Security Analysis of India's Electronic Voting Machines

Hari K. Prasad* J. Alex Halderman† Rop Gonggrijp
Scott Wolchok† Eric Wustrow† Arun Kankipati* Sai Krishna Sakhamuri* Vasavya Yagati*

*NetIndia, (P) Ltd., Hyderabad †The University of Michigan

April 29, 2010

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 because of 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 machine's simplicity and minimal software trusted computing base, it is 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 contains important lessons for Indian elections and for electronic voting security more generally.

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 [55], and the vast majority of voters used paperless direct-recording electronic (DRE) voting machines [30]. Though paperless DREs have been largely discredited in the academic security literature (e.g., [7, 8, 12, 13, 20, 31, 32, 39]), 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" [3]. 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 series 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 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 [29], 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 [9], Florida [33], Ireland [1], the Netherlands [22], and Germany [11]. 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 consider adopting a voting system that provides greater security and transparency, such as paper ballots.

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 results and the secrecy of the ballot. These 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 [51]. 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 [2], and Bangladesh [41]. Mauritius, Malaysia, Singapore, Namibia, South Africa and Sri Lanka are reportedly considering adopting similar systems [2]. We outline some of the challenges of deploying electronic voting in an emerging nation. This provides a starting point for future research into designing voting systems 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 present two demonstration attacks that we developed. In Section 4, we survey a number of ways that the EVM system can be attacked in spite of—and sometimes due to—its simple design. 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 the latest version of this report and a video of our demonstration attacks, visit http://**IndiaEVM.org**.

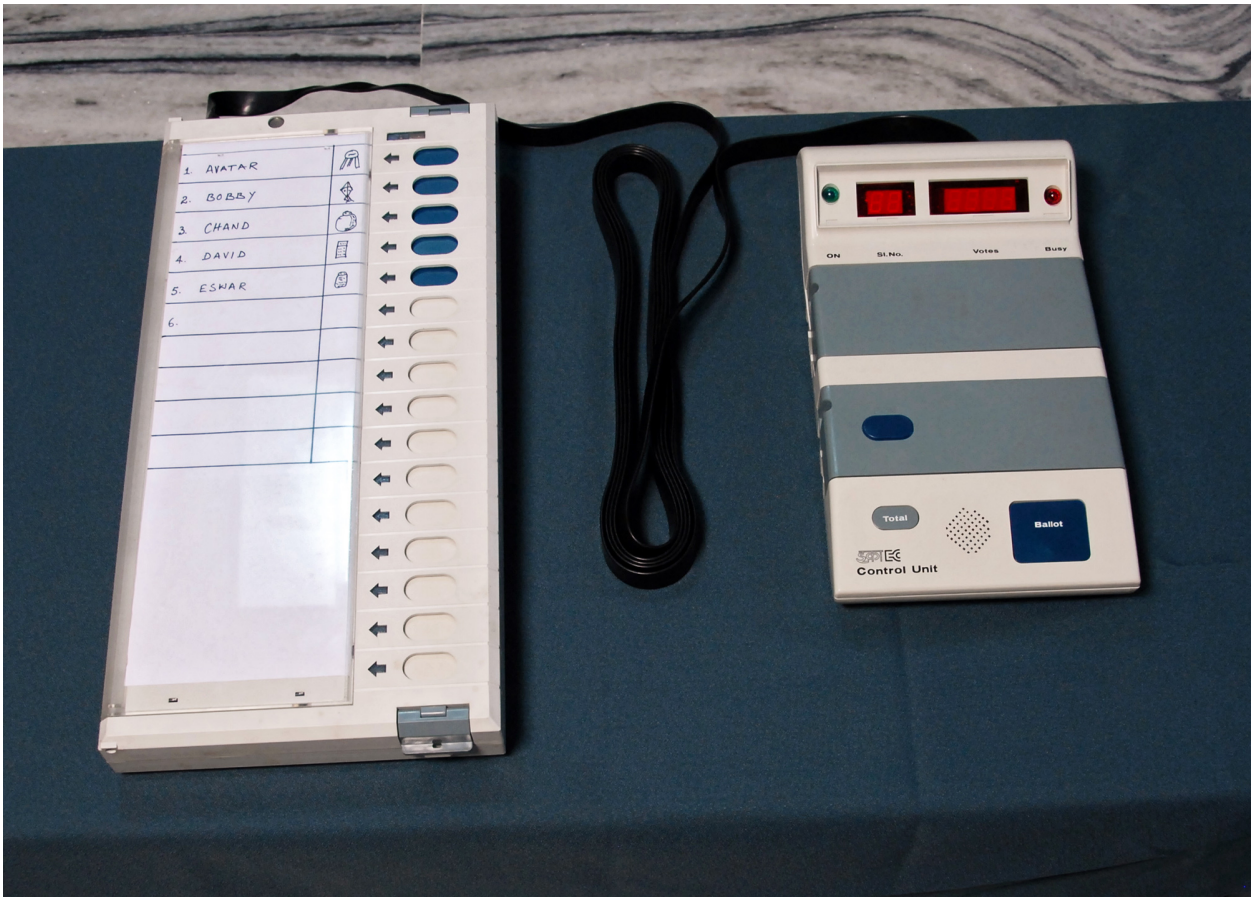

Figure 1: **Indian EVMs** consist of a BALLOT UNIT used by voters (*left*) and a CONTROL UNIT operated by poll workers (*right*) joined by a 5-meter cable. Inside the election booth, voters simply press the button corresponding to the candidate of their choice. We obtained access to this EVM from an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

2 Background

2.1 Electronic Voting in India

The Election Commission developed India's EVMs in partnership with two government-owned companies, the Electronics Corporation of India (ECIL) and Bharat Electronics Limited (BEL) [49, pp.1,9]. Though these companies are owned by the government, they are not under the administrative control of the Election Commission. They are profit-seeking vendors that are attempting to market EVMs globally [2].

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 [49, p.1]. They introduced the style of system used to this day, 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 [49, p.1]. In 2006, the manufacturers adopted a third-generation design incorporating additional changes suggested by the Election Commission.

According to the Election Commission, in July 2009 there were 1,378,352 EVMs in use. Of these, 448,000 were third-generation machines manufactured from 2006–2009, with 253,400 from BEL and 194,600 from ECIL. The remaining 930,352 were the second-generation models manufactured from 2000–2005, with 440,146 from BEL and 490,206 from ECIL [29]. (The first generation machines are deemed risky to use in national elections because their 15-year service life has expired [4], 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 [55].

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 national elections. It was provided by a source who 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 in the ballot unit selects its position in the chain.

Election procedures are described in a number of public documents [25]. 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 and switch 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.

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 [40]. 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. Counting officials manually record the totals from each machine and add them together to determine the results of the election. The machines are then placed in storage until the next election.

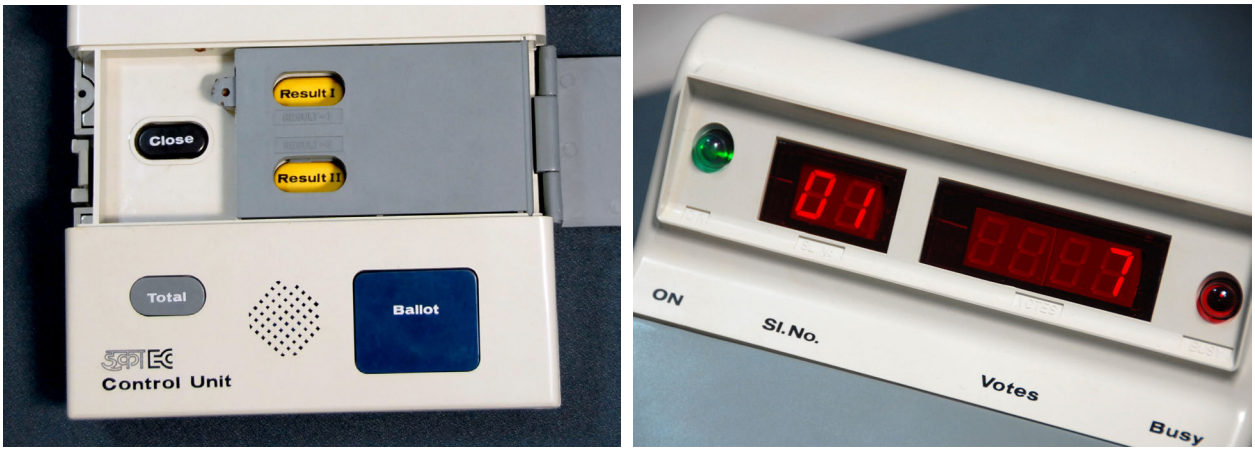

Figure 2: **Counting** — In a public counting session, workers remove a seal on the control unit and press the RESULT I button (*left*) to reveal the results. The machine sequentially outputs the number of votes for each candidate on a bank of 7-segment LEDs (*right*); here, candidate number 01 has received 7 votes.

2.3 Challenges for Electronic Voting in India

Indian EVMs are designed to face more difficult natural and operational challenges than other electronic voting systems studied in previous security reviews. These factors have influenced the simple design of the machines and impact our security analysis. Among these 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 [36], 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 adverse conditions and must be stored for long periods in facilities that lack climate control. An Election Commission report cites dangers from "attack by vermin, rats, fungus or due to mechanical danger, [that might cause] malfunction" [4].

Illiteracy Though many Indian voters are well educated, many others are illiterate. The country's literacy rate in 2007 was 66% [54], 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.

Unfamiliarity with Technology Some Indian voters 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 [16]. 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 5 per minute [4].

Any voting system proposed for use in India must be able to handle these types of 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 [36] was conducted by an "expert committee" comprised 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, but 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 [4] 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 that report, they reiterated their 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 addition 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 Fraud

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 [49, p.54]. Nevertheless, they paint a troubling picture of election security in India.

These reports are extensively surveyed by Rao [49]. For instance, in the 2009 parliamentary election, he relates that there were reported EVM malfunctions in more than 15 parliamentary constituencies across the country. Especially troubling are reports 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 [49, p.45] . Rao also relates reports from prominent politicians that engineers approached them in 2009 offering to fix elections through this method [49, pp.60-61].

Despite reports like these, 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 [49, p.98]. In a television interview, P.V. Indiresan, who headed 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 from Hindu scripture) [21].

We have had direct experience with attempted fraud. Hari Prasad, a coauthor of this report, 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.

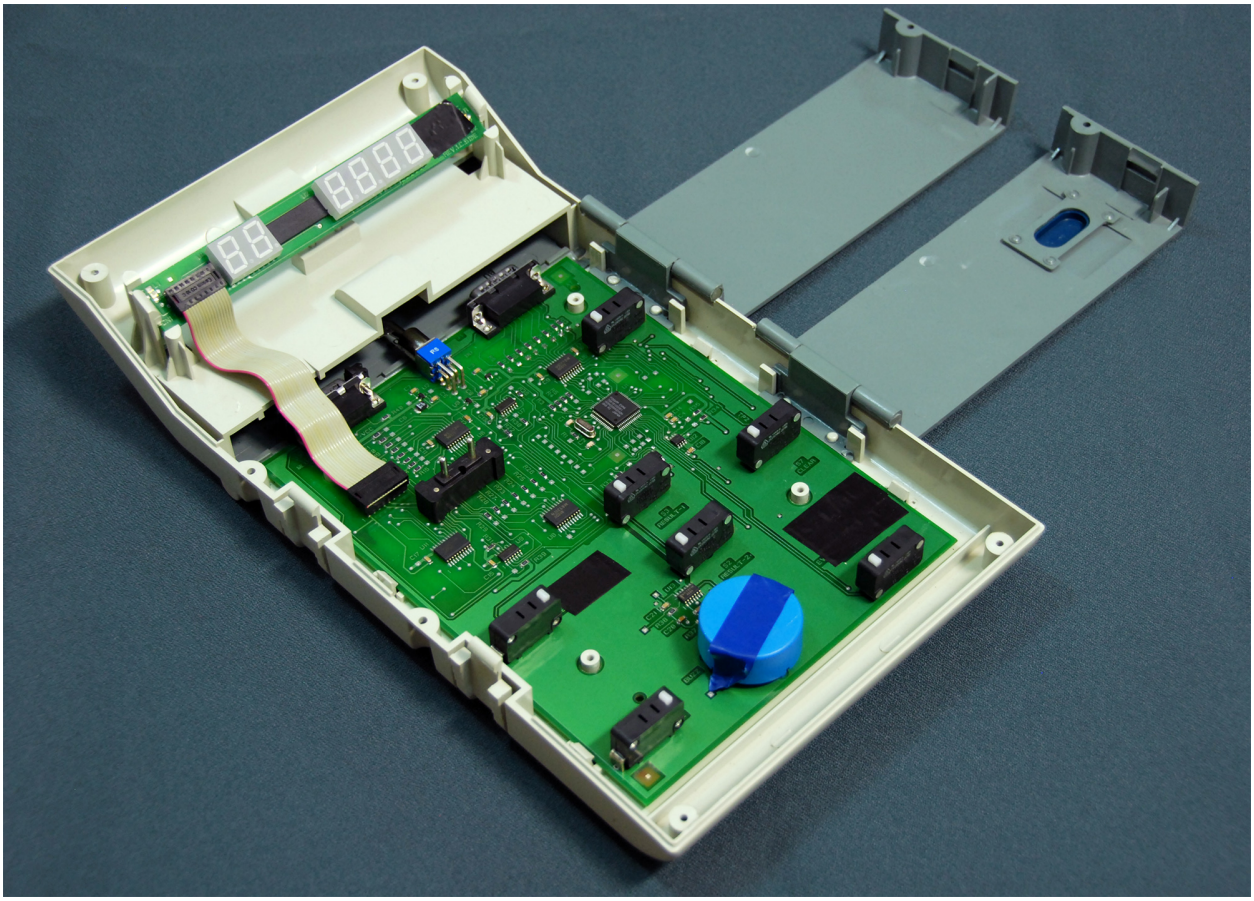

Figure 3: **Inside the Control Unit** — The control unit contains a main circuit board, as well as a smaller display board that shows the election results and other output. The hardware inside the EVM has never before been subjected to detailed public scrutiny.

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 [24]. 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 Figures 3 and 4. The centerpiece is the EVM's CPU, a Renesas H8/3644 series microcontroller driven by an 8.8672 MHz crystal oscillator. The election software is contained inside the CPU in a mask ROM during manufacturing, so the chip cannot be electronically reprogrammed. Also on the main circuit board are the switches for the buttons on the face of the device, a buzzer[1], two EEPROM chips used for non-volatile storage of vote data, the display board connector, and the connector for the ballot unit.

Control Unit Display Board The display board, also shown in Figures 3 and 4, 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 contains a simple circuit in which the control unit main board directly drives the 7-segment LEDs. The CPU

[1]The buzzer is extremely loud, especially with the case removed. During tests conducted at night, its sound would cause dogs all over the neighborhood to begin barking. For this reason, we covered the opening with blue electrical tape, which can be seen in the pictures throughout this report. Black tape in the pictures covers features that could be used to identify this individual machine, in order to protect the anonymity of the source.

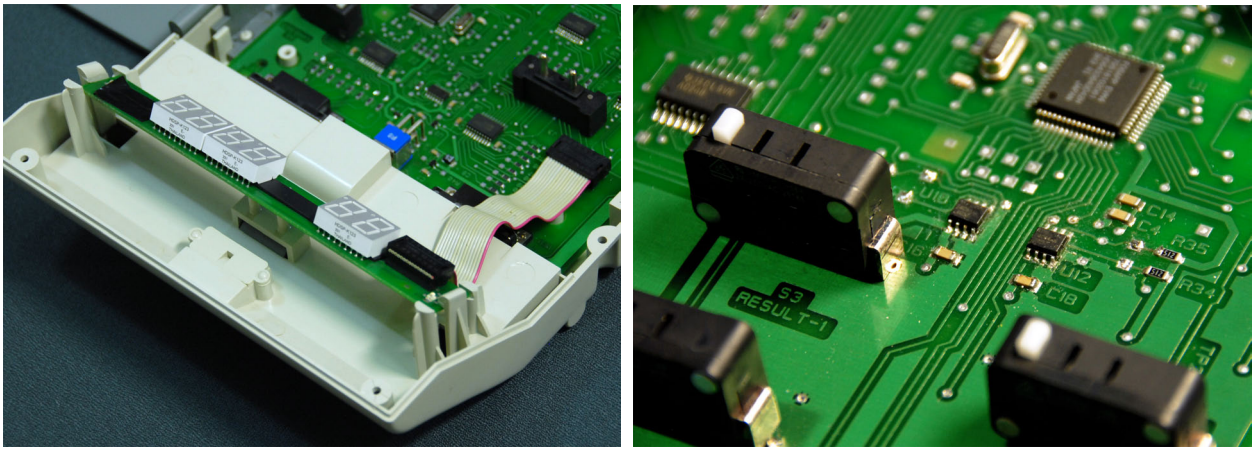

Figure 4: The **display board** in the control unit (*left*) is a simple electric circuit containing only LEDs and a connector. The 7-segment LEDs are raised slightly by a black plastic spacer. Most of the machine's logic is contained on the control unit **main board**, including the processor (*right-rear*) and two EEPROM memory chips that store the votes (*right-center*).

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 4-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. It communicates with the control unit as follows. First, the control unit sends the number of the ballot unit it wants to check. The first EPLD in each ballot unit reads this number, compares it to the position of the slider, and activates the second EPLD if the two numbers match. The second EPLD on the active ballot unit scans the 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 simply 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 [5]. 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, it would be straightforward to reverse engineer it using standard disassembly tools (e.g., [34]).

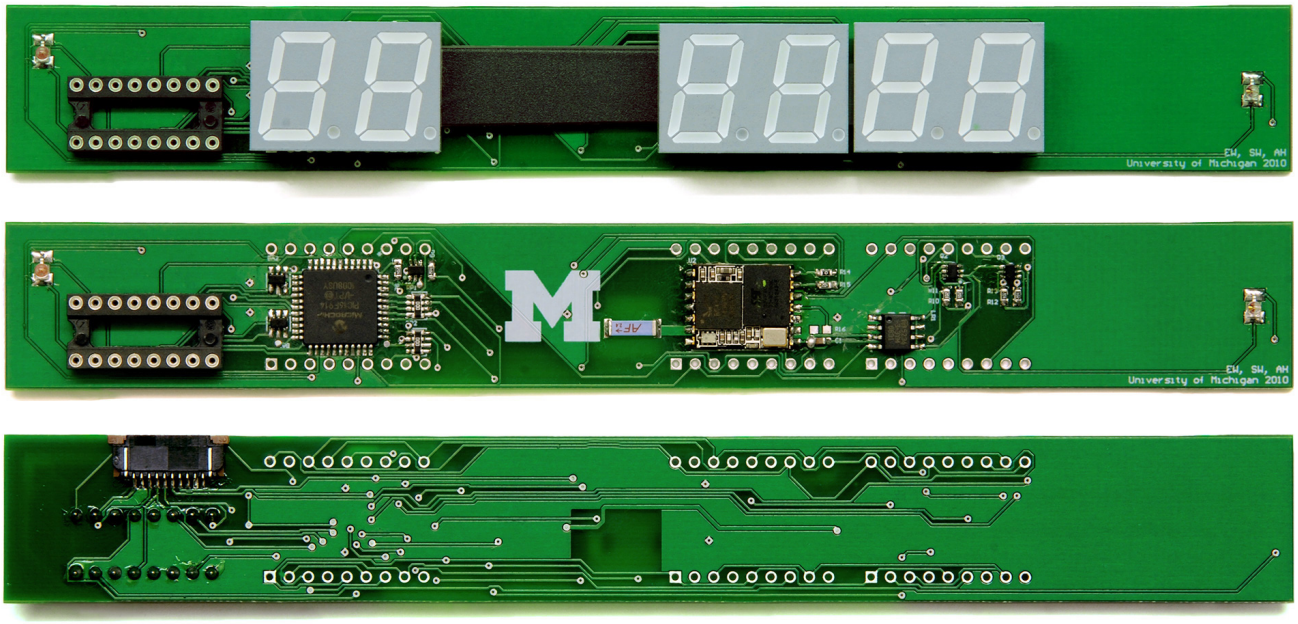

Figure 5: **Dishonest Display Attack** — We developed a dishonest display board, shown here at actual size (*top*). It looks almost identical to the real display board inside the control unit, but it contains extra components (*middle*) hidden beneath the 7-segment displays and plastic strip: a PIC microcontroller that replaces the election results with fradulent ones as they are displayed, and a Bluetooth radio module that allows the attacker to wirelessly signal which candidate should receive the stolen votes. The only visible component on the reverse side (*bottom*) is a connector used in testing, which can be removed before deploying the attack.

3 Demonstration Attacks

We implemented two demonstration attacks to illustrate and experimentally confirm the security problems with Indian EVMs. These demonstrations show that attacks against the EVMs are practical and that they can circumvent safeguards such as candidate order randomization. We built these attacks without access to the machines' source code and with only limited access to the EVMs during the design and testing process. Nonetheless, they are fully functional on the 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.

3.1 Dishonest Display Attack

For our first demonstration attack, we developed a dishonest display board, shown in Figure 5, that can replace the real display board in the control unit. Normally, the EVM display board shows the vote totals received by each candidate when the votes are counted. The dishonest display adds a separate, hidden microcontroller that sends its own signals to the 7-segment LEDs to show fraudulent vote totals.

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

We developed a working prototype 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 publically counted, perhaps years before the election. Election insiders and EVM manufacturer maintenence personnel routinely have sufficient access, and criminals would be able to obtain access in places where the physical security of the machines is lax.

Design Details Our dishonest display uses the same LEDs and connector found on the real display board and adds a Microchip PIC16F914 microcontroller, a KC Wirefree KC22 Bluetooth module, an Antenna Factor chip antenna, and various discrete components. To make the dishonest display look as much like the real board as possible, we conceal these extra components by placing them under the LEDs. Conveniently for attackers, the LEDs on the real board are raised about 2 mm by a plastic spacer. We omit the parts of this spacer underneath the LEDs to make room for our additional 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 cathodes of each digit. To select a 7-segment digit, the CPU drives its common-cathode 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. At any given time, even when the display is blank, at least 5 of the 6 selector lines are driven high, so our dishonest display can use them as its power source. (The 16-pin connector includes a separate wire for ground.) The control unit provides these signals through a digital isolator, which can source 25 mA per output pin. From this, we are able to draw a total current of about 150 mA—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 which candidate is to be favored or disfavored, and by what margin. There are many different ways that attackers could send such a signal—various kinds of radios, 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 its 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 [26, 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 implemen; however, it carries the risk that a third party might perform his own Bluetooth inquiry scan and detect the signaling.

Figure 6: **Wireless Signaling** — An application running on an Android mobile phone uses Bluetooth to tell our dishonest display which candidate should receive the stolen votes. Attacks using other forms of radio communication are also possible.

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 6. 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 acknowledgement 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., [31]), vote-stealing attacks need to keep the overall total number of votes cast the same 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 many attack scenarios considered in previous work, determining fraudulent vote totals is straightforward, even with this constraint. However, attacks that compromise a machine's input or output devices, such as our dishonest display, do not have access to vote data ahead of time, and so face a more difficult challenge.

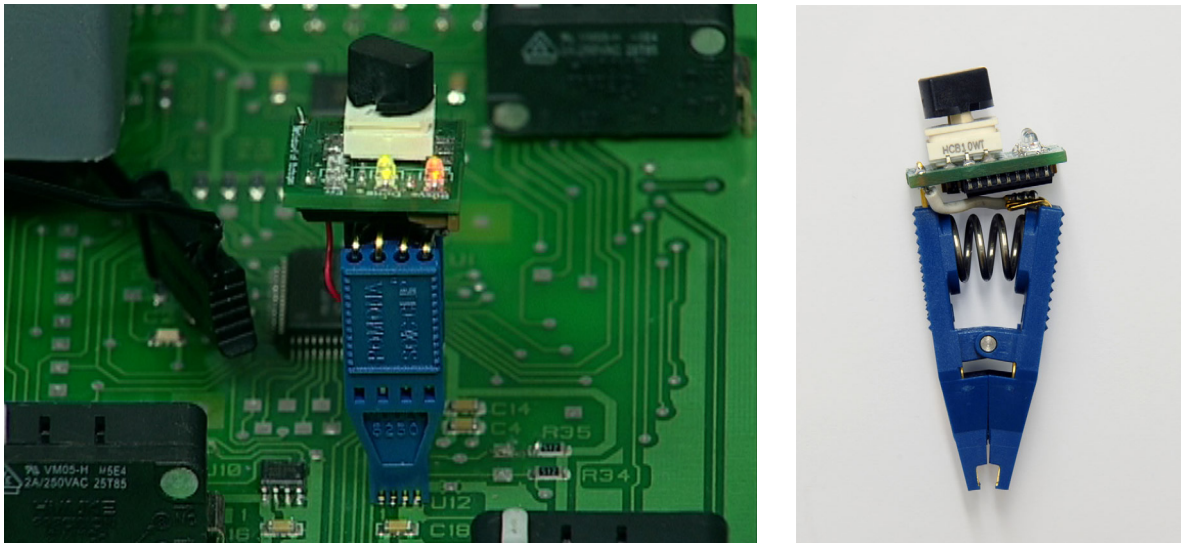

Figure 7: **Clip-on Memory Manipulator Attack** — We developed an attack device that attaches directly to the memory chips that store the votes in the control unit (*left*). Shown actual size (*right*), the device fits in a shirt pocket and can be used to steal votes or to violate ballot secrecy.

The dishonest display board can only see vote totals as they are displayed by the control unit CPU, must display each vote total promptly, and must advance the display to the next total after a brief time interval. As a result, it has to *commit* to a vote total for each candidate before it sees the vote totals for the remaining candidates. In other words, our vote-stealing algorithm must be *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.

3.2 Clip-on Memory Manipulator Attack

We also experimented with a second category of hardware-based attack: attacks that use new hardware to alter the internal state of the machine. Unlike the first category, which replaced hardware components with dishonest look-alikes, this category involves only the temporary application of new hardware.

The attack we prototyped is a device that clips directly to the EEPROM memory chips used to record votes inside the EVM. This small device, shown in Figures 7 and 8, fits discreetly in a shirt pocket. It facilitates two kinds of attacks: stealing votes and violating ballot secrecy.

The first attack is vote stealing. 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. In normal operation, the EVM limits the rate of voting to no more than 5 per minute. However, our device bypasses the software restrictions of the EVM, so an attacker is able to again forcibly take control of an EVM and stuff the electronic "ballot box" with any number of votes.

The second kind of attack is to violate ballot secrecy. Internally, the EVM records votes in the order in which they were cast, and our device can 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.

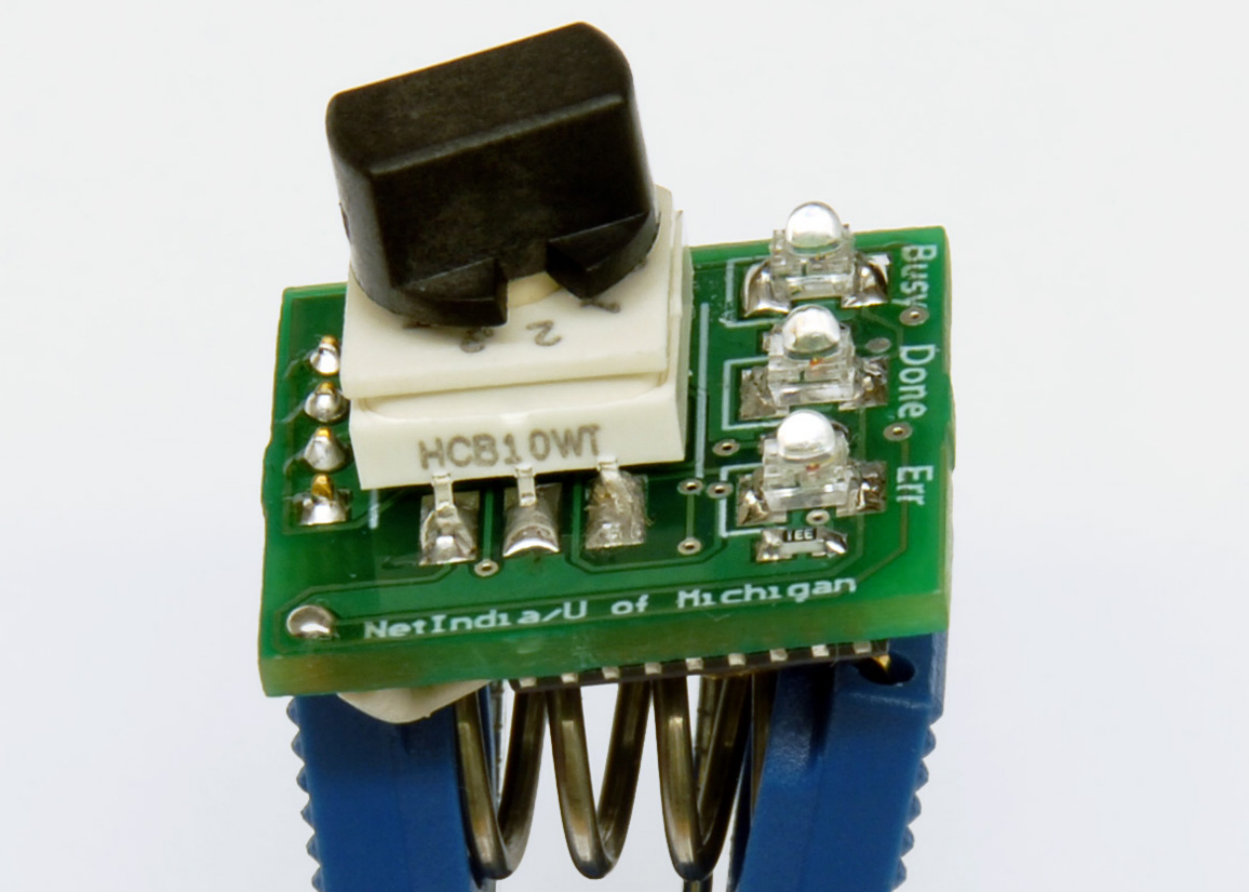

Figure 8: **Clip-on Memory Manipulator (close up)** — A rotary switch allows the attacker to select which candidate to favor.

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 with each representing a single vote for a single candidate. Our testing showed that these vote 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 the EEPROMs via I^2C. We avoid this condition by holding the CPU in reset, which effectively disconnects it from the I^2C bus by forcing the relevant GPIO 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. The device incorporates a Microchip PIC16F88 microcontroller, a 10-position rotary switch, and 3 colored LEDs corresponding to “Busy,” ”Done,” and ”Error” conditions. The PIC’s GPIO pins are connected to the LEDs, the rotary switch, the I^2C pins on the test clip, and UART lines on its

programming connector; the UART lines allow the device to be used as an EEPROM programmer when it is connected to a PC. In addition, the power and ground planes of the PCB are connected to the power and ground pins on the test clip so that the device can draw power from the EVM.

To use the device, the attacker connects a jumper wire to the control unit CPU to hold it in reset. Next, he clips the device to one of the EEPROMs on the control unit board. When the "Done" LED on the device lights, the attacker repeats this process for the second memory chip.

Stealing Votes To steal votes, the attacker indicates his favored candidate using the rotary switch, shown in Figure 8. The rotary switch selects a number from 0–9, and the attacker can use it to pick a favored candidate in any of the first 9 ballot positions, which normally include the major national parties.

When the switch is set to positions 1-9, the chip on the clip-on device executes a vote-stealing program we wrote. The program runs in two passes: first, it reads the list of votes and calculates how many votes to steal from each candidate, and second, it rewrites the list of votes, stealing votes as calculated in the first phase. To reduce the chance of failures caused by intermittent connections to the 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 just needs to reattach the device, and 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.

We implemented two algorithms for calculating the number of votes to steal. The first is a proportional boost algorithm, similar to that described in Section 3.1. The second guarantees the victory of the favored candidate by stealing a vote from each candidate in a round-robin fashion until the favored candidate is the winner.

Violating Ballot Secrecy Because votes are stored as individual records and in the order in which they were cast, an attacker could use the clip-on device to violate the secret ballot by extracting the vote records. Our demonstration attack device can accomplish this using a "tethered execution mode." When the rotary switch is set to position 0, the device can be connected to a laptop computer with a ribbon cable, and it awaits commands to read or write the EEPROM. This allows the attacker to download the vote records to the laptop.

After extracting the ordered 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 is publicly obtainable under Right to Information law in India. 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.

4 Vulnerability Analysis

Indian EVMs use a simple embedded system design, as described in Section 2.6. Superficially, this design might appear to be superior to the complex design used in most other deployed DREs. While many other DREs rely on commodity operating systems and run election software containing tens or hundreds of thousands of lines of code, the Indian EVMs' software is compact, consisting of only a few thousand instructions that run directly on the hardware. Prior work in EVM security has recommended minimizing the size of the TCB, yet, as we have demonstrated, this has not resulted in a secure system.

In this section, we describe a number of ways that criminals could still access the system, there are many ways that criminals could still attack the system given physical access to the components in the supply chain or physical access to the machines before or during elections, even if the software itself is completely error-free. Many of these attacks could be performed once and then continue to influence 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 these physical tampering attacks far easier.

Tampering with the Software before CPU Manufacture The EVMs are designed so that the firmware is stored in masked read-only memory in the microcontroller, and there is no provision for reading it out or verifying its integrity. This means that if the software was modified before it was burned into the CPUs, the changes could 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 the codebase of a voting system of such low relative complexity is not very hard and has been done (sometimes within a few weeks) with other voting systems in the context of academic research [32].

Substituting Look-Alike CPUs After the software is burned into the CPUs by the foreign chipmakers, these CPUs must be shipped to India where they will be assembled into the control unit circuit 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 using 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 chip makers 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 circuit 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 circuit 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.

Even if the software in the CPU is trustworthy, the system also treats its input and output devices as trusted components. An attacker could also 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 also trusted, 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 demonstrated the dishonest display board attack in Section 3.

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

Co-author Hari Prasad quickly constructed a proof-of-concept look-alike EVM to demonstrate some of the things dishonest software could do. He found that matching the electronic functionality was easy due to the simple design of the machine. A more difficult challenge was manufacturing a convincing-looking plastic housing. 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 while retaining 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 demonstrated such an attack in Section 3 and showed how it can be used to alter election results and to violate ballot secrecy.

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 [28] focus on guarding the EVMs from the time they are inspected before an election to 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" [49, p.217]. In one video [46], 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 [46]. However, these seals are extremely weak, consisting of stickers, strings, melted wax and plain paper labels (see Figure 9). None of the materials are hard to get or difficult to forge. The election authorities might switch to more sophisticated seals in the future, but this would still not be a sufficient countermeasure. Tamper-evident seals have been frequently discredited in scientific studies of electronic voting. For example, Appel reported [6] that the relatively sophisticated seals applied to the AVC Advantage in New Jersey were easy to defeat. His attacks centered around undetectably removing the seals and replacing them using simple, readily available tools. For example, the seals most similar to those used on India's EVMs were the plastic strap seal, defeated with a jeweler's screwdriver, and tamper-evident tape, defeated by applying a heat gun, carefully peeling it off, and reapplying it later. Other researchers who study tamper-evident seals have reported that nearly every kind they have experimented with is trivial to attack [35].

Even if the seals were difficult to attack, responding to broken seals presents additional challenges for election officials. What should officials do if they find that a large number of control unit seals have been broken before the count? Since a memory manipulation attack like the one we demonstrated could have

Figure 9: **Tamper-Evident Seals** — Frames from an official poll worker instruction video [46] (*top*) show how the control unit is sealed with red wax and string. The seals protecting the screw holes on the case (*bottom*) consist of printed paper stickers. Such low-tech seals could be easily faked and provide an extremely weak defense.

tampered with the votes without leaving any visible traces, they might decide to discard all the votes cast on the machines with the broken seals. However, this creates an even easier, low-tech attack: a dishonest insider or other criminal could simply break the seals on control units at polling places where voters are 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 EVM's 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" [4]. On the contrary, we conclude that these mock polls offer the least added security of any of the countermeasures we discuss here. 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 any of the attacks as proposed in this paper.

Secret Source Code The second- and third-generation EVMs use election software fused 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" [4]. 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" [21].

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" [37]. 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 using a microscope or more sophisticated methods have been known in the literature for over 15 years [5]. It is an expensive and time-consuming process, but it is routine in industry and it is now being done at the level of academic research (e.g., [45]). 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 [28]. 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 [49, 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 would prevent fraud, because malicious software in the EVMs has 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" [4, p. 4].

In reality the order of the candidates is less random than one would assume. Parliamentary candidates, for example, are split in three groups: (1) candidates of recognized national parties and state political parties in the states concerned, (2) candidates of registered unrecognized political parties and (3) other (independent) candidates. Within each group the candidates are all 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 how the first four buttons will be assigned.

To make a more accurate guess, a dishonest EVM would need to receive a signal from the attacker after the ballot order was determined. There are several methods that might be used to send such a signal:

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 [15], 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, including preparation of EVMs, and assisting the poll officials in counting. 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 [42], 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 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 $n \bmod 5$, 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 demonstrate, 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 time-stamp, presumably to prevent "secret knock" signaling or to be able to revert the effects of booth-capturing. Having a real-time clock gives the author of 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 Electronic 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. [39], SAIC [52], RABA [48], and Feldman et al. [31]. These works concentrated on vulnerabilities in voting machine 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 the procedures, code, and hardware reviewed [9]. 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 [8,13]. 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 [10]. 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 [12].

Security Problems in Simple Electronic Voting Systems A few other studies have examined relatively simple computer voting systems, though all have been far more complex than the Indian EVMs, incorporating some form of upgradeable firmware as well as external memories for ballot programming and vote tabulation. Several of these studies focus 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 [32]. 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 [7]. 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 [20]. 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 problems with 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" [13]. Much work has focused on reducing this software complexity. Sastry et al. point to 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" [51]. They recommend that the software be designed in ways that make verification easier, such as by reducing the amount of code that needs to be trusted.

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 external hardware. Simplicity alone cannot cure DRE security problems. Overly simple designs can leave out some of the protections that modern computer security design allows for, such as cryptographic integrity and confidentiality. Very simple and cheap hardware designs allow for easier reverse engineering and simple and cheap hardware tampering. The maximum amount of security in electronic voting systems would likely come from balance—designs that employ complexity intelligently, when it makes the system stronger.

Much other work has examined both hardware attacks outside the context of voting (e.g., [38,53]) and the general problem of security in embedded systems (e.g., [5,15,50]). Several authors have proposed end-to-end verifiable cryptographic voting systems [17–19,44,47], 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 requirements 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 at any time before ballots are counted 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 more difficult to detect.

It is highly doubtful that these problems could 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 for confidence 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-verified paper audit trail (VVPAT), which combines an electronic record stored in a DRE with a paper vote record that can be audited by hand [43]. 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 [14]. 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 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.

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.

References

[1] Minister Gormley announces Government decision to end electronic voting and counting project. http://www.environ.ie/en/LocalGovernment/Voting/News/MainBody,20056,en.htm, Apr. 2009.

[2] Singapore, Malaysia, South Africa approach BEL for EVMs. *The Hindu*, Apr. 2009. http://www.hindu.com/thehindu/holnus/002200904121051.htm.

[3] Compulsory voting not practical, says CEC. *Press Trust of India*, Apr. 2010.

[4] 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.

[5] R. Anderson and M. Kuhn. Tamper resistance: a cautionary note. In *Proc. 2nd USENIX Workshop on Electronic Commerce*, Berkeley, CA, USA, 1996. USENIX Association.

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

[7] 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. EVT/WOTE 2009*, Aug. 2009.

[8] 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. 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 08)*, July 2008.

[9] D. Bowen et al. "Top-to-Bottom" Review of voting machines certified for use in California. Technical report, California Secretary of State, 2007. http://sos.ca.gov/elections/elections_vsr.htm.

[10] J. Brunner. Evaluation & validation of election-related equipment, standards & testing(EVEREST). Technical report, Ohio Secretary of State, 2007. http://www.sos.state.oh.us/SOS/Text.aspx?page=4512.

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

[12] 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. 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 08)*, July 2008.

[13] 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. Technical report, California Secretary of State, Aug. 2007.

[14] J. A. Calandrino, J. A. Halderman, and E. W. Felten. Machine-assisted election auditing. In *Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 07)*, Aug. 2007.

[15] 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 '09)*, pages 400–409, 2009.

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

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

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

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

[20] 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 2009*, Aug. 2009.

[21] CNN-IBN. Interview with PV Indiresan. http://ibnlive.in.com/videos/97488/evms-rigged-poll-panel-challenges-doubters.html.

[22] A. U. de Haes. Dutch government bans electronic voting. *IDG News Service*, May 2008.

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

[24] Election Comission of India. The Commission's reply to Sh. V. V. Rao dated 29th March 2010. http://eci.nic.in/eci_main/recent/reply__sh.VVRao.pdf, Mar. 2010.

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

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

[27] Election Commission of India. Electronic voting machines–regarding. http://eci.nic.in/eci_main/press/current/pn080809.pdf, Aug. 2009. No.PN/ECI/41/2009.

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

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

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

[31] A. J. Feldman, J. A. Halderman, and E. W. Felten. Security analysis of the Diebold AccuVote-TS voting machine. In *Proc. USENIX/Accurate Electronic Voting Technology Workshop (EVT '07)*, 2007. http://itpolicy.princeton.edu/voting/ts-paper.pdf.

[32] R. Gonggrijp and W.-J. Hengeveld. Studying the Nedap/Groenendaal ES3B voting computer: a computer security perspective. In *Proc. USENIX/Accurate Electronic Voting Technology Workshop (EVT '07)*, 2007.

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

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

[35] R. G. Johnston and A. R. E. Garcia. Vulnerability assessment of security seals. *Journal of Security Administration*, 20, 1997.

[36] C. R. Kasarbada, P. V. Indiresan, and S. Sampath. Report of the expert committee for technical evaluation of the electronic voting machine, Apr. 1990.

[37] A. Kerckhoffs. Cryptographie militaire, 1883.

[38] S. T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, and Y. Zhou. Designing and implementing malicious hardware. In *Proc. 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, pages 1–8, Berkeley, CA, USA, 2008. USENIX Association.

[39] T. Kohno, A. Stubblefield, A. Rubin, and D. Wallach. Analysis of an electronic voting system. In *Proc. IEEE Symposium on Security and Privacy*, pages 27–40, May 2004. http://www.cs.washington.edu/homes/yoshi/papers/eVoting/vote.pdf.

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

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

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

[43] R. Mercuri. *Electronic Vote Tabulation: Checks and Balances*. PhD thesis, University of Pennsylvania, 2001.

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

[45] K. Nohl and D. Evans. Reverse-engineering a cryptographic RFID tag.

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

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

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

[49] G. V. L. N. Rao. *Democracy at Risk!* (Book on Indian EVMs published by Citizens for Verifiability, Transparency & Accountability in Elections), New Delhi, 2010.

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

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

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

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

[54] UNICEF. India statistics. http://www.unicef.org/infobycountry/india_statistics.html.

[55] Wikipedia. Results of the 2009 Indian general election by parliamentary constituency — Wikipedia, the free encyclopedia. http://en.wikipedia.org/w/index.php?title=Results_of_the_2009_Indian_general_election_by_parliamentary_constituency&oldid=347683199, 2010. [Online; accessed 17-April-2010].

J. Alex Halderman *Hari K. Prasad* *Rop Gonggrijp*

— Hyderabad, February 2010

About the Authors

Hari K. Prasad is managing director of NetIndia, (P) Ltd., a Hyderabad-based research and development firm. In 2009, the Election Commission of India publicly challenged Prasad to demonstrate that India's EVMs could be tampered with, only to withhold access to the machines at the last minute.

Dr. J. Alex Halderman is a professor of computer science at the University of Michigan. A noted expert on electronic voting security, Professor Halderman demonstrated the first voting machine virus and helped lead California's "top-to-bottom" electronic voting review. He holds a Ph.D. from Princeton University.

Rop Gonggrijp is a technology activist from Holland who was instrumental in having EVMs banned in the Netherlands. In 1993, Gonggrijp cofounded XS4ALL, the first ISP in the Netherlands to offer Internet service to the general public.

Scott Wolchok and **Eric Wustrow** are student researchers at the University of Michigan.

Arun Kankipati, **Sai Krishna Sakhamuri**, and **Vasavya Yagati** are engineers at NetIndia.

To contact the authors, please email authors@IndiaEVM.org.