THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

June 7, 2019

Revisiting the EVM Hacking Story

By: Prabir Purkayastha,Bappa Sinha

It has now been revealed that one EVM supplier has been using chips that can be reprogrammed. While this still does not mean that hacking an EVM is easy, the issue of securing public confidence for EVMs remains. A proposal that could do so is made here.

The 2019 general elections have seen, like in the polls of the recent past, controversies on the use of the electronic voting machines (EVMs).

The controversies have their origin in the fear of a number of voters that the EVMs are not hack-proof as the Election Commission of India (ECI) claims. Various contradictions have also emerged between the number of votes polled and the final vote account, both of which are on the website of the ECI.

To add grist to the EVM mistrust mill, information given in reply to a Right to Information (RTI) question by Bharat Electronics Ltd (BEL), one of the two manufacturers of EVMs, reveals that contrary to what the ECI has claimed on its website and in various documents, the EVMs do not have software burnt into one time programmable (OTP) chips but have chips that can be reprogrammed. Of course, this still means that if hackers want to reprogram (hack) the EVMs, they would need physical access to the EVMs that have been used in the elections, and even if the machines are hacked, the voter-verified paper audit trail (VVPAT) slips with the original vote cast would remain intact.

It is in this context that we would like to add a postscript to our article that we had published in *The India Forum* (5 April 2019).

> One of the key design principles of the EVMs, as claimed by the ECI, was that the software was burnt into an OTP chip which could only be programmed once during the time of manufacture of these EVMs and could not be reprogrammed subsequently...It turns out that this assertion by the ECI is false.

We had earlier maintained that large-scale hacking of EVMs was unlikely. This conclusion was based on our understanding of the key design principles of EVMs, and the elaborate administrative checks and balances, *including* the participation of the opposition parties in the monitoring process to ensure that hacking did not happen.

Importance of OTP Chips

One of the key design principles of the EVMs, as claimed by the ECI, was that the software was burnt into an OTP chip which could only be programmed once during the time of manufacture of these EVMs and could not be reprogrammed subsequently. This would then rule out hacking of the EVM by modifying the software.

It turns out that this assertion by the ECI is false.

In response to a RTI filed recently, BEL responded stating that the EVMs it manufactured used the MK61FX512VMD12 Microcontroller from NXP, a multi-national semiconductor manufacturer. The RTI response directed the reader to the NXP website for further information, which indeed does list this microcontroller. The Electronics Corporation of India Lts (ECIL), the other public sector undertaking (PSU) that manufactures EVMs, refused to disclose the identity of the manufacturer of the microcontroller used in its EVMs and VVPATs, citing commercial confidence under Section 8(1)(d) of the RTI Act.

The data sheet for MK61FX512VMD12 in NXP's website mentions that it is an ARM based microprocessor with 16Kbytes of EEPROM, 512KB of Flash and 128 KB of SRAM.

EEPROM stands for "electrically erasable programmable read-only memory" and as the name suggests this memory is electrically erasable and reprogrammable. The data sheet says that the 512 KB of flash memory can be partitioned such that a part of this memory can be used for storing software code, and the remaining for data. This flash memory is also rewritable. Both NXP and other vendors provide development kits through which software can be developed for these chips and transferred to them.

In the EVMs, the software is stored in either the EEPROM or in the Flash Memory (or both), both of which it now turns out can be reprogrammed. So, the ECI's assertion that the EVM software is stored in an OTP chip is clearly not right.

We need to pursue with the ECI why they have not followed the procedures they themselves claim to be following and what the Indirasen Committee Report on EVM, 2006 stated that BEL and ECIL are following, namely "the fixed nature of the software which is fused to the processor which is effectively unalterable".

According to a 2014 Press Information Bureau note, a salient feature of the EVMs is that, "(the) Program which controls the functioning of the control unit is burnt into a micro chip on a 'one time programmable basis'. Once burnt it cannot be read, copied out or altered." Why did the ECI not follow these directions? Or why did it not review the chip sets BEL and ECIL were using?

> We are in no way suggesting that the EVMs have been hacked in the recently concluded Lok Sabha Elections by using the newly revealed vulnerability of the chips. We have not seen any data to back up claims of extensive/selective hacking...

Interestingly, the NXP chip has tamper-detect features which may be used to detect some forms of hardware tampering and also Flash & SRAM tampering. These features might be used to mitigate other kinds of attacks like attempts to change the electronic vote counts stored in SRAM after the end of voting.

We are in no way suggesting that the EVMs have been hacked in the recently concluded Lok Sabha Elections by using the newly revealed vulnerability of the chips. We have not seen any data to back up claims of extensive/selective hacking and so making such claims would involve a leap of faith!

It is incumbent on the ECI to have an open and in-depth discussion with the technical community about the various design choices involved in the EVMs, rather than taking an adversarial position and stonewalling all such concerns raised about the EVMs and their design.

Without OTP chips, can the EVMs be easily hacked?

The answer is that they still cannot be hacked through, for example, wireless means as claimed in the farce of a press conference in London conducted by some mysterious persons who appeared through video. Nor can they be hacked through some unknown remote process. But ,yes, if physically, the EVMs are "accessed" -- read tampered with -- then they can be hacked by reprogramming the chips using a toolkit that is commercially available.

This is not very different from what we had said in our earlier article: that if the chip carrying the program (or the vote count) is physically replaced, the EVMs can be hacked. In this case, instead of replacing the chip, it can be reprogrammed after physically opening the EVM "box" and accessing the chip.

There still two other layers of protection: (i) the EVMs are stored under guard and also monitored by the political parties, and (ii) the EVMs are signed and sealed by the polling agents of the political parties, and the seals verified before counting. So the fact that the ECI's claim on one element of the protection – the use of OTP chips – is wrong, does not automatically mean that the EVMs can be easily hacked.

We still discount the possibility of the EVMs being hacked on a mass scale (or a scale enough to change the election results), since the reasons we had offered still remain valid. All the protections – against physical tampering of the EVM, the administrative checks and the vigilance of the opposition parties – need to be defeated for successfully changing the result of the elections.

Just to quantify the scale of hacking that would be required, let us look at, say, hacking 5-10% of the EVMs in 100 constitutencies. Given that there are about 1,800 booths/EVMs in a parliamentary constituency, we are talking about hacking 90-180 EVMs in each constituency and therefore a total of about 9,000-18,000 EVMs would need to be hacked. This means physically accessing EVMs on this scale, and to do so in a way that the people involved keep this a complete secret. And that the ECI is compromised to such an extent that 9,000-18,000 EVMs can be physically tampered, all of it in total secrecy.

How to convince voters that elections using EVMs are indeed fair?

As we had argued in our earlier article, there are two sets of issues in an election. One is finding out who has won the elections through a count of the ballots. This is what the EVMs are doing. The ECI is convinced that this is the only question that needs to be answered. What the commission is missing is that it has to also convince the losers and the people at large that its count is indeed the right one. This is the question that the ECI refuses to recognise; to our mind in an extremely pig-headed way.

> People do not believe that an intangible and invisible electronic record that can neither be seen nor touched can be the basis for deciding who has won or lost in elections.

The reason for arguing that a much larger number of VVPAT slips should be tallied with the EVMs emanates not from the belief that the machines have been or are being hacked, but as a credible check that confirms the EVM count. People do not believe that an intangible and invisible electronic record that can neither be seen nor touched can be the basis for deciding who has won or lost in elections.

We do not want to enter into the issue of deciding on the right number of VVPATs whose slips should be tallied with the EVM count for verification. We would like to take a more commonsensical approach to the EVMs and revisit Section 61A of the Representation of the Peoples Act, the 1988 Amendment through which EVMs were legally introduced. This section states:

61A. Voting machines at elections:—Notwithstanding anything contained in this Act or the rules made thereunder, the giving and recording of votes by voting machines in such manner as may be prescribed, may be adopted in such constituency or constituencies as the Election Commission may, having regard to the circumstances of each case, specify. *Explanation*.—For the purpose of this section, "voting machine" means any machine or apparatus whether operated electronically or otherwise used for giving or recording of votes and any reference to a ballot box or ballot paper in this Act or the rules made thereunder shall, save as otherwise provided, be construed as including a reference to such voting machine wherever such voting machine is used at any election.

This leaves out the question, what is the ballot that a voter casts? Is it the printed VVPAT slip or is it the electronic record in the EVM? Though the Supreme Court had decided that there should be VVPATs for all EVMs, it did not opine on the key question of what now constitutes the ballot, the electronic record or the VVPAT slip?

The issue of what constitutes the ballot has come up in different jurisdictions. A German Constitutional Court decided that the vote recorded in the electronic voting machine did not conform to legal requirements of the German Law on elections. But it made clear that the court's decision did not rule out the use of voting machines:

The legislature is not prevented from using electronic voting machines in elections if the possibility of a reliable examination of correctness, which is constitutionally prescribed, is safeguarded. A complementary examination by the voter, by the electoral bodies or the general public is possible for example with electronic voting machines *in which the votes are recorded in another way beside electronic storage*. (Italics added by the authors)

The Supreme Court of India, in its judgement on 2012, made clear the indispensability of a paper trail in the elections. It said:

...that the "paper trail" is an indispensable requirement of free and fair elections. The confidence of the voters in the EVMs can be achieved only with the introduction of the "paper trail". EVMs with VVPAT system ensure the accuracy of the voting system.

This has led to the introduction of VVPAT terminals with every single EVM in India. However, it still leaves open the question of what is the primary record, the electronic record or the paper trail? What happens if they do not match?

This question has already been raised before the ECI. The ECI has yet to give a clear opinion, though it appears to believe that in the case of a discrepancy, the EVM count should override the VVPAT slip count.

Now that we have VVPATs with every EVM, we believe that the ECI (and the Courts) need to take a different view of the EVM-VVPAT slip issue. In a workshop in Delhi on 18^{t} May, 2019 on "Strengthening Transparency, Accountability, and Independence of the Election Commission and the Electoral Process", a proposal was mooted to consider the EVM as a printing machine and the VVPAT slip as the ballot.

> The key issue here is not whether the EVMs are being hacked or can be hacked...The issue that comes out time and again is that a simple assertion by the ECI and technical experts of the infallibility of the EVMs will not convince the sceptics.

Rephrasing this, we can consider the EVM as a *printer of the voters' ballot and also an electronic calculator*. As a printer, it prints the ballot with the vote, and as a calculator, it totals up the vote. Legally, the ballot should be the VVPAT slip. In the case of a dispute, or a challenge by the defeated candidate, the VVPAT slips should be counted and the case decided on that basis.

It is clear that if a vote is not tangible, people will continue to have reservations about the outcome. The key issue here is not whether the EVMs are being hacked or can be hacked. Or are that the EVMs are much better than the old system where booth capturing had become a fine art. The issue that comes out time and again is that a simple assertion by the ECI and technical experts of the infallibility of the EVMs will not convince the sceptics. And if democracy demands that the electoral process kept be above suspicion, an electronic vote that has a physical existence that can be independently tallied is the obvious way to provide confidence in the sanctity of the elections.