a novel voting system first described more than a year ago by MIT professor Ron Rivest and his collaborator Warren Smith in which each voter casts three ballots, voting on exactly one of them for the candidates they do *not* support, and on two of them for the candidates they do. This paper fleshes out that system, pointing out how it might be made practical in real elections.

Alec Yasinsac and Matt Bishop analyze the role of redundancy and corroboration in vote counting processes in their article, "The Dynamics of Counting and Recounting Votes." They criticize some of the widely-accepted logic behind recount and audit processes, and point out the weaknesses of paper ballots and hand counting that must be considered when using them as a check on the validity of electronic counts. Based on this analysis, Yasinsac and Bishop outline a corroborative, redundant voting mechanism; its goal is to provide independent sets of electronic votes that can be used as checks on one another without the need for paper.

A key tool in securing e-voting systems has been the addition of *voter-verified paper trail* or *paper record* units to otherwise-all e-voting machines. The Attorney General of New Jersey this year issued requirements for systems employing that technology, and commissioned a study of the state's voting systems to see how well they met those requirements. In their article, "Evaluating Electronic Voting Systems Equipped with Voter-Verified Paper Records," authors Nirwan Ansari, Pitipatana Sakarindr, Ehsan Haghani, Chao Zhang, Aridaman K. Jain, and Yun Q. Shi from the New Jersey Institute of Technology, summarize the reports they submitted to the Attorney General in which they conclude that although the majority of the systems satisfy most of the criteria, there were several serious security and privacy problems that must be addressed.

Cryptographer David Chaum, along with Aleks Essex, Richard Carback, Alan Sherman, Jeremy Clark, Stefan Popoveniuc, and Poorvi Vora describe an ingenious augmentation to optical scan voting systems in their article, "Scantegrity: End-to-End Voter-Verifiable Optical-Scan Voting." The system lets voters take home a receipt from the polling place that doesn't show anyone else how they voted (and thus doesn't promote vote buying or coercion), but does permit voters to verify after the election that their votes were correctly recorded, that they were included in the count, and that they were correctly tallied—none of which are possible with classical optical scan systems.

From the Basque Country (and MIT) comes a paper by Iñaki Goirizelaia, Maider Huarte, Juanjo Unzilla, and Ted Selker that proposes security and reliability modifications to their Demotek voting system. They apply classic *N*-version programming techniques to the system's authentication and data transmission portions. The *N* different versions are coded by *independent* teams, and their results voted at each stage, so that common errors or malicious collusion between programmers is detectable and correctable, and so cannot undermine the election.

These articles represent a snapshot of the state of the election art as of 2008. We anticipate more research in the future to more deeply understand the security and privacy issues behind the conduct of public elections. □

Aviel D. Rubin *is professor of computer science and technical director of the Information Security Institute at Johns Hopkins University. He also directs the National Science Foundation-funded ACCURATE Center (http://accurate-voting.org/). Prior to joining Johns Hopkins, Rubin was a research scientist at AT&T Labs. He is the recipient of the 2004 Electronic Frontiers Foundation Pioneer Award. Rubin has a PhD from the University of Michigan. Contact him at rubin@jhu.edu.*

David R. Jefferson *is a computer scientist and researcher at Lawrence Livermore National Laboratory. His research interests center on supercomputing, especially scalable parallel simulation. Jefferson has a PhD in computer science from Carnegie-Mellon University. He has been an advisor on election technology issues to the past five California Secretaries of State. Contact him at d_jefferson@yahoo.com.*