Security Analysis of India's Electronic Voting Systems

Scott Wolchok, Wustrow, Halderman (UMich), Hari K. Prasad, Kankipati, Sakhamuri, Yagati (NetIndia), Rop Gonggrijp

"Reaffirm it's belief in the infallibility of the EVMs"

Goals

- To evaluate the claims of the Indian Election Commission that the EVM is "infallible" and "tamper-proof"

- Show the significant vulnerabilities in the EVMs and possible attack vectors

Electronic Voting in India

- The first EVMs proposed in the 1980s but were not adopted nationwide
- However, the systems style is used to this day
- The first nationwide EVMs were used in the 90s and have been updated a few times

Electronic Voting in India

- The Election Commission brought together a committee of engineers
- They assured the committee that the machine was completely secure

Electronic Voting in India

- The Election Commission brought together a committee of engineers

- They assured the committee that the machine was completely secure

- "Today the Commission once again completely reaffirms its faith in the infallibility of the EVMs. These are fully tamper-proof, as ever"

Electronic Voting in India

- The Election Commission brought together a committee of engineers
- They assured the committee that the machine was completely secure
- "Today the Commission once again completely reaffirms its faith in the infallibility of the EVMs. These are fully tamper-proof, as ever"
- Unfortunately, none of the committee members had any security background

Challenges for Voting Machines in India

- Cost for mass production

Challenges for Voting Machines in India

- Cost for mass production
- Illiteracy

Challenges for Voting Machines in India

- Cost for mass production
- Illiteracy
- Lack of Reliable power

Challenges for Voting Machines in India

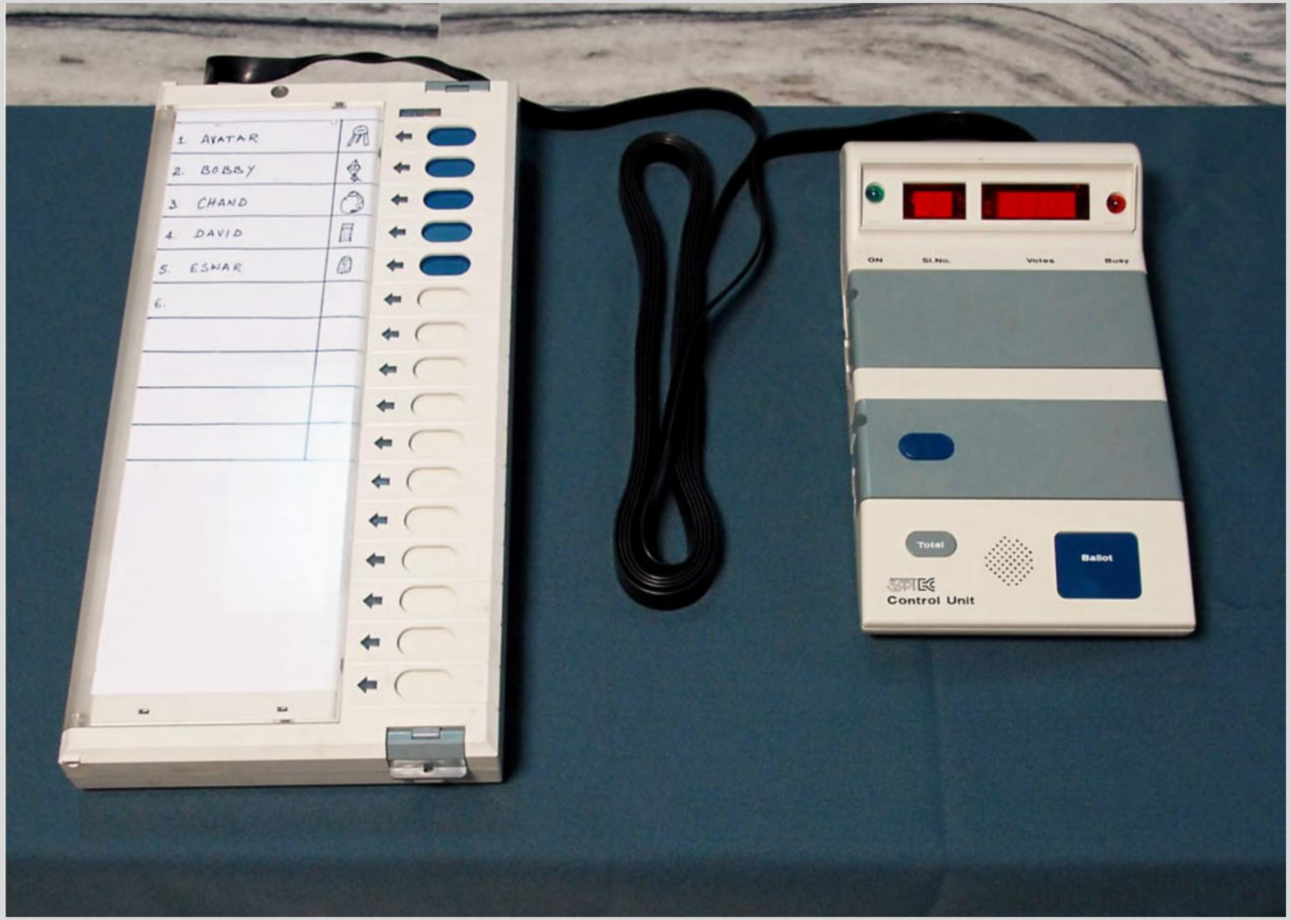
- Cost for mass production
- Illiteracy
- Lack of Reliable power
- Technology intimidation

Challenges for Voting Machines in India

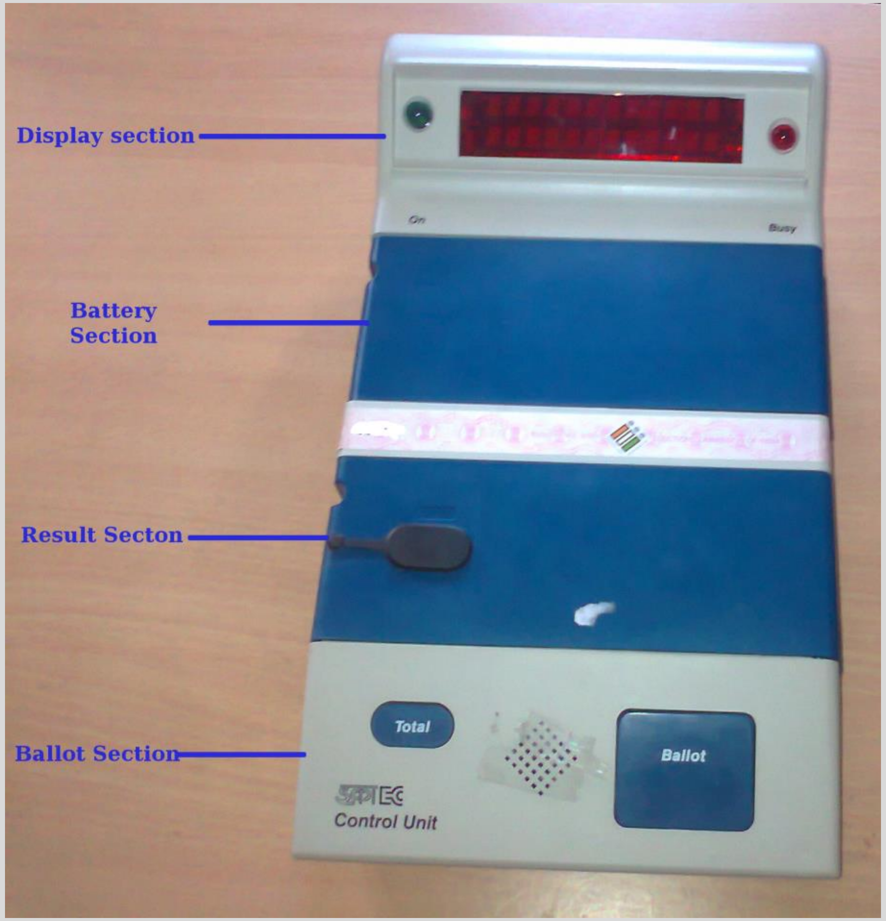
- Cost for mass production
- Illiteracy
- Lack of Reliable power
- Technology intimidation

- Any solution needs to be able to stand up to these requirements

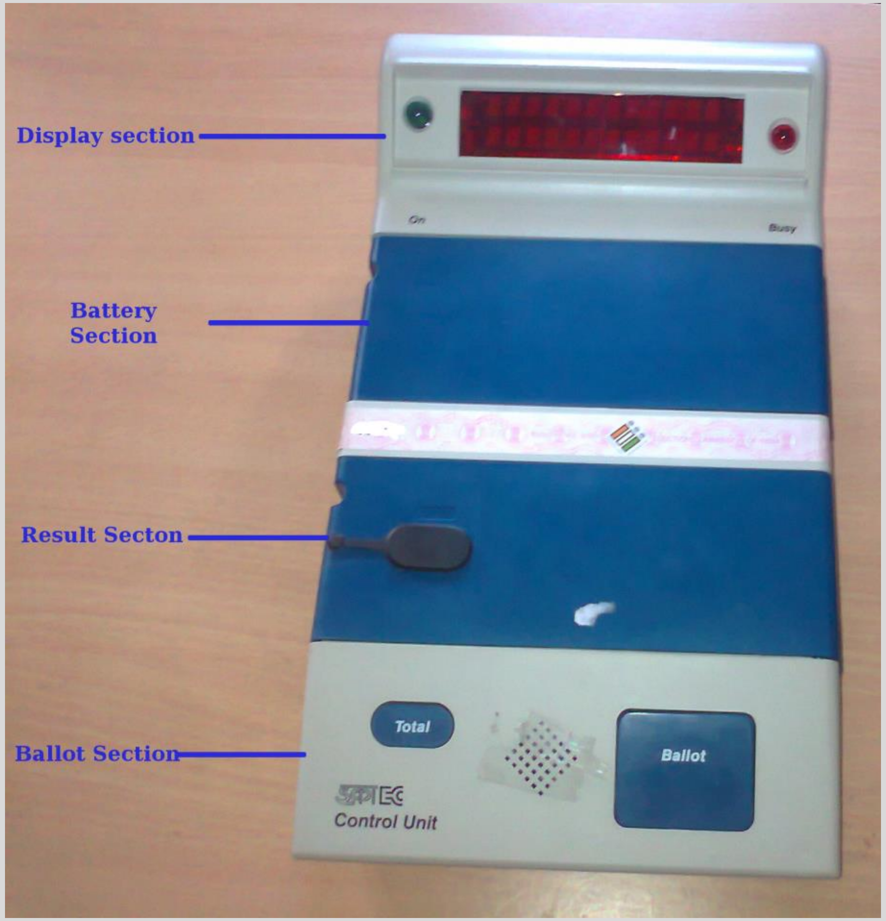
EVM Operation

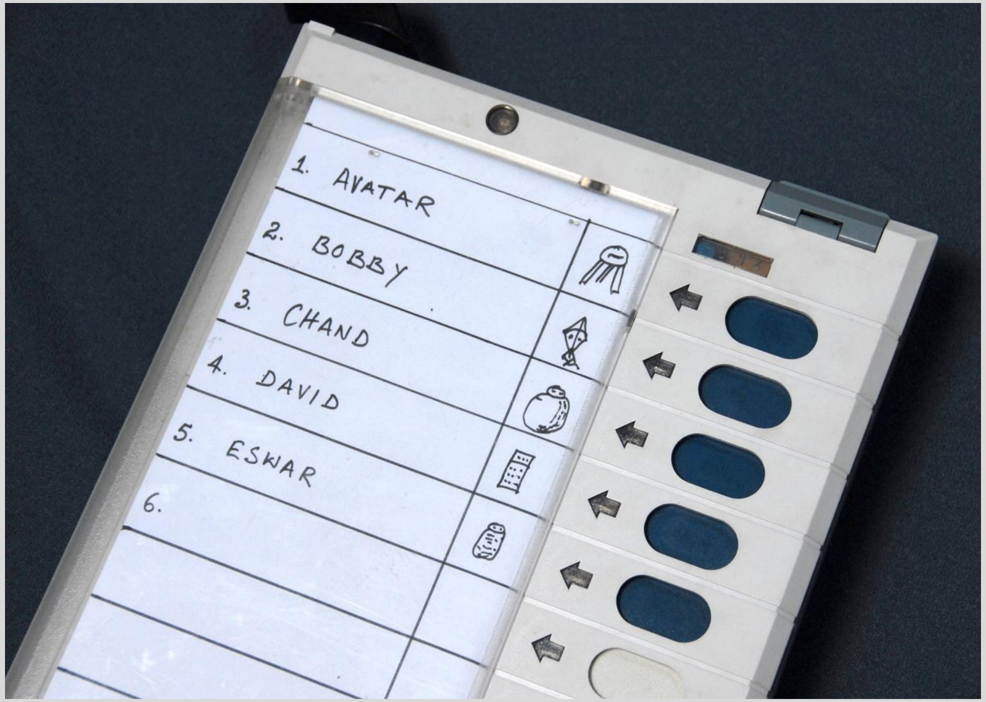


Consist of 2 Parts

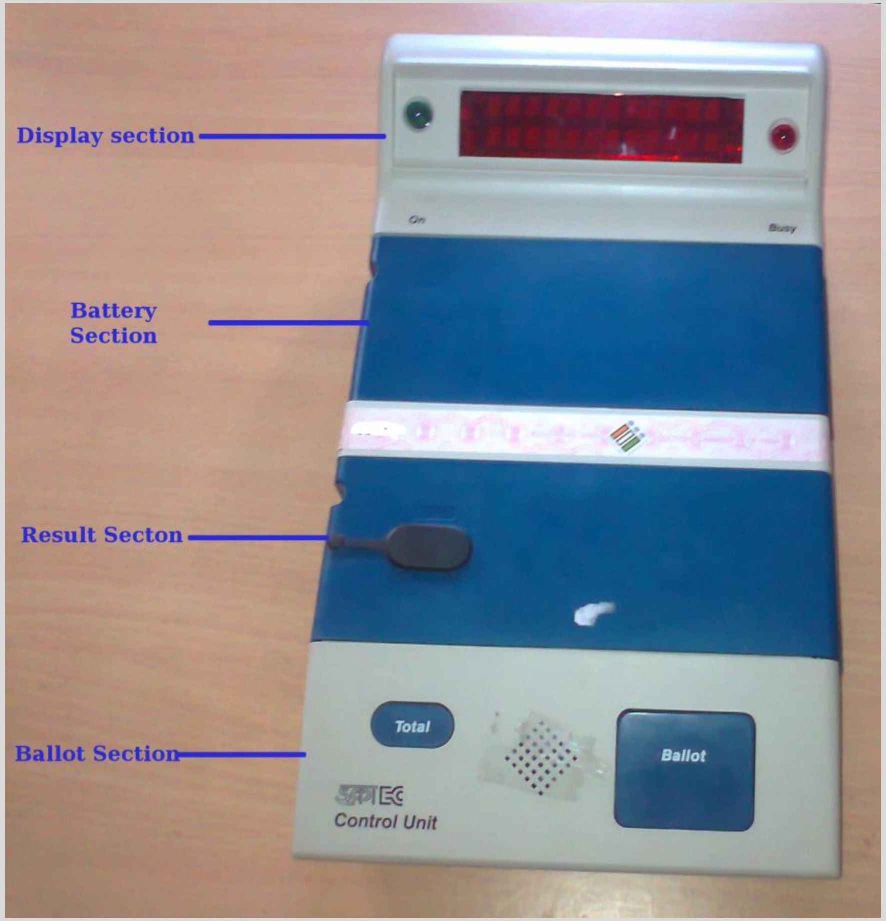


Consist of 2 Parts





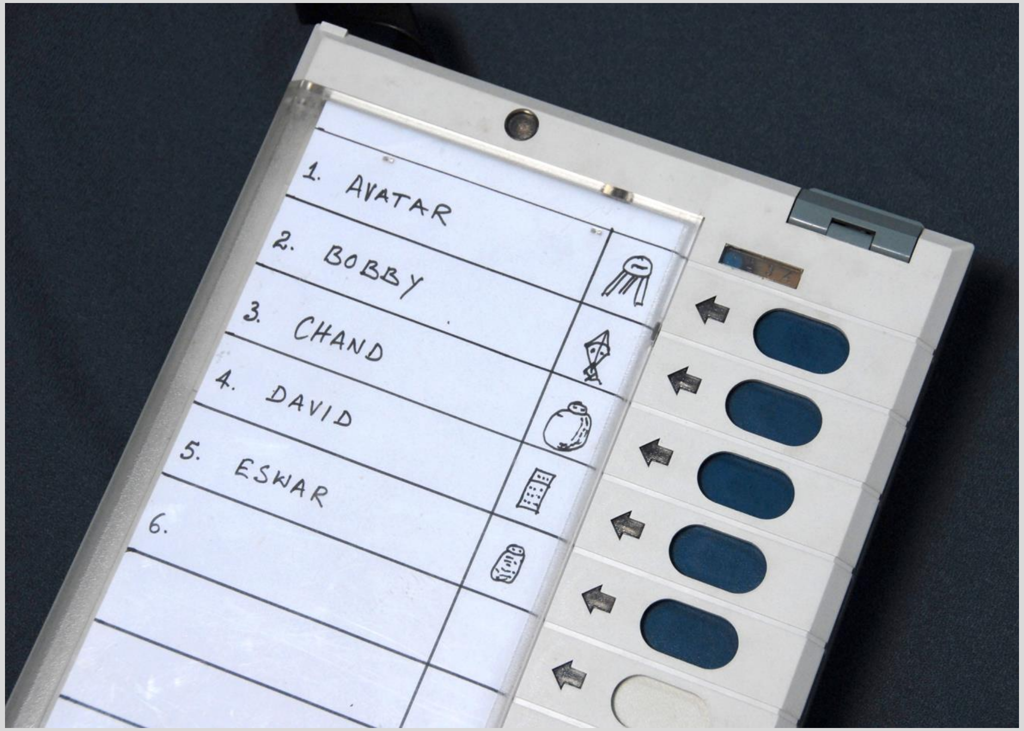
Control Unit



- Holds a microprocessor that controls the ballot machines
- Built in 7-segment LEDs for candidate # and vote count
- Constantly polls the ballot machine the check if there is a new vote

Ballot Machine

- Lists the candidates in the election
- Relays information back to the control unit
- Uses two EPLDs instead of a CPU to interpret control signals
- Gives visual and audio feedback to confirm correct vote (a red light and a beep)



Software

- Software is installed in order to be permanent and secret
- But can't be read or written to

- Is it gone forever?

Software

- Software is installed in order to he electronically erasable
- But can't be read or written too

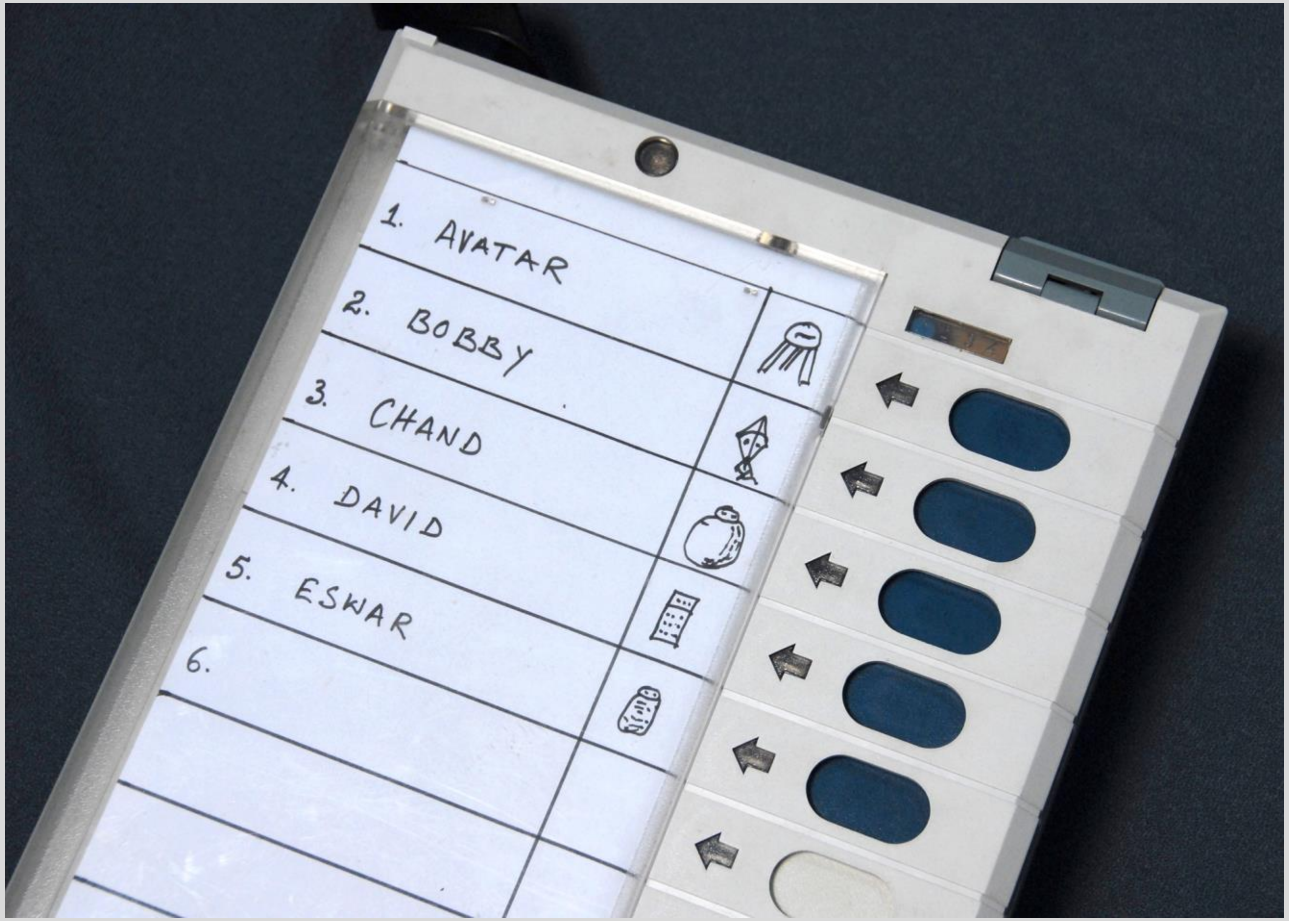
- No

- A well funded adversary can examine the chip under a microscope

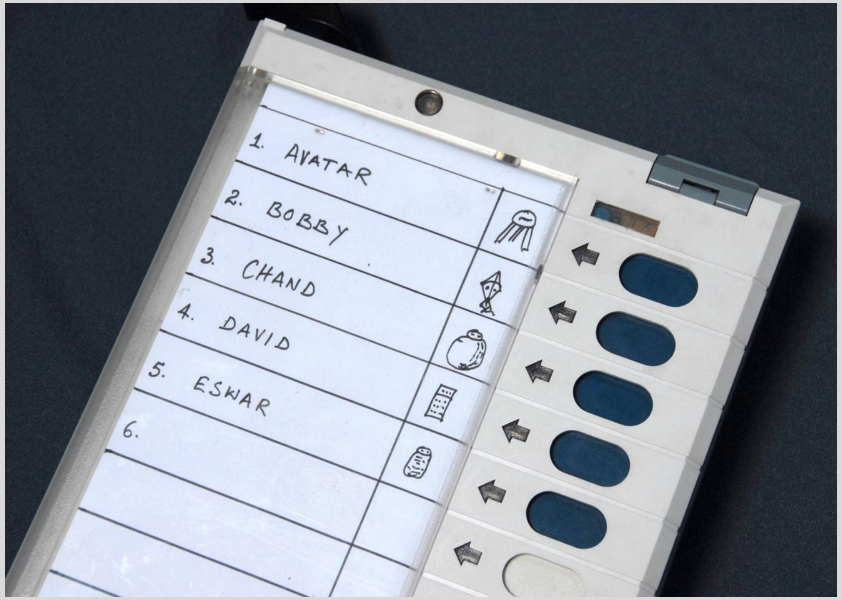
Pre-Election Process

- Election officials place paper names for the candidates in the ballot machine

- Name and party (logo)



Pre-Election Process



- # of candidates entered into the control unit
- A public mock election is held
- Publicly zero the ballot count in the control unit
- Machines are sealed to prevent tampering

Pre-Election Process

- # of candidates entered into the control unit
- A public mock election is held
- Publicly zero the ballot count in the control unit
- Machines are sealed to prevent tampering

Election – Ballot

- Voters are identified and given a black mark to prevent double voting
- In the booth:
  - A green light indicates 'ready'
  - Press the button for the candidate of your choice
  - A beep confirms you voted
  - A red light shows who you voted for

Election – Control Unit

- Press the ballot button to start allowing ballots
- The control unit queries each ballot machine
- Ballot machine checks EPLD (electronically programmable device) for a cast vote
- If yes, send vote to control unit
- If no, query the next ballot machine

How can this system be compromised?

Tampering with Software

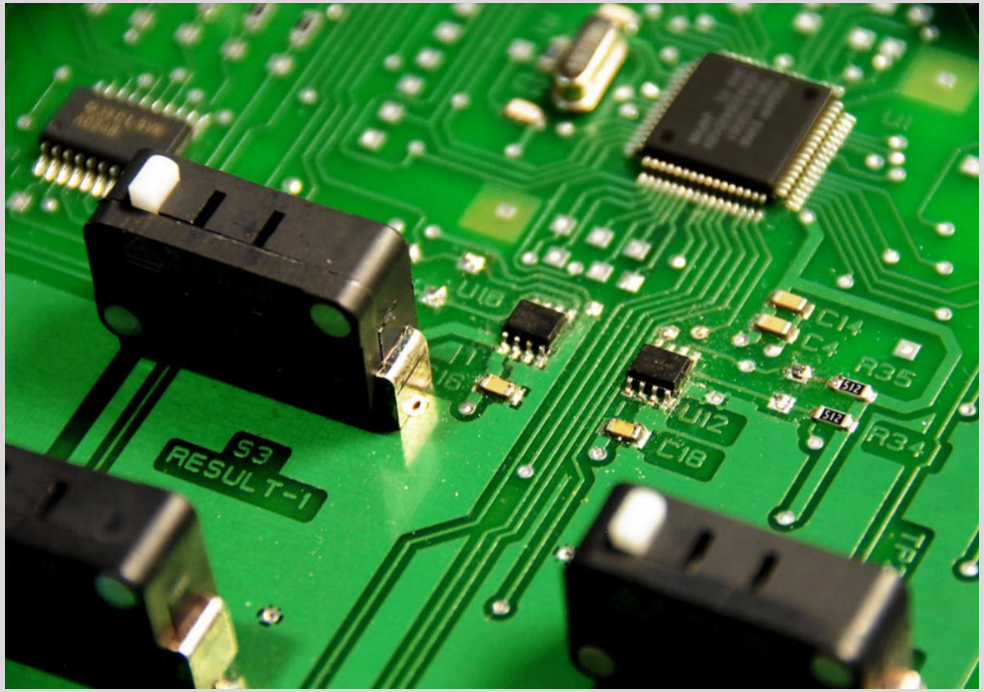
- Despite the fact that the software is not readable or writable, manufacturer or employees can compile different code
  - Without much chance of being caught

- For a well funded adversary, the chip can also be taken apart and examined under a microscope

- Reverse engineering from there is relatively straightforward

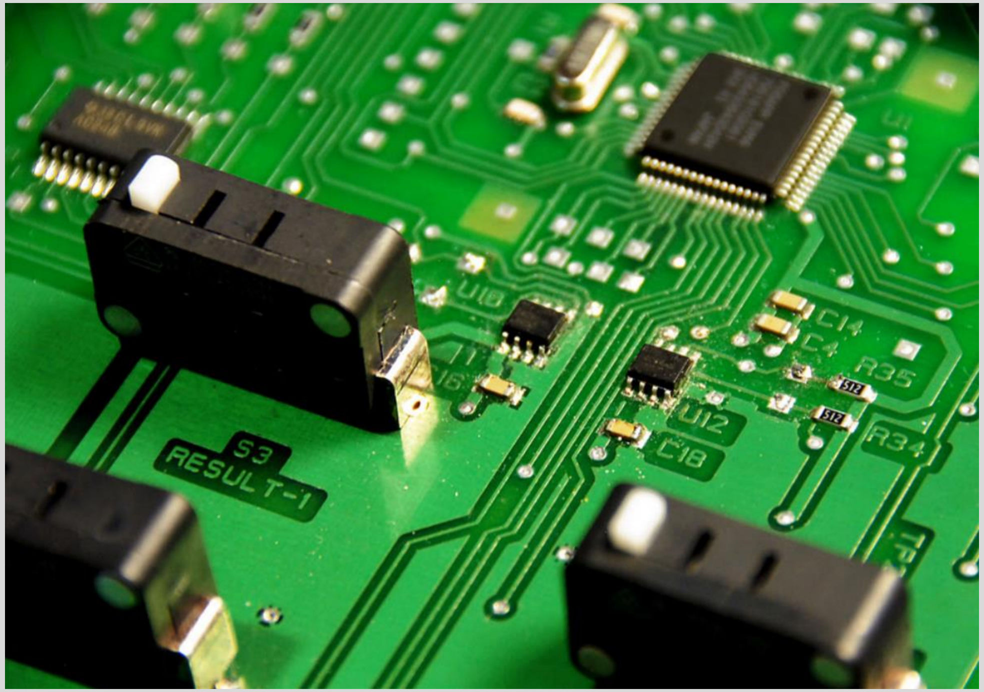
Substitute the CPU

- One of the claims made by the commission that evaluated these were that visual inspection would make attacks obvious



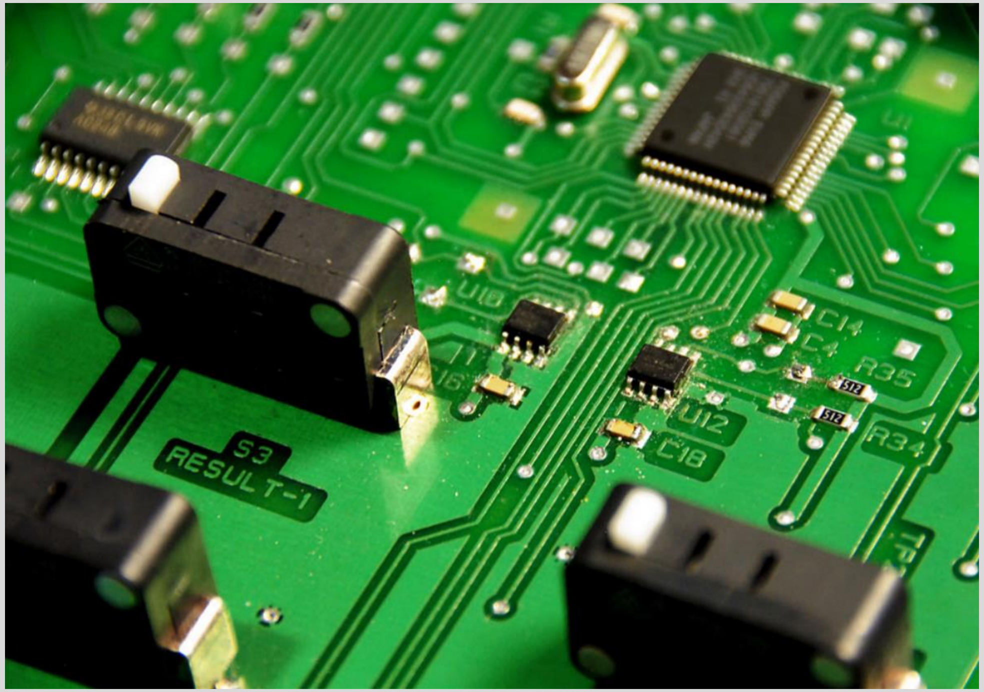
Substitute the CPU

- One of the claims made by the commission that evaluated these were that visual inspection would make attacks obvious
- But if the CPU is swapped at assembly, or in the supply chain, or by corrupt employees it's hard to detect
- Even harder to at the polling place since it is enclosed in a casing



Substitute the CPU

- The CPU can be programmed to miscount the votes when tallied
  - EPLDs on the ballot machine too
- Since there is no cryptography used, altering data is trivial and leaves no trace of misconduct
- Its simple design and commodity hardware makes it easy to replicate functionality

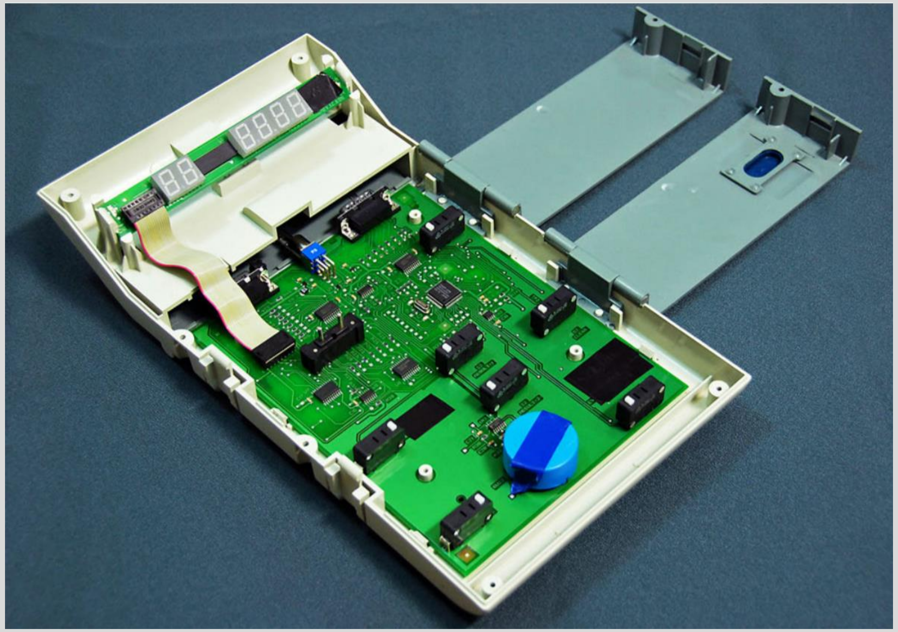


One Step Further – Swap the entire board

- Swapping the CPU requires soldering and some non-trivial effort

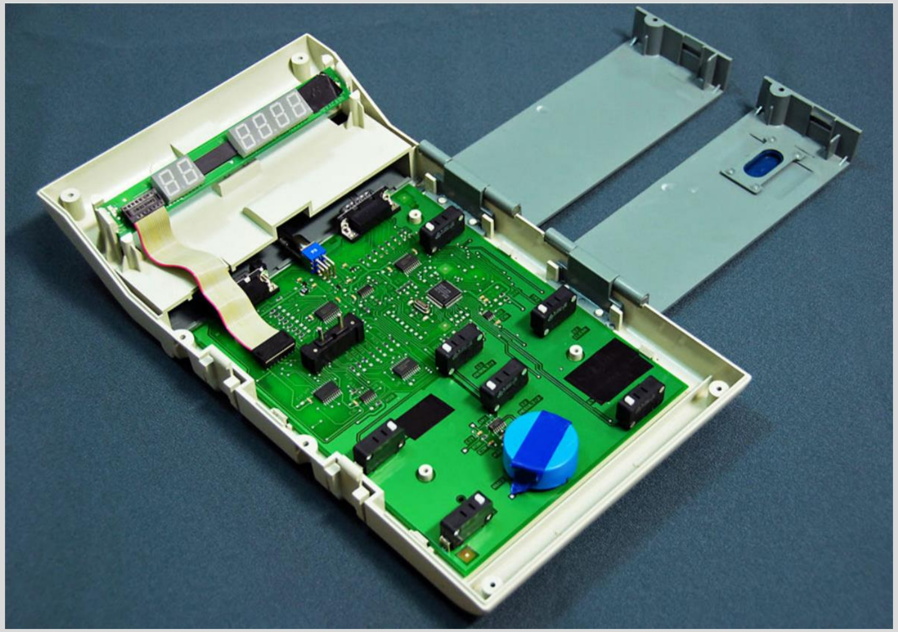
- A new board is easier to manufacture and trust between devices makes it easy

- With the simple design of the EVM, replicating the functionality of the control unit is not difficult



Swap the Entire Board – How?

- Between the election period and the tallying period, an adversary could replace a few voting machines
- Between elections, EVMs were stored in places like high schools and insecure warehouses
- Getting access during this time is possible



Swap the Whole Thing

- Without any authenticity checks, swapping the device would also go unnoticed
  - But hard to replicate plastic housing of board

Tampering with the State

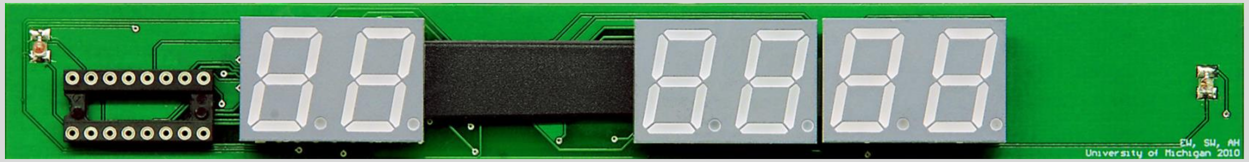
- Electrical components on either machine or between the two machines can be attached to modify device communication
- Masking/simulating votes
- Reading directly from EEPROM

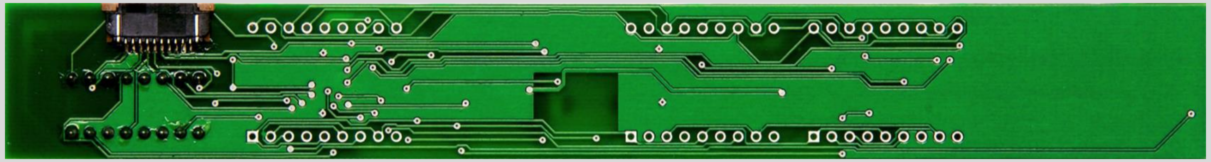
Attacks Carried Out

Dishonest Display – What

- Add a separate, hidden microcontroller to the board that changes the output of the LED

- Instead of modifying the voting operation, just change what the official sees by calculating incorrectly

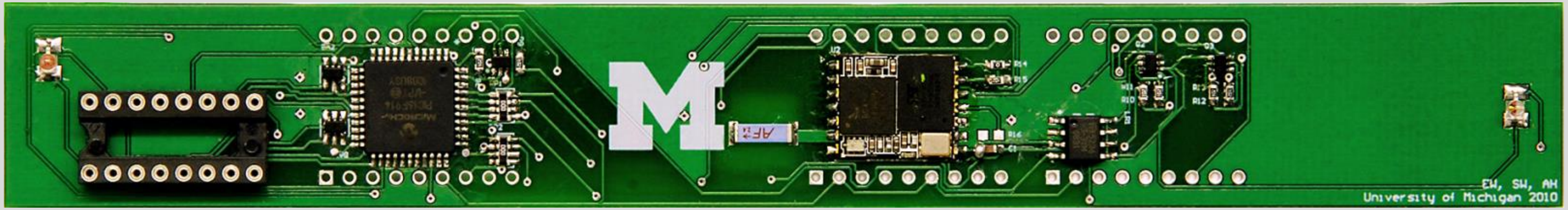




Dishonest Display – What

- A microcontroller with other parts can be swapped any point before the votes are tallied, perhaps years before

- Manufacturer maintenance or election insiders routinely have access to machines



Dishonest Display – How?

- A microcontroller, bluetooth module and a chip antenna circuit is added
  - Power supplied by EVM

- Hidden underneath the existing LEDs with 2mm clearance
  - Microcontroller reads select lines for

    for the LEDs

- Circuit tracks the total number of votes

Dishonest Display – How?

- A signaling mechanism over Bluetooth radio is used to choose favored candidate
  - Can be performed by ordinary phones

- The device looks for device with name "MAGIXX"

- The PIC stores the candidate in non-volatile memory until tallying

Dishonest Display – Detection?

Dishonest Display – Detection

- To combat tallies that look fraudulent an algorithm is created to calculate how many votes to steal

- Minimum threshold of votes
- Maintain consistency properties of reported results
- Enough that people can disclose their votes

- Subtract proportional amount from each candidate and add to favored candidate

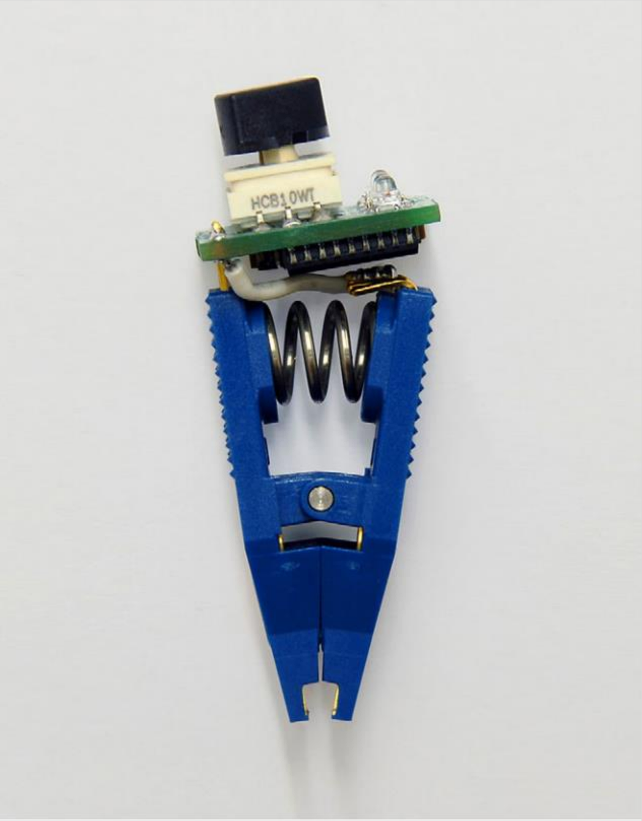
Clip-on Memory Manipulator – What

- The votes are stored in EEPROM on the control unit once the voting is complete

- A large gap between voting and tallying leaves the units vulnerable to tampering

- Tamper with the memory in EEPROM to modify/extract the ballots

- Data is stored sequentially and unencrypted



Clip-on Memory Manipulator – How?

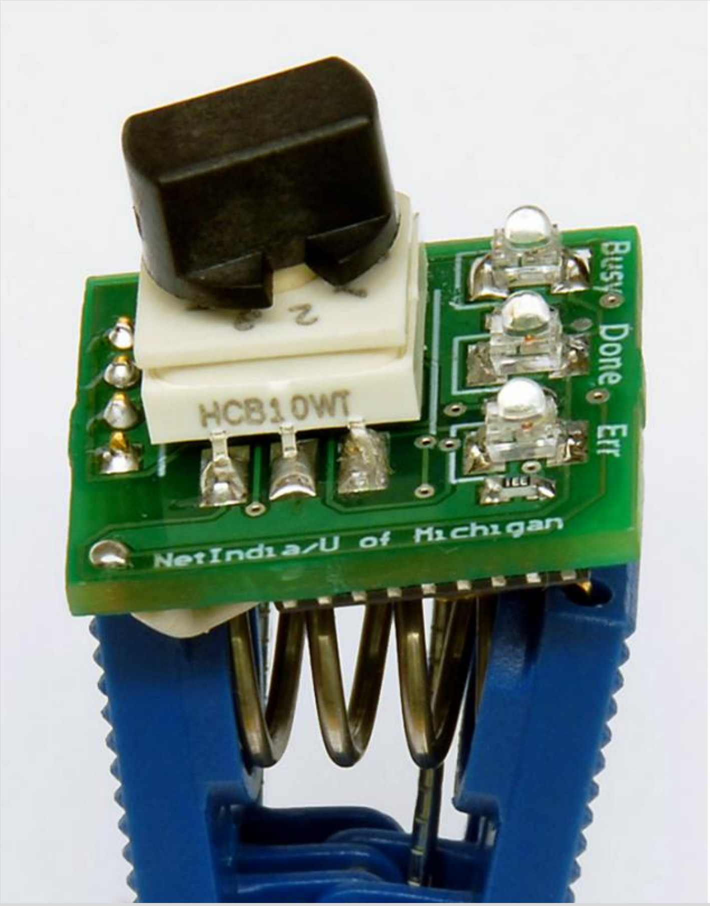
- I2C serial protocol is used for communication between CPU and EEPROM

- By holding the CPU in reset state, I/O signals are forced high-Z, allowing communication even when not in use

- A microcontroller clip is attached to the pins of the EEPROM and gets power from the EVM

Clip-on Memory Manipulator – Stealing Votes

- The clip has a rotary to choose a candidate to favor and modify their tally
- A vote stealing program computes how many votes to steal and rewrites the ballots
- Program handle failures by writing to one array at a time and marking dirty bits



Clip-on Memory Manipulator – Secrecy

- Ballots are stored in EEPROM in the order they are cast
- Attacker can examine public register to discover the order of voters
- Correlating the two completely compromises voter secrecy

Apparent Safeguards

- It's hard to compromise a million machines

Apparent Safeguards

- It's hard to compromise a million machines
    - Tightly contested elections can determine majority in parliament

Apparent Safeguards

- It's hard to compromise a million machines
    - Tightly contested elections can determine majority in parliament
- Physical security from personnel

Apparent Safeguards

- It's hard to compromise a million machines
  - Tightly contested elections can determine majority in parliament
- Physical security from personnel
  - Stored insecurely between elections

Apparent Safeguards

- It's hard to compromise a million machines
  - Tightly contested elections can determine majority in parliament
- Physical security from personnel
  - Stored insecurely between elections
- Tamper-evident seals

Apparent Safeguards

- It's hard to compromise a million machines
  - Tightly contested elections can determine majority in parliament
- Physical security from personnel
  - Stored insecurely between elections
- Tamper-evident seals
  - Known to be easy to break and fake

SEALING OF EVM

FIXING OF STRIP SEAL

Apparent Safeguards

- It's hard to compromise a million machines
  - Tightly contested elections can determine majority in parliament
- Physical security from personnel
  - Stored insecurely between elections
- Tamper-evident seals
  - Known to be easy to break and fake
- Mock elections

Apparent Safeguards

- It's hard to compromise a million machines
  - Tightly contested elections can determine majority in parliament
- Physical security from personnel
  - Stored insecurely between elections
- Tamper-evident seals
  - Known to be easy to break and fake
- Mock elections
  - Attacker can wait to signal after mock election

Conclusions - Contributions

- Claims made by the Indian Election Commission can't be backed up
  - EVMs are easy to tamper with and inherently insecure
- The device's simplicity make modifying it very easy
  - Mimicking functionality becomes easy
- The 'shows' of security (security theater) from mock elections and tamper-proof seals only lead to complacency

Discussion

- Machines in India face challenges not found in the US. With lack of electricity and unpredictable weather, how do you meet the needs of security while remaining simple?

- Given the number of machines needed, how do you achieve the security without costing too much money? (Current DREs in the US cost thousands of dollars)

- Is it better to go back to older forms of ballots rather than creating new attack vectors in machines under the above constraints?

1. AKHTAR
2. BOBBY
3. CHAND
4. DAVID