The Promise of Cryptographic Voting Protocols

Chris Karlof Naveen Sastry David Wagner
{ckarlof, nks, daw}@cs.berkeley.edu

June 6, 2005

Electronic voting has a credibility gap: many experts have sharply criticized current paperless systems, and this has led many advocates to call for voting systems to provide a paper trail retained by election officials. Meanwhile, two vendors have sprung up to propose an alternative solution that uses cryptography and sophisticated mathematics to give voters a receipt of their vote they can take home. Are these cryptographic schemes secure? Do they fix the integrity problems with today's paperless e-voting systems? We undertook a detailed investigation to find out. Based on our research, we have the opinion that cryptographic voting schemes hold great promise in the long run—but there is much work to do before they will be ready for prime time.

These new schemes are truly innovative. They offer an exciting property not available in any prior DRE system: voters can verify that their vote has been recorded and counted accurately, without endangering ballot secrecy or permitting voter coercion. At the same time, though, they use some of the most advanced cryptographic ideas around and must be carefully validated by independent experts before being deployed.

After the results of our study, we are not yet ready to endorse either of these systems for immediate use. A crucial component of any security analysis is having an entire, complete system to examine. Although Neff and Chaum present fully specified cryptographic protocols, many implementation details—such as human interfaces, systems design, and election procedures—are not available for analysis. We found several ways in which their schemes might be at risk, depending upon details of their systems that have not yet been disclosed. These weaknesses could potentially compromise election integrity, erode voter privacy, and enable vote coercion. Without a complete specification and implementation, we cannot gauge the severity of these potential weaknesses. However, we expect that a well designed implementation and deployment may be able to mitigate or even eliminate the impact of these weaknesses.

Despite these uncertainties, we remain optimistic about the long-term potential of cryptographic voting schemes. To help these schemes reach their potential, we have several recommendations:

- **Security certification:** Cryptographic voting systems are based on radically different principles than prior systems. Unfortunately, today's certification process is poorly suited to ensure that these new systems are trustworthy. A new framework is needed. We call for states to convene a panel of independent experts to perform a security evaluation of these schemes before they are certified or used in the large. Such a panel should include cryptographers, computer security specialists, election officials, human computer interaction specialists, and voting specialists. The panel should evaluate, among other things, whether the system provides appropriate levels of security, integrity, privacy, and transparency.

  The evaluation should be structured as a verification project, not a bug-finding effort. Evaluators should attempt to ascertain whether there is convincing evidence that the voting system will meet the panel's requirements. The system should only be deployed if this panel concludes the voting system is trustworthy.

- **Usability evaluation:** In addition to gauging the trustworthiness of the voting system with the security evaluation, experts must also assess voters' comfort with these voting systems. The public should not feel that a voting system is confusing or too difficult to use correctly. As part of this evaluation, human computer interaction specialists ought to perform a usability analysis for each voting system.

  We expect small scale trials to help with this evaluation. Afterwards, voters should be surveyed in order to evaluate their usability experience with the system. We caution, however, that a successful trial says little or nothing about the security or trustworthiness of the system, because any serious adversary would mostly likely wait to attack the real thing, rather than disrupting a trial.

- **Recoverability:** Although these schemes can detect many attacks on the voting system, recovery may be difficult in some cases. There are several ways that an adversary could disrupt the election in ways that are eventually detectable but irrecoverable. If this disruption was targeted in a way that disproportionately affects one party or candidate more than its opposition, this might call the results of the election into question.

  One way to ensure that we can recover from election failures is to use a voter verified paper audit trail (VVPAT) in conjunction with these schemes. A VVPAT system produces a paper record verified by the voter before her electronic ballot is cast. This paper record is cast into a ballot box, retained by election officials, and used primarily for recounts and auditing. This would make it possible to recount precincts, counties, or entire states if election fraud is discovered. A VVPAT would also provide an independent way to audit that the cryptography is correctly functioning and thus might enhance confidence, particularly among those who lack the mathematical training to understand these schemes.

- **Transparency:** Independent evaluation is essential if these schemes are to receive the public's confidence. We urge that all of the software, source code, documentation, manuals, training documents, and election procedures for any voting system be publicly disclosed in full, so that independent experts can evaluate the trustworthiness of these systems. This is particularly important for cryptographic voting schemes, as the history of cryptography shows that schemes shrouded in secrecy have a high rate of failure. To their credit, VoteHere has released source code for part of their system. Sadly, many other vendors have so far resisted calls for public disclosure.

We laud Neff's and Chaum's ambitious goal: developing a coercion free, privacy preserving voter-verifiable election system. Their systems represent a significant security improvement over current DRE-based paperless systems. Most notably, these schemes seek to give voters a way to know that their vote has been cast and counted correctly, since the receipt allows the voter to detect fraud and other failures. Although these cryptographic systems are not ready for deployment in the short term, we believe further investigation of cryptographic voting protocols has the potential to lead to significant improvements in election security.