To use or not to use? Electronic Voting Machines in Indian Elections.

Sandeep K. Shukla

Electronic Voting Machines (EVMs) are a very commonly discussed example of an embedded computing system which has also been at the center of political storm in India in the recent days. A number of allegations have surfaced that the EVMs are being reprogrammed or tampered with during elections to favor candidates of a specific political party. Given that EVMs are very classical embedded systems with simple microcontrollers whose program instructions are burnt into a ROM, and cast vote counts are stored in an EPROM, and few peripherals, one would think that it would be easy to verify by experts to indubitably establish their tamper proof design, and implementations. However, looking at various aspect of this simple yet very critical embedded system, it seems a lot more research is required on multiple aspects of the democratic franchise that are dispensed through these simple systems. It should be mentioned also that recently in response to 'right-to-information' query, one of the manufacturers divulged that new generation of Indian EVM are no longer having program instructions burnt into ROM but they are using a specific microprocessor with writable memory. This raises lot more questions than one would have raised with the previous generation EVMs. Furthermore, one of the two manufacturers refused to even entertain the query – raising further suspicion.

Before coming to the Indian case, let me focus on some other countries. In the Netherlands, electronic voting machines were abandoned in 2007 after several years of controversy regarding the security of the voting data, the machines, as well as the privacy of the voter. The engagement of civil society, computer experts and others paved the way to experimentation that showed the ease with which one can replace the memory chips in those machines in less than five minutes, allowing manipulation, thereby possibly subverting democracy. More concerning was the fact that with simple radio receivers, people could see variations in electro-magnetic signals that would allow one to detect who a voter is casting the vote for – from outside the polling station. After some iterations in the design, other such side channel attacks were found in certain versions of the machine, and eventually honoring the fact that integrity of the democratic process is more sacrosanct than efficiency – the Netherlands abandoned the electronic voting [1].

In 2009, the federal constitutional court of Germany ruled that electronic voting is unconstitutional [2]. The court ruled "*The use of Nedap electronic voting machines violated the principle of the public nature of elections (Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law)* ***that requires that all essential steps in the elections are subject to public examinability*** *unless other constitutional interests justify an exception.*" This is very significant. Given that **the legitimacy of democratic processes depends on the public's trust in the processes, any member of the public should be able to examine, if he/she desires so, to test and verify every step** – including the functioning of the voting machines, their design, the security and safety safe guards, and measures to secure their franchise.

If the voting machine design, software, or the security proofs are not possible to verify by members of the public, there is enough reason to worry about safeguarding our democracy.

Ireland also abandoned electronic voting in 2004. In the United states, 27 states are using electronic voting machines of which 15 are using verifiable audit trail. However, given the issues surrounding the hacking incidents during the last presidential election in the united states, there is reasonable doubt whether it is prudent to continue the electronic machine-based voting.

Coming back to the Indian case, the voting machines are quite simple, with a ballot unit, a control unit, display unit, and the wires connecting them. While the software is kept under extreme confidentiality with the government sector companies who manufacture these machines, the machine instructions were burnt into a ROM in the previous generation EVMs with the claim that it cannot be changed. The microcontroller being used is simple, and the memory units are connected with simple protocol. In 2010, a group of security experts got hold of a unit and showed that there are numerous ways to tamper with these machines within matters of few minutes [3]. One can replace the microcontroller, the memory units, and even the PCB board with relative ease provided physical access is possible. Also, if the EPROM is replaced with an attacker's chosen instructions, the behavior of the machine could be changed, including how it responds to pre-poll mock polling phase vs. real polling phase. Further, the display unit can be replaced, and clip on radio frequency devices may be used to control the behavior of the programs. Of course, the Indian authorities now have responded by adding mutual authentication between the components, and also doing some redesign. The design of the latest one uses MK61FX512VMD12 microcontroller from an MNC – which is of US origin. Moreover, this chip has programmable FLASH memory. Although, if the JTAG pins are fused, and memory lock bit is set – it cannot be written to. Unfortunately, it turns out neither Election Commission nor the Government has any appetite to get this design checked by cyber security experts in various IITs even though the technical expert committee formed by EC has not a single cyber security expert. The EC's claim is that the technical committee bereft of any expert in cyber security has certified it – so we no longer need any further check by outside experts.

Given the cloak of secrecy about the design, the program, and even the mechanisms of authentication – ***security by obscurity seems to be their goal***. Another defense is that the EVMs are very well protected during its storage, transfer, and randomized methods for allocating them to polling booths. Unfortunately, given the large population, and various uncertainties during a nationwide polling process, many of these safe guards might be violated if properly orchestrated. If none of these happen, even then, the fact that all the steps associated with the electronic voting machine design, manufacturing, and security studies are not subject to the verification and testing by the common people, and experts – there are scope of doubt about the security of the entire process. With the current advances in data science and exfiltration of personal data as exemplified in the Cambridge Analytica/Facebook case, it is not inconceivable that data analytics can pin point exactly which polling stations need to be tampered with, leaving the rest as it is –

and still manipulate the outcomes of the election. Therefore, it might be possible to manipulate only a few of the EVMS per parliamentary constituency to tamper with the results of that constituency. Which booths to target can be decided by appropriate use of data science on demographic data. This is not to say that such manipulations do happen, but the citizens should have a right to be fully convinced that it does not. Only way to do this is to provide copies of the machines to experts at various Indian institutes and have them thoroughly test the machines for security, side channels, programmability etc.

EC in the past sent out challenge to community to hack EVMs by inviting teams to their headquarters but they severely restrict the kind of tests that the teams can do – for example, using of oscilloscope on the pins by opening the boxes are not allowed. Therefore, side channel analysis, checking whether the micro-controller JTAG pins are fused etc – cannot be checked. It seems that only tests allowed are pressing buttons in order to change results. However, even if there are 10 buttons, there are 2^10 possible combinations, and each such combination has a factorial number of permutations to test – which is not possible to try for any one. Therefore, these 'come-and-hack' events are more of an eye wash than real honest attempt to convince the citizens about the security of these machines.

So as cyber security researchers, it seems to be incumbent on us to figure out systems whose safety and security can be verified by anyone – while it is secure enough without the need for obscurity/secrecy of the algorithms, designs, methods etc. That is the only way, electronic voting machines can be made acceptable to a democratic nation. Creating a cloak of secrecy to protect from tampering never works – all security researchers would agree.

This is an important need that embedded systems community can attempt to cater to, and at the same time, save the democratic election process in every democratic jurisdiction. If experts can show to anyone interested the risk, the potential attack surfaces, the side channel vulnerabilities, and make every bit of software/firmware, architecture, protocols open, and check the plausibility of exploitations that still may remain in the fully vetted system – that will put the population at ease regarding their enfranchisement – even with systems they do not fully understand.

I, therefore, request all readers to think about this problem, and demand EVM designs to be transparent and open, have experts to test them, do their risk analysis, before EVM is accepted as the instrument of our democracy.

1. https://www.ndi.org/sites/default/files/5_Netherlands.pdf
2. http://www.dw.com/en/german-court-rules-e-voting-unconstitutional/a-4069101
3. https://indiaevm.org/evm_tr2010-jul29.pdf