Remote e-Voting and Coercion: a Risk-Assessment Model and Solutions

Bernard Van Acker

IBM Global Services Belgium
Generaal Lemanstraat 69
B-2018 Antwerpen, BELGIUM
Bernard_Vanacker@be.ibm.com

Abstract. This paper, useful to anyone who has to address the public and representatives of the world of politics, focuses on the specific topic of resistance to vote-coercion. By using a model, we want to illustrate the implicit – and possibly realistic - assumption that vote-buying is not profitable or doable in current conditions. But these assumptions do not necessarily hold good in all environments. For those environments, recent - mainly cryptographic - publications show that coercion-resistant remote e-voting schemes are indeed possible.

1 Introduction

Throughout this e-Voting conference, the main requirements that any election should satisfy, will have been mentioned sufficiently; they are summarised well in article 21 of the Universal Declaration of Human Rights, which encompasses: the privacy of the vote, the accuracy of the count, the principle of one man, one vote, the freedom of vote.

As has also been mentioned many times, if we introduce remote e-Voting, we will drastically change the implementation (i.e. procedures) of elections, but there is a general consensus that the principles themselves should be strictly safeguarded.

One major concern that the political world has expressed on various occasions when talking about remote voting is that of vote coercion.

1.1. Definition

Coercion occurs when the vote is not free, i.e. when the voter is forced or bought into voting for an option which he would not have chosen had he not been under pressure or if he had not been offered a bribe.

[JJ02] has broadened the definition of coercion somewhat with forced abstention (a voter is forced into not turning out to vote), randomisation (a voter is forced into casting a random vote) and simulation (the coercer can impersonate the voter and thereby cast a vote in his or her place).

Vote coercion is by no means the only way a dishonest candidate or other party might alter the result of the elections: others are the bullying (or eliminating) of other candidates, or controlling the media. But these aspects are not specific to remote e-Voting, so we shall leave them out of scope.

1.2. Contingency under current legislation.

Under traditional voting methods, (1) the secrecy of the vote is guaranteed and (2) it is ensured furthermore that voters cannot prove to anyone else how they have voted. The second measure is followed very strictly: for example, a simple erasure on a paper ballot will render that ballot invalid[58]. The reasoning is that such an erasure could be a means by which the voter can prove how he/she voted.

1.3. Relevance for remote e-Voting schemes

Exposure to the risk of vote-buying is an argument used in public debates against remote voting procedures.

As an illustration, a citation of the republican Livingston in 1994 before the US Subcommittee on elections59 : "Telephone voting conjures up endless images of interest- groups paying armies of volunteers or goons to go out on the street, enter people's homes and intimidate or otherwise deprive them of their franchise in order to have people vote for a candidate for whom that they might otherwise have had no intention of voting."

Until recently, there seemed to be a consensus that remote e-Voting schemes offered little or no protection against vote coercion. This, together with the forecast costs of projected pilots, caused some initiatives to be broken off in the Netherlands around the end of 2001, beginning of 2002 [EPN02][60].

As we shall see below, this changed a few years ago, and positive proposals are now available.

---

[58] Example in Belgian legislation of local elections: Article 51 Loi électorale: « Ceux dont la forme et les dimensions auraient été altérées, qui contiendraient à l'intérieur un papier ou un objet quelconque ou dont l'auteur pourrait être rendu reconnaissable par un signe, une rature ou une marque non autorisée par la loi. »

[59] before the US House of Representatives, committee on House Administration, Subcommittee on Elections, on 22nd September 1994.

[60] A new pilot, restricted to Dutch citizens residing abroad, has been launched since then and is scheduled for use in the European elections in June 2004.

2 The risk and the impact of voter coercion

In an attempt to rationalise the discussion about the risk of vote coercion, we shall present here a rough-and-ready economic model. The aim here will be only to *define* both the presence of a risk and the impact of vote coercion,[61] and in this way identify the factors that might have an effect on them.

2.1. Rough economic model: Supply ad demand of votes.

A. the model.

The model will acknowledge that a candidate has a "default popularity" that will not depend on the resources (time & money) he puts into his/her campaign. But on the other hand, the model will allow those resources to affect the result somewhat in either of two ways:

- either by persuading voters to vote for the candidate voluntarily
- or to buy/coerce voters into voting for the candidate against their will.

The above distinction is important. A candidate who relies solely on persuasion doesn't need any proof to make sure that someone voted for him; on the other hand, coercion requires the ability of voters to prove how they voted. We will return to this point later.

We distinguish two kinds of players:

1) a candidate or party who is looking for votes, and who has at his disposal a number of resources, which may be time and/or money, of either himself or one of his supporters

2) the voters, for whom we take the original voter's preference as our starting point.

Throughout this description, we shall make the following assumptions:

1) The budget (the resources in terms of time and/or money) at the disposal of the candidate is fixed in advance[62].
2) A section of the electorate will not change its mind. Two categories here:
    a. Voters who were going to vote for the candidate anyway.
    b. Voters who would never vote for the candidate, no matter what the resources put in place to persuade, buy or coerce them into voting that way.

---

[61] Much more advanced models of the electoral market exist, which are outside the scope of this paper and can be found elsewhere, for example Besley, T. and Coat, S., "An Economic Model of Representative Democracy", Caress Working paper 95-02, 1995, 44p.

[62] Observed on at least one occasion: local elections 2000, Belgium. Also, in Belgium, budgets are restricted by law.

We will now describe two scenarii.

The first scenario makes the assumption that was implicitly made in Switzerland when introducing the first remote e-Voting scheme in 2003:

- The cost of persuading a voter into voting is less than the cost of coercing voters. This can be defended in countries with a high standard of living (we shall call this “the Swiss model”);

In the second scenario, we shall make the opposite assumption and see what the consequences are.

In the first scenario (”the Swiss model“) illustrated in figure 1, we distinguish two groups that may be influenced:

- The voters who did not originally intend to vote for the candidate, but who might be persuaded to vote voluntarily; this is illustrated by the green area in the colour picture).
- The voters who originally did not intend to vote for the candidate, cannot be persuaded to vote voluntarily; but who might be coerced into voting for the candidate. This is illustrated by the orange area in the picture below.

Remember that the curve can, and will, shift left or right dramatically, depending on the popularity of the candidate or party, which is desirable in free and fair elections anyway.

If we add up the costs, and look at the *total cost* of paying to get a certain number (percentage) of votes, we get indeed the following illustration.

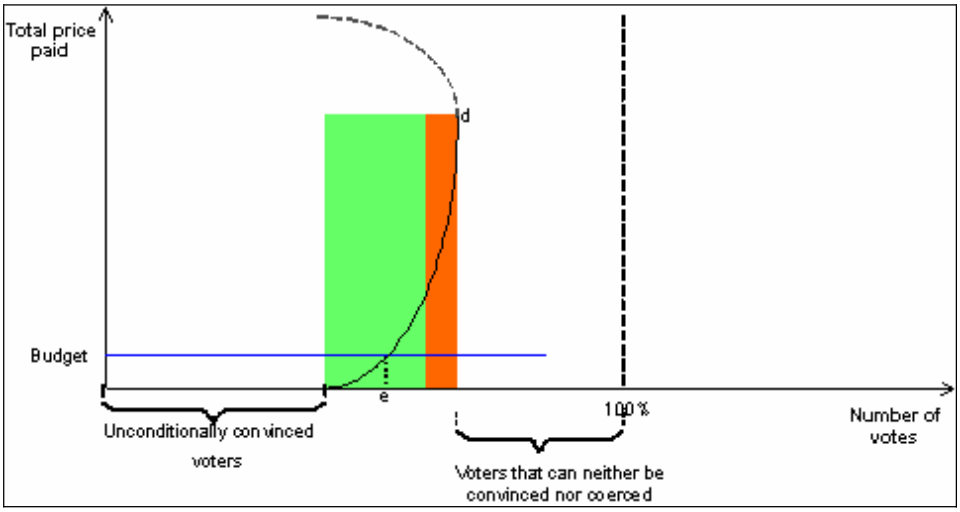

Figure 1: The total price of paying to get a certain result, versus a given budget (Swiss model).

If coercion is too blatant and so becomes too obvious, this may have a negative effect on the preference of even voters who were originally in favour of the candidate. We illustrate this by the dotted line starting from point d; the shape and position of that line are purely illustrative.

In this simple model, the candidate can keep "paying for" votes, either by persuasion or by coercion, until the total price to be paid equals his budget. This is illustrated by the intersection of the black line and the blue (fixed budget) line, which gives e votes (see point e on the X axis).

In figure 1 (illustrating the "Swiss model" scenario), the intersection occurs at the area of voters who can still be persuaded. In that example, no coercion has taken place.

In this "Swiss model", many politicians will recognise the situation: if they had more money and – more importantly - *time*, they would spend it all on the yet-to-be-convinced citizens, i.e. by persuasion. The idea of coercion wouldn't even cross their minds. A slight opportunity might exist among groups who support the candidate, but who lack rationality (e.g. very young supporters).

But in other situations, the "Swiss model" (the assumption that the cost of coercing people would be greater that that of persuading them) may be invalid, for example in unstable countries or situations. In the second scenario, the illustrative graph might very well look like figure 2 below:

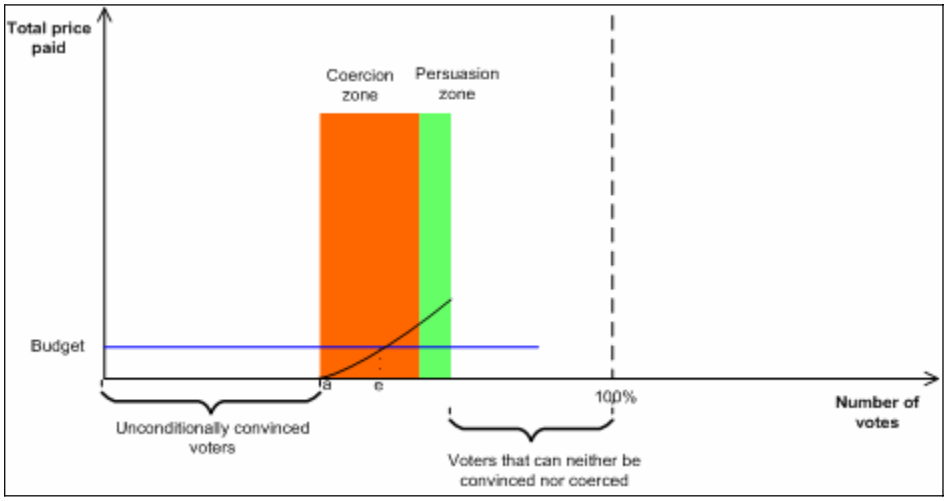

Figure 2: The total price to be paid for a certain result, versus a given budget (non-Swiss model).

In this scenario, the most "efficient" way of spending one's budget is to coerce a number of voters (by vote-buying or otherwise).

B. Influencing Factors

B.1. Probability-influencing factors.

For coercion to be an option, and hence a non-zero risk, one of the following should apply: (a) we are in a non-Swiss scenario as illustrated in figure 2, (b) in the Swiss model, the number of persuadable persons is smaller and (c) in the Swiss model, the curve representing the total cost is flatter in the persuasion area.

All this assumes no negative impact on popularity due to coercion itself (remember: illustrated by the dotted line starting from point d).

B.2. Impact-influencing factors.

In the figure 2, the impact of coercion was the segment between a and e, and has obviously been influenced by the slope of the curve between a and e.

The higher the cost of coercion (represented by an upward shift of the cost curve in the coercion zone), the smaller the impact of coercion, even if there is a risk. The same is true for both the Swiss and the non-Swiss model.

This is also true for a lower coercion effectiveness (represented by a leftward shift or rotation of the cost curve). This will be discussed extensively below.

a) The budget.

If the budget is low, the impact (coercion or persuasion) is smaller anyway. This is relevant where budgets are limited by law, as in Belgium.

This model was mentioned just to rationalise the discussion, not to give an economic "justification" of remote e-Voting systems.

2.2. Practical risks with traditional voting methods

Under traditional voting methods, the voter hides himself physically from any witnesses to cast his vote. Various officials are present to ensure that the vote is secret, that no proof of the vote is taken and that no one steals the vote. A risk that remains is the use of long lists[63], on which one can give preference votes to more than one candidate. In for example the local elections at Antwerp, the number of possible combinations was so large that one could have encoded a passport number in binary form, just by casting valid preference votes. No such abuses have been reported, however.

Another risk that remains valid is that of forced abstention, already mentioned above; this might be relevant in situations where violence is to be expected at polling stations; following our model this should increase risk and impact of it.

2.3. Practical risks with remote voting

When a vote is cast remotely, no witnesses are present to ensure voting freedom. Until recently, this led observers to believe freedom with remote voting was simply not possible. We will see some recent developments below that tend to show the opposite.

Force abstention persists here, with the difference that it will be more costly, since voters are scattered around remote locations; under our model, the impact should be lower here.

3 Contingency against coercion.

Contingency can act upon the cost or upon the effectiveness of coercion.

The cost of coercion can be increased – and hence our cost-curve in figure 3 shifted upwards - for example by requiring that a coercer be physically present, or by incorporating voting credentials into valued assets like identity cards, as mentioned in [Ch01].

---

[63] To be mathematically precise: where the lg (number of voters) is smaller than or equal to the number of candidates on one list. Example: 16,777,216 voters, and 24 candidates per list.

But effectiveness can also be reduced, and our cost curve in figure 3 thereby rotated leftwards. As we shall indeed show below, systems have been proposed that make it easy to lie about one's vote, and hence impossible for a voter to prove how he/she voted. In that case, offering bribes or threatening voters cannot make any difference to their voting behaviour, no matter what the budget spent. In our graph, the curve in the "coercion area" will then become ultimately a vertical line (as will the coercion area itself). Like [JJ02], we shall call such electoral systems "Coercion-Resistant".

In each of the three main categories of remote voting systems traditionally offered, namely[64] mixed nets using public key encryption like [Ch81; PO01], systems that rely on homomorphism like [CF85; Co86; Iv91] and systems that use blind signatures like [JL97; JLS99; KKP03], protection against coercion often remained unmentioned, or was indicated as being an open problem.

But in recent years, specialists in cryptography have been designing ways to vote remotely and/or electronically, while limiting the opportunity to prove to an outsider how the vote was cast.

Examples[65] are Hirt and Sako's method [HS00], Chaum's pre-encrypted ballots [Ch01], Chaum's coercion-free receipt [Ch03], and the planned system with loose sheets for the IBM social elections[66].

3.5. Further developments: Re-used voting booth secrecy.

With the above mentioned techniques, we have mainly limited the period during which coercion can take place, or made it more expensive, for example by requiring the physical presence of a coercer or vote- buyer at a given time.

Could we achieve the same level of coercion-resistance with remote voting as in a traditional voting booth?

An honest attempt to achieve exactly that will take into account the following comparison with remote authentication.

Remote authentication requires firstly an administration (registration authority) to invest time in verifying a person's true identity. Often this even requires the person to be physically present.

This "investment" brings benefits later on in remote electronic transactions when authentication is required. In other words, the fact of having been physically present once in the past is reused several times when remote authentication is needed.

---

[64] References are not exhaustive

[65] See http://home.tiscali.be/bernardvanacker/remoteVoting/CoercionFreeTechniques.html for a description of these alternatives

[66] The proposed system for the IBM social elections was using a scheme similar to the example in [MSV03];

We can imagine a similar investment for coercion resistance. We could devise a procedure to shield voters from anyone when they perform a secret action, for example by inviting the user to go into a booth (similar to a voting booth) at the site where also the authentication material is handed over.

Once outside the booth, he/she will not be able to prove anything about the secret action performed in the booth (eg whether or not he/she shuffled a pile of loose paper sheets containing both valid and invalid keys).

Under this scenario, the only option left open to a coercer would be to prevent the citizen from voting at all (the ”forced abstention attack“, supra), or to force him/her into voting randomly, which amounts to the same thing. Since this risk also exists with traditional voting methods, the protection against vote-buying would be the same as when voting at the polling station.

Of course, the citizen should remember well what he/she had done in private. This aspect and the aspect of user acceptance needs to be investigated, as has been done for the e-Voting pilot in Vienna [DPK03] and for in-booth electronic voting in Belgium [DKP03].

4. Conclusion

Firstly, we presented a model to help decide whether any anti-coercion measures were necessary.

For where required, we showed a few examples of ways to protect against voter coercion. We also said it ought to be possible to achieve the same level of protection for privacy and against voter coercion when using remote e-voting compared with when voting in person at the polling station. Essential here is the way keys are distributed. How readily users will accept these procedures and techniques remains to be investigated.

References

[Ch81] Chaum, D.: Untraceable Electronic Mail, return Addresses, and Digital Pseudonyms, Communications of the ACM 24, 2, (Feb. 1981), p 84-88;

[Ch01] Chaum, D.: Physical and Digital Secret Ballot Systems,patent application WO00155940A1 2001.

[Ch03] Chaum, David., "Secret-Ballot receipts and Transparent Integrity", 2003, available at www.vreceipt.com/article.pdf

[CF85] Cohen, J.D. and Fischer, M.J.: A Robust and Verifiable Cryptographically Secure election Scheme: Proceedings of IEEE Conference on Foundations of Computer Science, 1985.

[Co86] Cohen, J.D.: Improving Privacy in Cryptographic Elections: Yale University Computer Science Department Technical Report YALEU/DCS/ TR-454 , February 1986.

[DKP03] Delwit, P. ; Kulahci, E. ; Pilet, J-B.: Vote électronique et participation politique en Belgique: presentation at the Belgian Parliament in December 2003, available on http://www.belspo.be/belspo/home/publ/index_fr.stm

[DPK03] Dickinger, A.; Prosser, A.; Krimmer, R.: Studierende und elektronische Wahlen: eine Analyse; e-Democracy: Technologie, Recht und Politik. Prosser, A. and Krimmer, R., Oesterreicchische Computer Gesellschaft, 2003, pp 145-144.

[DO01] Dare, P.; Owlett, J.: Method and system for supply of data; UK Patent Office application 0126596.6, 2001;

[EPN02] EPN: Kiezen op afstand, dichterbij dan u denkt; EPN- Platform voor de informatiesamenleving, Den Haag, 2002; p 28 and 41.

[HS00] Hirt, M; Sako, K.: Efficient Receipt-free Voting, based on homomorphic Encryption, Eurocrypt 2000, 18p.

[Iv91] Iversen, K, R.: A Cryptographic Scheme for Computerized General Elections, Advances in Cryptology: Proc of Crypt '91, LNCS 576, Springer-Verlag, pp 405-419, 1991.

[JJ02] Juels, A ;Jacobsson, M.: Coercion-Resistant electronic elections, RSA Laboratories, 2002.

[JL97] Juang, W.S.; Lei, C.L.: A secure and Practical Electronic Voting Scheme for Real World Environments, IEICE Trans. on Fundamentals, Vol E80-A, No.1, , January, 1997., pp. 64-71.

[JLS99] Juang, W.S.; Lei, C.L.; Chang, C.Y.: Anonymous channel and authentication in wireless communications, Computer communications 22 (1999) p1502-1511;

[KKP03] Kofler, R.; Krimmer, R.; Prosser, A.:Electronic Voting: Algorithmic and Implementation Issues: Proceedings of the 36th Hawaii International Conference on System Sciences, 2003.

[MSV03] Marino, A.; Seliger, F.; Van Acker, B.: System for achieving anonymous communication of messages using secret key cryptography, patent application FR920030081, 2003.