Security Analysis of India's Electronic Voting Machines

Scott Wolchok
Eric Wustrow
J. Alex Halderman
The University of Michigan

Hari K. Prasad
Arun Kankipati
Sai Krishna Sakhamuri
Vasavya Yagati
Netindia, (P) Ltd., Hyderabad

Rop Gonggrijp

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, have been praised for their simple design, ease of use, and reliability, but recently they have also been criticized following widespread reports of election irregularities. Despite this criticism, many details of the machines' design have never been publicly disclosed, and they have not been subjected to a rigorous, independent security evaluation. In this paper, we present a security analysis of a real Indian EVM obtained from an anonymous source. We describe the machine's design and operation in detail, and we evaluate its security in light of relevant election procedures. We conclude that in spite of the machines' simplicity and minimal software trusted computing base, they are vulnerable to serious attacks that can alter election results and violate the secrecy of the ballot. We demonstrate two attacks, implemented using custom hardware, which could be carried out by dishonest election insiders or other criminals with only brief physical access to the machines. This case study carries important lessons for Indian elections and for electronic voting security more generally.

Categories and Subject Descriptors

K.4.0 [**Computers and Society**]: General

General Terms

Security, Design, Human Factors

1. INTRODUCTION

India is the world's largest democracy. In recent national elections, more votes were cast than the combined population of the United States and Canada [57], and the vast majority of voters used paperless direct-recording electronic (DRE) voting machines [25]. Though paperless DREs have been largely discredited in the academic security literature (e.g., [4, 5, 9, 10, 17, 29, 30, 38]), 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" [27]. 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" [48]. To justify these claims, officials frequently cite the design of the EVMs, which is vastly simpler than that of most other DREs used globally, and a number of procedural safeguards. However, the details of the machines' design have been a closely guarded secret, and, until now, they have never been subjected to a rigorous independent security review.

In this paper, we analyze the security of India's EVMs and related procedural safeguards. We show that while the machines' simplicity makes them less susceptible to some of the threats faced by DREs studied in prior work, it also subjects them to a different set of highly dangerous attacks. We demonstrate two attacks that involve physically tampering with the EVMs' hardware. First, we show how dishonest election insiders or other criminals could alter election results

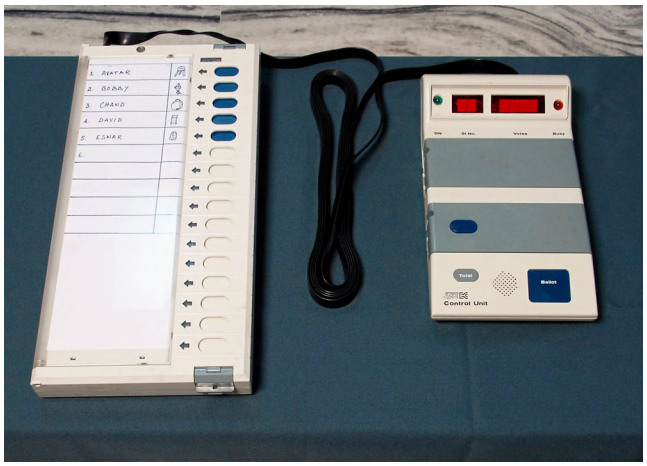


Figure 1: **Indian EVMs** consist of a BALLOT UNIT used by voters (*left*) and a CONTROL UNIT operated by poll workers (*right*) joined by a 5-meter cable. Voters simply press the button corresponding to the candidate of their choice. We obtained access to this EVM from an anonymous source.

CCS'10, October 4–8, 2010, Chicago, Illinois, USA.

by replacing parts of the machines with malicious look-alike components. Such attacks are made far simpler and cheaper by the EVMs' minimalist design, and they could be accomplished without the involvement of any field-level poll officials. Second, we show how attackers could use portable hardware devices to extract and alter the vote records stored in the machines' memory, allowing them to change election outcomes and violate ballot secrecy. This attack is technically straightforward because the EVMs do not use even basic cryptography to protect vote data internally. It could be carried out by local election officials without being detected by the national authorities or the EVM manufacturers' agents.

Though EVM manufacturers and election officials have attempted to keep the design of the EVMs secret, this presents only a minor obstacle for would-be attackers. There are nearly 1.4 million EVMs in use throughout the country [26], and criminals would only need access to one of them to develop working attacks. Dishonest insiders or other criminals would likely face *less* difficulty than we did in obtaining such access. There are many other possibilities for manipulating Indian EVMs, both with and without the involvement of dishonest election insiders. Depending on the local context and security environment, the nature and scale of potential manipulations may vary, but neither the machines' simplicity nor their secret design keeps them safe.

This study establishes that the EVMs used in India are not tamper-proof and are susceptible to a range of attacks. The use of similar paperless DREs has been discontinued in California [6], Florida [31], Ireland [33], the Netherlands [19], and Germany [8]. Indian election authorities should immediately review the security procedures now in place and should inspect all EVMs for evidence of fraud. Moving forward, India should adopt a different voting system that provides greater security and transparency.

Research Contributions

1. We present the first rigorous, independent security analysis of the electronic voting system used in India and find significant security flaws that compromise the integrity of the results and the secrecy of the ballot. Indian voting machines use a vastly different design than most other DRE voting systems studied in the literature, and we describe it in greater detail than was previously available to the public.

2. We explore the role of simplicity in electronic voting security. Previous studies have focused on problems caused by software complexity and have proposed minimizing the size of the trusted computing base (TCB) as a partial remedy [53]. India's EVMs use an extremely simple design with a small software TCB, yet we find that this makes physically tampering with the devices relatively easy. These findings underscore that the problems with DREs are due not only to complexity but also to lack of transparency.

3. We perform the first major security study of an electronic voting system used in an emerging nation. Voting systems in India must satisfy different constraints than systems used in the United States and Europe, which have been the focus of research to date. The Indian EVM manufacturers are exporting machines to other countries, including Nepal, Bhutan [47], and Bangladesh [40]. Mauritius, Malaysia, Singapore, Namibia, South Africa and Sri Lanka are reportedly considering adopting similar systems [47]. We outline some of the challenges of deploying electronic voting in an emerging nation. This provides a starting point for future research into voting system designs that meet the needs of these countries.

Outline The remainder of this paper is organized as follows. In Section 2, we review how electronic voting was introduced in India, describe how EVMs are used in elections, survey reports of fraud, and describe the EVM hardware based on our examination and experiments. In Section 3, we explain a number of ways that the EVM system can be attacked in spite of—and sometimes due to—its simple design. In Section 4, we present two demonstration attacks that we developed. Section 5 discusses current procedural countermeasures and why they are ineffective or even harmful. We place our work within the context of previous electronic voting security studies in Section 6. Finally, we draw conclusions and consider the way forward in Section 7.

For updates, additional details, and video of our demonstration attacks, visit http://**IndiaEVM.org**. To contact the authors, email authors@IndiaEVM.org.

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, 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 [47].

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.

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 [26]. (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 [57].

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

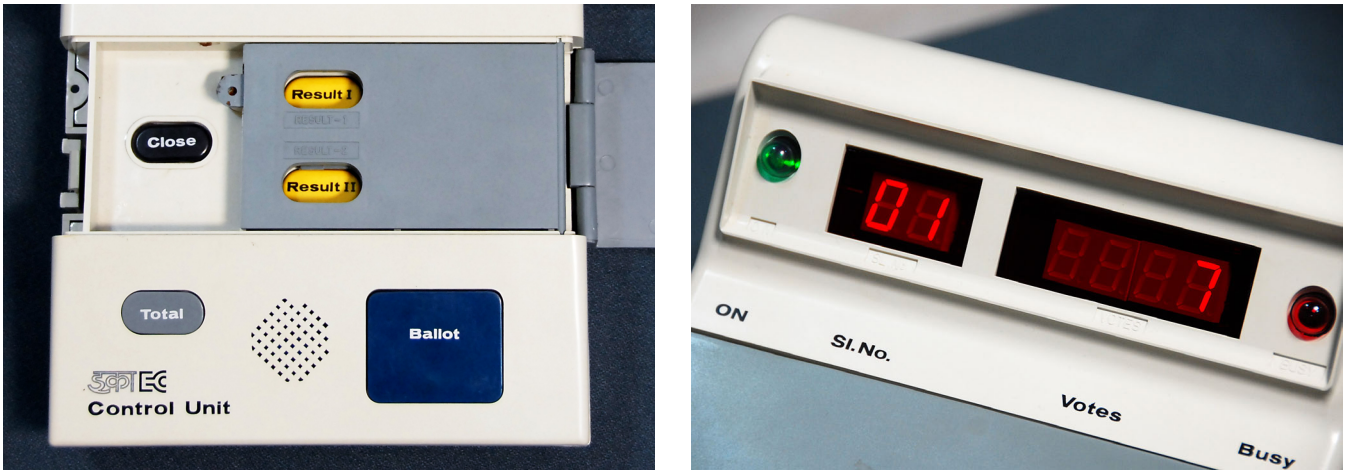


Figure 2: **Counting Votes** — The EVM records votes in its internal memory. At a public counting session, workers remove a seal on the control unit and press the RESULT I button (*left*) to reveal the results. The machine sequentially outputs the number of votes received by each candidate using a bank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

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., [20]). 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 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 [39]. 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.

2.3 Challenges for Electronic Voting in India

Indian voting machines must be designed to function under more challenging environmental conditions and operational constraints than other electronic voting systems studied in previous security reviews. These requirements have influenced the simple design of the current machines and impact our security analysis. Among the challenges are:

Cost With well over a million EVMs in use, the cost of the system is a major concern. The current EVMs are built from inexpensive commodity parts and cost approximately $200 for each set of units [35], far less than many DREs used in the U.S., which cost several thousand dollars.

Power Many polling places are located in areas that lack electricity service or have only intermittent service. Thus, the EVMs operate entirely from battery power, rather than merely using a battery as a backup.

Natural Hazards India's varied climate has great extremes of temperature, as well as other environmental hazards such as dust and pollution. EVMs must be operated under these adverse conditions and must be stored for long periods in facilities that lack climate control. An Election Commission report cites further dangers from "attack by vermin, rats, fungus or due to mechanical danger, [that might cause] malfunction" [1].

Illiteracy Though many Indian voters are well educated, many others are illiterate. The country's literacy rate in 2007 was 66% [56], and only about 55% among women, so handling illiterate voters must be the rule rather than the exception. Thus, ballots feature graphical party symbols as well as candidate names, and the machines are designed to be used without written instructions.

Unfamiliarity with Technology Some voters in India have very little experience with technology and may be intimidated by electronic voting. For example, "Fifty-year-old Hasulal Topno [... an] impoverished Oraon tribal, who gathers firewood from the forest outlying the Palamau Tiger Reserve, a Maoist hotbed 35 km from Daltonganj town" told a reporter, "I am scared of the voting machine," prior to its introduction in his village [13]. Nirmal Ho, "a tribal and a marginal farmhand in the Chatarpur block of Palamau district," said he was "more scared of the EVMs than the Maoists" on account of his unfamiliarity with technology. To avoid further intimidating voters like these, India's EVMs require the voter to press only a single button.

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].

Any voting system proposed for use in India must be able to function under these constraints.

2.4 Official EVM Security Reviews

There have been two official technical evaluations of EVM security performed at the behest of the Election Commission. The first was conducted in 1990 prior to the decision to introduce EVMs on a national scale, in response to "apprehensions articulated by leaders of political parties" about the machines' security. The study [35] was conducted by an "expert committee" composed of C. Rao Kasarbada, P.V. Indiresan, and S. Sampath, none of whom appear to have had prior computer security expertise. The committee had no access to EVM source code; instead, it relied on presentations and demonstrations by the manufacturers. Their report identifies two potential attacks: replacing the entire system with a fake one, and inserting a device between the ballot unit cable and the control unit. Both attacks, the report states, can be defeated by inspection of the machine. In the report's conclusion, the committee "unanimously certified that the System is tamperproof in the intended environment."

The Election Commission conducted a second "expert committee" study [1] in 2006 to evaluate upgrades for the third-generation EVMs. This time the committee members were A.K. Agarwala and D.T. Shahani, with P.V. Indiresan serving as chair. All three were affiliated with IIT Delhi, but, like the first committee, none appear to have had prior computer security expertise. Again, the committee members did not have access to EVM source code and relied on presentations, demonstrations, and site visits with the manufacturers. In their report, the commission reiterated the belief that the machines were "tamper-proof"; however, they also recommended a small number of changes to enhance the security of the machines. These included the adoption of "dynamic key coding" of button presses from the ballot unit, to protect against simplistic attacks on the cable, and the addition of a real-time clock and time-stamped logging of every key press, even if invalid, to provide a record of any attempt to activate malicious logic by a "secret knock." Some of these changes were adopted in third-generation EVMs, but they cannot prevent the attacks we demonstrate in this paper. We discuss implications of these safeguards in Section 5.

2.5 Reports of Irregularities

In recent years there have been numerous allegations and press reports of election irregularities involving Indian EVMs. It is difficult to assess the credibility of these charges, since there has apparently never been a prosecution related to EVM fraud, and there has never been a post-election audit to attempt to understand the causes [50, p. 54]. Nevertheless, they paint a troubling picture of election security in India.

Reports of malfunctions have been extensively surveyed by Rao [50]. For instance, he relates that in the 2009 parliamentary election there were reported EVM malfunctions in more than 15 parliamentary constituencies across the country. Especially troubling are claims that when the voter pressed a button for one candidate, a light would flash for another, which could be explained by a simple attack on the EVM cable [50, p. 45]. Rao also relates reports from prominent politicians that engineers approached them in 2009 offering to fix elections through this method [50, pp. 60–61].

Despite these incidents, experts for the Election Commission have equated any questioning of the security of the EVMs with an attack on the commission's own impartiality and integrity [50, p. 98]. In a television interview, P.V. Indiresan, who chaired the Election Commission's 2006 technical review, went as far as to liken doubting the security of the EVMs to "asking Sita to prove her virginity [*sic*] by having *Agni pariksha* [trial by fire]" (a reference to a famous episode in the *Ramayana*) [18].

We have had direct experience with attempted fraud. Hari Prasad, a coauthor of this study, was approached in October 2009 by representatives of a prominent regional party who offered to pay for his technical assistance fixing elections. They were promptly and sternly refused.

2.6 EVM Hardware Design

The manufacturers and the Election Commission have never released a detailed technical description of the EVMs' inner workings, citing security and intellectual property concerns [28]. We will now describe the hardware of the EVM we examined, based on our own observations and testing.

Control Unit Main Board The control unit contains the main circuit board, shown in Figure 3. The centerpiece is the EVM's CPU, a Renesas H8/3644-series microcontroller driven by an 8.8672 MHz crystal oscillator. The CPU is custom manufactured with the election software permanently recorded in an internal mask ROM. This prevents the software from being electronically reprogrammed. Also on the

main circuit board are the switches for the buttons on the face of the device, a buzzer, two EEPROM chips used for nonvolatile storage of vote data, the display board connector, and the connector for the ballot unit.

Control Unit Display Board The display board, shown in Figure 3(c), holds "Power" and "Busy" LEDs, as well as six 7-segment LED digits. It connects to the main board via a 16-pin ribbon cable. It implements a simple circuit in which the control unit main board directly drives the 7-segment LEDs. The CPU illuminates one 7-segment digit at a time, rapidly cycling through them to give the appearance that they are all lit continuously.

Ballot Unit Board The ballot unit board is also a very simple device. It has no CPU of its own; instead, it uses two electronically programmable logic devices (EPLDs) to interpret signals from the control unit CPU and interface with the candidate buttons and LEDs on its face. It also contains a four-position switch used to select the ballot unit's position in a multi-unit chain.

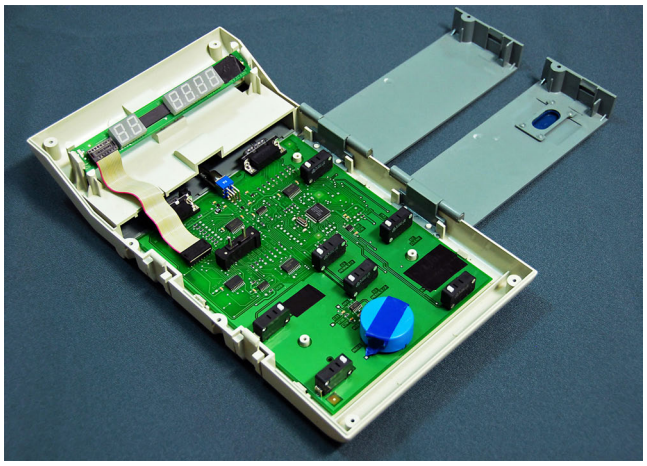
Ballot Unit Communication The control unit and the ballot unit are connected through a 5 m cable with one end connected to the 15-pin ballot port on the control unit main board and the other end fixed permanently inside the ballot unit. The the control unit initiates communication by sending the number of the ballot unit it wants to query. The first EPLD in each ballot unit reads this number, compares it to the position of the unit's four-position switch, and activates the second EPLD if the two numbers match. The second EPLD on the active ballot unit scans the candidate buttons and, if one is pressed, it communicates that information back to the control unit. The control unit then signals the first EPLD to activate the corresponding LED, indicating a successful vote. If no button is pressed on the active ballot unit, the control unit tries the next ballot unit in the chain.

Software Despite design features that make the election software difficult to extract from the control unit processor, a real criminal would have a variety of options for reading it out, including decapsulating the chip and examining it under a microscope [2]. Since we did not have permission to render our EVM unusable, we did not attempt to extract the software by these methods; however, once the software was extracted, reverse engineering would be straightforward using standard disassembly tools (e.g., [32]).

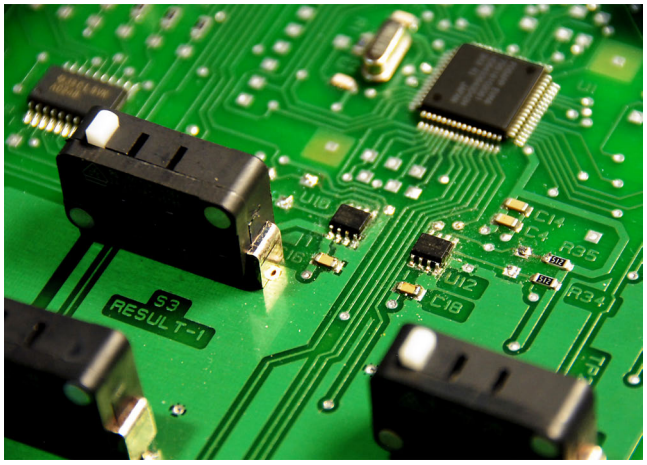
3. VULNERABILITY ANALYSIS

Prior studies of electronic voting security have recommended avoiding complexity and minimizing the size of the trusted computing base. In light of this advice, India's EVMs might superficially appear to be superior to most other deployed DREs. The EVMs use a simple embedded system design, as described in the previous section, and while many other DREs rely on commodity operating systems and run election software containing tens or hundreds of thousands of lines of code, the EVM software is compact, consisting of only a few thousand instructions that run directly on the hardware. Nevertheless, as we will explain, this has not resulted in a secure system.

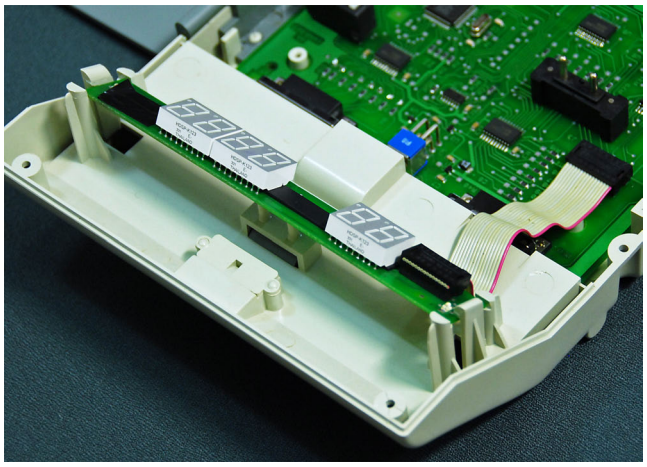
In this section, we describe a number of ways that attackers could manipulate the EVMs. These attacks are possible even if the voting software is completely error-free. Many of them could be performed once and then continue to influence



(a) Inside the control unit



(b) Main board (*detail*)



(c) Display board

Figure 3: **EVM Hardware** — The hardware inside the EVM (*a*) has never before been subjected to detailed public scrutiny. Most of the machine's logic is contained on the control unit MAIN BOARD, including the processor (*b*, rear) and two EEPROM memory chips that store the vote data (*b*, center). Election results and other output are shown on a smaller DISPLAY BOARD (*c*), which is a simple electric circuit containing only LEDs and a connector. Note that the 7-segment LEDs are raised slightly by a black plastic spacer.

election outcomes for the life of the machine. Significantly, we find that while the simple design of the EVMs makes certain software-based attacks less likely than in other DREs, it makes attacks involving physical tampering far easier.

Tampering with Software before CPU Manufacture The EVM firmware is stored in masked read-only memory inside the microcontroller chips, and there is no provision for extracting it or verifying its integrity. This means that if the software was modified before it was built into the CPUs, the changes would be very difficult to detect.

The software is integrated into the CPU by the manufacturer, Renesas, a Japanese company. (Other EVM models use CPUs made by Microchip, an American company.) Consider the engineer responsible for compiling the source code and transmitting it to the CPU manufacturer. He or she could substitute a version containing a back door with little chance of being caught. This fact alone would be great temptation for fraud.

Similarly, employees at the chipmakers could alter the compiled program image before burning it into the chips. While more involved than modifying source code, reverse engineering firmware of such low complexity is not difficult and has been done (sometimes within a few weeks) with other voting systems in the context of academic research [17,29,30].

Substituting Look-Alike CPUs After the software is burned into the CPUs by the foreign chipmakers, these CPUs are shipped to India to be assembled into the control unit main boards. Attackers might try to substitute look-alike CPUs containing software that counts the votes dishonestly. Other than the firmware, the CPUs are a commodity part, so obtaining and programming identical hardware would be straightforward. The EVM designers could have made such attacks more difficult by building a cryptographic mechanism for identifying the original CPUs, such as a challenge-response protocol based on a secret contained in the original firmware. Since they did not, this attack would only require creating new software with nearly identical functionality to the original, a task that is relatively easy because of the EVMs' simple design.

The real chips could be swapped with dishonest ones in the supply chain or by attackers with access to the assembled machines. Prior to assembly, they could be swapped by corrupt employees at the chipmakers or the couriers that transport them. Customs officials in the exporting countries could also have an opportunity to swap the chips, perhaps at the request of foreign intelligence agencies.

In addition to the main CPU used in the control unit, the programmable logic devices in the ballot unit might also be targeted in such an attack. A well-funded adversary could construct a look-alike chip package containing both a radio receiver and a processor.

Substituting Look-Alike Circuit Boards After the control unit's main board is manufactured, swapping in a dishonest CPU would require desoldering and replacing the surface-mounted chip, taking a skilled worker with adequate tools perhaps 10 minutes. However, attackers might find it faster to construct an electrically-compatible dishonest main board and substitute it for the original. Making a new board is relatively easy because of the simple design and function of this component. Replacing it would only require opening the control unit, swapping out the snap-fitted board, and reconnecting the cable to the display unit.

The system also treats its input and output devices as trusted components. An attacker could steal votes by replacing the circuit board in the ballot unit with one that falsely responds to key press events, or by replacing the display board in the control unit with one that reports inaccurate vote totals. The connections between these components are trusted too, so an attacker could try to insert a device between the ballot unit and control unit in order to intercept the key press signals and replace them with votes for different candidates. These attacks are straightforward because the machine's design includes no way for the boards to authenticate each other. We constructed a demonstration dishonest display board, which we describe in Section 4.1.

Substituting Look-Alike Units Voters and poll workers have no practical way to verify that the EVMs they use are authentic, so attackers might try to build identical looking but dishonest control units or ballot units and substitute them before an election. Since the units we examined have no effective way to verify the authenticity of the units they are paired to, replacing either unit with a dishonest one would allow the attacker to alter election results.

Prior to this study, Hari Prasad constructed a proof-of-concept look-alike EVM. He found that matching the electronic functionality was easy due to the simple design of the machine, but duplicating the plastic housing was more difficult. For this reason, attackers may prefer to tamper with real machines (if they can get access to them) by replacing chips or entire circuit boards within the original cases.

Tampering with Machine State Even if every component of the system behaves honestly, attackers could still attempt to manipulate the system by directly accessing or manipulating the internal state of the machine in ways not contemplated by its designers. For example, by attaching additional hardware to the control unit's circuit board, an attacker could directly read and write the EEPROM chips that record the votes. This is made easier because the machines are designed to use a simple I^2C serial interface to link the CPU to the memory chips, and because the simple software design does not attempt to cryptographically protect or authenticate the data stored there. We constructed a device that demonstrates such an attack, which we describe in Section 4.2.

4. DEMONSTRATION ATTACKS

We implemented two demonstration attacks to illustrate and experimentally confirm some of the EVM security problems we described in the previous section. We built these attacks without access to the machines' source code and with only limited access to an EVM during the design and testing process. Nonetheless, they are fully functional on real EVMs. A criminal who employed methods like these could alter vote totals in real elections or undermine ballot secrecy to determine how each voter voted.

4.1 Dishonest Display Attack

For our first demonstration attack, we developed a dishonest display board (see Figure 4) that can replace the real display board in the control unit. Normally, when votes are counted, the EVM display board shows the number of votes received by each candidate. The dishonest display adds a separate, hidden microcontroller that intercepts the vote totals and substitutes fraudulent results.

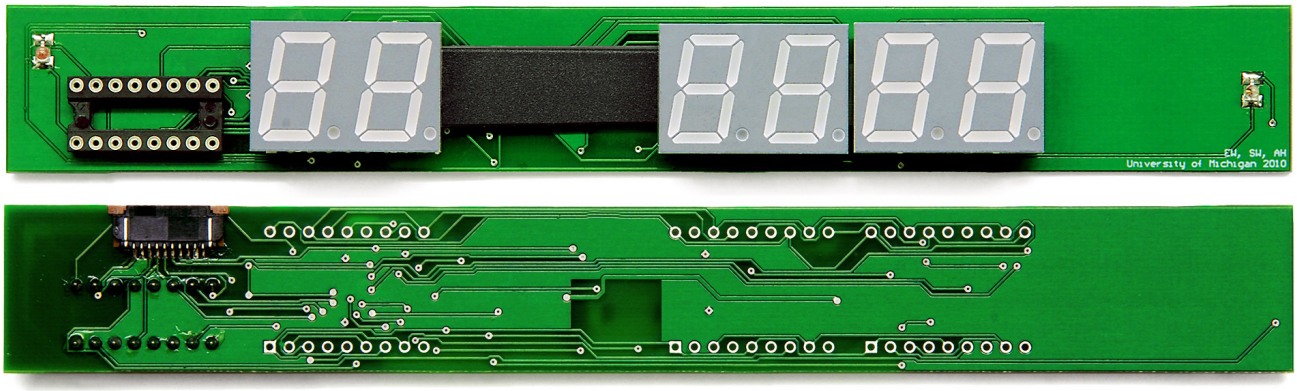
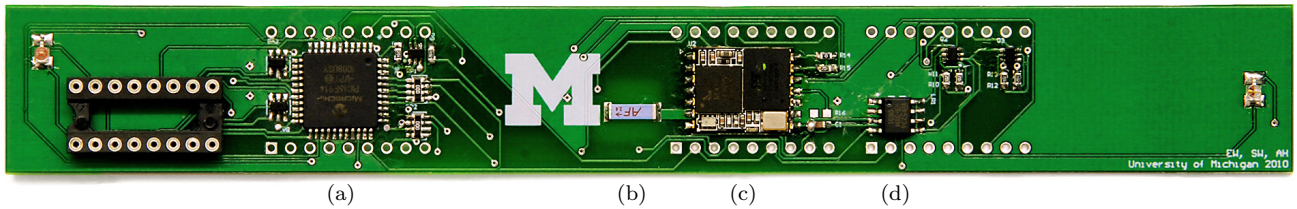


Figure 4: **Dishonest Display Attack** — We developed a dishonest display board, shown here at actual size. It looks almost identical to the real display board inside the control unit, but it shows fraudulent vote totals when results are counted. The only visible component on the reverse side is a programming connector, which could be removed before deploying the attack. Malicious election insiders or other criminals could install dishonest displays with little outward evidence of tampering.



(a) (b) (c) (d)

We hid new components beneath the 7-segment displays and black plastic spacer. A PIC microcontroller (a) replaces the real vote totals with dishonest ones when the machine shows results. A chip antenna (b) and Bluetooth radio module (c) let the attacker wirelessly signal which candidate to favor. The circuit draws all its power from the main board, via a voltage regulator (d).

To accomplish this, the dishonest display reads the electrical signals from the control unit that would normally control the 7-segment LED digits. This allows it to detect when the control unit is attempting to display election results. It also interprets the "total votes" output to determine the real overall number of votes so that it can make the dishonest votes add up correctly. Finally, it calculates and shows plausible but fraudulent vote counts for each candidate.

We developed a working prototype of the dishonest display board in less than a week, with no access to the EVM and from parts costing just a few dollars. We later refined the design to make the attack harder to detect and to add a wireless signaling mechanism.

Election results could be compromised by inserting a dishonest display into an EVM control unit at any point before votes are publicly counted, perhaps years before the election. Election insiders and EVM manufacturer maintenance personnel routinely have sufficient access, and criminal outsiders could be able to obtain access in places where the physical security of the machines is lax.

Design Details Our dishonest display uses the same kind of LEDs and connector found on the real display and adds a Microchip PIC16F914 microcontroller, a KC Wirefree KC22 Bluetooth module, an Antenna Factor chip antenna, and various discrete components (see Figure 4). To match the appearance of the real display, we conceal these extra components underneath the 7-segment LEDs. Conveniently for attackers, the LEDs on the real display are raised about 2 mm from the circuit board by a plastic spacer. We omit parts of this spacer underneath the LEDs to make room for the hidden components.

The EVM controls its 7-segment LED displays by multiplexing. The interface uses seven SEGMENT LINES, where each line is connected to a particular segment position on all six displays, and six SELECTOR LINES, which are connected to the common cathode of each digit. To control a 7-segment digit, the CPU drives its selector line low while keeping the others high and uses the segment lines to control which of the segments are lit. Each 7-segment display is lit for approximately 1.5 ms before switching to the next display, and persistence of vision effects make it appear as though all six displays are lit continuously. The microcontroller in the dishonest display monitors the selector lines and segment lines in order to determine the digits that the EVM processor is trying to display, and it computes its own vote totals as a function of this input. It implements a simple state machine to track the display of the election results.

The dishonest display draws power from the EVM, so it does not require a separate battery. The 16-pin display connector includes a ground line but no dedicated power line. However, at any time, at least five of the six digit selector lines are driven high, so the dishonest display can use them as its power source. The control unit provides these signals through a digital isolator, which is rated to source 25 mA per output pin. We are able to draw a total of about 150 mA from the six lines—enough to drive the LEDs or the Bluetooth radio, but not both simultaneously. Our solution is to keep the radio off until the display is blank, as it is during most of the polling process.

Signaling Which Candidate to Favor Once the dishonest display is installed in an EVM (possibly months or years before the election), the attacker must communicate

Figure 5: **Wireless Signaling** — An application running on an Android mobile phone uses Bluetooth to tell our dishonest display which candidate should receive stolen votes. Attacks using other forms of radio communication are also possible.

which candidate is to be favored (or disfavored), and by what margin. There are many different ways that attackers could send such a signal — with various kinds of radios, using secret combinations of key presses, or even by using the number of candidates on the ballot. We discuss these in more detail in Section 5.

To demonstrate the potential for wireless signals, we implemented a signaling mechanism based on the Bluetooth radio protocol. Wireless signaling could be performed at any time before votes are publicly counted. The dishonest display can then store the chosen candidate in the PIC's non-volatile Flash memory until counting is performed. We tested two methods for Bluetooth-based signaling, both of which can be triggered using ordinary mobile phones. Though the use of mobile phones is technically prohibited within 100 meters of polling stations [22, Section XVII.10], this rule is infrequently enforced, and a concealed phone could be discreetly operated inside the polling booth.

In the first method, the dishonest display performs a Bluetooth inquiry scan shortly after power on and looks for a device with a name of the form "`MAGIC`*xx*," where `MAGIC` is some secret word and *xx* is a pair of digits that are taken to be the number of the favored candidate. The process is extremely simple to implement; however, it carries the risk that a third party might perform his own Bluetooth inquiry scan and detect the signaling.

We also developed a more robust signaling method based on the Bluetooth RFCOMM protocol, which provides a reliable stream of communication similar to TCP. Our prototype implementation consists of an application running on an Android phone, shown in Figure 5. It sends a short message to the dishonest display via RFCOMM indicating the favored candidate and the proportion of votes to grant that candidate. The application verifies success by waiting for an acknowledgment from the dishonest display. Our application does not use any special Android features, so it could be ported to any smartphone platform that supports RFCOMM, such as the iPhone or Windows Mobile.

Online Algorithms for Vote Stealing As noted in prior work (e.g., [29]), vote-stealing attacks need to preserve the overall total number of votes in order to avoid being detected by comparison with other records of the number of voters who used the machine. We also note that to avoid raising suspicion when there is a small number of voters at a polling place or for a single candidate, a vote-stealing attack should avoid decreasing a candidate's vote total below the size of the largest group of voters that might confirm independently that every member of that group voted for the candidate (for example, a family or a group of close friends).

In most attack scenarios considered in previous work, determining fraudulent vote totals is straightforward, even with these constraints. However, some attacks that compromise a machine's input or output devices do not have access to the full election results ahead of time, and this creates a more difficult challenge. For instance, our dishonest display sees the candidate results one at a time as the machine tries to show them, and it must commit to and output a fraudulent result for each candidate before it learns the vote totals for the remaining candidates. This means our vote-stealing algorithm must operate *online*.

Despite this added complication, we implemented an online proportional boost vote-stealing algorithm that ensures no candidate's votes falls below a certain threshold, maintains some consistency properties of the reported results, and delivers extra votes to its favored candidate. For each nonfavored candidate, it calculates the maximum votes that can be stolen given the overall vote total, the totals outputted so far, and the need to reserve a certain number of votes for the remaining candidates to prevent them from falling below the minimum vote threshold. If the favored candidate has not been encountered yet, it subtracts either this maximum or the target proportion of the candidate's real votes, whichever is less. When the favored candidate is displayed, it adds the number of votes stolen so far plus a conservative estimate of the votes it will be able to steal from the remaining candidates. For subsequent candidates, it adds an additional constraint that prevents the sum of the votes stolen from all of them from exceeding this estimate.

4.2 Clip-on Memory Manipulator Attack

We implemented a second attack that demonstrates how malicious hardware can alter the internal state of the machine. Unlike the dishonest display attack, which involved replacing hardware components with dishonest look-alikes, this second attack involves only the temporary application of new hardware.

We constructed a device that clips directly to the EEPROM memory chips that record the votes inside the EVM. This small device, shown in Figure 6, fits discreetly in a shirt pocket. It facilitates two kinds of attacks: stealing votes and violating ballot secrecy.

Any time between the start of polling and the public count, dishonest election insiders or other criminals could use the clip-on device to change the votes recorded in the EVM. In India, counting sometimes takes place weeks after voting, so criminals could wait for an opportunity to tamper with the machines while they are in storage. Another variation of this attack is an electronic version of the booth capture attack described in Section 2.3. The EVM is designed to limit the rate of voting to no more than five per minute. However, our device bypasses this restriction, so an attacker who forcibly took control of an EVM could use it to stuff the electronic "ballot box" with any number of votes.

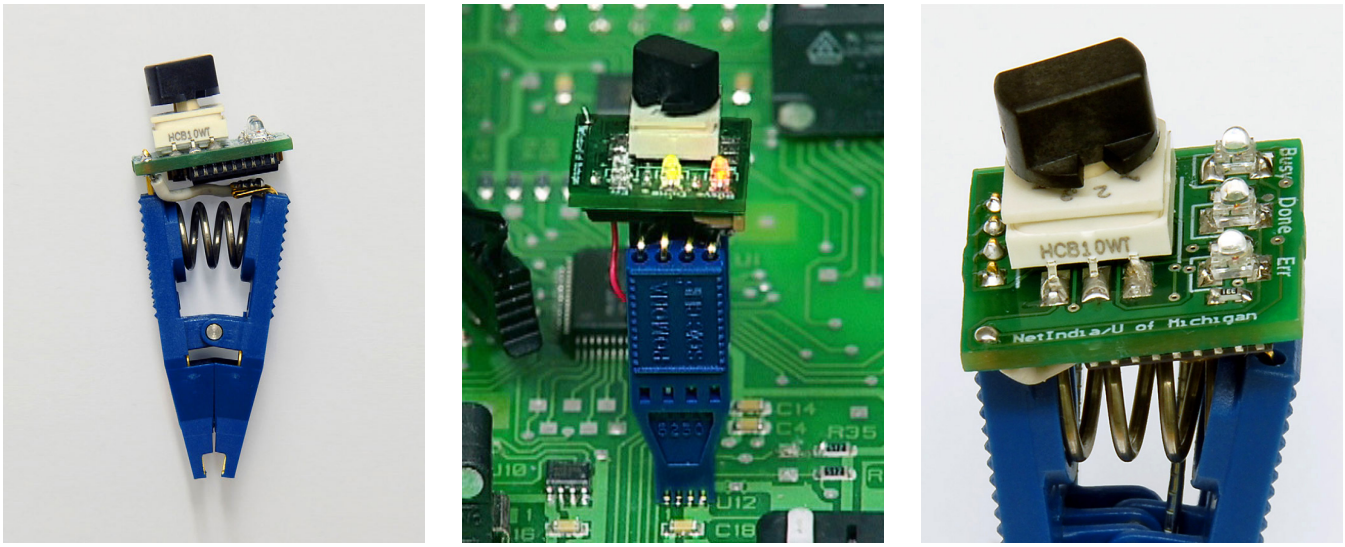


Figure 6: **Clip-on Memory Manipulator Attack** — We developed an attack device that can interface with the EVM's memory to change votes or violate ballot secrecy. The device (shown actual size, *left*) fits in a shirt pocket. It attaches directly to the memory chips that store the votes in the control unit (*middle*). A rotary switch (*right*) selects which candidate to favor.

Internally, the EVM records votes in the order in which they were cast, and our device can also be used to extract these records. An attacker who observed the order in which voters used the machine could then determine which candidate each voter selected.

Vote Storage and Layout The EVM records votes in two electronically-erasable, programmable read-only memory (EEPROM) chips, which are designed to provide a long-lasting record of the election results even if the machine loses power. The chips are standard 8 KB 24LC64 EEPROMs in an 8-pin SOIC package. Each of the two chips holds two complete copies of the vote data, for a total of four redundant copies. The vote data consists of a series of one-byte candidate numbers, each representing a single vote for a single candidate. Our testing shows that these records are stored in the order in which the votes were cast. Each chip also stores a copy of additional machine state, such as a unique identifier, the number of candidates, and the state of the election (e.g., voting open, voting closed, results tabulated, etc.).

The CPU interfaces with the EEPROMs through an I^2C-style serial protocol. Although the protocol allows all the chips to share a single bus, the system has two I^2C buses, each connecting the CPU with one of the two EEPROMs. In apparent violation of the I^2C protocol, the CPU holds the I^2C lines low when the EEPROMs are not in use, which prevents our device from communicating with them. We avoid this condition by holding the CPU in reset, which effectively disconnects it from the I^2C bus by forcing the relevant I/O pins into a high-impedance state.

Clip-on Device Design Our clip-on attack device is made from a small PCB mounted on top of a Pomona 5250 8-pin SOIC test clip. It incorporates a Microchip PIC16F88 microcontroller, a 10-position rotary switch, and three color LEDs that represent "Busy," "Done," and "Error" conditions. The PIC's I/O pins connect to the LEDs, the rotary switch, the I^2C pins on the test clip, and UART lines on a programming connector. The UART lines allow the device to be used as an EEPROM programmer when it is connected to a PC. The device draws all its power from the EVM.

To use the device, the attacker opens the EVM control unit and connects a jumper wire to the CPU to hold it in reset. Next, he powers on the machine and clips the device to one of the EEPROM chips. When the "Done" LED lights, the attacker disconnects the device and repeats the process for the second memory chip.

Stealing Votes To steal votes, the attacker indicates his favored candidate using the rotary switch, shown in Figure 6. The rotary switch selects a number from 0 to 9, and the attacker can use it to pick a favored candidate in any of the first nine ballot positions, which normally include the major national parties.

When the switch is set to positions 1–9, the clip-on device executes a vote-stealing program. The program runs in two passes: first, it reads the vote data and calculates how many votes to steal from each candidate; second, it rewrites the list of votes, stealing votes as calculated in the first phase. To reduce the chance of failure caused by an intermittent connection to the EEPROM chip, we implemented a rudimentary error recovery mechanism. The changes are written to the first array of votes and then copied to the second array, with each array being marked dirty while it is being written. In case of an error, the attacker merely needs to reattach the device—it will detect the condition and recover by using the clean array of votes as a backup. The stealing process takes only milliseconds per vote, so even in a large polling place, this part of the attack would take at most several seconds.

Violating Ballot Secrecy An attacker could also use our clip-on device to violate the secret ballot. The device can be connected to a laptop computer with a serial cable, and, when the rotary switch is set to position 0, it awaits commands to read or write the EEPROM. This allows the attacker to download the machine's ordered vote records to the laptop.

After extracting the vote records, the attacker would only need to determine the order in which voters used the machine to learn which candidate each chose. An attacker might do this by examining the register that voters sign, in order, as they enter the polling place. This information can be obtained by the public under India's Right to Information law. Generally there is only one EVM per polling place per race, so the votes in the EVM will match the recorded order of the voters.

5. INEFFECTIVE COUNTERMEASURES

India's EVMs and election procedures incorporate a number of features designed to prevent fraud. Unfortunately, these mechanisms are not sufficient to prevent the attacks we have demonstrated, and, in some cases, may actually make security worse. We discuss the most important of these countermeasures here.

Safety in Numbers Physically tampering with a large fraction of EVMs might be difficult because there are so many in use. However, in close races an attacker might be able to change the election outcome by tampering with only a few machines. A small number of tightly contested seats often determine which party holds a majority in the parliament, so a national-level attacker could focus on tampering with machines in these districts.

Physical Security Documented election procedures [24] focus on guarding the EVMs from the time they are inspected before an election until the final public counting session. Security in the period after the counting seems considerably more lax, even though hardware replacement attacks would be equally effective during this period. States have reportedly stored EVMs at places like high schools or "the abandoned godown [warehouse] of Konark Jute mill" [50, p. 217]. In one video [45], the "Strong Room" in which EVMs are stored prior to counting appears to be a closet with a fiberboard door and a paper sign that says "Strong Room."

Tamper-Evident Seals Poll workers attempt to protect the EVMs from tampering using an elaborate system of seals placed over different parts of the machine at various points in the election cycle [45]. However, these seals are extremely weak, consisting of stickers, strings, melted wax and plain paper labels (see Figure 7). None of the materials are difficult to obtain or manipulate.

Election authorities might switch to more sophisticated seals in the future, but this would not be sufficient to make the EVMs secure. Tamper-evident seals have been thoroughly discredited in scientific studies of electronic voting. For example, Appel reports [3] that it is easy to defeat the seals applied to AVC Advantage DREs in New Jersey. He shows how to undetectably remove and replace the seals using simple, readily available tools. He defeats a plastic strap seal with a jeweler's screwdriver, and he circumvents tamper-evident tape by carefully peeling it off with the aid of a heat gun. Other researchers who study tamper-evident seals have reported that nearly every kind they have experimented with is trivial to attack [34].

Even if the seals were difficult to attack, responding to broken seals presents additional challenges for election officials. What should officials do if, after an election but before votes are counted, they discover that a large number of control unit seals have been broken? This could be evidence of a memory manipulation attack like the one we demonstrated, which would leave no other visible traces, so officials might decide to discard all votes from machines with broken seals. However, this would create an even easier, low-tech attack opportunity: a dishonest insider or other criminal could simply break the seals on control units at polling places where voters were likely to favor an opponent.

Mock Elections The Election Commission attaches great value to the small "mock polls" that are conducted before each election. Their 2006 technical experts' report states: "Most importantly it is noted that the EVMs are subject to mock-poll validation at various stages in front of all party representatives. This is the best proof of validation of fairness of the program as well as data being stored inside" [1]. On the contrary, we conclude that these mock polls offer very little protection. It would be trivial to program a dishonest EVM so that fraud would go unnoticed in pre-election mock polls. For example, it could be instructed to cheat only after several hours have passed or after the EVM has recorded hundreds of votes. Although mock polls might protect against non-malicious malfunction, or against a simplistic attacker who switched the wires to the buttons and LEDs, it cannot protect against the attacks we propose in this paper.

Secret Source Code The second- and third-generation EVMs use election software masked into the microcontroller and are designed to make it difficult to read out the code. The Election Commission's experts cited this as a major security feature: "The program is burnt into the microchip on a 'one time programmable' basis (OTP) and once burnt it cannot be read, copied out, altered and re-fed into the chip at all" [1]. However, this also makes it difficult for even the EVM manufacturers to verify that the correct code is actually present in the chips. One of the expert committee members claimed in an interview that "even the BEL and ECIL," the companies that make the machines, "cannot read what is in the code" [18].

Even if the correct software is there, it is risky to design a voting system such that its security depends on keeping the program secret. If the secret software *does* become known to attackers, there is no way to recover except by changing to new software—an expensive and time-consuming proposition. Discovering the secret requires only a single weak link, such as a dishonest insider at BEL or ECIL, or a security breach of their software development systems. As Auguste Kerckhoffs famously said of good military cryptographic design, "It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience" [36]. This advice is equally true for EVM code.

In fact, the program *can* be read from the chips, given sufficient resources. Techniques for reverse engineering chips by carefully opening them and inspecting them under a microscope have been known in the literature for over 15 years [2]. Though expensive and time-consuming, these procedures are routine in industry and are now being performed at the level of academic security research (e.g., [44]). Thus, the secret code could be revealed by one well-funded attacker with access to a single EVM.

Machine Distribution Before each election, authorities use an elaborate two-stage process to shuffle batches of EVMs among parliamentary districts and to assign them to polling places within each district [24]. This might make it harder for an attacker who has placed dishonest hardware into a small

number of EVMs to target a specific region, yet the process is insufficiently transparent and may actually introduce a new risk. The random assignments are made using custom software that, to our knowledge, is not published. If *this* software is dishonest, it could output assignments that appear to be random but actually place EVMs that have already been tampered with in the places the attacker wants to target. Additionally, many parliamentary districts are as large as voting districts, so randomization within the district would not hamper an attacker who sought to steal votes for those seats [50, p. 161].

Candidate Ordering The final ballot positions of the candidates are only known a few weeks before the election. The Election Commission's expert report claims that this prevents fraud, because malicious software in the EVMs would have no means of knowing which candidate to favor: "It is noted that for biasing the program to favor a particular candidate, the 'key number' allotted to the candidate is essential to be known, and this information for various elections to be conducted in the future cannot possibly be known at the EVM's manufacturing stage. Hence no bias can be introduced in the program at the time of manufacture of the chip" [1, p. 4].

In practice, the order of the candidates is less random than one might assume. Parliamentary candidates, for example, are split into three groups: (1) candidates of recognized national parties and state political parties, (2) candidates of registered unrecognized political parties and (3) other (independent) candidates. Within each group the candidates are listed alphabetically. So if four national parties participate in a district, then, based on likely candidates for these four, an attacker can make an educated guess about how the first four buttons will be assigned.

A dishonest EVM might also be commanded by a signal sent by the attacker after the ballot order is determined. There are several signaling methods that could be used:

Secret Knocks An attack might be designed to be signaled by a designated sequence of inputs before or during the election. Depending on the mode of attack, this might be a series of button presses on the ballot unit, a series of votes during the mock election, or even a series of real votes made by the attacker's accomplices.

Tampering During First-Level Checking The Election Commission mandates "first level checking" of EVMs before elections by authorized technicians of the EVM manufacturers [21] in order to detect and remedy hardware problems. This means a group of technically skilled insiders has full access to the machines after the election process is set in motion. These authorized technicians are also sometimes involved at various later stages of the election, such as preparing EVMs for polling and assisting officials during the count. Dishonest technicians could open and manipulate hardware or perform secret knocks during these checks.

Using the Total Number of Candidates Signaling many EVMs individually would be relatively labor intensive. However, as noted by Mehta [41], an attacker can send signals to EVMs throughout an election district with another kind of covert channel. This is done by taking advantage of a procedural peculiarity of Indian elections. Candidates can register to be on the ballot and then withdraw after the order of candidates is determined [23, 48]. This means an attacker can gain some control over the total number of candidates

(a) Workers seal the control unit with wax and string.

(b) Paper seals (here, broken) cover the screw holes.

Figure 7: **Tamper-Evident Seals** — Frames from an official training video [45] show how poll workers seal the control unit doors using red wax and string (*a*). The paper tags are signed by candidates' representatives, but these signatures are not routinely verified. Seals placed over screw holes on the underside of the control unit consist of printed paper stickers (*b*, upper left and right). All these low-tech seals can be easily faked and provide extremely weak protection.

on the ballot by registering a number of dummy candidates and then having some of them withdraw. If there are n candidates, the dishonest machines might be programmed to steal a percentage of votes in favor of candidate n mod 5, for instance. This would allow the attacker to pick any of the first five candidates to favor (all likely national party candidates) and to send the signal throughout the district by having between zero and four dummy candidates withdraw.

EVM Upgrades The third-generation EVMs manufactured after 2006 add a number of additional safeguards recommended by the Election Commission's technical expert committee. These safeguards do not prevent the attacks we propose, and some of them may actually harm security. For example, the committee recommended adding a real-time clock and logging all key presses with a timestamp—presumably to prevent "secret knock" signaling or to be able to revert the effects of booth capture. Having a real-time clock gives any dishonest software in the EVM another way to find out whether a real election is occurring, which helps it cheat while avoiding detection in mock polls and other testing. Logging every key press together with the time also provides an even stronger way for attackers to violate ballot secrecy. If attackers can observe which machine a voter used and record the time, they can later consult the records in that machine to determine which candidate the voter chose.

6. RELATED WORK

Security Problems in Complex E-Voting Systems Numerous studies have uncovered security problems in complex touch-screen DRE voting machines. Several early studies focused on the Diebold AccuVote-TS, including security analyses by Kohno et al. [38], SAIC [54], RABA [49], and Feldman et al. [29]. These works concentrated on vulnerabilities in the voting machine's firmware. They uncovered several ways that malicious code could compromise election security, including the possibility that malicious code could spread as a voting machine virus.

Following these studies, several states conducted independent security evaluations of their election technology. In 2007, California Secretary of State Debra Bowen commissioned a "top-to-bottom review" of her state's voting machines, which found significant problems with procedures, code, and hardware [6]. The review tied many problems to the complexity of the machines' software, which, in several systems, comprised nearly one million lines of code in addition to commercial off-the-shelf operating systems and device drivers [5, 10]. Also in 2007, Ohio Secretary of State Jennifer Brunner ordered Project EVEREST—Evaluation and Validation of Election Related Equipment, Standards and Testing—as a comprehensive review of Ohio's electronic voting machines [7]. Critical security flaws were discovered, including additional problems in the same systems that had been studied in California. The analysts concluded that still more vulnerabilities were likely to exist in software of such complexity [9].

Security Problems in Simple E-Voting Systems A few other studies have examined relatively simple computer voting systems, though these systems are still complex compared to the Indian EVMs, incorporating some form of upgradeable firmware as well as external memories for ballot programming and vote tabulation. Several of these studies focused on replacing memory chips that store election software. Gonggrijp and Hengeveld examined Nedap DRE voting machines and demonstrated software attacks based on replacing the socketed ROM chips [30]. Appel et al. performed an extensive analysis of the AVC Advantage DRE and warned against attacks based on replacing the ROM chips or swapping the Z80 processor with a dishonest look-alike [4]. They briefly suggest a hardware-based attack that would change the signals from the machine's candidate buttons before they were recorded by the CPU. Checkoway et al. also examined the AVC Advantage DRE and reverse-engineered the hardware and software [17]. They built hardware devices to interface with the machine's proprietary memory cartridges and created vote-stealing software that employed return-oriented programming to bypass the machine's memory protection hardware.

The Role of Complexity in Voting Security Much has been written about the problem of complexity in DREs. The California top-to-bottom review focused on vulnerabilities in complex software. One report concluded that "the Diebold software is too complex to be secure. Put another way: If the Diebold system were secure, it would be the first computing system of this complexity that is fully secure" [10]. Sastry et al. focus on the size of the software source code that must be analyzed: "One problem with current DRE systems, in other words, is that the trusted computing base (TCB) is simply too large" [53]. They recommend that election software be designed in ways that make verification easier, such as minimizing the amount of code that needs to be trusted.

Rivest and Wack [52] address the problem of complexity by proposing that voting systems should be *software independent*; that is, each should be designed so that "an undetected change or error in its software cannot cause an undetectable change or error in an election outcome." Some mechanisms for achieving software independence also protect against *hardware* changes—for instance, rigorous post-election audits of paper ballots in a precinct-count optical scan system—but it is possible for a system to be software-independent while still being vulnerable to hardware attacks like those we describe.

The complexity of DRE voting systems has been a significant source of vulnerability, but it is certainly not the only source. As we have demonstrated, DREs can be tampered with by substituting dishonest hardware components or by altering the internal state of the machine using malicious hardware devices. Simplicity alone cannot cure DRE security problems. Furthermore, when designs are overly simple, they may make it impossible to apply certain defenses, such as cryptographic integrity and confidentiality protections. Very simple and cheap hardware designs allow for easier reverse engineering and simple, inexpensive hardware tampering. The maximum amount of security in electronic voting systems will likely come from balance—designs that employ complexity intelligently, when it makes the system stronger.

Much other work has examined hardware attacks outside the context of voting (e.g., [37, 55]) and the general problem of security in embedded systems (e.g., [2, 12, 51]).

Several authors have proposed end-to-end verifiable cryptographic voting systems (e.g., [14–16, 43, 46]), which allow voters to independently check that their votes have been counted correctly. Though these schemes hold great promise, it remains to be seen whether they can be adapted for use under the challenging conditions of Indian elections.

7. CONCLUSIONS

Despite elaborate safeguards, India's EVMs are vulnerable to serious attacks. Dishonest insiders or other criminals with physical access to the machines can insert malicious hardware that can steal votes for the lifetime of the machines. Attackers with physical access between voting and counting can arbitrarily change vote totals and can learn which candidate each voter selected.

These problems are deep rooted. 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. The technology's promise was that attacks on the ballot box and dishonesty in the counting process would be more difficult. Yet we find that such attacks remain possible, while being potentially more difficult to detect.

It is highly doubtful that these problems can be remedied by simple upgrades to the existing EVMs or election procedures. Merely making the attacks we have demonstrated more difficult will not fix the fundamental problem: India's EVMs do not provide transparency, so voters and election officials have no reason to be confident that the machines are behaving honestly.

India should carefully reconsider how to achieve a secure and transparent voting system that is suitable to its national values and requirements. One option that has been adopted in other countries is to use a voter-verifiable paper audit trail (VVPAT), which combines an electronic record stored in a DRE with a paper vote record that can be audited by hand [42]. Existing EVMs do not have updatable software, but it would be possible to add a VVPAT by interposing on the cable between the control unit and the ballot unit. Another option is precinct-count optical scan (PCOS) voting, where voters fill out paper ballots that are scanned by a voting machine at the polling station before being placed in a ballot box. Attacking either of these systems would require tampering with both the paper records and the electronic records, provided that routine audits are performed to make sure these redundant sets of records agree [11]. A third option is to return to simple paper ballots. Despite all of their known weaknesses, simple paper ballots provide a high degree of transparency, so fraud that does occur will be more likely to be detected.

Using EVMs in India may have seemed like a good idea when the machines were introduced in the 1980s, but science's understanding of electronic voting security — and of attacks against it — has progressed dramatically since then, and other technologically advanced countries have adopted and then abandoned EVM-style voting. Now that we better understand what technology can and cannot do, any new solutions to the very real problems election officials face must address the problems, not merely hide them from sight.

J. Alex Halderman Hari K. Prasad Rop Gonggrijp
— Hyderabad, February 2010

Acknowledgments

The authors gratefully acknowledge the anonymous source who, at considerable risk, provided the EVM for us to study. We also thank the many individuals and groups who contributed time, facilities, and insight to make this study possible, including Mark Brehob, Satya Dosapati, Prabal Dutta, Georg Essl, Edward W. Felten, Nadia Heninger, Till Jaeger, Michael Maltabes, Kalyan Manukonda, Rahul Mehta, V.V. Rao, Subramanian Swamy, and the University of Michigan RAX Lab. We are particularly indebted to G.V.L. Narasimha Rao, whose efforts to increase election transparency in India paved the way for this research, and who provided indispensable guidance and advice throughout the process.

8. 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] A. W. Appel. Certification of December 1, 2008. http://citp.princeton.edu/voting/advantage/seals/appel-dec08-certif.pdf.

[4] A. W. Appel, M. Ginsburg, H. Hursti, B. W. Kernighan, C. D. Richards, G. Tan, and P. Venetis. The New Jersey voting-machine lawsuit and the AVC Advantage DRE voting machine. In *Proc. Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE),* Montréal, Canada, Aug. 2009.

[5] A. Aviv, P. Cerný, S. Clark, E. Cronin, G. Shah, M. Sherr, and M. Blaze. Security evaluation of ES&S voting machines and election management system. In *Proc. USENIX/ACCURATE Electronic Voting Technology Workshop (EVT),* San Jose, CA, July 2008.

[6] D. Bowen. "Top-to-Bottom" Review (TTBR) of voting machines certified for use in California. California Secretary of State, Aug. 2007. http://sos.ca.gov/elections/elections_vsr.htm.

[7] 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.

[8] Bundesverfassungsgericht (German Constitutional Court). Judgment [...] 2 BvC 3/07, 2 BvC 4/07, official English translation. Mar. 3, 2009. http://www.bverfg.de/entscheidungen/rs20090303_2bvc000307en.html.

[9] K. Butler, W. Enck, H. Hursti, S. McLaughlin, P. Traynor, and P. McDaniel. Systemic issues in the Hart InterCivic and Premier voting systems: Reflections on Project EVEREST. In *Proc. EVT,* San Jose, CA, July 2008.

[10] J. A. Calandrino, A. J. Feldman, J. A. Halderman, D. Wagner, H. Yu, and W. P. Zeller. Source code review of the Diebold voting system. Part of California TTBR, Aug. 2007.

[11] J. A. Calandrino, J. A. Halderman, and E. W. Felten. Machine-assisted election auditing. In *Proc. EVT,* Boston, MA, Aug. 2007.

[12] C. Castelluccia, A. Francillon, D. Perito, and C. Soriente. On the difficulty of software-based attestation of embedded devices. In *Proc. 16th ACM Conference on Computer and Communications Security (CCS),* Chicago, IL, pages 400–409, Nov. 2009.

[13] M. Chatterjee. Tribal voters in Jharkhand reckon with EVM technology. In *Indo-Asian News Service,* Nov. 20, 2009.

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

[15] D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, and P. Vora. Scantegrity: End-to-end voter-verifiable optical-scan voting. In *IEEE Security & Privacy,* 6(3):40–46, May 2008.

[16] D. Chaum, P. Y. A. Ryan, and S. A. Schneider. A practical, voter-verifiable election scheme. University of Newcastle upon Tyne, Technical Report CS-TR-880, Dec. 2004.

[17] S. Checkoway, A. J. Feldman, B. Kantor, J. A. Halderman, E. W. Felten, and H. Shacham. Can DREs provide long-lasting security? The case of return-oriented programming and the AVC Advantage. In *Proc. EVT/WOTE,* Montréal, Canada, Aug. 2009.

[18] CNN-IBN TV. Interview with P. V. Indiresan. July 20, 2009. http://ibnlive.in.com/videos/97488/evms-rigged-poll-panel-challenges-doubters.html.

[19] A. U. de Haes. Dutch government bans electronic voting. In *IDG News Service,* May 19, 2008. http://news.idg.no/cw/art.cfm?id=003AE63C-17A4-0F78-31DDDC0DCFA62609.

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

[21] Election Commission of India. Protocol for first level checking of EVMs before elections. Oct. 12, 2007. http://eci.nic.in/eci_main/CurrentElections/ECI_Instructions/ins_121007g.pdf.

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

[23] Election Commission of India. Handbook for candidates. 2009. http://eci.nic.in/eci_main/ElectoralLaws/HandBooks/Handbook_for_Candidates.pdf.

[24] Election Commission of India. Handbook for returning officers. 2009. http://eci.nic.in/eci_main/ElectoralLaws/HandBooks/Handbook_for_Returning_Officers.pdf.

[25] Election Commission of India. Schedule for general elections, 2009. Mar. 2009. http://www.elections.tn.nic.in/forms/pn020309.pdf.

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

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

[28] Election Commission of India. The Commission's reply to Sh. V. V. Rao. Mar. 29, 2010. http://eci.nic.in/eci_main/recent/reply_sh.VVRao.pdf.

[29] A. J. Feldman, J. A. Halderman, and E. W. Felten. Security analysis of the Diebold AccuVote-TS voting machine. In *Proc. EVT,* Boston, MA, Aug. 2007.

[30] R. Gonggrijp and W.-J. Hengeveld. Studying the Nedap/Groenendaal ES3B voting computer: A computer security perspective. In *Proc. EVT,* Boston, MA, Aug. 2007.

[31] A. Goodnough and C. Drew. Florida to shift voting system with paper trail. In *The New York Times,* Feb. 2, 2007.

[32] The IDA Pro disassembler and debugger. http://www.hex-rays.com/idapro/.

[33] Irish Department of the Environment, Heritage & Local Government. Minister Gormley announces Government decision to end electronic voting and counting project. Apr. 23, 2009. http://www.environ.ie/en/LocalGovernment/Voting/News/MainBody,20056,en.htm.

[34] R. G. Johnston. Tamper-indicating seals. In *American Scientist,* pages 515–523, November–December 2006.

[35] C. R. Kasarbada, P. V. Indiresan, and S. Sampath. Report of the expert committee for the technical evaluation of the electronic voting machine. Apr. 1990. http://www.scribd.com/doc/6794194/Expert-Committee-Report-on-EVM, pages 21–37.

[36] A. Kerckhoffs. La cryptographie militaire. In *Journal des Sciences Militaires*, 9:5–38, Jan. 1883, :161–191, Feb. 1883.

[37] S. T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, and Y. Zhou. Designing and implementing malicious hardware. In *Proc. First USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET),* San Francisco, CA, Apr. 2008.

[38] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach. Analysis of an electronic voting system. In *Proc. IEEE Symposium on Security and Privacy,* Oakland, CA, pages 27–40, May 2004.

[39] 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.

[40] S. Liton. E-voting in DCC polls. In *The Daily Star,* Apr. 14, 2010. http://www.thedailystar.net/newDesign/news-details.php?nid=134325.

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

[42] R. Mercuri. Electronic vote tabulation: Checks and balances. Ph.D. Thesis, University of Pennsylvania, 2001.

[43] C. A. Neff. Practical high-certainty intent verification for encrypted votes. Oct. 2004. http://votehere.com/old/vhti/documentation/vsv-2.0.3638.pdf.

[44] K. Nohl and D. Evans. Reverse-engineering a cryptographic RFID tag. In *Proc. 17th USENIX Security Symposium,* San Jose, CA, July 2008.

[45] Office of Chief Electoral Officer, Delhi. Documentary on preparation of EVM at R.O. level. http://www.youtube.com/watch?v=wRJQTTrumNI.

[46] S. Popoveniuc and B. Hosp. An introduction to Punchscan. In *Proc. IAVoSS Workshop on Trustworthy Elections (WOTE),* Cambridge, UK, Oct. 2006.

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

[48] 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.

[49] RABA Innovative Solution Cell. Trusted agent report: Diebold AccuVote-TS voting system. Jan. 2004.

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

[51] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady. Security in embedded systems: Design challenges. In *ACM Trans. Embed. Comput. Syst.,* 3(3):461–491, Aug. 2004.

[52] R. L. Rivest and J. P. Wack. On the notion of "software independence" in voting systems. http://vote.nist.gov/SI-in-voting.pdf, 2006.

[53] N. Sastry, T. Kohno, and D. Wagner. Designing voting machines for verification. In *Proc. 15th USENIX Security Symposium,* Vancouver, Canada, July 2006.

[54] Science Applications International Corporation. Risk assessment report: Diebold AccuVote-TS voting system and processes. Sept. 2003.

[55] G. Shah, A. Molina, and M. Blaze. Keyboards and covert channels. In *Proc. 15th USENIX Security Symposium,* Vancouver, Canada, July 2006.

[56] UNICEF. India statistics. http://www.unicef.org/infobycountry/india_statistics.html [accessed Apr. 17, 2010].

[57] 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].