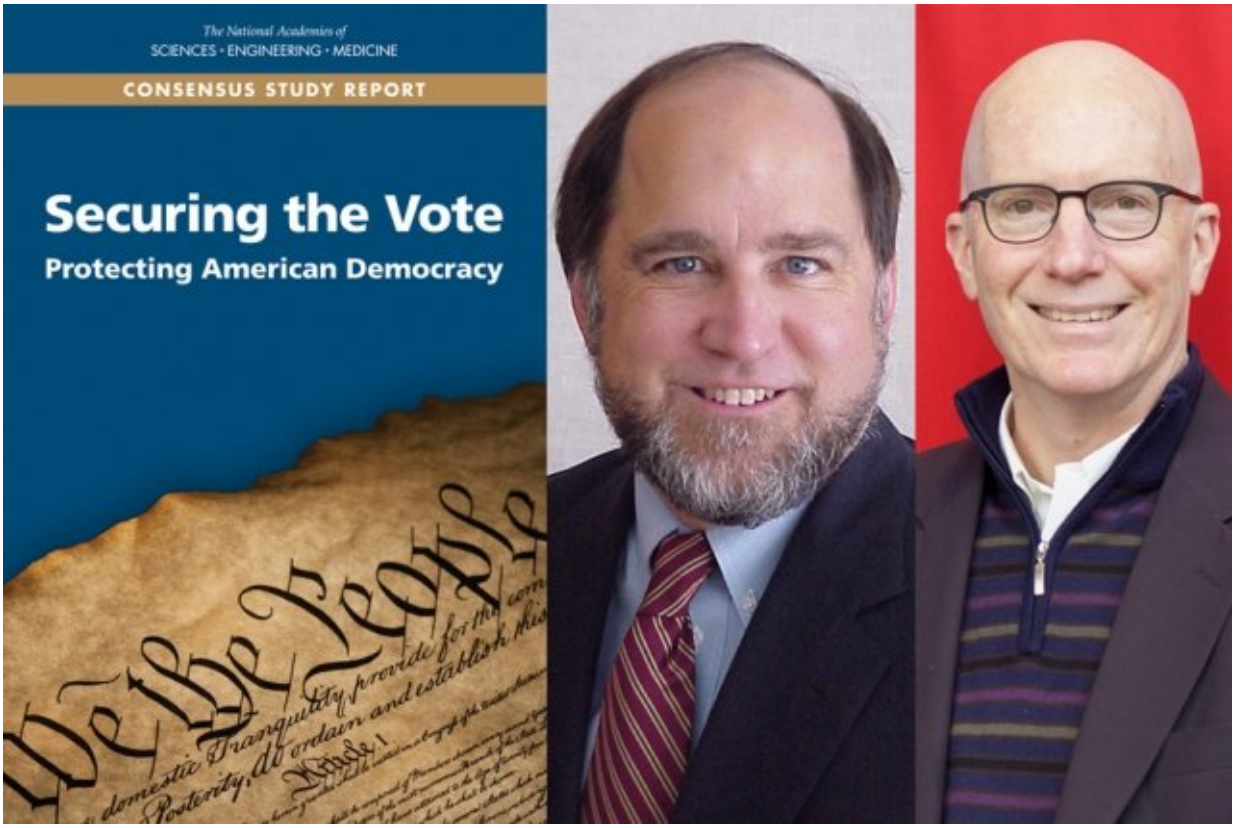
Report outlines keys to election security

September 25 2018, by Peter Dizikes



With the U.S. midterm elections approaching, a new report on keeping voting systems safe from hackers was co-authored by MIT professors Ronald L. Rivest (left) and Charles Stewart III. Credit: Charles Stewart and Ronald Rivest

The most secure form of voting technology remains the familiar, durable innovation known as paper, according to a report authored by a group of election experts, including two prominent scholars from MIT.

The report, issued by the National Academies of Science, Engineering, and Medicine, is a response to the emerging threat of hackers targeting computerized voting systems, and it comes as concerns continue to be aired over the security of the U.S. midterm elections of 2018.

The U.S. has a decentralized voting system, with roughly 9,000 political jurisdictions bearing some responsibility for administering elections. However, for all that variation, and while many questions are swirling around election security, the report identifies some main themes on the topic.

"There are two really important avenues that are emerging," says Charles Stewart, the Kenan Sahin Distinguished Professor of Political Science and founder of MIT's Election Data and Science Lab. "One is just securing the election, and the other is building in resilience and fail-safe mechanisms."

In this context, "securing the election" means keeping voting systems safe from hackers in the first place; fail-safe mechanisms include paper ballots that can be used for audits and recounts.

The other MIT co-author of the report is Ronald L. Rivest, a computer encryption pioneer and Institute Professor in the Department of Electrical Engineering and Computer Science. Given the distinct challenges of combining anonymity at the ballot box with verification of voting, Rivest notes, a paper trail remains a necessary component of secure voting systems.

"I think that the three most important recommendations of the report, at least from a security perspective, are probably: (a) use paper ballots, (b) check the reported election outcomes by performing 'risk-limiting audits' of the cast paper ballots, and (c) don't transmit cast votes over the internet," Rivest says.

The report, "Securing the Vote: Protecting American Democracy," was released this month by the National Academies. The co-chairs of the committee releasing the report are Lee C. Bollinger, president of Columbia University, and Michael A. McRobbie, president of Indiana University.

Rivest and Stewart are two of the 12 co-authors of the high-level report, which examines a range of voting issues and contains a series of recommendations. In addition to having a paper trail, the recommendations include securing and updating voter registration databases, robust checks on the security of voting by mail, Congressional funding for security standards developed by the National Institute of Standards and Technology and the U.S. Election Assistance Commission, and robust auditing of elections to make sure systems are working.

Stewart and Rivest both acknowledge that they are often asked why internet voting is not a reality, given that we conduct other kinds of sensitive activities online, including banking.

"Probably the most common question that I get when I talk to the public about these issues," Stewart says, "is, 'Why can't we vote on the internet?'"

Systems with the right combination of verification and anonymity are hard to develop, however, and as both scholars point out, other online activities such as banking are hardly foolproof. And while banks have systems to compensate customers should fraud occur, a one-time event like an election does not provide the same opportunities for remedies.

The good news, Stewart suggests, is that election officials themselves tend to have a keen awareness of the best practices in their field.

"From my experience I know that every state election official and just about every local election official that I've talked to is aware that cybersecurity is a top priority," Stewart says. However, he adds, election officials do not necessarily control the purse strings and often cannot fund the security measures they value: "Often times, election officials don't have control over their own destiny."

More information: Securing the Vote: Protecting American Democracy: www.nap.edu/read/25120/chapter/1

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology