

Voting AND verifiability

RSA co-founder **Ron Rivest** (he's the "R" in RSA) recently spoke with *Vantage* about one of his long-time passions: the development of trustworthy voting systems. Rivest is Viterbi Professor of Computer Science in MIT's Department of Electrical Engineering and Computer Science, a member of the school's Computer Science and Artificial Intelligence Laboratory (CSAIL), and a leader of the lab's Cryptography and Information Security Group.



VANTAGE: You've been working on voting issues for a number of years. When and how did you get involved?

RON RIVEST: Voting has been a part of cryptography research for quite a while, going back to the 1980s and the early days of public key cryptography. But it wasn't until the 2000 presidential election, which was so hotly contested, that the urgency of trying to do something better became apparent.

The presidents of MIT and CalTech—Chuck Vest and David Baltimore—created the Caltech/MIT Voting Technology Project, of which I was a charter member, and we began working on voting issues in a more serious way. I was also involved in founding the Workshop on Trustworthy Elections. Most recently, I worked on the 2009 election in Takoma Park, Maryland, where new principles of trustworthy voting were put into practice.

You've described the 2000 election as a "9.0 earthquake" that put a spotlight on shortcomings in the U.S. voting systems. What needed fixing?

It became clear that our election systems were working in the dark. There wasn't much attention being paid to voting procedures and equipment. In particular, the issue of verifiability—really knowing that you've got the right election outcome, reflecting the will of the people—emerged as a strong theme, both in the theoretical research community and among folks involved in the practical aspects of voting.

One of your slides is titled, "Voting is a hard problem." Why is that?

The problem of voting is challenging because the requirements seem contradictory or intractable. On the one hand you want to maintain voter privacy—that is to say, you don't want a voter, even voluntarily, to be able to prove to somebody else how they voted. On the other hand, you need to have auditability. You'd like voters to be able to confirm that their vote counted the way they wanted it to. And you want election officials to be able to ensure the integrity of voting results. And those requirements, when put together, make voting a unique problem that's different from banking or other applications.

Why shouldn't a voter be free to show someone else how they voted?

We've had a long history in this country of people selling their votes. To negate that, you have to make it difficult to sell your vote. For example, giving the voter a paper receipt that says "this is how I voted" doesn't work because that paper can then be sold as proof of how they voted. In a similar way, a receipt would also make people more vulnerable to coercion. Enforcing privacy is an important element of the voting process, although you may need certain exceptions for people with disabilities, military personnel serving overseas, and so on.

So you don't favor the recent trend toward divorcing the voting process from a particular time and polling place?

No. I'm not a proponent of voting by mail or over the Internet. There is a saying I made up that goes, "Best practices for Internet voting are like best practices for drunk driving." Many people strongly favor Internet voting, but I think they don't appreciate the privacy issue or the security situation. They see the benefits of increased convenience for voters, but the tradeoff for that increased convenience is such a dramatic loss of security that, in my opinion, it's just not prudent to go there.

Some proposals for Internet voting try to compensate for the loss of privacy by having special voting kiosks that are connected to the Internet. But you still have all the security issues with the Internet itself. If you have a denial-of-service attack mounted against a particular city or state on election day, you've got a real problem. Systems connected to the Internet become vulnerable to malicious attack: worms, viruses, botnets, and so forth. Partisans could block certain classes of voters from voting, either by location or some other attribute.

Since 2000, there has been a trend away from pure electronic systems and toward systems that combine paper ballots and optical

scanning. Is this progress?

Yes. There's been a realization that a voter-verified paper record is a big help in ensuring election integrity. For those people who always want to be at the bleeding edge of technological innovation, this seems like a step backwards, but it's a step forward.

What are the basic requirements for ensuring voting integrity?

I see them as being three-fold. First, you want to know that each individual's vote was cast as intended. The second step is knowing that the vote was collected properly and that the pile of votes you collected to be counted is the correct pile. That's a chain-of-custody issue. And the third step is doing the counting properly, making sure that the tally is accurate and complete. A new category of end-to-end voting systems addresses all three aspects of the challenge.

How do end-to-end systems improve verifiability?

There are many different proposals, but most include a private voting experience at a polling place, a cryptographic back end, and some kind of Web bulletin board or website where voters can verify that their vote was counted the way they wanted. The end-to-end principle is a good one, and I think it will be with us for a long time.

Has this been tried in an actual election?

Yes. The November 2009 Takoma Park election that I mentioned was historic because it was the first time that these principles had been tried out in a binding political election. The team that put it together included a dozen researchers, including myself, and Takoma Park election officials, who were wonderful to work with and very open to trying something new.

Takoma Park used the Scantegrity II system, which evolved from ideas put forward by David Chaum, who is a famous cryptographer. It starts off like a regular paper-based, optical scan system. The voter goes to a polling site, fills in the bubbles, and then casts the paper ballot, which is scanned immediately. That part of the process is enforced to be private. The part that is not private is when the voter goes home and checks that her vote was cast in the way she intended. There may be other people around then, but that interaction is done in an interesting way, using cryptographic methods, so the voter can't prove to someone else how they voted.

Is the Takoma Park election scheme repeatable?

That's a question the Scantegrity team is discussing. What are the next steps? Will there be similar, perhaps expanded, elections in the future? There is no Scantegrity company or product one can buy. It's a research prototype, somewhere between an academic study and a real product. If a vendor wanted to pick this up and start working with it, it is at a stage where they could go forward with it.

What are some other problems that stand in the way of efforts to improve voting systems?

It's difficult for startups and new ideas to move forward. One reason is that the market for voting systems is very fragmented while, at the same time, there is a lot of consolidation on the



Voting is complicated, and you can't go at it with a monomania. You really have to balance all the different considerations and make sure the right priorities are reflected.

vendor side. The Constitution gives each state the right to determine how voting should proceed in that state. And states often delegate the choices of voting equipment to the local jurisdictions. So many small sales are made. Some states have uniform voting systems, but that's the exception. More often it is town by town or county by county. That makes it harder to break into the market, improve standards, or put other changes into effect.

Another challenge is that the federal process for certifying voting equipment needs to be redesigned. A technical guidelines committee I served on is drafting new voting system regulations and there's vigorous debate and deliberation by academics, vendors, voters, and election officials about what the new standards should be.

Is there still the potential for an explosive situation like what happened in Florida?

Yes. There is still widespread use of voting systems where the election outcome can't be verified to the extent you'd like. If you have a very close election and you don't have paper records

you can go back and recount, you've got the potential for a flare-up of accusations, paranoia, and conspiracy theories. But many more states have moved to voter-verifiable paper records as a foundation for their voting systems. So we're moving in the right direction.

Paper ballots were used in the contested senatorial election in Minnesota between Al Franken and Norm Coleman. It would have been a disaster if there hadn't been paper records to recount. As it was, the recount took quite a bit of time, but it was a very civilized process, and the result, in the end, was accepted.

Are there other bright spots you've seen?

There are many very good people working to improve our voting systems. Occasionally someone gets on their high horse and says, "Everything's got to be done this way." But there's a much better spirit of dialogue and collaboration than there used to be. Voting is complicated, and you can't go at it with a monomania. You really have to balance all the different considerations and make sure the right priorities are reflected. ■