

Can Electronic Voting Machines subvert elections?

Can Electronic Voting Machines subvert elections?

By Rajeev Srinivasan¹

“The right of voting for representatives is the primary right by which all other rights are protected. To take away this right is to reduce a man to slavery.” – Thomas Paine, *Dissertation on First Principles of Government*, 1795

“Those who cast the votes decide nothing, those who count the votes decide everything” – Joseph Stalin

“The first stage of fascism should more appropriately be called Corporatism because it is a merge of State and corporate power” – Benito Mussolini

1. Abstract

Are India’s election results an accurate reflection of the will of the people? Or is it possible that the Electronic Voting Machines (EVM) that are deployed in large numbers in India’s elections can be manipulated to subvert the voters’ intent? If that is the case, it would be a serious matter, because that would reduce India’s democracy, of which most Indians are so proud, to a charade. In this essay, we consider the ways in which EVMs could have been used to defraud the Indian voter in 2009. We emphasize that this essay is only about the **possibility** of fraud; it is beyond the scope of this note and will take further analysis and research to demonstrate actual fraud, if such existed.

2. Introduction

A number of elections around the world have been condemned for various levels of fraud, misdemeanor and felony over the years. Undoubtedly, some of the criticism is well-deserved (for instance, the routine instances of 100% voter turnout in certain totalitarian countries). In some cases, it appears elections were “stolen” through manipulation of the vote tally, thus, in effect, perverting the “will of the people”, that cornerstone of a genuine democratic, republican regime.

Although some of the most egregious examples have been in developing countries, for instance Zimbabwe in 2008ⁱ and Mexico in 2006ⁱⁱ, the one that has got the most attention was the US Presidential election in 2004, and there is a websiteⁱⁱⁱ devoted to the idea that John Kerry was defeated by George W Bush through explicit and subtle fraud^{iv}. It is also widely believed that Al Gore was defeated in 2000 through manipulation and fraud. It is ironic that the Americans, who lecture everyone else about free and fair elections, should have – if the critics are right – suffered some of the worst outrages against democracy. Intriguingly, this has made them more, not less, allergic to EVMs.

¹ Rajeev Srinivasan is a management consultant in strategy, innovation and energy. He has spent over twenty years in the computer industry, mostly in the Silicon Valley, in engineering and management roles. His columns appear in *rediff.com*, *The Pioneer*, *The New Indian Express* and *Mint*. He also teaches periodically at various IIMs.

Can Electronic Voting Machines subvert elections?

Let us now fast forward to 2009. The recent elections in Iran, which allowed President Mahmoud Ahmedinejad to retain power, have been roundly condemned by the western media^v as fraudulent, although they have not explained how the alleged fraud was committed: it is not known if it involved EVM fraud. Most of the criticism is based on two factors: a) the extraordinary margin of victory (two-thirds majority, when all the opinion polls had predicted a tight race), and b) the massive public protests.

While the western media's desire for democracy is admirable, their moral indignation would probably have been far more muted if their preferred candidate, Mir-Hossein Moussavi, had won. Iranians with long memories remember the CIA-engineered coup that overthrew the legitimately-elected Mohammed Mossadeq in 1953 in order to control Iran's oil.

The allegations in the western media that there was 'fraud' in the Iranian elections^{vi, vii} are based on circumstantial evidence – that "it was a landslide", and "opposition polls suggested that he [Mr. Moussavi], not Mr. Ahmedinejad, was the one with the commanding lead."

This is in interesting contrast with India's April-May 2009 general election. The entire spectrum of local media had projected a tight race, and given the UPA a narrow lead. But in the event the UPA was declared a landslide winner; this discrepancy was not commented upon with the same fervor by the western media. This leads to the conclusion that their preferred candidate won, and therefore the military-industrial-media complex in the west saw no reason to complain.

Remarkably, however, a UPA minister, Glubam Nabi Azad, Congress general secretary in charge of Orissa, has alleged that there was voting machine fraud in that state.^{viii} This raises the question: if Orissa suffered, why would the rest of the country not have been subject to fraud as well?

Circumstantial evidence suggests that there might have been a limited number of constituencies in which fraud was perpetrated. For instance, some MPs had victories that were practically miraculous: exit polls suggested they would lose, they were trailing badly during the counting, but there was a last-minute reprieve for them. In other cases, areas that were strongholds for one party mysteriously chose the other side. In some other cases, the losing parties could not account for the erosion of their committed support, wherein tens of thousands of their loyal votes apparently failed to materialize. Admittedly, none of this is proof of actual EVM fraud, however, unless further research demonstrates it.

Regrettably, the history of voting machines has been checkered at best. The fundamental problem is twofold: one, that there is no easy way of formally verifying and certifying them, and two, that there are increasingly resourceful hackers who can circumvent any simple-minded security schemes implemented by election officials. It is suicidal to repose an absurd amount of trust in them, as seems to be the norm in India.

3. EVMs around the world

There is a veritable tsunami of negative reports about Electronic Voting Machines from all over the world. There is no country in which EVMs have been welcomed so enthusiastically as they have been in India, and perhaps this is with good reason. Hardly any major developed country uses EVMs to any extent: indeed, despite the fuss over “hanging chads” and other arcana in their 2000 elections, even Americans who are partial to technological solutions have resisted the siren-song of voting machines after due consideration.

Here is a sample of the concerns raised about EVMs from a variety of perspectives:

- United States (data from www.electionfraud2004.org and others as indicated):
 - In April 2004, California banned 14,000 EVMs because the manufacturer (Diebold Election Systems) had installed uncertified software that had never been tested, and then lied to state officials about the machines. The machines were decertified and criminal prosecution initiated against the manufacturer.^{ix}
 - In the 2004 Presidential elections, in Gahanna, Ohio, where only 638 votes were cast, Bush received 4,258 votes to Kerry’s 260
 - A study by UC Berkeley’s Quantitative Methods Research Team reported that irregularities associated with EVMs may have awarded 130,000 – 260,000 votes to Bush in Florida in 2004
 - There have at least the following bills in the US legislature, all of which were the result of perceived problems with EVMs. (It is not known if any of them has passed; HR = House of Representatives, the lower house, and S = Senate, the upper house):
 - HR 550: Voter Confidence and Increased Accessibility Act of 2005
 - HR 774 and S 330: Voting Integrity and Verification Act of 2005
 - HR 939 and S 450: Count Every Vote Act of 2005
 - HR 533 and S 17: Voting Opportunity and Technology Enhancement Rights Act of 2005
 - HR 278: Know your Vote Counts Act of 2005
 - HR 5036: Emergency Assistance for Secure Elections Act of 2008
 - In 2006, a team of Princeton University computer scientists studied Diebold Election Systems EVMs, and concluded that it was insecure and could be “installed with vote-stealing software in under a minute”, and that the machines could transmit viruses from one to another during normal pre- and post-election activity^x. Diebold, now Premier Election Systems, is the largest US manufacturer of EVMs
 - In 2006, computer scientists^{xi} from Stanford University, the University of Iowa and IBM suggested that Diebold had “included a ‘back door’ in its software, allowing anyone to change or modify the software... A

Can Electronic Voting Machines subvert elections?

malicious individual with access to the voting machine could rig the software without being detected”

- Germany (2009)
 - The Federal Constitutional Court of Germany declared EVMs unconstitutional^{xii}
- The Netherlands (2006)
 - The ministry of the interior withdrew the licenses of 1187 voting machines because it was proven that one could eavesdrop on voting from up to 40 meters away. The suit was brought by a Dutch citizen’s group named “We Do Not Trust Voting Machines”^{xiii}. This group demonstrated that in five minutes they could hack into the machines with neither voters nor election officials being aware of it.
- Finland (2009)
 - The Supreme Court declared invalid the results of a pilot electronic vote in three municipalities.^{xiv}
- United Kingdom (2007)
 - The Open Rights Group declared it could not express confidence in the results for the areas that it observed^{xv}. Their report cites “problems with the procurement, planning, management and implementation of the systems concerned.”
- Ireland (2006)
 - Ireland embarked on an ambitious e-voting scheme, but abandoned it due to public pressure^{xvi}
- Brazil (2006)
 - There were serious discrepancies in the Diebold systems predominantly used in Brazil’s 2006 elections^{xvii}
- India
 - 2004 General Elections: allegations that good old booth-capturing was taking place^{xviii} in Bihar, even with the spanking-new EVMs
 - 2009 General Elections: Subramanian Swamy alleged in April 2009 that a group of people who had been convicted in the US for hacking bank accounts and credit cards had been recruited by a certain political party to possibly rig the elections.
 - The Shiv Sena alleged that EVM malfunction caused its candidate Mohan Rawale to lose in South Mumbai. Said Rawale: “I wonder how I got only 5 votes from an area that is a Shiv Sena stronghold”^{xix}
 - Journalist Cho Ramaswamy discussed how in MDMK leader Vaiko’s constituency, Virudhunagar, Tamil Nadu, “while counting, the votes increased by 23,000 more than the polled votes”^{xx}
 - An ongoing debate and additional new information is posted on S Kalyanaraman’s live blog^{xxi} which is updated often; a detailed analysis is at Senthil Raja’s blog^{xxii} of May 24th

A report^{xxiii} in *Newsweek* magazine provides more details about how people around the world are rejecting electronic voting. The Open Rights Group has provided many examples and more details about some of the above in its paper “Electronic Voting: A

Can Electronic Voting Machines subvert elections?

challenge to democracy?”^{xxiv}. Their conclusion: “E-voting threatens the integrity of our elections and we oppose its use in our democracy.”

4. Possible ways of manipulating EVMs

Are EVMs particularly bad, compared to the old paper ballot box? The answer has to be a resounding “yes”. The reason is that paper ballots, despite their many flaws^{xxv}, have one sterling characteristic: there is an audit trail, an actual piece of paper exists, and a recount, while laborious and time-consuming, is possible.

EVMs have the great advantage of quick tabulation of results. But the problem is fundamental: trust. Since the vote cast does not result in anything palpable, but only creates a digital impulse, it is hard to verify the accuracy of the result, and therefore it is hard to trust.

Digitized data is malleable and easily manipulated: indeed, this is one of its principal attractions in ordinary computing. For instance, a digital photograph can be enhanced, edited, color-corrected, cleaned-up, brightened, the background changed, and otherwise modified in ways that a traditional analog (most film is analog) photograph cannot be. Unfortunately, this very malleability is a problem when it comes to voting, because it is hard to *prove* that the voting data has not been tampered with. It would be hard to detect any manipulation unless expensive and thorough preventive steps are taken.

Data can be manipulated at almost every step on the way: during vote, in transit, or during counting. None of this is easily detected because the EVM is presented to the user as a typical “black box” which is deemed unalterable and tamper-proof. In other words, the hardware and software installed, are deemed trustworthy by edict, and not based on formal verification by a third party.

This trust is misplaced. Embedded systems – that is computers that run just their installed programs (for instance in a watch or a microwave oven), rather than a computer like a PC which an end user can add programs to and run in a manner he pleases – are notoriously prone to error, which is why the Y2K bug was considered so dangerous: there was concern that embedded systems in planes, banks, electric utilities, transportation systems, etc. would fail catastrophically. This is the reason why some critical systems (eg. control systems for nuclear power plants) continue to be electro-mechanical rather than digital.

There are several technical reasons why embedded systems are tricky: one is that the software used in these systems (which have limited memory, unlike capacious PCs) is tightly-written machine-language code, which is hard for humans to comprehend, unlike code that is written in a high-level language such as Java or C++.

Secondly, the software may not be adequately tested taking into account the various extreme cases of data it might encounter. This can be compared to a 1994 problem with Intel’s Pentium chips^{xxvi}: they were found to produce erroneous results in some simple

Can Electronic Voting Machines subvert elections?

arithmetic calculations. When unanticipated data is entered, the system may behave erratically.

The above examples pertain to inadvertent errors; similarly, manufacturing faults in the hardware may result in malfunctions. More sinister issues arise from malicious and intentional tampering. The programs used are proprietary and not open for inspection, unlike, say, open source programs which any individual can test out.

There are several ways in which the fraud can be perpetrated with EVMs^{xxvii}:

- Tampering with the software to add malicious code to alter vote totals or favor any candidate
- Tampering with the hardware of the machine to alter vote totals or favor any candidate
- Intentional mis-configuration of the ballot design to misidentify a candidate's party
- Abusing the administrative access to the machine by election officials might also allow individuals to vote multiple times

The most obvious way to add malicious code is to create a Trojan Horse^{xxviii}, a program that has an undocumented back-door entry, known only to the writers of the program. Under normal circumstances, the program will function as specified, in this case correctly capturing the voter's choice. However, the Trojan Horse can be triggered off by some specific mechanism, such as by pressing a particular sequence of buttons on the EVM. Before or during the voting process, some individual can trigger off the Trojan Horse, which becomes active. This individual could well be a party cadre who is a legitimate voter in that constituency.

The Trojan could then work some algorithms – for instance, it could assign every twelfth vote to the desired party, regardless of which blue button the voter pressed. Algorithms can be quite sophisticated, giving a percentage of the vote that is not suspiciously high (90%) but plausible – say 42% in a constituency with a multi-cornered contest.

Furthermore, the Trojan Horse could be programmed to erase itself when the EVM is turned off at the end of the day's voting. It may leave no trace of its erstwhile existence. Trojan Horse programs are well-known among the hacker community, and are not particularly difficult to write. But they are fiendishly difficult to find and eradicate.

How does the Trojan Horse program get embedded in the machine in the first place? One of the objections to this scenario is the question as to how the malicious code is introduced into the EVMs in all 828,804 polling stations? Wouldn't this level of tampering require the connivance of hundreds of thousands of people in the polling booths?

In fact, no. This can be done at a single point, in the factory, where an innocuous 'update' of the software can be infected with the rogue add-on. Only one or two people need to ever know about this, if they are well-placed within the factory^{xxix} or in the election

Can Electronic Voting Machines subvert elections?

machinery. In this context, the previous UPA government's selection of Naveen Chawla as Chief Election Commissioner, despite allegations of bias against him^{xxx}, looks dubious.

A startling new revelation suggests how this not-so-innocent 'update' could have been performed in 2009. Writing in the blog taragana.com^{xxxii} on June 19th, Azera Rahman provides the following information from Amol Newaskar, general manager of BEL in Bangalore. Here is the quote, verbatim:

“However, the ones manufactured from 2007 onwards have improvised [sic] features like in-built clocks which record the exact time a ballot is cast” Newaskar said. “Not just that, the EVM also records the exact time when the whole balloting process starts and when the last vote is cast. It gives an hourly update of the number of votes cast, and if there is any unusual trend in the process, it can be easily detected. Thus, the whole process becomes tamper-proof”, he added... The Election Commission, according to Newaskar, placed an order for 182,000 EVMs to BEL for the 2009 general election – all of which were supplied by January. The other company authorized by the Election Commission to manufacture EVMs is the Hyderabad-based Electronics Corporation of India (ECIL) that has supplied 78,000 machines with the improvised [sic] features...”

This could well be the smoking gun. The 'improvised' code in the 260,000 new EVMs could well hold the key. Exactly what was changed? Does this possibly have an embedded Trojan? Has any independent verification authority certified the new code? Doesn't this new code invalidate the Indiresan Committee report of 2006? Can the instances of suspected fraud be correlated with polling stations where the new EVMs were deployed? Is the new data collected as described above stored in a non-reprogrammable and permanent manner? How can researchers get access to it?

A second objection^{xxxiii} is procedural: how is the Trojan Horse triggered? The assignment of the buttons to parties is done late in the game, so that it would require at least one person to keep track of the buttons and trigger the Trojan Horse in each of the 800,000+ polling stations – and it is hard to keep a secret that so many people know. Once again, the answer is a no. First of all, there is no need to subvert every one of the polling stations, it would be sufficient to concentrate on only a few constituencies and the associated polling booths.

Second, another possibility is that the Trojan is the norm, and it will run by default *unless* the triggering is done, in which case it will become dormant. More alarmingly, there is the possibility of remote control, by substituting radio-aware chips for the normal chips in the voting machines. According the Election Commission's^{xxxiiii} FAQ, “the microchip used in EVMs is sealed at the time of import. It cannot be opened and any rewriting of program can [sic] be done by anyone without damaging the chip.” This implies that the chip is “imported” from somewhere, and any number of manufacturers especially in China have mastered the art of making fake chips. Why isn't there transparency about the chip and its manufacturers?

Can Electronic Voting Machines subvert elections?

Imagine that the new chip that was swapped in has a radio capability. That means it can be controlled by a cellular signal or other radio signal. For instance, it might be possible to send a signal via a standard GSM or CDMA cellular handset, if the chip is compatible. Thus, it may be possible for a single person to drive around to all the polling booths in a constituency, and, from outside, trigger the Trojan Horse. This drastically reduces the number of people who need to be involved! It does not have to be a low-level party cadre, it can be the district head, for instance. Thus, if only 50 constituencies were tampered with, only 50 highly trusted people need to know about the whole operation.

Radio-aware chips are common, especially now that RFID (radio-frequency identity tagging) is becoming widespread. There is the interesting case of the Iraqi Air Force and its Hewlett-Packard printers. Unbeknownst to the Iraqis, American officials swapped out the standard printer chips with chips that were additionally GPS-aware and could broadcast their location. When the printers ended up in Iraqi anti-aircraft batteries, a GPS satellite passing by overhead could accurately pinpoint the location of the printers, allowing warplanes to target them. HP has also announced^{xxxiv} another chip “the size of a grain of rice” that can store 100 pages of text and swap data via wireless.

The examples above only consider the possible fraud before and during voting; similar scenarios can be developed while the machines are in transit, and while the counting is going on. These possibilities merely scratch the surface; undoubtedly, resourceful minds have come up with even better ways of doing the deed. Here are in fact some of the specifics discovered in the Brazil case:

Problems from the Brazil case referred to above:

- a. The boot system may be modified by software
- b. It is possible to modify the internal programs by external digital methods
- c. The OS (Windows CE) does not possess strong resources of security
- d. The system of physical seals is insufficient and the case is easy to open, without destroying anything
- e. It is possible to reconfigure the security resources by means of jumpers on the motherboard
- f. There exists an internal socket for multimedia memory cards
- g. The external button labeled “battery test” can be used for attacks set off by a voter

A query to a computer science researcher in the US produced the following response which I quote in its entirety:

Shipping bug free software is proven to be impossible and it is found that in practice it is significantly harder to produce software without any security holes than it is to find and exploit a bug^{xxxv}. This raises significant questions about reliability of electronic voting machines. Malicious logic can be easily hidden by a “company insider” within the code, such that the machine records votes incorrectly to favor one candidate over another. While a study conducted by the researchers at the Rice

Can Electronic Voting Machines subvert elections?

University elucidated the ease with which voting systems could be infected by a Trojan horse^{xxxvi}, it is found that the Web sites and databases of major corporations are regularly hacked. Often a well-designed Trojan horse can tell when it's being tested and they may appear only for brief instants of time, while completely disappearing at other times^{xxxvii}. A number of methods for hiding Trojans in voting machines have been suggested ranging from as simple as misleading documentation to burying the malicious code deep in subroutines, macro expansions, header files, conditional compilations or making changes directly to object or machine code thereby bypassing the human readable source code completely^{xxxviii}.

Is it possible to reduce the probability of EVM fraud? Yes, one way is through deep testing, although that is still not entirely foolproof:

- Parallel testing, where an independent set of results is compared against the original machine results. During election, Statistically significant numbers of voters need to verify that their intended vote matches the electronic and paper votes
- Statistically significant number of voting machines can be randomly selected from polling stations and used for testing. This can be defeated by Trojan Horses
- Logic and accuracy testing before elections
- Independent software verification and certification. Can use code signatures to ensure software is identical. Open source may also be a good idea

5. Process improvements needed

At the heart of the problem is a system issue: the EVMs are a useful technology that has been thrown into the chaotic election process without due thought, understanding or introspection. They are like guns: they can be used well or they can be used badly. Throwing technology at a problem does not solve it. On the contrary, the EVM makes the process more opaque and more easily subverted. A full system review needs to be done before India continues with EVMs in future elections.

Writing in the IEEE *Computer* magazine of May^{xxxix} 2009, respected computer scientist and networking expert Andrew Tanenbaum suggested that it is necessary to take “a system view, incorporating a trustworthy process based on open source software, simplified procedures, and built-in redundant safeguards that prevent tampering.”

Tanenbaum outlines a nine-step process that he believes is necessary as an adjunct to EVMs, and necessary to make the process fool-proof. These are quite elaborate, with fool-proof encryption, and in summary they are:

- a. Generate and distribute precinct master keys (for cryptography)
- b. Create voter registration records
- c. Mail proof of registration to voters
- d. Prepare voting machines (by hashing the voting list with the precinct's public key^{xl} and writing onto a read-only medium)
- e. Assemble key pairs at precinct (for decryption of the voting list)
- f. Check in voters (they have to bring in the card they received in the mail)

Can Electronic Voting Machines subvert elections?

- g. Have voters cast their votes
- h. Tabulate votes
- i. Publish results

It is clear that in the Indian case, none of the essential cryptography was done, and as per Tanenbaum, that would mean the EVMs are not likely to produce reliable results.

6. PILs in Indian courts

There have been a number of cases (usually Public Interest Litigation) filed in Indian courts about the possibility of EVM fraud. Retired computer science professor Satinath Choudhary^{xli} claimed that “producing doctored EVMs is child’s play” as early as 2004. The *Linux Journal*^{xlii} at the time suggested that the fact that details of the hardware and software in the EVMs had not been published and the source code not made available meant citizens “could not be assured of the fairness of the EVM”. According to Choudhary, the Supreme Court had ruled in his PIL as follows: “Heard the petitioner, who is appearing in-person. In case the petitioner files any representation, the Election Commission may consider his suggestions. With the observations made above, the writ petition stands disposed of.” However, the Election Commission did nothing to take into account his concerns and suggestions. In his followup, Choudhary suggests a number of steps that should be taken.

Banwarilal B. Purohit vs. Election Commission of India was filed in 2004 in the Maharashtra High Court at Nagpur. The deposition of Ravi Visvesvaraya Prasad, an electrical and computer engineer, provides substantial insight into the ways in which EVMs can be manipulated.^{xliii}

Shailendra Pradhan filed a PIL in 2009 in the Madhya Pradesh High Court at Jabalpur, with the Election Commission and the manufacturers as respondents, suggesting that the lack of a voter-verifiable audit system made EVMs faulty and that there was no basis for the belief that the embedded programs are tamper-proof, among other claims.^{xliv}

The PMK, which suffered a shock defeat in Virudhunagar constituency, has filed^{xlv} an appeal to the Election Commission and will file a PIL if the appeal to the EC fails.

The DDMK has filed a PIL in Madras High Court against EVMs.^{xlvi}

7. Next steps

In order to give voters and observers a certain sense of comfort that they can indeed depend on the EVMs, a number of steps need to be taken urgently. First of all, there is the Expert Committee Report^{xlvii} on EVMs. The report considers a number of possible fraud scenarios, including the tampering of various parts of the system. In all the cases considered, the report found that the EVM has sufficient safeguards to ensure fair polling. But the Report does not go beyond a ‘black box’ analysis, and does not give any information about the reliability or otherwise of the operating system used, the circuit

Can Electronic Voting Machines subvert elections?

boards, or the chipset, not to mention the embedded software. This report also does not necessarily respond to all the concerns raised by Tanenbaum, Choudhary and Prasad above, it would be a good first step to analyze the EVMs in light of this new set of concerns.

Secondly, the new and 'improved' 2009 EVMs reported by Newaskar are obviously outside the ambit of the 2006 report, and so it is necessary to constitute a new Committee to investigate them.

Thirdly, the 2006 report says on Page 4: "a log is maintained of all key presses". This is intended as a permanent record of all activity on the EVM itself, and it is claimed that the record is tamper-proof and cannot be erased electronically and that it is available for an extended period.

Therefore, researchers should acquire via a Right-To-Information petition the complete logs of all EVMs (including the time-stamp data Newaskar refers to with the new EVMs) in at least one sample constituency where they suspect fraud. If the log is a permanent and tamper-proof record as claimed, a painstaking analysis of the log using data-mining techniques should indicate the presence or absence of fraud. If this exercise is done over the entire constituency, not on a sampling basis but on a survey basis, it would be possible to get a complete picture of whether the EVMs functioned as advertised.

Once this step is completed, if suspicions persist, a random sample of the logs from a statistically valid sample of EVMs from around the country needs to be taken, and the same kind of detailed data-mining analysis performed on them to see if there are any suspicious patterns of keystrokes emerging: for instance, are there sequences that look like triggers for Trojan Horses? Are there suspiciously uniform patterns of voting?

The next step would be to scrutinize the actual source code of the software that is installed in the systems. Given the gravity of the function performed by them, there is no room for opaqueness: the public has a right to know exactly what the code contains, and the manufacturer should be forced to reveal it. The code, and its embedded version, must be given to independent labs for thorough testing to see if there are anomalies. The same is true of the hardware, including the chip as well as the schematics of the EVM itself.

Another, parallel, step would be to build an actual proof-of-concept on the EVM of how a Trojan Horse can be implemented with the kinds of characteristics described above. The manufacturers of the EVM should provide complete technical details of the chips, along with any firmware and software used, as well as sample chips and EVM devices to independent testing labs so that they could demonstrate Trojan Horse on the actual EVM devices.

In light of all of the above, it is clear that there is reasonable doubt about the reliability of EVMs. A PIL should be filed in the Supreme Court to postpone any further use of EVMs until a proper audit and verification has been performed on them.

Can Electronic Voting Machines subvert elections?

Finally, the kinds of procedural checks and balances recommended by Tanenbaum and other experts need to be incorporated into the system before another election in India that depends entirely on EVMs.

8. Conclusion

Given the poor experience with Electronic Voting Machines worldwide, it is difficult to believe that India's EVMs are somehow far superior to those used elsewhere, and somehow immune to fraud. This has to be demonstrated. *A priori*, the evidence suggests that India's EVMs are susceptible to fraud in a number of dimensions.

It appears that both technical and procedural measures must be put in place to allay the concerns about the reliability, or lack thereof, of electronic voting machines.

It is entirely possible that the election machinery has taken every possible step in good faith, but that clever criminals have subverted the system for their own ends. Improved transparency, and public scrutiny of the system, including an analysis of ways in which it can be made more secure are urgent and imperative before any future elections.

ⁱ "Opposition vows to fight Zimbabwe election fraud", Reuters, Sun Mar 23, 2008

<http://www.reuters.com/article/worldNews/idUSL236998620080323>

ⁱⁱ "Fraud video claim in Mexico poll", BBC, Tue Jul 11, 2006

ⁱⁱⁱ www.electionfraud2004.org, which the opening quote from Thomas Paine has been taken

^{iv} "Was the 2004 Election Stolen?", Robert F Kennedy Jr, Rolling Stone, Jun 1, 2006

^v "Landslide or Fraud? The Debate Online Over Iran's Election Results", New York Times, June 13, 2009

<http://thelede.blogs.nytimes.com/2009/06/13/landslide-or-fraud-the-debate-online-over-irans-election-results/>

^{vi} "Neither Real nor Free", Editorial, New York Times, Jun 15, 2009

^{vii} "Iran Elections: Mahmoud Ahmedinejad and Hossein Mousai both claim victory", UK Telegraph, Jun 12, 2009

^{viii} "EVMs 'manipulated' in Orissa polls, claims Azad, Union Health Minister", IANS, 18 Jun 2009

^{ix} Wikipedia entry on "Electronic voting"

^x Wikipedia entry on "Electronic voting"

^{xi} "The Diebold Bombshell", OpEdNews.com, 23 July 2006

^{xii} German Federal Constitutional Court, Press Release No. 19/2009, of 3 Mar 2009

^{xiii} "Dutch government scraps plans to use voting computers in 35 cities including Amsterdam", AP, 30 Oct 2006

^{xiv} Wikipedia entry on "Electronic voting"

^{xv} "ORG Election Report highlights problems with the voting technology used", 20 Jun 2007

^{xvi} "Are electronic voting machines tamper-proof?" Subramanian Swamy, The Hindu, 17 Jun 2009

^{xvii} "Brazil: The Perfect Electoral Crime", James Burk, Portland Indymedia Center, 21 Oct 2006, quoting

Amilcar Brunazo Filho, www.votoseguro.org

^{xviii} "On New Voting Machine, the Same Old Fraud", New York Times, 27 Apr 2004

^{xix} "Sena alleges EVM malfunction in South Mumbai", Rediff.com, 16 May 2009

^{xx} "Rahul could become a desirable leader", Rediff.com, 19 May, 2009

^{xxi} <http://sites.google.com/site/hindunew/electronic-voting-machines>

^{xxii} <http://psenthilraja.wordpress.com/2009/05/24/remote-controlling-evm-manufacturing-election-results/>

^{xxiii} "We Do Not Trust Machines", Evgeny Morozov, Newsweek, 1 Jun, 2009

^{xxiv} <http://www.openrightsgroup.org/wp-content/uploads/org-evoting-briefing-pack-final.pdf>

Can Electronic Voting Machines subvert elections?

- ^{xxv} According to the faq by the Election Commission at //eci.nic.faq/EVM.asp the great advantage of the EVM is speed of tabulating the results
- ^{xxvi} “Ideas and Trends: The Chip on Intel’s shoulder”, New York Times, 18 Dec, 1994
- ^{xxvii} Wikipedia entry on “Electoral fraud”
- ^{xxviii} Obviously named after the mythological – and malicious -- Trojan Horse the Greeks gifted to Troy. See the Wikipedia entry on “Trojan Horses”
- ^{xxix} In the case of India, it is the BEL in Bangalore and ECIL in Hyderabad which produce the EVMs
- ^{xxx} The outgoing Chief Election Commissioner made a *suo moto* recommendation that Naveen Chawla, Election Commissioner, should be removed, based on a report by the Shah Commission investigating the Emergency that indicted Chawla for having been ‘authoritarian and callous’ and for gross misuse of power. It declared that he was “unfit to hold any public office which demands an attitude of fair play and consideration for others”
- ^{xxxi} “Electronic voting machines – the leitmotif of Indian democracy”, AzeraRahman, <http://blog.taragana.com/n/electronic-voting-machines-the-leitmotif-of-indian-democracy-86599/>
- ^{xxxii} <http://theoverlord.wordpress.com/2009/05/19/the-indian-electronic-voting-machines>
- ^{xxxiii} Ibid. eci.nic.faq/EVM.asp
- ^{xxxiv} “Tiny wireless memory chip debuts”, BBC, 17 Jul, 2006
- ^{xxxv} Bannet, J.; Price, D.W.; Rudys, A.; Singer, J.; Wallach, D.S., “Hack-a-vote: Security issues with electronic voting systems,” IEEE Security & Privacy, vol.2, no.1, pp. 32-37, Jan.-Feb. 2004.
- ^{xxxvi} D. S. Wallach, “Electronic voting: Accuracy, accessibility and fraud.”, Report for Democratic National Committee. www.democrats.org/pdfs/ohvrireport/section07.pdf
- ^{xxxvii} P. G. Neumann, “Security criteria for electronic voting,” 16th National Computer Security Conference, September, 1993
- ^{xxxviii} Barbara Simons, “Who gets to count your vote? Computerized and internet voting,” talk at Spatial Cognition Research Center, 2003
- ^{xxxix} “Trustworthy voting: from machine to system”, Nathanael Paul and Andrew S. Tanenbaum, IEEE Computer, May 2009
- ^{xl} Public-key private-key systems of cryptography are essentially tamper-proof
- ^{xli} “Winning elections made easy”, Satinath Choudhary, Indian Express, 19 Apr 2004. He was president, Better Democracy Forum, The Bronx, New York.
- ^{xlii} “India’s electronic voting faces lawsuit over accountability”, Linux Journal, 3 May, 2004
- ^{xliii} www.scribd.com/doc/15745499/EVMs-Supporting-Documents
- ^{xliv} www.samarthbharat.com/files/evmpetition.pdf
- ^{xlv} “PMK to move court against EVMs”, The Hindu, 14 Jun, 2009
- ^{xlvi} “PIL to ban use of EVMs in future elections admitted in Madras High Court”, 26 May, 2009
- ^{xlvii} www.scribd.com/doc/6794194/Expert-Committee-Report-on-EVM has the report dated Sep 2006, retrieved under RTI