EVM Hacking demonstration

Why in news?

\n\n

In Delhi Assembly on May 9th, the Aam Aadmi Party (AAM) legislator used an electronic voting machine (EVM) prototype to highlight a possible hacking of the actual EVM used by the Election Commission of India (ECI).

\n\n

What are arguments of the demonstrators?

\n\n

\n

- It registered votes for candidates and allowed for the ballot unit to display total votes polled by each candidates checked at the end of polling.
\n
- It also demonstrated that **the use of malicious code by a voter affiliated to a certain party could fix the results** to be different from the actual tally and in favour of that party and, demonstrated that the machine could be hacked.
\n
- It indicated that this is how EVMs are being hacked in the country and that it is easily possible to do the same with the ECI's EVMs.
\n
- The ECI as an authority is in charge of only certain aspects of safekeeping and monitoring of EVMs and that many others such as **procurement of microcontrollers from abroad, calibration of machines are done externally.**
\n
- It is in these stages that the manipulation can be done beforehand.
\n

\n\n

What is the real scenario?

\n\n

\n

- In reality, the ECI’s EVM does not allow for any Trojan horse (malicious code) enabled key presses.
  \n
- Only one key press on the ballot unit is allowed during the act of voting and recognised by the control unit, so the use of a secret code to lock the tally in favour of a party as alleged by the demonstration does not hold true in the case of the ECI’s EVM.
  \n
- For the demonstrated things to happen, a large-scale operation of changing the microcontroller embedded in every EVM to be used in an election is required.
  \n
- This is only possible if there is direct collusion between the ECI authorities who are in charge of storage, commissioning and allocation.
  \n
- Quality control checks are done during and after manufacture of EVM’s.
  \n
- The ECI's new models (M2 and M3) prevent tamper-proofing by time-stamping key presses and provide for encryptions and tracking software that handle EVM logistics.
  \n

\n\n

What is the way forward?

\n\n

\n

- EVM-hacking demonstration did not raise any relevant questions about the technical and procedural safeguards that are already in place and set by the ECI.
  \n
- The EVM needs to constantly evolve in order to remain secure and workable under any condition while at the same time keeping its operations simple.
  \n
- The answers to the present stability in the AAP’s electoral growth lie in the application of its politics and not in technology.
  \n
- The solution to the AAP’s problems lies in politics, not wild accusations about EVMs.
  \n

\n\n

\n\n

Source: The Hindu

\n