Challenges behind hacking EVM

What is the issue?

\n\n

The claims of hacking Electronic Voting Machine (EVM) are raising andit is important to look at some of the fundamental technical elements of EVM hacking.

\n\n

What is the underlying mechanism?

\n\n

- \n
- There are two ways by which an electronic device can be hacked - wired and wireless.
- \n
- In order to hack a machine, the best way is to establish a wired link with its control unit and the microprocessor can do basic mathematical operations based on the given input.
- \n
- The information fed to the system is processed by the control unit and the output is sent to the memory of the system, which can be read or retrieved at a later stage.
- \n
- Hacking a device through a wired connection essentially means designing another electronic device, which is able to send a specific pattern of information to the device’s control unit.
- \n
- In a demonstration at the University of Michigan, scientists used this kind of hacking in the context of an EVM.
- \n
- In that demonstration, they used a specifically designed chip that was physically plugged into its control unit.
- \n
- However, in wireless hacking, you do not need a physical connection with the device.
- \n
- But a basic understanding of the control unit or the target device and its operational instructions is still needed.

\n

\n\n

What are the challenges?

\n\n

\n

- In order to hack a device using a wireless link, the device needs to have a radio receiver which comprises an electronic circuit and an antenna.
  \n
- The Election Commission claims that EVMs do not have any such circuit element.
  \n
- Even when an electronic circuit (transceiver), which is ultra-small, is designed and is artificially inserted in an EVM, one would need millions of such specifically designed transceiver sets, plugged into the control unit of each EVM.
  \n
- Also, such advanced electronic devices are extremely complex and cannot be bought easily.
  \n
- There are only around half a dozen companies in the world with the expertise to design and fabricate such a device at the chip level.
  \n
- The designers would also need access to the actual circuit board of the EVM in order to design the electronic interface.
  \n
- Also, the overall cost of getting such devices in millions for each EVM is very expensive.
  \n
- One would also need a specifically designed antenna, which interfaces with the transceiver circuit.
  \n
- Though, transceiver circuits can be miniaturised and can remain hidden from our eyes, theantenna would always remain visible due to its size.
  \n
- Thus, it is almost impossible to hide the antenna, which will always stick out of the system in order to ensure a seamless wireless link.
  \n
- Considering all this, large-scale deployment of such a technology would be a huge project in itself, where the Election Commission, EVM manufacturers as well as chip-making companies would be involved.
  \n

\n\n

Can paper-based voting be an effective alternate?

\n\n

\n
- Paper-based voting is not a solution for faults in EVMs because it is even more susceptible to being hacked.
\n
- This susceptibility might be through booth capturing, artificial manipulation of ballots, change of ballot paper, and many different ways.
\n
- In the current age, where printers and computers are readily available, it would take a couple of hours to duplicate ballot papers, print them and dispatch them with miscreants to the specific voting booths.
\n
- Western countries that have refused to opt for EVMs are small, have a small number of voters, and have strong policing systems that prevent manual hacking and manipulation of ballots.
\n
- Thus, India should address the defects of EVMs, if at all needed, rather than going back to the previous mode of voting.
\n

\n\n

\n\n

Source: The Indian Express

\n