Bringing order to the EVM debate

Subhashis Banerjee Subodh Sharma

Computer Science and Engineering
(also associated with the School of Public Policy)

IIT Delhi

February 22, 2019

Whether or not to use EVMs (electronic voting machines) for elections in India has been a raging debate of late, often bordering on the theatre of the absurd. There have been claims of hacking of EVMs and counter-claims of impossibility, steadfast assurances about their safety from election commissioners and technocrats, open challenges though ECI (Election Commission of India) sponsored 'hackathons', and even live television shows by masked hackers alleging murder conspiracies!

Public arguments on computer security in India have often been outrageous. On the one hand there have been fatalistic claims that all computer systems can be hacked and that it is just a matter of time before they will be. There indeed are computer systems that are provably secure, but sometimes such guarantees are difficult even for many well-designed ones. The question of whether they can be hacked or not is often 'undecidable', even in a technical sense, and is hence futile.

On the other hand, the fact that a system has not yet been hacked have sometimes been claimed as a proof of its infallibility, and public dares and open challenges have been thrown dramatically. That a system has not been hacked provides no guarantee that it cannot be. Ultimately the onus of establishing trust, either formally through verifiable proofs, or even informally using best practices and due-diligence, must always lie with the designers.

It is difficult to appreciate how difficult the EVM design problem is till one considers the generic requirements outlined below.

Correctness demands that all votes are accurately counted and there are no false or duplicate votes.

Secrecy demands that it should be impossible to determine who an individual voted for, provided the voting is not completely lopsided for any candidate or for any social or political groups. **Anonymity** - indistinguishability from a specified number of other voters - follows from secrecy. Note that secrecy and anonymity are necessary conditions for **coercion-free** voting, though the converse is not true. Sufficient conditions for coercion-free voting will require methods and processes beyond an EVM.

Verifiability demands that it should be possible to prove to every voter individually that their vote has been accounted for correctly in the aggregate without revealing, or even determining, the vote. Verifiability also implies **non-repudiability**, i.e., if a voter falsely claims to have voted differently from what she actually did, it should be possible to prove that the claim is false without determining who she voted for. Note that whereas verifiability requires that the EVM must record both the vote and some function of the identity of the voter, secrecy requires that the EVM should not allow the inference of the mapping between the two.

Identity verification must be certified by the polling officer and can either be offline or online, and must have its own guarantees.

Reliability has three main requirements. **Un-hackability** demands that the EVM should be tamper-proof, through any direct or even side-channel attacks. **Fault tolerance** demands that the system should be resilient to network and component failures. In particular, there should never be any data loss. **Consistency** demands that the design and implementation of all EVMs must be identical, and provably so at all stages of the election.

Finally, **auditability** and **self-certifiability** demand that it should be possible to verify the above invariant conditions at all stages of voting, including before the start, at any time during voting, and after the voting finally ends. The events of start and end of polling must be recorded and signed with the digital credentials of the polling officers. Moreover, the EVM machine should be able to self-certify and provide proofs of all the above invariants at any stage.

Some of the above may appear to be dependent or even contradictory at the first glance, but careful reflection should convince the reader that they are, in fact, not.

Designing a provably correct EVM satisfying all the above properties is an as yet unsolved problem of computer science. Rebecca Mercuri, a computer scientist and the original proponent of a VVPAT based design, claimed that the verification of a design for an EVM such as above will be an intractable problem. It may well be so, though that does not suggest that rigorous verification of suitable design abstractions cannot be worked out.

The crucial question, then, is to precisely evaluate to what extent does the ECI's EVM satisfy the above properties and how does it compare with manual paper based ballot? For example, merely tallying the EVM count with manual VVPAT count, without guaranteeing that there is no spurious voting, does not establish correctness, even with statistical sampling. VVPATs, or even secure strongrooms, do not guarantee against pre-designed adversarial, side-channel or Trojan attacks.

This is not to say that the ECI's EVM is necessarily a worse option than manual ballot which does not even guarantee correctness and, at best, only approximately satisfies secrecy, anonymity and fault-tolerance. Manual ballot, however, has the advantage of not taking away agency from the poll officials, whose understanding of the process enables them to improvise on the spot to try and ensure correctness. In contrast, the obscurity of an EVM makes its correctness analysis absolutely crucial.

Public posturing by the ECI, based on pronouncements by a hand-picked set of experts, does not engender confidence. For informed risk assessment it is imperative that the complete design, analysis and the hardware synthesis specifications be made public at the earliest so that the EVM may be subjected to rigorous scrutiny by the general public, institutions, political parties, their representatives and even experts. After all, security by obfuscation belongs to the time of Julius Caesar and is unacceptable in the modern technological age.