EVM Secruity

In the recent past, there have been some queries in the minds of common people about the security features of Electronic Voting Machines (EVMs) of Election Commission of India (ECI). The Election Commission has, time and again, stated that ECI-EVMs and its systems are robust, secure and tamper-proof.

The following FAQs give a detailed view of security features including latest technological features of EVMs and stringent administrative measures taken at every step of its usage from manufacturing to storage.

1. What is meant by Tampering of EVM?

Tampering means alteration in the software program written either on existing microchips of Control Unit (CU) or introducing malicious software program by inserting new microchips in CU and also making keys - pressed in Ballot Unit (BU) not record faithfully in the Control Unit.

2. Are the ECI- EVMs hackable?

No. M1 (model one) of EVM machines were manufactured till 2006 and had all necessary technical features making M1 non-hackable contrary to claims made by some activists.
On the recommendations of the Technical Evaluation Committee in 2006, M2 model of EVMs produced after 2006 and upto 2012 incorporated dynamic coding of key codes thereby enabling transfer of the key – press message from Ballot Unit (BUs) to Control Unit (CUs), in an *encrypted form as an additional security feature*. It also contains Real time setting of each key press so that
sequencing of key presses including so called malicious sequenced key presses can be detected and wrapped.
Further, the ECI- EVMs are not computer controlled, are stand alone machines and not connected to the internet and /or any other network at any point of time. Hence, there is no chance of hacking by remote devices.
The ECI-EVMs do not have any frequency receiver or decoder for data for wireless or any external hardware port for connection to any other non-EVM accessory or device. Hence no tampering is possible either through hardware port or through Wireless, Wi-Fi or Bluetooth device because CU accepts only encrypted and dynamically coded data from BU. No other kind of data can be accepted by CU.

3. Can ECI-EVMs be manipulated by Manufacturers?

Not Possible.
There is very stringent security protocol at manufacturer level regarding security of software. The Machines have been manufactured in different years starting from 2006. After manufacturing, EVMs are sent to State and district to district within a State. The manufacturers are in no position to know several years ahead which candidate will be contesting from a particular constituency and what will be the sequence of the candidates on the BU. Also, each ECI-EVM has a serial number and the Election Commission by use of EVM –tracking software

can find out from its database which machine is located where. So, any manipulation at manufacturing stage is ruled out.

4. Can Trojan Horse be incorporated into the chip in CU?

Sequence of voting in EVM eliminates the possibility of injection of Trojan Horse as mentioned below. The stringent security measures by ECI make it impossible to introduce Trojan Horse in the field.
Once a ballot key is pressed in CU, the CU enables BU for registering the vote and waits for the key pressing in the BU. During this period, all keys in the CU become Inactive till the entire sequence of casting of that vote is complete. Once any of the keys (candidates vote button) is pressed by a voter in BU, the BU transmits the key information to CU. The CU gets the data and acknowledges it by glowing the corresponding LED lamps in BU. After the enabling of ballot in CU, only the 'first key press'is sensed and accepted by CU. After this, even if a voter keeps on pressing the other buttons that is of no use as there will not be any communication between CU and BU as the result of those subsequent key presses, nor will BU register any key press. To put it in other words, there can be only one valid key press (the first key press) for every ballot enabled using CU. Once a valid key press (voting process) is complete, until another ballot enabling key press is made there will not be any activity between the CU and the BU. Hence, sending of any malicious signal, by way of so called 'sequenced key presses', is impossible in the Electronic Voting Machines being used in the country.

5. Are Old model ECI- EVMs still in use?

M1 model of EVM machines were produced up to 2006 and were last used in 2014 General Elections. In 2014, EVM machines which completed 15 years of economic life and also because M1 were not compatible with VVPAT (voter-verified paper audit trail) , ECI decided to discontinue use of all M1 EVMs manufactured upto 2006. There is a Standard Operating Procedure laid down by ECI to discard EVMs. The process of destruction of EVM & its chip is carried out in the presence of Chief Electoral Officer of the state or his representatives inside the factory of manufacturers.

6. Can ECI-EVMs be Physically Tampered with/ their components be changed without anyone noticing?

In addition to the existing security features in earlier models M1 & M2 of ECI-EVMs, the new M3 EVM produced after 2013 have additional features like Tamper Detection and Self Diagnostics. The tamper detection feature makes an EVM inoperative the moment anyone tries to open the machine. The Self diagnostic feature checks the EVM fully every time it is switched on. Any change in its hardware or software will be detected.
A prototype of a new model M3 with above features is going to be ready shortly. A Technical Experts Committee will examine it and then production will commence. About Rs. 2,000 crores have been released by the Government to procure M3 EVMs with above additional features and new technological advancements.

7. What are the latest technological features to make ECI-EVMs tamper proof?

The ECI-EVMs use some of the most sophisticated technological features like one time programmable (OTP) microcontrollers, dynamic coding of key codes, date and time stamping of each and every key press, advanced encryption technology and EVM-tracking software to handle EVM logistics, among others to make the machine 100% tamper proof. In addition to these, new model M3 EVMs also have tamper detection and self-diagnostics as added features. Since, software is based on OTP the program cannot be altered, re-written or Re-read. Thus, making EVM tamper proof. If anyone make, attempt, the machine will become in operative.

8. Do the ECI-EVMs use foreign technology?

Contrary to misinformation and as alleged by some, India do not use any EVMs produced abroad. EVMs are produced indigenously by 2 PSUsviz. Bharat Electronics Ltd., Bengaluru and Electronics Corporation of India Ltd., Hyderabad. The Software Programme Code is written in-house, by these two companies, not outsourced, and subjected to security procedures at factory level to maintain the highest levels of integrity. The programme is converted into machine code and only then given to the chip manufacturer abroad because we don't have the capability of producing semi-conductor microchips within the country.
Every microchip has an identification number embedded into memory and the producers have their digital signatures on them. So, the question of their replacement does not arise at all because microchips are subjected to functional tests with regard to the software. Any attempt to replace microchip is detectable and can make EVM in-operative. Thus, both changing existing programme or introducing new one are detectable making EVM in-operative.

9. What are the possibilities of manipulation at the place of storage?

At the district headquarters, EVMs are kept in a *double-lock system under appropriate security. Their safety is periodically checked.* The officers do not open the strong room, but they check whether it's fully protected and whether the lock is in proper condition or not. *No Unauthorized person can get access to the EVMs at any point of time*. During non election period, Annual Physical Verification of all EVMs is done by DEOs and report sent to ECI. Inspection & checking have recently been completed.

10. To what extent are allegations of EVM tampering in local body polls true?

There is a misunderstanding in this regard due to lack of knowledge about jurisdiction. In case of elections to Municipal bodies or Rural bodies like Panchayat Elections, the EVMs used do not belong to the Election Commission of India. Above local bodies elections come under the jurisdiction of State Election Commission/s (SECs), which procure their own machines and have their own handling system. *ECI is not responsible for functioning of EVMs used by SECs in above elections.*

11. What are the different levels of checks and balances ensuring tamper proofing of ECI-EVMs?

- *First Level Checking:BEL/ECIL engineers certify originality of components after technical and physical examination of each EVM,* undertaken in front of representatives of political

parties. Defective EVMs are sent back to factory.

The FLC Hall is sanitized, entry is restricted and no camera, mobile phone or spy pen is allowed inside. Mock poll of at least 1000 votes is conducted on 5% EVMs selected randomly by reps of political parties and the result shown to them. The entire process is video graphed.

- *Randomization:* EVMs are randomized twice while being allocated to an Assembly and then to a polling booth ruling out any fixed allocation. Mock Poll at polling station is conducted in front of polling agents of candidates on the poll day, before polls begin.

After Poll, EVMs are sealed and polling agents put their signature on the seal. Polling agents can travel upto strong room during transportations.

- *Strong Rooms*: Candidates or their representatives can put their own seals on the strong rooms where polled EVMs are stored after the poll and also camp in front of strong room. These strong rooms are guarded 24x7 in multilayers.
- *Counting Centres:* The polled EVMs are brought to the Counting Centres and Unique IDs of the seals and CU are shown to reps of candidates before start of counting.

12. Can a manipulated ECI- EVM be re-inducted in the polling process without anyone coming to know?

Question does not arise.

Looking at the above series of fool-proof checks and balances that are undertaken by the ECI to make EVMs tamper proof, it is evident that neither the machines can be tampered-with nor defective machines can get re- inducted into the polling process at any point of time because Non ECI -EVMs will get detected by the above process and mismatch of BU & CU. Due to different level of stringent checks and balances neither ECI-EVMs can leave the ECI system nor any outside machine (Non-ECI –EVM) can be inducted into the system.

13. Why have Developed Nations like the US and European Union not adopted EVMs and some have discontinued?

Some countries have experimented with electronic voting in the past. The problem faced with the machines in these countries was that they were computer controlled and *connected to the network, which in turn, made themprone to hacking* and hence totally defeating the purpose. Moreover, there were not adequate security measures and safeguards in their corresponding laws regulations for security, safety and protection. In some countries, Courts struck down the use of EVMs on these legal grounds only.

Indian EVM is stand-alone whereas, USA, The Netherlands, Ireland & Germany had direct recording machines. India has introduced paper audit trail, though partly. Others did not have audit trail. Source code is closed during polling in all of the above countries. India also has closed source burnt into memory and is OTP.

ECI-EVMs, on the other hand, are stand-alone devices not connected to any network, thus making it impossible for anyone to tamper with over 1.4 million machines in India individually. EVMs are most suited for India, looking at the country's past poll violence and other electoral malpractices like rigging, booth capturing etc. during the polls.

It is worth mentioning that in contrast with countries like Germany, Ireland and the Netherlands. Indian Laws & ECI regulations have in-built adequate safeguards for security & safety of EVMs

Besides, Indian EVMs are far superior on account of secured technological features. Indian EVMs also stand apart because VVPATs going to be used with EVMs in phases to make entire process transparent for voters.
In case of The Netherlands, rules regarding storage, transport and security of machine were lacking. Machines produced in The Netherlands were also used in Ireland & Germany. In a judgment in 2005, German Court found voting device ordnance unconstitutional on the ground of violation of the privilege of the public nature of election& the basic law. So, these countries discontinued the use of machines produced in The Netherlands. Even, today many countries including USA are using machines for voting
ECI –EVMs are fundamentally different from the voting machines and processes adopted in foreign countries. Any comparison based on computer controlled, operating system based machines elsewhere will be erroneous and ECI –EVM cannot be compared with.

14. What is the status of VVPAT enabled machines?

The ECI has conducted elections in 255 assembly constituencies and nine Lok Sabha constituencies using Voters Verified Paper Audit Trail (VVPAT). The use of M2 and new-generation M3 EVMs along with VVPAT is the way forward for further confidence and transparency of the voters.