Towards a Fraud Prevention E-Voting System

Dr. Magdi Amer
Faculty of Computer Science
Umm A-Qura University
Makkah, KSA

Dr. Hazem El-Gendy
Faculty of Engineering
Canadian University in Egypt
Cairo, Egypt

***Abstract*—Election falsification is one of the biggest problems facing third world countries as well as developed countries with respect to cost and time. In this paper, the guidelines for building a legally binding fraud-proof Electronic-Voting are presented. Also, the limitations are discussed.**

Keywords—e-voting, security

I. INTRODUCTION

Dictators harm the countries they control. Furthermore, their harm usually extends to the rest of the world through wars they introduce and terrorist activities they host and fund. Therefore, it is the duty of everyone to work towards enforcing free election in the entire world.

Also, guaranteeing the transparency of elections, reducing the cost of elections and their times are key objectives. This motivated the trend towards electronic elections which can facilitate achieving these objectives plus being convenient. However, the move towards e-elections raises the question of guaranteeing absence of falsifications and assuring transparency.

Building electronic voting system has been an active field of research. A survey of the current legally binding electronic voting system can be found in [1], and a survey on cryptographic techniques used in e-voting can be found in [2]. There are also several research papers on increasing the reliability of the e-voting process by using verifiable voting receipts that doesn't break the privacy requirements of the election, such as [3], [4], [5].

The purpose of this paper is to provide Rules that need to be taken into consideration when building an electronic voting system to prevent vote falsification.

In this paper, the Egyptian elections will be taken as an example. The Egyptian voting process and the vote falsification practices will be explained in the next section. In the third section of the paper, software architecture guidelines will be presented. The advantages of these guidelines and the fraud prevention requirements will be discussed in the fourth section. The conclusion of this paper will be presented in the last section.

II. THE DEFECTS OF THE EGYPTIAN VOTING SYSTEM

Egypt is one of the countries that had never conducted a proven fraud-free presidential election since it was established some thousand years ago.

The current voting system is paper based. Each voter will be assigned to a polling station based on the home address indicated in his/her National Identification card (NID), which is a unique number identifying each citizen similar to the social insurance number (SIN) used in North America. The right to vote depends on the nationality, age and criminal records. Some employees, such as police members and judges, are prevented from voting.

On the election days, voters go to their assigned polling station, sign in front of a judge that verifies their identity, take a watermarked voting ballot, choose the candidate that they want and place the ballot in the ballot box. At the end of the election, ballots are manually counted and the result will be announced.

In this manual system, voting falsification may be conducted by candidates and by voting administrators.

Candidate vote fraud can be conducted through a technique called the circulating ballot. In this technique a candidate's accomplice prints a single falsified paper ballot. The falsification doesn't need to look authentic, it only need to be good enough not to be detected when being placed in the ballot box. The candidate's accomplice goes to the polling station, takes a ballot, keeps it empty, and replaces it with the falsified ballot which he/she places in the ballot box. The candidate's accomplice will get out of the polling station and mark the empty paper ballot with the candidate he/she is representing. The candidate's accomplice will give the pre-marked ballot to the voter willing to 'sell' his/her vote for some money, items or services. The voter will go, take and empty ballot and keep it empty and replace it with the pre-marked ballot. When the voter returns the empty ballot to the candidate's agent, the voter will have earned whatever fees he/she agreed upon.

Vote falsification can also be conducted by government with the complicity of the voting authority supervising the polling stations. Voting authority may replace the ballot box with other boxes filled with ballots choosing the government's candidate. This operation is virtually undetectable as long as the fake ballot box contains the same number of ballots as the original box. This can occurs at night in case of a multi-days election, or during the transport of the ballot boxes to the counting centers.

Another vote falsification technique is to add fictitious voters to the voting database and send polling boxes corresponding to these fictitious voters to the polling station without having to replace the original ballot boxes. Another technique is to fill ballots on behalf of voters that did not show on the voting day. Both these techniques can be detected by election observers as the number of actual voters will be much lower than the number of counted votes, but it is hard to prove.

III. RULES

In this section, the system architecture for electronic voting will be presented with emphasis on the elements needed to improve the vote falsification prevention capabilities of the system.

1) Each polling station will contain an online system for voter registration that is not connected to the voting system. The purpose of the registration system is to ensure that the voter has the right to vote and that he or she did not previously vote in another polling station. This allows vote organizers to provide the voters with the option to vote in any polling station, provided that the vote organizing committee is capable of handling large numbers of voters at polling stations in more popular locations.

2) Approved voters will be given a voting token. The voting token is similar to the metallic game tokens used with game machines. These tokens need to be inserted in the voting station to allow the voter to vote and are used to prevent a voter from trying to vote multiple consecutive times at the voting stations.

3) The order of voters in the registration system should be different from the order of voters in the voting stations to prevent linking between both systems to deduce the voter's choices. The simplest way to achieve this is to have some walking distance between the registration station and the voting station that the voters will walk freely, not in lines, without maintaining a specific order.

4) Each polling station will contain one or more voting stations. A unique secret key will be assigned to each polling station and to each voting stations. Before the beginning of the election, each voting station will be programmed with the table schedule of the election days and opening and closing time. Any attempt to vote outside these pre-defined times will not be accepted. Any attempt to temper with the system time will result in the voting station locking itself and becoming unusable for the election.

5) When the voter begins the voting session, a global unique identifier will be assigned to the voter, which is called the Voter Identifier Number (VIN). The voter will choose the candidates that he or she wants from the screen and then presses a button to finalize the voting session. The choices of the voter will be printed and shown to the voter through a class, as described in [6]. The printed paper ballot will contain the VIN, the timestamp, the polling station ID, the voting station ID and a serial number representing the number of votes conducted through this voting station. The voter may press the green button to confirm the choices and terminate the voting session, in which case the paper will be dropped in the ballot box. Pressing on the red button will invalidate the voter choices and the paper will be dropped in a paper shredder, in which case the voter may use the voting station again to correct the vote.

6) Each voting station is connected to a local database. Depending on the election budget, solutions for increasing the database reliability should be implemented. In case of a complete database failure, the result will be provided by counting the printed votes in the ballot boxes.

7) At the end of each voting session, votes will be recorded on the local database. The polling station ID, the voting station ID, the VIN, the timestamp will be stored, as well as the choices of the voter, which will be encrypted using the polling station and voting station keys. The encryption algorithm chosen should combine parameters such as the VIN and the timestamp in the encryption algorithm to produce different results for each vote.

8) At the end of the election, each polling station will use its local database as well as the paper ballots to calculate the number of votes each candidate got. If both results match, the results of this polling station will be announced pending confirmation from the central voting server.

9) These votes will be sent to a central server though a network or using devices such as CDs. The center server will check that the votes were encrypted using legitimate voting station and polling station keys. Any mismatch will invalidate the electronic results of that polling station.

10) A mismatch between the paper count and the electronic count at a polling station or a mismatch between the encrypted votes and the keys of the polling station and the corresponding voting stations will invalidate the votes at that polling station. The decision on how to handle the situation will depend on the decision of the judges supervising the elections.

11) If no trace of vote manipulation is found, the central server will calculate the total votes for each candidate and publish the results. All the tables related to the vote will be made public after the decryption of the vote fields, allowing any third party to check the results.

IV. PROTECTION AGAINST VOTE FALSIFICATION

Following the rules presented in the previous section will help achieving a high level of protection against results falsifications.

First of all, candidates will not be able to bribe voters to manipulate their votes as the candidate will have no mean of checking the choices that the voters made in the election. Nevertheless, in case of corrupted election organizers, the voter may be allowed to take a picture of the printed election paper ballot, thus providing the candidate with the proof needed to allow vote selling. This risk may be reduced by using anti-flash glass over the paper ballot and the screen of the voting station to prevent digital pictures from being taken.

Moreover, government attempts to falsify the election without hacking the programs used in the election are easy to detect and thus cannot succeed.

Replacing the actual voting boxes with fake ones is useless, as the result comparison between the paper ballot and the electronic voting database will show a mismatch which will invalidate the election at this polling station.

Entering votes for voters that did not show cannot happen. The voting station is protected from clock manipulation and from entering votes outside the pre-defined opening hours and

dates of the election. The government cannot determine the list of voters that did not show till the end of the election, by which time it will be too late for the list to be useful.

Adding fictitious citizen to the voters' database and using them to enter fake vote is hard to implement. Having a person entering multiple consecutive votes during the election days will be easily detected by other voters and thus impractical. The maximum damage that a corrupted government can make is to issue multiple fake IDs to government agents and use them to vote multiple times in multiple polling stations. The logistics associated with such a plan makes this approach difficult to achieve and will place an upper limit on the number of fake votes that can be added using such a technique.

There is a risk of taking a legitimate voting station and hiding it from the public and use it to enter fake votes. This risk can be eliminated by assigning a known number of voting stations to every polling station and to make the public aware that they should report any polling station that has some missing voting stations. Moreover, statistical analysis showing a large vote bias at a specific voting station compared to other voting stations at the same polling station will be a valid proof of vote falsification.

If a corrupted government succeeds in breaking the voting application, there is hardly any solution that can be used. The work of [3], [4], [5] is very interesting as it provides a mean of detecting vote falsification while keeping the vote confidentiality, but this requires the protection of the encryption keys, which cannot be protected if the entire governmental entity supervising the election is corrupted. The only way to protect the elections in this case is to allow an international entity to supervise the election and trust it with the encryption keys. The same international entity should also be allowed to inspect voting station software during the election to detect any software manipulation.

V. Conclusion

A world with no dictatorships will be a peaceful and prosperous world. In this paper, the rules for building a system resilient against vote falsification were presented. A solution that can protect the election against a widely speed corruption in the organization supervising the election is not yet possible. The only feasible way that the current level of technology allows is to call for the establishment of an international organization that supervise the setting of the voting stations and that is trusted with the issuing and safekeeping of the needed encryption keys.

Acknowledgment

This research was conducted with the collaboration of Ambassador Mahmoud Mostafa from the Egyptian Ministry of Foreign Affairs, as part of the ministry effort to build an electronic voting system for Egyptians living abroad.

References

[1] D. Demirel, R. Frankland and M. Volkamer, "Readiness of various evoting systems for complex elections", Technische Universtität Darmstadt, Tech. Rep. TUD-CS-2011-0193, 2011, pp. 1–14.

[2] M.J. Moayed, A. Abdul Ghani and R. Mahmod, "A survey on Cryptography Algorithms in Security of Voting System Approaches", International Conference on Computational Sciences and Its Applications(ICCSA), 2008, pp. 190 - 200

[3] D. Chaum, "Secret-ballot receipts: True voter-verifiable elections", IEEE Security & Privacy, Volume: 2 , Issue: 1, 2004, pp. 38 - 47

[4] Y. Lee, S. Kim and D. Won, "How to Trust DRE Voting Machines Preserving Voter Privacy" IEEE International Conference on E-Business Engineering (ICEBE), 2008, pp. 302 – 307

[5] L. Rura, B. Issac and M. K. Haldar, "Secure Electronic Voting System Based on Image Steganography", IEEE Conference on Open Systems (ICOS), 2011, pp. 80 – 85.

[6] R. Mercuri, "A Better Ballot Box?", IEEE Spectrum, Volume: 39 , Issue: 10, 2002, pp. 46 - 50.