End to End Cryptographic Internet Voting Considered Harmful

Position Paper

Jeremy Epstein
SRI International

End to end cryptographic-based Internet voting systems are good science but bad public policy, and their use should be discouraged. In this white paper I'll explain why. By "cryptographic Internet voting systems" I mean any system where cryptographic methods are used to allow voters to cast their votes from their home computers in such a way that they can verify after the fact that their votes were counted, but cannot demonstrate how they voted.

First, the essence of a voting system is transparency: ordinary voters should be able to understand and observe the vote casting and counting process, even with relatively nominal education. This premise is important even if almost no one chooses to take advantage of this opportunity, and is frequently enshrined in state law and policy through requirements such as posting precinct totals on the door of the polling place, allowing representatives of political parties to observe the counting process, and making the pre-election testing of voting machines open to the public.

End-to-end cryptographic Internet voting systems have none of these characteristics. While voters may be able to understand how to cast a vote using a cryptographic system, and perhaps are capable of checking their cryptographic receipt after the election, for all but the most technically sophisticated voters the process is simply magic. They cannot in any sense understand how a cryptographic operation (such as, but not limited to three part ballots) provide the anonymity and auditability necessary for an election. They cannot observe that ballots containing marks or holes are counted by machine or by people; they cannot observe the recount process in a meaningful way; they cannot understand how individual privacy is safeguarded. They simply have to rely on scientists' assurances that the mathematical proofs show that the votes have been counted correctly – from the perspective of a non-expert, this requires the same level of trust in magic as trusting that the vendors of a DRE system have built software that counts votes correctly.

Second, the concept of an Internet-based system is built on a foundation of quicksand, regardless of whether that system is cryptographically based or "traditionally" based (i.e., a web site that stores data in a database that uses cryptography for protecting data from tampering, but does not rely on homomorphic encryption or other cryptographic techniques for privacy). The cryptographic system cannot address the likely case where malicious code is modifying the voter's votes by manipulating the software that creates the voting data. Even displaying the vote data to the voter before it is cast doesn't help – malicious software can easily wait until the final vote is approved by the voter before making a change. This technique is well understood by developers of malicious software, who will silently conduct financial transactions against a victim's account, despite showing "normal" results.

Third, and perhaps most importantly, such systems are incomprehensible by the people responsible for decision making in voting system acquisition, namely legislators, state Boards of Election, and local Boards of Election. Regarding legislators, in many states the law specifically identifies types of voting systems that may be used and under what circumstances. To change this law to allow “safe” Internet voting schemes without allowing unsafe schemes requires extremely precise crafting of language which is well beyond the understanding of legislators and their aides, many of whom work only part-time in their legislative role[i]. State Boards of Election are usually the best equipped to understand technology issues and make recommendations to the legislature, but they rarely have technical staff with the level of expertise that would be necessary to understand a cryptographic voting system. In some cases they hire outside technical experts, but this is rare. And local boards of election, who in many states are responsible for procurement of voting equipment, generally have little or no technical expertise. As a result, if cryptographic voting is legalized, legitimate cryptographic voting systems are likely to be crowded out by systems that have few if any of the same safety and auditability properties (even if not well understood by the populace) in favor of systems with better user interfaces, more persuasive sales forces, etc.

Research on cryptographic voting systems for end-to-end secure voting should continue, but it should not be used in real elections until techniques are developed that can be understood by voters, election officials, and legislators with ordinary educational backgrounds, and system-minded analysts can gain some reasonable assurance that the embedding for the cryptography into real systems is nonsubvertible.

This paper was prepared with support from ACCURATE: A Center for Correct, Usable, Reliable, Auditable and Transparent Elections, under National Science Foundation Grant Number 0524111.

[i] For example, in Virginia, the legislative session is 60 days in even numbered years and 30 days in odd numbered years, and virtually all legislators have other jobs the rest of the year (legislative pay is about $18,000/year). Legislative aides similarly work only part time, and legislators typically only have one or two aides who cover the complete range of legislation.