Electronic Voting Machines as instruments for democracy[i]

Contents

Overview of the issues

Electronic Voting Machines (EVMs) are the magic machines that convert candidates into representatives. This magic depends on the number of votes that are counted on the EVM as having been cast in favor of a candidate. Much of the candidates and the people accepting the EVM count as a representation of the people's mandate depends on their trust in the EVMs. This trust is currently based on the *Voting Test* conducted before polling starts.

However, neither the EVMs nor the VVPATs pass the *Auditability Test*. The Auditability Test requires the EVM to allow the voter to verify *their* vote has not only been captured but counted for their candidate and allow each candidate to verify that all the votes counted were from genuine voters and not the machine. No EVM currently passes this test.

Do EVMs capture the voters intent?

The trust in Electronic Voting Machine's (EVM) ability to capture votes and count them correctly comes from the conviction that the Polling Agents of various political parties participate in a mock poll conducted by the Presiding Officer in each voting booth. The mock poll is meant to demonstrate the tally of votes cast in favor of the candidates by each polling agent is reflected correctly on counting. This *Voting Test*, in other words, declares a machine to be capable of capturing votes correctly if it is impossible to distinguish the results declared by manually counting the votes recorded on paper from those counted by the machine.

The Voting Test is eerily similar to the test of machine intelligence devised by Alan Turing, the founding father of Computer Science. According to the Turing Test a machine will be declared intelligent if an interrogator cannot distinguish between responses of a machine and a human who are challenged with similar questions[ii].

John Searle, Professor Emeritus of Philosophy at the University of California Berkeley, challenged the Turing Test[iii] asserting that imitating instructions is not a sufficient condition to conclude machines are intelligent or they can think. He required the ability to establish *meaning* on part of the one challenged with questions to declare that they could think. Searle devised a test called Chinese Room Test to demonstrate the ability of a machine to respond to questions in Chinese based on a script and rules to illustrate that the machine still had no means to establish the meaning of the questions or answers.

Searle undisputedly demonstrated that the inability to distinguish responses of a machine from a human was insufficient to establish intelligence.

What would undisputedly establish the ability of a machine to capture votes and count them correctly?

The meaning of a vote lies in it being cast by a real voter and being counted for the candidate it was intended for. The meaning of a vote would be altered by allowing it to be cast by a non existent voter or counting it as a vote for an unintended candidate. To demonstrate that an EVM captures votes and counts them correctly it will have to allow the voter to verify their vote has not only been captured but counted for their candidate even after it is cast. It will have to verify to the candidate and the voters that the votes polled by a candidate were all cast by real and legitimate voters and were all meant for the candidate.

Currently *no* EVM can establish the meaning in votes is unaltered and that every vote cast is genuine and counted in favor of the candidate it was meant for.

Joseph Weizenbaum, Professor at MIT and one of the fathers of modern Artificial Intelligence, created ELIZA[iv], an early natural language processing computer program, to demonstrate the superficiality of communication between humans and machines. The response of the ELIZA to human interaction varied to the same questions giving the appearance of being human. Weizenbaum established how a simple set of instructions can allow the machine to respond differently to the same questions.

Without auditing the code of a computer program it's foolhardy to assert the behavior of a computer program. The program embedded in the chips of the EVM is not in public domain. It is therefore impossible for anyone to inspect it and certify its behaviour. There is no third-party audit of the program supplied for embedding into the chips and one embedded into the chips. Unsurprisingly there is a petition seeking an audit of the source code pending before the Supreme Court. To complicate matters even more, this program is embedded into the chips by vendors outside India[v] and the Electronics Corporation of India (ECIL) and Bharat Electronics Limited (BEL) only assemble the EVM. In a meeting I had in August 2009 with the then Chairman of the Technical Committee of the Election Commission of India and the then Election Commissioners confirmed that they have not even used a checksum or any other mechanism besides the Voting Test to verify that the EVM is running the program supplied by them.

In 2009 I had reported to the Election Commission of India the presence of coded results of the entire Lok Sabha elections on their website a good 10 days before voting was over[vi]. This led Dr. Subramaniam Swamy to petition the courts for EVMs that had Voter Verified Paper Trail (VVPAT). Hundreds of candidates across India have cried foul over EVMs when they appear to have favored their opponents. Even the political parties, have not demonstrated trust when they have suffered and forgotten the unfairness once in power. Behind closed doors, they are familiar with the technical details of hacking EVMs in a block where their opponents have more support. It is little surprise, therefore, that a 2011 Report of the National Institute of Standards and Technology found that voter-marked paper ballots are the only way to securely record and preserve voter intent[vii].

By now it should be obvious that like any machine subjected to the Turing or Searle test, an EVM subject to the Voting Test can be programmed to work differently at different times, either triggered by a stimulus, internal programming, or simply by randomness. The machine passing the Voting Test is no evidence of its inability to generate votes on its own or to not count votes in favor of one candidate over votes for another.

Do VVPATs capture the voters vote better?

Consider the likelihood that you will deposit money in a machine that is demonstrated to accept money to a particular bank account in a test but does not issue any receipt of the transaction or has no possibility of an audit to verify that the deposits not only went to the correct account but also did not get altered. Why should you do differently with your vote that is a blank cheque to not just your tax money but also to your rights?

EVMs do not provide voters with a receipt of the vote they cast. It is a huge leap of faith that the machine not only allocated the vote to the candidate intended by the voter but also allowed the same vote to be counted for the same candidate. Given the stakes, electoral malpractices are rampant. The Election

Commission has not simplified voting, it has made the simple process of making a choice extremely complex, drawing attention away from the ability of the vote to be counted, to the paraphernalia of elections. This is almost like the magician or thief who distract attention from what they are really doing in order to perform magic and trickery.

Instead of providing a receipt to the voter, Dr. Subramaniam Swamy's petition to the courts resulted in EVMs that were called EVMs with VVPAT. The VVPAT was introduced to create an audit trail of votes cast on an EVM. VVPAT is an "audit trail" that assumes each voter verified the vote printed by the VVPAT EVM. Voters have no means to confirm verification of the printout shown to them. The printout is merely a paper vote, it is NOT a voter *verified* vote. The voter has no ability to endorse their verification on the printout shown to them. They have no recourse to cancel or object to an incorrect printout without facing disproportionate penalties and no means to demonstrate the stealing of votes. The term VVPAT is therefore incorrect. There is no means to establish that voter verification happened.

The printout of the VVPAT does not have any means of authenticating itself as a voter verified or genuine vote. It is quite possible that the counted printouts from VVPAT may not be the ones printed during the voting. The printouts can neither establish that they were cast by legitimate voters nor that they were cast for the candidate they indicate. The printouts from the VVPAT are not counted by any third-party auditor. The same entity that has counted the votes on the control unit counts the VVPAT. This is bad auditing practice.

If the print outs were voter *verified* votes, they could be counted to verify the votes counted from the control units of EVM. The control units of EVMs would deem to have counted correctly if the VVPAT votes match.

The Election Commission agreed to count only votes from a small percentage of selected polling booths (each booth has an EVM). To confirm that the votes counted across EVMs by the control unit is the same as those counted by the VVPAT the votes polled for each candidate on the control unit and in the paper trail should not be statistically different.

A good deal about choosing the number of EVMs to count depends on the variability expected between the EVMs. Each EVM or booth has demographically high variation or could be homogeneous. For example, because of their demographic makeup, some polling booths could be expected to be favoring one candidate over another. In case of high variability, larger number of booths will need to be compared for VVPAT and control unit counts. There were an average of 1,708 EVMs in every Parliamentary Constituency in 2014. While each EVM could store 3,840 votes, an average of 904 voters assigned to cast votes on every EVM during the 2014 elections. This means a greater variability has been introduced between booths than necessary. Typically for constituencies that have 1,708 EVMs and high variability in booth voting, a choice of less than 200 booth VVPAT for counting would be poor to certify that the control units have counted identically as the control units.

While there has been debate on how many comparisons will establish confidence that the choice of EVMs selected to confirm the match between the control unit and the paper trail was not biased or just a fortuios one, the fundamental question about passing the Auditability Test remains to be asked.

That said, VVPAT itself does not satisfy the Auditability Test.

The global echo

Hacking elections to steal them is unfortunately widespread across the world. The use of electronics has made it easier, not more difficult, to hack into elections as such hacks are difficult to detect. The 2006 Robin Williams stared *Man of the Year* is the story of the American Presidential Elections being fixed by EVMs.

In March 2017 Wikileaks disclosed that "the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive. The malware includes "software that enables hackers to remotely control a compromised device — are "very, very complex""[viii]. The malware also includes code that can be implanted on devices not connected to the Internet by using thumb drives or other devices.

It is also widely known that chip makers build backdoors[ix] for future exploitation of hardware. Unfortunately, there is no way of guaranteeing that chips haven't been tampered with. Experts note that as few as 1,000 transistors in a chip could cause them to do a lot of "very interesting" things with those extra transistors, if the rouge transistors, or transistors not part of the original design, are programmed to respond to a specific 512-bit sequence of numbers, you might have to cycle through every possible numerical combination of 512-bit sequences to discover the code using software testing. Surveillance cameras[x] across the world have been recognized as easy targets for hackers[xi]. These can also work in tandem with other devices in their proximity to regulate rogue chips. Security experts say maintenance, repair businesses, and subcontractors may also pose a greater danger to hacking hardware[xii]. Even missile systems have been hacked remotely due to such vulnerabilities[xiii].

"Even if most voting machines aren't connected to the Internet, says cybersecurity expert Jeremy Epstein[xiv], "they are connected to something that's connected to something that's connected to the Internet". Adds Alex Halderman, a computer scientist at the University of Michigan, "Before every election, the voting machines have to be programmed with the design of the ballots — what are the races, who are the candidates"[xv]. The programming is usually done on a computer in a central election office or by an outside vendor.

The multiple ways electronics undermines peoples voices in elections is evidenced in the recent US Presidential election. According to FBI investigations, Russia allegedly took advantage of the many online vulnerabilities in America's voting network to control the 2016 Presidential election in the United States[xvi]. The voting network that was allegedly compromised includes software companies, online registration sites, and vital information that election officials willingly send to each other over email. The hack reportedly affected 39 states, twice as many as were originally reported. According to the Central Intelligence Agency, the Federal Bureau of Investigation and the National Security Agency they had evidence of Russian efforts to undermine confidence in the US electoral system and affect the outcome of the US Presidential elections[xvii].

Elizabeth Warren told CNN that the 2016 Democratic Primary was rigged[xviii]. Interestingly an analysis of US Democratic Party Primaries with or without paper trails shows a voter preference to Bernie Sanders over Hilary Clinton wherever paper trail was used casting a shadow on the lack of transparency of electronic voting[xix]. According to the Electronic Privacy Information Centre "investigations undertaken by private security firms, apart from the FBI, indicate that the attacks on the 2016 U.S. Presidential election also threaten democratic institutions in other countries"[xx].

Channel 4 secretly filmed Managing Director of Cambridge Analytica's political division, Mark Turnbull and chief executive Alexander Nix boasting about tampering with over 200 elections around the world, in places like Sri Lanka, Nigeria, India and Argentina[xxi].

The future of trusting the vote in the machine is dull, dark and gloomy. The Election Commission of India has demonstrated naiveté if not ignorance in asserting that electronics makes the elections unhackable[xxii].

The need for the Auditability Test

There is no certainty about the votes that are counted on EVMs unless the EVM passes the Auditability Test. The Audibility Test will need the EVM to allow the voter to verify their vote has not only been captured but counted for their candidate even after it cast. It will have to allow the voter or candidate to verify that the votes polled by a candidate were all cast by real and legitimate voters and were all meant for the candidate. This will necessitate providing voters either a receipt or a vote "account", like a bank account, whose "balance" they can verify. Voters will need a receipt or a passbook entry that their vote has been deposited to the account of the candidate. They will need the ability to verify, anytime, that the ECI records still have the same entry as in their passbook. If such passbooks are created, they will even be have the ability to move their vote to any other candidate any time, not merely after 5 years.

This will also require the ability to audit the votes deposited in each candidate's account and verify them as having been generated by a genuine voter, and not spontaneously by the program itself, and having been meant for the candidate.

Only then will the people be sovereign in the democratic republic of India.

---

[i] Deposition submitted by Dr. Anupam Saraph to the Citizen Commission on Elections chaired by Justice (retd.) Madan Lokur. Dr. Saraph sits on the board of Moneylife Foundation, is Adjunct Professor of Governance and Sustainable Development of Complex Systems at the Symbiosis Institute for Computer Studies and Research and a former Advisor to various local state and national governments on governance and IT. He has been researching electoral fraud from 2009 and deposed before the Election Commission and the Law Commission.

[ii] Turing Alan, Mind, Volume LIX, Issue 236, 1 October 1950, Pages 433–460, https://doi.org/10.1093/mind/LIX.236.433

[iii] Searle, John. R. 1980. Minds, brains, and programs. Behavioral and Brain Sciences 3 (3): 417-457

[iv] Joseph Weizenbaum. 1966. ELIZA—a computer program for the study of natural language communication between man and machine. Commun. ACM 9, 1 (January 1966), 36-45. DOI=http://dx.doi.org/10.1145/365153.365168

[v] http://eci.nic.in/eci_main1/current/FAQ-English14012017.pdf

[vi] https://www.huffingtonpost.com/cleo-paskal/how-secure-are-indias-ele_b_5317788.html

[vii] https://www.elections.virginia.gov/Files/Media/Agendas/2017/20170908BWP.pdf

[viii] https://wikileaks.org/ciav7p1/?

[ix] https://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch

[x] https://www.wsj.com/article_email/surveillance-cameras-made-by-china-are-hanging-all-over-the-u-s-1510513949-lMyQjAxMTA3MzE4NDMxMzQ2Wj/

[xi] https://www.wsj.com/article_email/surveillance-cameras-made-by-china-are-hanging-all-over-the-u-s-1510513949-lMyQjAxMTA3MzE4NDMxMzQ2Wj/

[xii] https://www.popularmechanics.com/technology/gadgets/a2686/4253628/

[xiii] http://www.newsweek.com/german-missile-hackgerman-missilespatriot-missilesturkish-syrian-602566

[xiv] https://www.npr.org/2017/06/14/532824432/if-voting-machines-were-hacked-would-anyone-know

[xv] https://www.npr.org/2017/06/14/532824432/if-voting-machines-were-hacked-would-anyone-know

[xvi] https://www.vox.com/world/2017/6/13/15791744/russia-election-39-states-hack-putin-trump-sessions

[xvii] https://www.independent.co.uk/news/world/americas/russia-election-hacking-us-investigations-everything-we-know-interference-donald-trump-hillary-a7742426.html

[xviii] https://www.bbc.com/news/world-us-canada-41850798

[xix] https://drive.google.com/file/d/0B6mLpCEIGEYGYl9RZWFRcmpsZk0/view?pref=2&pli=1

[xx] https://epic.org/foia/fbi/russian-hacking/

[xxi] http://www.okayafrica.com/wed-stage-the-whole-thing-cambridge-analytica-executive-on-rigging-kenyan-elections/

[xxii] http://eci.nic.in/eci_main1/current/FAQ-English14012017.pdf