DEBATE AROUND EVMs- EXPLAINED!

CLARIFICATION ON ALL ISSUES

DOUBTS CREATED AROUND EVM

Hacked EVM

Vote Stuffing after Poll Closure

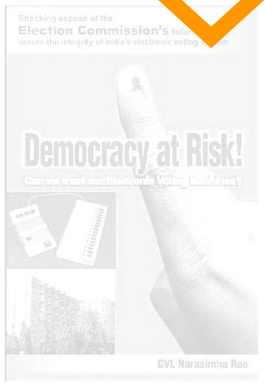
Remotely Altered Control Unit Display

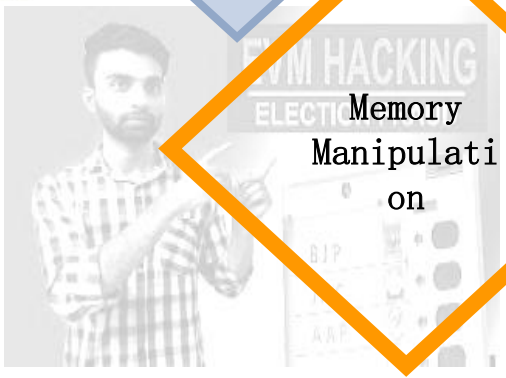
Memory Manipulation

Replaced Microcontroller or Memory chips

Altered software code

International Comparison





NO POSSIBILITY OF EVM HACKING

'Hacking' is unauthorised access to or control over computer network security systems for some illicit purpose.

In the case of ECI EVMs, the word **'Hacking' is not applicable** for following reasons:

- The EVM is a **stand-alone** machine and is not connected to any network through wire or wirelessly.
- The SW programme in the OTP Microcontroller can **neither be read nor modified.**

NO POSSIBILITY OF REMOTELY ALTERED DISPLAY THROUGH WIRELESS COMMUNICATION

It is alleged this can be done by either replacing the original display module with another display fitted with a wireless device or inserting an extra circuit board which can communicate with an external unit via a wireless device and tamper the result by controlling the CU display used for declaring the result.

- Such a modification would require unfettered access to the EVM after FLC – **Ruled out.**

MEMORY MANIPULATION RULED OUT

- It is alleged that voting data can be altered by clipping a Memory Manipulator IC to the memory chip where Vote data is stored.

➢ This would need,

- Full and free access to CUs after the Polling is over- Ruled Out !!
- Breaking the seals and locks of the strong room in the presence of two layers of security plus the representatives of the candidates camping near the strong room- Ruled Out !!

REPLACEMENT OF MICROCONTROLLER/MEMORY CHIP or MOTHERBOARD IMPOSSIBLE

Administrative Safeguards

- Chip replacement would require access to EVM Warehouses – Ruled Out.
- Any chip replacement before FLC will get caught during FLC.
- Chip Replacement after FLC would require access to Strong Rooms and breaking of EVM Pink Paper seals– Ruled Out.

Technical Security

- BUs and CUs communicate only amongst themselves and go into error mode if connected to any other machine. Thus, any modified EVM (with microcontroller /memory changed) would not be usable even if someone is able to hypothetically bypass security arrangements and modify EVM.

TAMPERED SOURCE CODE "TROJAN" RULED OUT

- It is alleged that Trojan can be introduced in the following manner
  - by reprogramming the chip, or
  - by the chip manufacturer during fusing of the software.

- ➢ Re-programming **Ruled Out** as these are OTP chips.
- ➢ Code tampering by the chip manufacturer **Ruled Out** as it will get caught during the code integrity check.

NO POSSIBILITY OF VOTE STUFFING AFTER POLL CLOSURE

Administrative safeguards

- Poll closed by pressing the "CLOSE" button on the CU after last vote, Representatives of candidates who are present signs on the seals.
- EVM seals checked on counting day.

What if seals broken and votes stuffed while transporting?

- EVM does not accept any votes after CLOSE button pressed in CU.

What if CLOSE button not properly pressed and Votes Stuffed while transporting?

- Poll Closure time recorded in the PO's diary and any votes polled in the EVM after this time can be identified due to time stamping of key presses.

DEFECTIVE VS TAMPERED

DEFECTIVE/NON-FUNCTIONING VS MANIPULATION/TAMPERED (1/2)

- **Tampered** machine is one which would behave in a predefined biased manner to favor someone.
- **Malfunctioning** machine is one which would randomly behave erroneously, but without a predefined biased manner.
- **Defective or Non-functioning** machine is one which becomes in-operative.
- While 1-2% EVMs may become Defective/Non-functional (and are replaced with good EVMs), **no case of Malfunctioning EVM (i.e. one recording wrong vote) ever reported.**
- **Question of Tampering absolutely ruled out** due to several layers of technical and administrative safeguards.

DEFECTIVE/NON-FUNCTIONING VS MANIPULATION/TAMPERED (2/2)

Defective/Non-functional	Manipulation/Tampering
An EVM can be said defective/non-functional, if they do not work due to any mechanical/electronic fault.	An EVM can be said manipulated/Tampered, if someone has made unauthorised alteration to interfere in its working. The same is ruled out due to technical security implemented in EVM and administrative safeguards prescribed by ECI.
Dictionary meaning- 'Failing to work or function properly'.	Dictionary Meaning- 'to interfere in an illegal & disruptive manner or to make alterations or adjustments, especially secretly so as to subvert an intended purpose or function.
EVMs, like any other machines can become non functional. Such defects get detected during the 3 mock polls and are replaced.	A tampered EVM must behave in a pre-defined and biased manner to favour a particular candidate and this partisan behaviour of the machine must be replicable/demonstrable.
All such defective EVMs are promptly removed from the election process and replaced with a full functional EVM.	No evidence of any incident of any EVM Tampering, ever has been produced.

DEFECTIVE EVM PROTOCOL

Defective EVMs

EVMs that fail to function due to any mechanical, structural or physical defect like faulty switches, broken button, faulty connections etc.

However, these **NEVER record Wrong Vote**.

- EVMs are checked for defects 3 times - during FLC, candidate setting, before start of poll.
- Serial Numbers and defects of these EVMs are noted and EVMs are sent to the manufacturers for analysis and repair.
- Manufacturers follow same security protocols during repair as they do for manufacturing new EVMs.

Electronic Voting in Other Countries

VARIOUS FORMS OF ELECTRONIC VOTING IN OTHER COUNTRIES

Electronic Voting (Fully /Partially)

- 19 Countries using electronic voting in some form through EVMs (Direct Recording Machines), some with Paper Trail.
- India, USA, Canada, Australia, Belgium, Bulgaria, Italy, Switzerland, Mexico, Brazil, Chile, Peru, Venezuela, Armenia, Namibia, Nepal, Bhutan, Bangladesh.

Electronic Counting

- 13 Countries are using e-technology for counting of votes
- Argentina, Brazil, Venezuela, Dominican Republic, Lithuania, Bulgaria, Belgium, Australia, South Korea, Philippines, Mongolia, Bhutan, Namibia.

Country Specific Details

Other countries using EVMs (DRMs):

USA, Australia, Belgium, Bulgaria, Italy, Switzerland, Canada, Mexico, Argentina, Brazil, Chile, Peru, Venezuela, Namibia, Nepal, Bhutan, Armenia, Bangladesh.

❖Currently, in the **USA**, the Direct Recording Machines are used in 27 states, among which paper audit trails are used in 15 states.

❖The other voting methods include: **Optical Scan Paper Ballot Systems, Ballot Marking Devices, and the Punch Card Ballot.**

Why Some Countries Discontinued Electronic Voting

ECI EVM	Foreign EVM
Standalone	Mostly networked
Manufactured in Premium PSUs	Manufactured entirely by private entities
Verified and certified by an independent Technical Experts Committee	No such robust and independent certification/ checks
Data is stored internally and not transferrable by any device	Voting data recorded in the DRM is transferred by means of CD, etc
Full end to end security protocol and administrative safeguards for the use, storage, transportation and tracking	No such protocols, e.g. in Ireland
Administrative and physical security as per legal framework across the country.	No such legal framework, e.g. in Netherlands
Voter verifiability and auditability of every vote cast	Lack of such facility in the NEDAP machines- un-Constitutional by German Supreme Court as lacked public examinability