The Journal of Systems and Software 82 (2009) 2081–2090

Contents lists available at ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

Approach to designing bribery-free and coercion-free electronic voting scheme

Yu-Fang Chung [a,*], Zhen-Yu Wu [b]

[a] Electrical Engineering Department, Tunghai University, Taiwan
[b] Computer Science and Information Engineering Department, National Taiwan University, Taiwan

ARTICLE INFO

Article history:
Received 7 December 2008
Received in revised form 4 May 2009
Accepted 2 July 2009
Available online 17 July 2009

Keywords:
Electronic election
Bribery
Coercion
Invisible channel
Biometrics receipts

ABSTRACT

Electronic voting has been in development for more than 20 years, during which it has produced outstanding results both in theory and in practice. However, bribery and coercion remain an open problem, as there is still no suitable manner to prevent or fight them. Publications emphasizing practicality has not been able to achieve effective protection, probably due to their overtly simple protection method, while publications emphasizing theories are difficult to put into practice due to the complicated protection method devised by them. Thus, how to design a scheme that can flawlessly prevent problems of bribery and coercion as well as put into practice easily becomes a significant issue. In this paper, we suggest that designers apply two indispensable design components, invisible channel and biometrics receipts, to design a prevention e-voting scheme, and also to introduce several feasible technology to help with its implementation. Followingly, a prevention electronic voting scheme that matches our ideal is proposed. We expect this study to arouse the interest of more researchers regarding the subject.

1. Introduction

Election is a kind of decision-making process, where people vote for candidates whom they think are suitable for a position. Traditional elections generally require the following three steps to completing the voting process: passing confirmation, taking a ballot into voting booth to vote, and counting and announcing of ballots. Also, it should basically have three security features: a voter must be provided with a valid identity; an election must be held following a fair and secret ballot; a ballot should not be affected by bribery or coercion.

With the rapid development of technologies and popularity of the Internet, varying kinds of application technologies are all tending towards digitization, such as electronic(e)-commerce, e-democracy or e-government, etc. E-voting is of course one of the targets. Compared to traditional elections, the greatest plus in e-voting is its mobility. Through transmission of voting information over the Internet, it not only saves lots of time for voters and paper for ballots, but also due to the convenience in voting raises the percentage of people voting.

The concept of e-voting was firstly proposed by Chaum (Chaum, 1981). E-voting has been in development for more than 20 years now. Below is an overview of its architecture and security requirements.

Similar to traditional elections, an e-voting scheme is composed of three entities, including Authentication Center (AC), Tally Center (TC), and voters. The AC is a trusted unit responsible for certifying the legality of the voter. The TC collects and verifies legality of ballots, and then does the counting and finally announces the election result at the end of the election. Voters should be legal members who have the right to vote.

As (Fig. 1) shows, the main election procedure composes of three phases: authentication phase, voting phase, and announcing phase. In the authentication phase, the AC through verifying certificate confirms the legality of voters and issues valid ballots which permits voters to vote. In the voting phase, a voter cast the vote on the desirable candidate by sending the ballot to the TC. The TC verifies ballots, counts them, and then announces the election result at the announcing phase.

The security requirements for e-voting schemes are born of the special features in traditional elections. The requirements mainly include the following:

1. **Anonymity**: No one can connect a ballot to its voter.
2. **Eligibility**: Only those members who are eligible to vote can take part in the election.
3. **Fairness**: The number of votes obtained by each candidate cannot be known before the announcement of the election result.
4. **Mobility**: Voters can cast their votes from anywhere instead of being confined to a specific location.
5. **Uniqueness**: Each eligible voter can cast a vote only once in each election.

* Corresponding author. Tel.: +886 923 287287.
E-mail address: yfchung@thu.edu.tw (Y.-F. Chung).

0164-1212/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2009.07.023

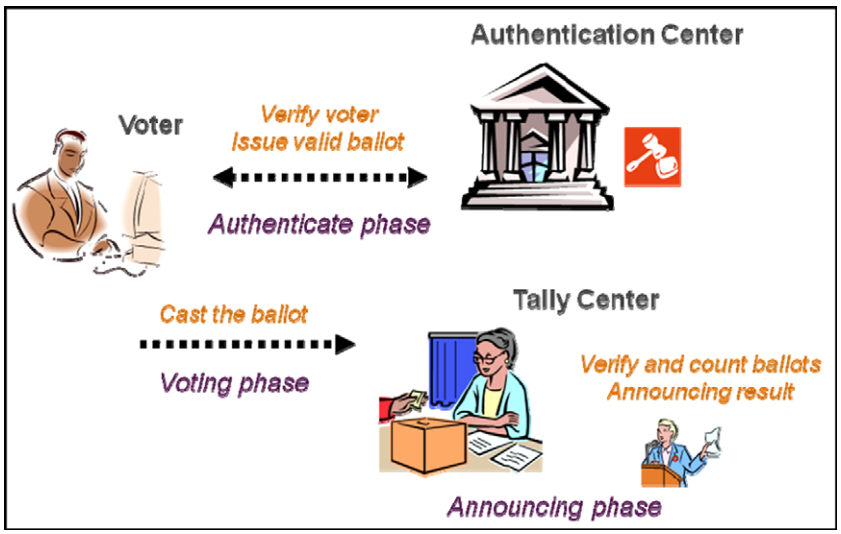

Fig. 1. Procedure of electronic election.

6. **Verifiability**: Voters can find out from the election result whether their votes have been counted.
7. **Uncoercibility**: Voters can still freely choose their desired candidate under bribery and coercion conditions.

The first six requirements are satisfied in most e-voting schemes. The last requirement, uncoercibility, is however never completely met. The reason lies in the ability of bribers and coercers to verify the contents of a voter's ballot through various means of verification. Therefore, previous e-voting schemes were only able to avoid certain verification behaviors and not all. Therefore, to design a complete e-voting scheme that can totally guard against bribery and coercion, we must first understand some common coercer's or briber's verification behaviors (Fan and Sun, 2006; Juels et al., 2005; Hwang and Wu, 2007), as listed below.

1. **Checking election results**: Generally, most e-voting schemes give voters receipts so that voters can verify that their votes have been counted. When voters are coerced or bribed to vote for a particular candidate and then their receipts are taken as the exhibit that the votes have been cast accordingly, such a behavior is called checking election results.
2. **Comparing ballots transmitted**: Some e-voting schemes do not give voters a receipt for verifying whether their vote has been counted. They choose to trust the TC in the counting of votes or use other methods that have no relevance to receipts to verify the votes. At this time, a coercer's or briber's verification behavior for checking election results has in fact no effect. To verify that a voter has followed the instructions in casting the vote, a coercer or briber usually intercepts the ballot during transmission and compares it with the expected value, for which this behavior is called comparing ballots transmitted. In this situation, coercers and bribers need not to wait for the final result to know whether or not a voter has cast the vote accordingly to their instructions.
3. **Acquiring ballot parameters**: The value of a ballot transmitted may be encrypted using random numbers or it could be mixed with nonpublic parameters, so coercers and bribers fail to compare the intercepted voting information against an expected value. Being able to judge whether the vote of a voter matches their expectation, coercers or bribers must find some way to acquire from the voter the parameters related to casting of the vote and kept by the voter. This behavior is named acquiring ballot parameters.
4. **Watching over election process**: Some e-voting schemes may allow voters to secretly convey to the Election Center (EC) at any time during an election which candidate they are voting for. For example, volition of a voter is sent out through an anonymous or untappable channel during the election authentication phase. To prevent the above from happening, coercers or bribers watches over the entire election processes. All parameters generated by a voter and all actions such as sending the certificate, selecting a significant parameter, choosing the content of the ballot, and using a key to encrypt the vote are disclosed to the coercers or bribers. It is hard for voters to violate the order of coercers or bribers since most information is revealed. This behavior is called watching over election process.
5. **Blending in randomization factors**: Assume that ballots generated by an e-voting scheme are composed of random numbers, candidate number or other information. Coercers or bribers may also insert a random number to a ballot, which will not change the form of the ballot but makes the content of the ballot meaningless and unidentifiable by the election committee. These invalid ballots are possibly meant for a certain candidate. If the amount of invalid ballots gets large, the final election result may change and go as coercers or bribers desired. This behavior is called blending in randomization factors.
6. **Substituting voting**: Most electronic applications based on cryptography have a master key or other objects of similar concept. E-voting scheme also has this very important key. This key is similar to a voter's identity, including the certificate used for voting, signature, and receipt; all could have some kind of relation to the key. If some others should obtain this key, they can completely substitute the voter at voting during the entire election. Once the key is known to coercers or bribers, all coercion-free and bribery-free methods turn useless since the key allows them to perform all procedures of an election without the voter. This behavior is called substituting voting.

The first four behaviors occur because coercers or bribers implement passive verification; as long as the values match their expectation, they recognize that the voters have indeed followed their orders. However, the last two behaviors are more active kind of interference. Through interference, coercers or bribers ensure that the election result is as they desired it to be.