A CASE STUDY ON INDIAN E.V.M.S USING BIOMETRICS

Aduri Kishore Reddy
Assistant Professor, Department of ECM, KL University, A.P,India, krish.aduri@gmail.com

Abstract
With significant Indian federal funds now available to replace outdated electronic voting machine throughout the India are adopting paperless electronic voting systems with biometric applications from a number of different vendors. We present a security analysis of the source code to one such machine used in a significant share of the market. Our analysis shows that this voting system with the biometric is far below even the most minimal security standards applicable in other contexts. We identify several problems including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, poor software development processes and rigging by using electronic voting machine. We show that voters, without any insider privileges, can cast unlimited votes without being detected by any mechanisms within the voting terminal software. In this paper we are giving an idea for avoiding the rigging from electronic voting machines by implementing the biometric systems on electronic voting machines in Indian elections. We suggest that the best solutions are voting systems having a “implementation of biometric systems on electronic voting machines.”

Index Terms: Electronic voting machines, Biometric system, Security problems, Generic Algorithms

1. INTRODUCTION
1.1 Electronic Voting in India
The EVMs are developed by Electronics Corporation of India (ECIL) and Bharat Electronics Limited (BEL) though these companies are owned by the Indian government.

In 1980s by ECIL, The first EVMs are developed. 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. In 2006, the manufacturers adopted a third-generation design incorporating additional changes suggested by the Election Commission.

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.

According to Election Commission of India 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. In the 2009 parliamentary election, there were 417,156,494 votes cast, for an average of 302 votes per machine.

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

1.2 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., SAIC, RABA, and Feldman et al. 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 “top-to-bottom review” of her state’s voting machines, which found significant problems with procedures, code, and hardware. 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. 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. 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.

To Avoid the Security Problems and Rigging in Voting Systems, we have to develop a new Mechanism for E.V.M. Our goal is adding the biometric system to E.V.M.s

2. BIOMETRIC SYSTEMS

In the mid-1960s, the Royal Canadian Mounted Police adopted an automated video tape-based filing system allowing identification officers to make fingerprint comparisons on-screen. A similar ‘Video file System’ was installed at New Scotland Yard in 1977. Around the same time, the USA’s Federal Bureau of Investigation was working with industry to build the first automated fingerprint card reader, which was implemented in 1974. Over the next five years, the FBI and other organizations in Canada, Japan and the UK, developed further core technologies including fingerprint matching hardware, plus automated classification software and hardware. By the early 1980s, this culminated in the automatic fingerprint identification system, which allowed the automatic matching of one or many unknown fingerprints against an electronic database of known prints; another major forward step in the world of crime detection and international security. Such systems have since reduced the manual capture, store, search and match processes for fingerprints from weeks and months, to hours and minutes, and have led to AFIS being deployed by law enforcement agencies in Europe and worldwide.

Now a Days we are using the figure prints for biometric as uses impressions printed on paper or card with ink, or digital scans of an individual’s fingers to record their unique characteristics. The risk of a duplicate print/scan occurring is now estimated at being 10 to the 48th power: in other words, each finger print is as close to being ‘unique’ as you can get. Fingerprints therefore remain the most powerful and widely used biometric technology in forensics. A common statistic however, is that 30% of crime scenes include palm prints, which is why these are also captured and processed using the latest AFIS solutions.

3. IMPLEMENTATION

Our idea is to implement a new Electronic voting machine with biometric that is shown in following figure as a sample. In this EVM’s we have to use figure print of persons.
Before the Elections, the government of our country has to take the minimum two figure prints for our biometric system from each and every persons of society. The finger prints are stored in a permanent data base. Elections before two days, we are copying the data from permanent data base to temporary database. This is the basic background work of electronic voting mechanism with biometric system.

In the polling booth we have to connect the temporary database with electronic voting machine with the biometric systems. The basic idea of our problem is to avoid the rigging, that’s why we have to implement a code that works as if a person gives a thumb impression to a particular party then immediately increases a count variable of object (party symbol) and remove the particulars of a person from temporary Data base. After completion of voting, we have to check the count value of id of party name. We have to check the temporary database for highest value of count the highest value of party is winning party.

4. GENETIC ALGORITHM

switch (n) {
  Case “one”:
    Count=count+1;
    Delete (person_finger_id);
    break;

  Case “two”:
    Count=count+1;
    Delete (person_finger_id);
    Break;

  Case “three”:
    Count=count+1;
    Delete (person_finger_id);
    Break;

  ....

  Case “n”:
    Count=count+1;
    Delete (person_finger_id);
    Break;

  Default:
    print(“please give u r finger print”);
}

Algorithm1: Genetic Algorithm for Removing Data From Temporary database

FUTURE WORK

Twins has the same finger prints, in that situation this is failure if the person is not having the correct identities in his/her finger in this situations this is also failure. Our future work is to avoid this problem.

CONCLUSION

To avoid the rigging concept in today’s EVM’s this is best approach for done the elections with effective manner and simple way. This is the suitable EVM for elections. Our analysis shows that this voting system with the biometric is far above even the most minimal security standards applicable in other contexts

REFERENCES