

# Threat Analysis of Cryptographic Election Schemes

P Y A Ryan\*, Thea Peacock†

June 5, 2006

## Abstract

We discuss some vulnerabilities, threats and counter-measures for voter-verifiable, cryptographic election schemes: Chaum [1], Neff [7] and Prêt à Voter schemes [2]. Our analysis shows that such schemes are potentially prey to a wide variety of threats, both technical and socio-technical. On the other hand, counter-measures can be deployed to all the threats identified. This paper strives to take initial steps towards a more systematic threat analysis for such schemes. We briefly address the issue of how to ensure such threat analyses are as systematic and complete as possible.

## 1 Introduction

Traditional voting systems typically depend on rather strong trust assumptions: that officials act honourably, that hardware and software behaves correctly etc. Often such trust assumptions turn out to be ill-founded, as vividly documented in the US context in [3] for example.

Recently cryptographic schemes hold out the promise of providing a high degree of assurance with minimal trust assumptions by introducing a high degree of transparency and verifiability. Notable examples are the Chaum [1], Neff [6], [7] schemes and Prêt à Voter [2].

Such schemes provide a high degree of assurance with minimal trust assumptions. However, careful analysis shows that great care still needs

---

\*University of Newcastle

†University of Newcastle

to be taken in implementing such schemes and in embedding them in the surrounding socio-technical system. In this position paper, we identify a number of vulnerabilities of such voter-verifiable schemes.

## 2 Voter-verifiability

The key idea behind voter-verifiable schemes, in very abstract terms, is to provide the voter, at the time of vote casting, with a (unique) receipt with their vote in encrypted form. Once the election has closed, receipts are posted to a secure Web Bulletin Board (WBB) and voters are invited to check that their receipt is accurately posted and included in the tabulation process. The tabulation, performed by a number of trustees or tellers with appropriate keys, is performed in a publicly verifiable fashion but in such a way as to ensure secrecy, i.e. decrypted votes cannot be linked back to receipts. Various mechanisms are deployed to ensure that votes will be correctly encrypted and subsequently decrypted.

This approach has been realised in a number of ways in various schemes. The Chaum scheme implements receipt encryption using visual cryptography whilst Neff's uses ElGamal. Below we give a sketch of the Prêt à Voter scheme that we will use to illustrate the threats.

## 3 Outline of Prêt à Voter Scheme

We now present a brief outline of the supervised version of the Prêt à Voter scheme. For full details see [2]. Once registered in the polling station, voters select a ballot form, sealed in an envelope, at random. A typical example is shown below.

Democritus	
Plato	
Socrates	
Thales	
	<i>7r.J94K</i>

In the isolation of the booth, the voter makes her selection by, for example, placing a cross in the right-hand (RH) column against the candidate

of choice. The left-hand (LH) column, that carries the candidate list, is discarded leaving the ballot receipt. In this case, voting for Plato, the receipt would appear as follows:

X
<i>7rJ94K</i>

The voter then leaves the booth and casts their vote in the presence of an official: the receipt is placed under an optical reader, or similar device, to record the cryptographic value at the bottom of the strip, and the numerical representation of the cell into which the cross has been entered. The voter retains a digitally signed, franked hard copy of the RH strip as her receipt.

The candidate lists on the ballot forms are randomised. Thus, with the LH strip removed and in the absence of the appropriate decryption keys, the RH strip does not indicate how the vote was cast.

The cryptographic value printed on the bottom of the receipt, the “onion”, is the key to extraction of the vote. Buried cryptographically in this value, is the seed information needed to reconstruct the candidate list. Thus, only a threshold subset of tellers holding the appropriate keys are able to reconstruct the candidate order and so interpret the vote value encoded on the receipt.

Once the election has closed, the receipts are transmitted to a central tabulation server which posts them to a secure Web bulletin board (WBB). This is an append-only, publicly visible facility. Only the tabulation server can write to this and, once written, anything posted to it will remain unchanged. Voters can visit this WBB and confirm that their receipt appears correctly.

After a suitable period to allow voters to check their receipts, the tellers perform a robust, anonymising, decryption mix on the batch of posted receipts. The receipt allows voters to prove the absence or corruption of their receipt in the event that it fails to appear correctly on the WBB.

Various mechanisms are deployed to detect and deter any corruption in the construction of the ballot forms. The approach suggested in [2] is to perform a random pre-audit of the ballot forms.

## 4 Cryptographic Voting Protocols: Chinks in the Armour

The vulnerabilities described here can be placed in four main categories: subliminal channels, “social engineering”, denial of service attacks, collusion attacks and implementation flaws.

### 4.1 Subliminal Channels

Subliminal channels provide a means to transmit information over a channel in a way that is hidden from the legitimate users of the channel. They can arise whenever there are alternative valid encodings of the “intended” information. Additional information can be encoded in suitable choices between these alternatives. Public access to the WBB makes this a particularly virulent threat for voter-verifiable schemes.

A standard counter-measure is to require the use of pre-determined randomness. The difficulty with this approach is ensuring that the devices adhere to this pre-determined entropy. One possibility is to use trusted hardware, but this of course necessitates the reintroduction of trust assumptions.

Subliminal channels, as identified by Karlof et al at least, are not a problem for Prêt à Voter. This is due mainly to the rather special way that votes are encoded in Prêt à Voter. Most cryptographic voting schemes require the voter to supply her vote choice to the device, which then produces a (verifiable) encryption. In the case of Prêt à Voter, the voter’s choice is encoded in a randomised frame of reference. It is the information that allows this frame of reference to be recovered, the “seed” value, that is encrypted, and this can be done without needing to know the vote value. In Prêt à Voter, the ballot forms are generated in advance and allocated randomly to voters. Thus, the cryptographic commitments are made before any linkage to voter identities or vote choices are established.

### 4.2 Side-channel Attacks

In any scheme in which the vote-capture devices learns the voter’s choice, there is the possibility leaking the voters choices via side-channels, e.g., hidden wires, wireless-enabled devices, etc. In the case of Prêt à Voter, as

explained above, the capture device does not learn the voter’s selection and hence such channels are not, in fact, a problem. Of course, there may still be threats of voters being induced to take camera phones into the booths and so communicating a proof of their selection to coercers or vote buyers.

### 4.3 Kleptographic Channel Attacks

Prêt à Voter is still vulnerable to another form of subliminal channel: a kleptographic channel [?]. In the case of Prêt à Voter, the authority creating the ballot forms could carefully select the seed values in such a way as to encode information about the candidate list in the onion values. This encoding would use some secret key shared with a colluding third party. Thus, seeds would be chosen so that a keyed hash applied to the onion value would carry information about the corresponding candidate order.

It is possible to eliminate this kind of attack by arranging for the seeds to be created in a distributed fashion by several entities in such a way that no single entity can control or know the resulting seed values. Ryan et al [9] describes such a mechanism, in which several trustees create encrypted proto-ballot forms in a kind of pre-mix roughly mirroring the tabulation mixes.

### 4.4 Social Engineering Attacks

Many cryptographic voting schemes involve a moderately elaborate “ceremony”, to borrow a term from Benaloh. For example, cut and choose protocols are often used to check that vote values are correctly encoded in the receipts. The sequence of steps in the protocol is thus highly significant. By re-ordering the steps in the protocol, or introducing extra ones, the voting device may be able to corrupt votes with impunity. If voters are alert enough to notice the manipulation this would not be a problem. But is it unlikely that voters will understand the procedures and the appreciate their motivation.

In Prêt à Voter, the analogue of the “cut-and-choose” element of the Chaum or Neff schemes is performed by independent auditing authorities by checking a random selection of the ballot forms. Thus the voters are not required to perform a cut-and-choose protocol. The authority commits to the crypto material on the ballot forms ahead of the election. A random selection of these are checked by independent auditors for well-formedness.

This approach sidesteps the social engineering style attacks against the voters but at the cost of requiring certain trust assumptions about the probity and independence of the auditing authorities.

## 4.5 Denial of Service

There are several ways in which denial of service (DoS) attacks could disrupt or invalidate an election. For all such attacks, adequate error-handling and recovery strategies need to be in place. In addition, some form of back-up is desirable, e.g. a *voter-verifiable paper audit trail* (VVPAT) [5]. Of course, such paper audit trails should not be regarded as infallible and incorruptible either. Ultimately one may need to fall back on the receipts held by the voters, but here we would be relying on a good proportion of the voters retaining their receipts.

Whilst these schemes succeed in removing the need to trust the devices and tellers for the accuracy requirement, we may still be dependent on them to some extent for availability. Unless suitable measures are taken, the failure of a teller for example, could at least hold up and in the worst case block the tabulation. Corruption of the digital copies of receipts would call the election into doubt. Thus measures must be taken to make the scheme robust against (manifest) failure or corruption of devices. In other words, we have ensured that, with high probability, failures or corruption will be detected, but we still have to address the issue of error handling and recovery.

A recent enhancement to Prêt à Voter is to replace the decryption mixes with re-encryption mixes. This has a number of advantages, one being that recovery from DoS failures is much easier. There are a number of reasons for this:

- The mix tellers do not need secret keys, they simply re-randomise the encryption. A failed mix teller can therefore simply be replaced without having to surgically extract keys.
- The mix and audit can be independently re-run. With (deterministic) decryption mixes, the selection of links for audits cannot be independently selected on the re-run of the mix without compromising secrecy.

The use of threshold encryption schemes would also help to foil DoS attacks by ensuring the failure of a proportion of the (decryption) tellers could be tolerated.

A further possibility is to introduce a VVPAT [5]-style mechanism. At the time of vote casting, as the device scans the voter's receipt, it generates an extra copy. Once this copy has been verified by the voter (and possibly an official), it is entered into a sealed audit box. This provides a physical back-up of receipts cast, should recovery mechanisms need to be invoked.

## 4.6 Invalid Digital Signatures

In the Chaum scheme, digital signatures act as a counter-measure against faked receipts being used to discredit election integrity. However, a device that falsified signatures could be used to discredit voters, leaving them without a way to prove a dishonest system [4].

Voters should thus be provided with devices capable of verifying the digital signatures. Such devices could be provided at the polling stations by various independent organisations, such as the Electoral Commission, etc. This would enable the immediate detection of booth devices providing invalid digital signatures on ballot receipts. Similar measures could be utilised for Prêt à Voter.

Given the observation that encrypted receipts can be cast in the presence of officials and other observers, we have the possibility of checking digital signatures at the time of casting and applying physical authentication mechanisms, such as franking, to the receipt.

We note that, in common with much of the literature, we are assuming the existence of a secure WBB. More precisely, we are assuming that it is possible to implement a WBB in such a way as to provide universal read access and restricted append only access to the appropriate entities. In particular, we need to ensure that when a voter confirms that their receipt is accurately displayed on the WBB this will guarantee that it will be fed accurately into the tabulation mix. There must be no way then for the system to corrupt the receipt values displayed to the voters or to alter the values after they have been verified. In practice, implementing such mechanisms will itself be extremely challenging along with the issues of trusted channels from the WBB to the voters.

## 4.7 Undermining Public Confidence in the Secrecy of Encrypted Receipts

Another potential attack against schemes employing encrypted receipts, is as follows. The Mafia claim to have a way of extracting a vote from the encrypted receipt. If a sufficient number of voters were convinced by such a claim, and so influenced to alter their vote, it may be possible to undermine the outcome of the election. Countering such a psychological attack, other than by voter education, is difficult.

Such attacks to undermine confidence are of course not unique to cryptographic schemes, but arguably are of particular concern where encrypted receipts are used.

## 4.8 Chain Voting

Chain voting is a well known style of attack that can be effective against some conventional paper ballot schemes. In this attack, the coercer smuggles an unused ballot form out of the polling station and marks his preferred candidate. The voter is told that they will be rewarded if they emerge with a fresh, unmarked form. This can then be marked again and passed to the next voter.

Neither the Chaum nor the Neff schemes, in which the ballot forms and receipts are generated on demand in the booth, are vulnerable to this style of attack. Prêt à Voter is, however, potentially vulnerable, as the ballot forms are pre-printed.

A counter-measure that is quite effective against this style of attack against conventional paper voting systems, is to follow the procedure used for example in France: voters are only registered at the point of casting their vote (in a sealed envelope). As a result, ballot forms are no longer a controlled resource, but are freely available at the polling station. Now, when a voter emerges with a blank form it proves nothing to the vote buyer. Unfortunately, this counter-measure ceases to be effective where encrypted receipts and WBBs are used: now the vote buyer can check on the WBB that the form that they pre-marked for the convenience of the voter was in fact cast.

Observe that at the time of making her candidate choice, it is only necessary for the voter to see the candidate list . A possible counter-measure therefore is to conceal the onion by, for example, a “scratch strip”, similar

to that used in lottery tickets. The procedure could then be for the voter to register and collect a fresh ballot form, with scratch strip intact. The voter goes to the booth, marks her selection, then detaches and destroys the LH strip. She exits the booth and takes her receipt to an official who checks her identity and that the scratch strip is intact. The voter, or an official, now removes the strip and records the receipt as previously described.

A rather different counter-measure is to return to an on-demand creation of ballot forms, e.g. printing in the booths. An implementation of this in which forms are distributed with the candidate list in encrypted form and only decrypted and printed in the booth, can be found in [9]. This avoids chain-voting and certain chain of custody issues but at the cost of having to re-introduce the voter involvement in the “cut-and-choose” along with post-auditing to the protocol. The trade-offs involved in this are investigated in [8].

This approach might still be vulnerable to a form of randomising attack: if a coercer can get hold of blank forms they could mark them arbitrarily. The coercer cannot induce voters to vote for their preferred candidate, but they could in effect nullify votes.

#### **4.9 Authority knowledge**

In the current version of Prêt à Voter, the authority has knowledge of ballot form information, i.e. the crypto seeds used to generate the candidate offsets, hence the onions, and, in particular, the association between these values. This means that the authority has to be trusted not to leak this information. Even if the authority is entirely trustworthy, there is always a danger of this information being leaked during distribution or storage of the ballot forms, i.e., chain of custody issues.

The pre-mix approach of [9] alluded to earlier as a counter to kleptographic attacks, would also be effective here to eliminate the authority knowledge problem.

#### **4.10 Enforcing the Destruction of the Left-hand Strips**

After the voter’s selection has been marked on the ballot form, the left-hand strip must be destroyed. Failure to do so would allow the voter to use it as proof of her vote to a third party. Clearly, this would lay the system open to coercion.

Several ways of enforcing this are possible. The voter could be required to destroy the LH strip in the presence of an official, preferably in a mechanical shredding device. This could be done at the time of casting the ballot form, as suggested above. However, care would have to be taken to ensure that the official is not able to record the association of the receipt and candidate list. This of course results in the need to place some trust in these officials. One might arrange for several officials to observe the casting.

Another possibility is to have devices in the booth that would automatically cut off and destroy the LH strip and then pass the receipt into a scanner. This would make the voter’s interaction simpler, but such devices would entail trust assumptions again.

A further, rather appealing, possibility is to make “decoy” left-hand strips freely available in the booths, so the voter cannot convince the coercer that the one she emerges with is genuine.

#### 4.11 Confusion of Teller Modes

As previously mentioned, the tellers perform an anonymising decryption mix on the receipts posted to the WBB. However, they also have a role in checking the construction of ballot forms, both by auditors and, potentially, voters [2]. For ballot forms selected for audit, the onions are sent to the tellers, who return the corresponding seed values. The auditors then re-compute the onion values and candidate offsets, and check that they are correct. In voter checking, the tellers return the candidate ordering corresponding to the onion value sent by the voter.

The checked forms should then be discarded. If the audited forms were later used to cast a vote, there could be a threat to ballot secrecy. Conversely, it should not be possible to run a check on a form that has been used to cast a vote.

To counter this, ballot forms could be checked by voters in the presence of an official, who then ensures that used forms are discarded. Forms could be invalidated once used, for example, using the described scratch strip mechanism. An authentication code could be overprinted on the scratch strip that would be necessary to enable the checking mode. Revealing the onion would entail removing the scratch strip and the code along with it, ensuring that the form could not be reused later.

## 5 Conclusions

We have presented an analysis of threats to voter-verifiable election schemes. The analysis presented here does not constitute an exhaustive, systematic, identification of all the system-based threats to voter-verifiable schemes. Arguably, complete coverage for such an analysis could never be guaranteed given the open-ended nature of systems. However, we feel that this analysis constitutes a useful first step towards a more systematic analysis technique for voting systems.

We have the start of a taxonomy of attacks, i.e., classification into subliminal channels, side-channels, kleptographic channels, social engineering threats, implementation problems, etc. It seems likely that a design-level, information flow analysis should help guide further analysis. This will be pursued in future research.

Finally, we conclude that, provided that a full socio-technical perspective is taken during the design and evaluation of the voting systems, there is every reason to suppose that cryptographic schemes of this kind can provide trustworthy, verifiable elections.

## 6 Acknowledgements

The authors would like to thank Michael Clarkson, Michael Jackson, Steve Kremer, Thomas Tjøstheim, Andrey Povyakalo, Mark Ryan and Luca Vigano for fruitful discussions and DSTL and the EPSRC DIRC project for partial funding of this work. We should like also to thank the the anonymous reviewers for many helpful observations and suggestions.

## References

- [1] D. Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security and Privacy*, 2(1):38–47, January-February 2004.
- [2] D. Chaum, P.Y.A. Ryan, and S. Schneider. A practical, voter-verifiable election scheme. In *European Symposium on Research in Computer Security*, number 3679 in Lecture Notes in Computer Science. Springer-Verlag, 2005.

- [3] Andrew Gumbel. Steal this vote! October 2005.
- [4] C. Karlof, N. Sastry, and D. Wagner. Cryptographic voting protocols: A systems perspective. In *USENIX Security Symposium*, number 3444 in Lecture Notes in Computer Science, pages 186–200. Springer-Verlag, 2005.
- [5] R. Mercuri. A better ballot box? *IEEE Spectrum Online*, October 2002.
- [6] A. Neff. A verifiable secret shuffle and its application to e-voting. In *Conference on Computer and Communications Security*, pages 116–125. ACM, 2001.
- [7] A. Neff. Practical high certainty intent verification for encrypted votes, 2004. <http://www.votehere.net/documentation/vhti>.
- [8] P.Y.A. Ryan. Putting the human back in voting protocols. In *Fourteenth International Workshop on Security Protocols*, Lecture Notes in Computer Science. Springer-Verlag, 2006. To appear.
- [9] P.Y.A. Ryan and S A Schneider. Prêt à voter with re-encryption mixes. Technical report, University of Newcastle upon Tyne.