2012 International Conference on Information and Network Technology (ICINT 2012)
IPCSIT vol. 37 (2012) © (2012) IACSIT Press, Singapore

Improvement on Exiting Indian EVMs

Manish Shrivastava [+] and Anita Khanna

Institute of Technology, Guru Ghasidas University, Bilaspur

Abstract. Elections in India are conducted almost exclusively using electronic voting machines developed over the past two decades by a pair of government-owned companies. These devices, known in India as EVMs, In this paper, I proposed some improvement on exiting EVM, I describe the machine's design and operation in detail, and evaluate possibilities of manipulation on EVM which could be carried out by dishonest election insiders or other criminals with only brief physical access to the machines. Because of these problems associated with EVM, it is necessary to modify and improve the EVMs by which we can secure about voting as well as stop any kind of manipulation and also stop booth capturing. The proposed modification and improvement is done by self authentication by the voter itself on EVM. This case study carries important lessons for Indian elections and for electronic voting security more generally.

Keywords: EVM, control unit, authentication .

1. Introduction

Electronic Voting Machine (EVM) retains all the characteristics of voting by ballot paper, while making polling a lot more expedient. Being fast and absolutely reliable, the EVM saves considerable time, money and manpower. Indian election authorities continue to insist that the electronic voting machines used in India, widely referred to as EVMs, are fully secure. For example, the Election Commission of India, the country's highest election authority, asserted in an August 2009 press statement: "Today, the Commission once again completely reaffirms its faith in the infallibility of the EVMs. These are fully tamper-proof, as ever" [8]. As recently as April 26, 2010, Chief Election Commissioner Navin B. Chawla was quoted in the media as saying the machines were "perfect" with no need for "technological improvement" [12].In this paper, I proposed some improvement on EVM. First There are possibilities for manipulating voting (bogus voting) on EVMs, with the involvement of dishonest field-level poll officials and candidate agent. Second, we know that Booth Capture a serious threat against paper voting before the introduction of EVMs was booth capture, a less-than-subtle type of electoral fraud found primarily in India, wherein party loyalists would take over a polling station by force and stuff the ballot box. Better policing makes such attacks less of a threat today, but the EVMs have also been designed to discourage them by limiting the rate of vote casting to five per minute [1].but there is still chance of booth capturing, because of these problems associated with EVM, it is necessary to modify and improve the EVMs by which we can secure about voting as well as stop any kind of manipulation and also stop booth capturing. The proposed modification and improvement is done by self authentication by the voter itself on EVM.

2. Background

2.1. Electronic voting in India

The Election Commission of India developed the country's EVMs in partnership with two government-owned companies, the Electronics Corporation of India (ECIL) and Bharat Electronics Limited (BEL) [50,

[+] Corresponding author. Tel.: + 91-9827116390 ;fax: +91-7752-260148.
E-mail address: manbsp@gmail.com.

pp. 1,9]. Though these companies are owned by the Indian government, they are not under the administrative control of the Election Commission. They are profit-seeking vendors
that are attempting to market EVMs globally [11].

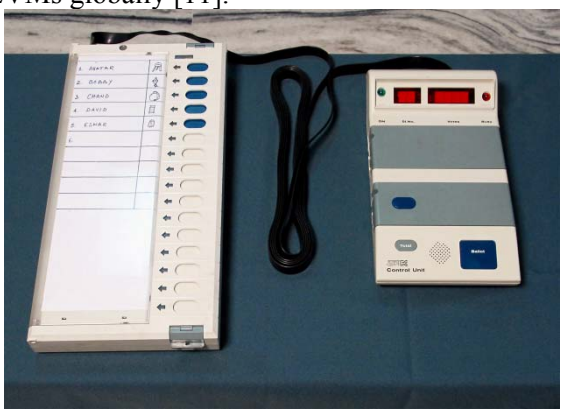

Fig. 1: Indian EVMs consist of a BALLOT UNIT used by voters (left) and a CONTROL UNIT operated by poll workers (right) joined by a 5-meter cable. Voters simply press the button corresponding to the candidate of their choice.

The first Indian EVMs were developed in the early 1980s by ECIL. They were used in certain parts of the country, but were never adopted nationwide [50, p. 1]. They introduced the style of system used to this day (see Figure 1), including the separate control and ballot units and the layout of both components. These first-generation EVMs were based on Hitachi 6305 microcontrollers and used firmware stored in external UV-erasable PROMs along with 64kb EEPROMs for storing votes. Second-generation models were introduced in 2000 by both ECIL and BEL. These machines moved the firmware into the CPU and upgraded other components. They were gradually deployed in greater numbers and used nationwide beginning in 2004 [50, p. 1]. In 2006, the manufacturers adopted a third-generation design incorporating additional changes suggested by the Election Commission.

Fig. 2: Counting Votes—The EVM records votes in its internal memory. At a public counting session, workers remove a seal on the control unit and press the RESULT I button (left) to reveal the results. The machine sequentially outputs the number of votes received by each candidate using a bank of 7-segment LEDs (right). Here, candidate number 01 has received 7 votes.

According to Election Commission statistics, there were 1,378,352 EVMs in use in July 2009. Of these, 448,000 were third-generation machines manufactured from 2006 to 2009, with 253,400 from BEL and 194,600 from ECIL. The remaining 930,352 were the second-generation models manufactured from 2000 to 2005, with 440,146 from BEL and 490,206 from ECIL [7]. (The first generation machines are deemed too risky to use in national elections because their 15-year service life has expired [1], though they are apparently still used in certain state and local contests.) In the 2009 parliamentary election, there were 417,156,494 votes cast, for an average of 302 votes per machine [14].

The EVM we tested is from the largest group, a second-generation ECIL model. It is a real machine that was manufactured in 2003, and it has been used in national elections. It was provided by a source who has requested to remain anonymous. Photographs of the machine and its inner workings appear throughout this paper. Other types and generations of machines have certain differences, but their overall operation is very similar. We believe that most of our security analysis is applicable to all EVMs now used in India.

2.2. EVM operation and election procedures

India's EVMs have two main components, shown in Figure 1. There is a CONTROL UNIT, used by poll workers, which stores and accumulates votes, and a BALLOT UNIT, located in the election booth, which is used by voters. These units are connected by a 5 m cable, which has one end permanently fixed to the ballot unit. The system is powered by a battery pack inside the control unit. The EVMs are designed for one- or two-race elections, as are typical in India; we describe single-race operation here. The ballot unit has 16 candidate buttons. If any are unused, they are covered with a plastic masking tab inside the unit. When there are more than 16 candidates, an additional ballot unit can be connected to a port on the underside of the first ballot unit. Up to four ballot units can be chained together in this way, for a maximum of 64 candidates. A four-position slide switch under the ballot unit door selects the unit's position in the chain.

Election procedures are described in a number of public documents (e.g., [5]). Prior to the election, workers set up the ballot unit by attaching a paper label that shows the names of the candidates and their party symbols (to aid illiterate voters) next to the candidate buttons. After sealing the label under a plastic door, workers configure the number of candidates using a CAND SET button on the control unit. On the morning of the election, poll workers perform a small mock election to test the machine. They then publicly set the 4 totals to zero by pressing the CLEAR button, after which the control unit display shows that a total of zero votes have been cast. Workers can check this count at any time by pressing the TOTAL button. Seals are then placed on various parts of the control unit to block access to counting and clearing functions until later in the election process.

When a voter arrives, workers verify his or her identity and record the voter's presence by obtaining a signature or thumb print. To prevent double voting, they mark the voter's right index finger with indelible ink [9]. Next, a poll worker presses the BALLOT button on the control unit to allow one vote. This causes a green READY light to glow on the ballot unit. The voter enters the polling booth and presses the button for the candidate of his or her choice. A red light next to the candidate button glows, the ready light turns off, and the control unit emits a loud beep to indicate that the vote has been cast. The red light then turns off automatically. This process repeats for each voter.

At the end of the poll, the presiding officer removes a plastic cap on the control unit and presses the CLOSE button, which prevents the EVM from accepting further votes. The ballot unit is disconnected and the control unit is placed in storage until the public count, which may occur weeks later.

On the counting day, the control units are delivered to a counting center. In public view, an election official breaks a seal on the control unit and presses the RESULT I button, shown in Figure 2. The display on the control unit shows a sequence of outputs: the number of candidates, the total votes, and the number of votes received by each candidate. Officials manually record the totals from each machine and add them together to determine the election result. The machines are then placed in storage until the next election.

3. Proposed System

Our aim is to modify and improve the Electronic Voting Machine by which we can secure the information about the voting as well as stop the any kind of tampering and also stop the mass forcing voting by the gangsters. The proposed modification to be done by self authentication by the voter itself on the EVM machines. The authentication process will be happen in two stages.

First stage authentication is through UID (Unique Identity Card)

Second stage authentication is through Finger print matching

If the voters pass through these two authentication process then he/she will get permission to cast their vote and the EVM machine will automatically activated to select the option in the ballot unit. All the data

will store in an integrated memory in an encrypted mode. For storing voting information in an encrypted mode, we have to increase the memory as well as we need to modify the software for secure encryption. Also we have to modify the Control unit on EVM by integrating the Finger print matching device and UID swapping machine.

4. Methodology

Our aim is to modify the CONTROL UNIT only not in the BALLOT UNIT. In the control unit we need to integrate two devices for authentication of the voter. One is for Swapping machine which will recognize the UID card of individual voters and another device is for scanning Thumb impression. For storing the information of voters of that particular booth we have to increase memory capacity. Also the authentication process will be verified from the database which is already stored in the memory earlier. For verification we have proposed here software modification in the EVM which will verify the thumb impression as well as UID card from database. If the voter is passed through the two stage authentication process he/she will get chance to cast their vote and the control unit will activate the ballot unit for selecting the option.

Methodology steps to improve the EVMs are as follows:

1. Integrate the UID Swapping Machine on the Control Unit of EVM
2. Integrate the finger print identification device (Scanning machine to scan the thumb impression) on the Control Unit of EVM.
3. Increase the Memory capacity.
4. Design a database for storing voter's information coming with UID.
5. Develop software which will verify the authentication process of voters.
6. High security encryption methods for secure information of the voters.

5. Conclusion

Despite elaborate safeguards, India's EVMs are susceptible to serious attacks. Dishonest insiders or other criminals with physical access to the machines. The design of India's EVMs relies entirely on the physical security of the machines and the integrity of election insiders. This seems to negate many of the security benefits of using electronic voting in the first place. Election commission should carefully reconsider to achieve a secure and transparent voting system that is suitable to its national values and requirements. These is achieved by integrating two devices for authentication of the voter. One is for Swapping machine which will recognize the UID card of individual voters and another device is for scanning Thumb impression. If the voter is passed through the two stage authentication process he/she will get chance to cast their vote and the control unit will activate the ballot unit for selecting the option. After this modification there is no possibilities for bogus voting and booth capturing.

6. References

[1] A. K. Agarwala, D. T. Shahani, and P. V. Indiresan. *Report of the expert committee for evaluation of the upgraded electronic voting machine (EVM).* Sept. 2006.http://www.scribd.com/doc/6794194/ Expert-Committee-Report-on-EVM, pages 2–20.

[2] R. Anderson and M. Kuhn. *Tamper resistance: A cautionary note*. In Proc. Second USENIX Workshop on Electronic Commerce, Oakland, CA, 1996.

[3] J. Brunner. *Evaluation & Validation of Election-Related Equipment, Standards & Testing* (EVEREST). Ohio Secretary of State,Dec. 2007. http://www.sos.state. oh.us/SOS/Text.aspx?page=4512.

[4] D. Chaum. *Secret-ballot receipts: True voter-verifiable elections*. IEEE Security & Privacy, 2(1):38–47, Jan. 2004.

[5] Election Commission of India. *Election laws*. http://eci.nic.in/eci_main/ElectoralLaws/electoral_law. asp.

[6] Election Commission of India. *Handbook for presiding officers*. 2008. http://eci.nic.in/eci_main/ ElectoralLaws/HandBooks/Handbook_for_Presiding_Officers.pdf.

[7] Election Commission of India. *Information under RTI on EVMs*. July 2009. No. RTI/2009-EMS/39. 22

[8] Election Commission of India. *Electronic voting machines– Regarding*. Aug. 8, 2009. No. PN/ECI/ 41/2009.

[9] R. K. Kumar. *The business of 'black-marking' voters*. In The Hindu, Mar. 17, 2004. http://www.hindu.com/2004/03/17/stories/2004031700571300.htm.

[10] R. Mehta. *How 100,000 EVMs can be tampered by just 10–12 people at top*. http://rahulmehta.com/ evm1.pdf, 2009.

[11] Press Trust of India. Singapore, Malaysia, South Africa approach *BEL for EVMs*. Apr. 12, 2009. http://www.hindu.com/thehindu/holnus/002200904121051.htm.

[12] Press Trust of India. *Compulsory voting not practical*, says CEC. Apr. 26, 2010. http://news.rediff.com/report/2010/apr/26/compulsory-voting-not-practical-says-cec.htm.

[13] G.V.L. N. Rao. *Democracy at Risk! Citizens for Verifiability, Transparency & Accountability in Elections*, New Delhi, 2010. http://indianevm.com/book.php.

[14] Wikipedia. *Results of the 2009 Indian general election by parliamentary constituency*. http://en.wikipedia.org/w/index.php?title=Results_of_the_2009_Indian_general_election_by_parliamentary_constituency&oldid=347683199 [accessed Apr. 17, 2010].