A Threat Analysis of Prêt à Voter

Peter Y.A. Ryan[2] and Thea Peacock[1]

[1] School of Computing Science, University of Newcastle, Newcastle upon Tyne, NE1 7RU, United Kingdom
[2] Department of Computing Science and Communications, University of Luxembourg 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg
peter.ryan@uni.lu

Abstract. It is widely recognised that the security of even the best-designed technical systems can be undermined by socio-technical weaknesses that stem from implementation flaws, environmental factors that violate (often implicit) assumptions and human fallibility. This is especially true of cryptographic voting systems, which typically have a large user base and are used infrequently.

In the spirit of the this observation, Karlof et al [11] have performed an analysis of the Chaum [5] and Neff [18] schemes from the "systems perspective". By stepping outside the purely technical, protocol specifications, they identify a number of potential vulnerabilities of these schemes. In this paper, we perform a similar analysis of the Prêt à Voter [6].

Firstly, we examine the extent to which the vulnerabilities identified in [11] apply to Prêt à Voter. We then describe some further vulnerabilities and threats not identified in [11]. Some of these, such as chain-voting attacks, do not apply to the Chaum or Neff schemes, but are a potential threat in Prêt à Voter, or indeed any crypto system with pre-printed ballot forms. Where appropriate, we propose enhancements and countermeasures.

Our analysis shows that Prêt à Voter is remarkably robust against a large class of socio-technical vulnerabilities, including those described in [11].

1 Introduction

Voting systems are the bedrock of democratic societies, and date back several millennia. While many different mechanisms for voting have been proposed [10], they usually share a similar set of goals such as accuracy, ballot secrecy, verifiability and coercion-resistance [13], [7].

In an attempt to improve the accessability and efficiency of the election process, democracies have experimented with various automated voting systems that increase speed and accuracy of ballot counting. Arguably, some of these new mechanisms offer greater secrecy, and in the case of remote systems, increased voter participation. However, these attempts have been fraught with problems, many of which are due to reliance on computer hardware and software performing as intended or claimed [3], [2], [12], [14].

D. Chaum et al. (Eds.): Towards Trustworthy Elections, LNCS 6000, pp. 200–215, 2010.

Recent proposals for cryptographic voting systems strive to resolve many of these problems by introducing transparency and verifiability. Notable examples are the Chaum [5] and Neff [17], [18] schemes and Prêt à Voter [6]. These strive to provide assurance of secrecy and accuracy without any reliance on the underlying technical system, i.e. software, hardware etc. Instead, the assurance is derived from the properties of the cryptography and a high degree of transparency in the vote recording and counting stages.

While it is important to analyse the core protocol in order to assess its security [4], [13], it is also essential to consider its interaction with the surrounding system, e.g. computer hardware and software, voters and voting officials. In addition, collusion between parties can make the attacks more difficult to detect and resolve. This point was argued by Ryan [21], and more recently, demonstrated by Karlof et al [11] in their examination of the Chaum and Neff schemes from the "systems perspective".

In this paper, we continue this theme with an analysis of Prêt à Voter, and in doing so, find that it is remarkably robust against many of the vulnerabilities described in [11]. In addition, we identify some new vulnerabilities, and offer mitigation strategies, particularly where they may apply to Prêt à Voter.

The structure of the paper is as follows. In Section 2 we briefly describe the Chaum and Neff schemes. In Section 3, we recall the potential weaknesses identified in [11]. In Section 4, we present an outline of the Prêt à Voter scheme. Section 5 examines the extent to which the attacks of [11] also apply to Prêt à Voter. Following this, in Section 6, we identify further possible attacks and suggest mitigations. In Section 7 some other vulnerabilities of Prêt à Voter are described, along with some counter-measures. Finally, we summarise and conclude in Section 8.

2 The Chaum and Neff Voting Schemes

Although the mechanisms differ in several ways, Prêt à Voter and the Chaum and Neff schemes all provide voter verifiability. More precisely, after a vote is cast, the voter is provided with a physical receipt which encodes the value of her vote, and so ensuring secrecy. The voters can later check that their ballot receipt has been correctly posted to the *Web Bulletin Board* (WBB). Tabulation is performed by decryption and anonymisation via robust anonymising mixes. To ensure accuracy, various checking mechanisms are deployed to detect any failure or corruption in either the encryption or decryption of the receipts.

Due to space constraints, we only summarise the key features of the Chaum and Neff schemes, and refer the reader to [6], [4] , [18], [19] for details, or [13], [23] for overviews.

In the booth, the voter interacts with a machine, during which the voter's choice is communicated to the machine and encoded in a receipt. The voter is given the opportunity to verifying that their vote is correctly encoded. This is achieved by way of a "cut-and-choose" protocol, in which the device commits to two or more encryptions of the vote, one of which the voter chooses to retain.

The remaining encryptions are then opened, verified and discarded. A digital copy of the chosen receipt is retained by the device and, once the voting period has ended, is posted to a WBB . The voter retains a hard copy of her encrypted ballot receipt, which she can subsequently check on the WBB to make sure that the receipt has been correctly recorded.

The receipts are shuffled and decrypted in a series of anonymising mixes to ensure that no link remains between the encrypted ballot receipts and the final decrypted vote values. The results of each stage of the mix process are posted to the WBB.

Aside from the details of the cryptographic primitives involved and the mix processes, the essential difference between the two schemes is in the format of the receipt.

In the Neff scheme, the receipt consists of a matrix of El Gamal ciphertexts of the digits "0" or "1". A chosen candidate is distinguished by the arrangement of digits in the corresponding row.

In the Chaum scheme uses the RSA algorithm and the voter's choice is represented using visual cryptography [16] to generate a 2-D ballot image showing the candidate name, which is split between two encrypted, transparent layers. The ballot image is visible when the two sheets are accurately overlaid but, when separated, each sheet is a pattern of random pixels. The voter selects one layer to retain as a receipt, so without knowledge of the crypto keys, the receipt does not reveal the voter's choice.

3 Cryptographic Voting Protocols: Chinks in the Armour

The vulnerabilities considered in [11] fall into three main categories: those due to subliminal channels, "social engineering"-style attacks against the cryptographic protocols and denial of service attacks. In this section, we briefly recall each of these vulnerabilities and how they may apply to the Chaum and Neff schemes.

3.1 Subliminal Channels

Subliminal channels provide a means for a malicious agent 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. There are two classes of subliminal channel identified in [11]: *random* and *semantic*.

The Neff scheme makes use of randomised crypto variables in the creation of the ballot receipt giving rise to a possible *random* subliminal channel. By judicious selection of random values, the voter's choice could be encoded in the encrypted receipt [11]. Any agent with knowledge of the coding strategy could then gather this information by observing the posted receipts.

Random channels do not occur in the Chaum scheme, as it uses deterministic algorithms. However, *semantic* subliminal channels, can occur if there are

alternative valid representations of the ballot image. Certain information could then be conveyed by altering the ballot image, for example by adjusting the font size or positioning of the image. Note that, in contrast to the random channel of the Neff scheme, this channel emerges after the anonymising mixes, when the decrypted ballot images emerge. Thus a malicious device would presumably encode information about the voter identity rather than the vote value.

Mitigation. Counter-measures for random subliminal channels are tricky, since the randomness may be essential for security properties. A possible approach, attributed to Neff [11], is to require the use of pre-determined randomness, e.g., from pre-generated tapes. In effect, the non-determinism is resolved before the voter's choices are communicated to the system. The difficulty with this approach is ensuring that the devices adhere to this pre-determined entropy. In personal communication, Neff describes a recent implementation of his scheme, in which ballots are created in advance by a multi-authority process similar to a mix-net. The function of the device is completely deterministic, so there is no possibility of a subliminal channel. In addition, the voter only makes one random choice for the entire ballot, rather than for each option, as described in [11]. Details of these innovations can be obtained from [1].

With the Chaum scheme, one could enforce a standard format for each the ballot image for each candidate option. This also runs into the difficulty of monitoring and enforcing adherence. It is also difficult to square with the possibility of "write-ins" that the scheme enables. In personal communication, Chaum observed that such semantic channels are not strictly subliminal: exploitation of such channels would be detectable.

Another possibility is to use trusted hardware [11], but this is contrary to the principle of transparency and minimal dependence which the Chaum, Neff and Prêt à Voter (see later) schemes aim to achieve.

3.2 Social Engineering Attacks

Both the Chaum and Neff schemes require non-trivial interactions between the voter and the machine. Both schemes involve "cut-and-choose" protocols, and the sequence of steps in the protocol can be highly significant. These are designed to detect any attempt to construct receipts that do not encode the voter's true choice. We will refer to the choice the voter makes in a "cut-and-choose" step as the "protocol choice" to distinguish this from the voter's candidate choice.

By re-ordering the steps in the protocol, or introducing extra ones, the machine could learn the voter's protocol choice before it has to commit to the receipt encoding [11]. In this case the device can corrupt the vote value with impunity. Voters may not notice or appreciate the significance of such changes in the protocol execution.

Similarly, the machine could feign an error and re-boot after it learns the voter's protocol choice. Relying on the voter making the same choice in the second round of the protocol, the machine then constructs a receipt for a different candidate. If the voter changes her mind, the machine re-boots again until the voter gets it "right" [11].

Another possible vulnerability of the Chaum scheme, not identified in [11], but mentioned in [21], is as follows. The machine attempts to corrupt the vote value by incorrectly constructing one of the layers. If the voter chooses the other layer for retention, the corruption will go undetected. However, if the voter chooses the corrupted layer (which would lead to detection), the machine could try to fool the voter by printing "destroy" instead of "retain" on the layer that the voter chose as the receipt. If the voter fails to notice this, or simply ignores it, the corruption will again pass undetected. This is another way that a corrupt machine could undermine the "cut-and-choose" element of the protocol. Even if the voter does notice the switch and is confident that they are right, it may be difficult to demonstrate this to a voting official.

Mitigation. We refer the reader to [11] or [23] for suggested mitigations. The obvious approach is to try to ensure that voters understand the procedures and appreciate their motivation. This is similar to the notion of instilling a "security culture" in an organisation. In practice of course, this may not really be feasible. In the context of an election system, where the set of users can be vast and usage infrequent, the possibilities for voter eduction is limited.

An alternative solution is to make the voter experience much simpler, as with Prêt à Voter. However such simplicity seems to be at the cost of needing to place more trust in the system.

3.3 Denial of Service

There are several ways in which DoS attacks could disrupt or invalidate an election. See [11] for a discussion. 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) [15]. We return to these attacks and counter-measures later, when we examine the robustness of Prêt à Voter.

4 The Prêt à Voter Scheme

We now present an overview of the Prêt à Voter scheme. For full details see [6]. Prêt à Voter is inspired by the Chaum scheme, but replaces the visual cryptographic techniques with a conceptually and technologically simpler mechanism to represent the encrypted vote value in the ballot receipt. In the polling station, voters select a ballot form at random, an example of which is shown below.

Obelix	
Idefix	
Asterix	
Panoramix	
	$7rJ94K$

In the booth, the voter makes her selection in the usual way by, for example, placing a cross in the right-hand (RH) column against the candidate of choice. She now separates the (RH) and left-hand (LH) sides, and the latter, which carries the candidate list, is discarded to leave the ballot receipt. Supposing a vote for Idefix, the receipt would appear as follows:

X
$7rJ94K$

She then leaves the booth and authenticates herself with an official, who scores off her name in the register. 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 the hard copy of the RH strip as her receipt. An anti-counterfeiting device would be incorporated, and the receipt would be digitally signed when the vote is cast.

Possession of a receipt might appear to open up the possibility of coercion or vote-buying. However, the candidate lists on the ballot forms are randomised, so the order in which the candidates are shown is unpredictable. Clearly, as long as the LH strip is removed, the RH strip alone does not indicate which way the vote was cast.

The crypto 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. This information is encrypted under the secret keys of a number of tellers. Thus, only the tellers acting in consort are able to reconstruct the candidate order and so interpret the vote value encoded on the receipt.

Once the election has closed, all the receipts are transmitted to a central tabulation server which posts them to a secure 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, the tellers take over and perform a robust, anonymising, decryption mix on the batch of posted receipts. Various approaches to auditing the mixes can be used to ensure that the tellers perform the decryptions correctly. Details of this can be found in [6].

Another place where the accuracy of the scheme could be undermined is in the vote capture stage, and the encoding of votes in the receipts. In the case of Prêt à Voter, this could occur if the ballot forms are incorrectly constructed, i.e., the candidate list shown does not correspond to the crypto seeds buried in the onion value. Various mechanisms can be deployed to detect and deter such corruption. The approach suggested in [6] is to perform a random pre-audit of the

ballot forms. In other words, both independent third parties and the voter can check the well-formedness of the ballot forms. The checks performed in each case, however, differ. The former involves extracting the crypto seeds, re-computing the onions and checking that they correspond to the candidate permutation.

Later in this paper, we discuss an alternative approach using on-demand creation and printing of forms along with a "cut-and-choose mechanism" and post-auditing.

For full details of the mechanisms used to detect any malfunction or misbehaviour by the devices or processes that comprise the scheme, see [6].

5 Systems-Based Analysis of Prêt à Voter

In this section we examine the extent to which the vulnerabilities identified in [11] apply to Prêt à Voter.

5.1 Subliminal Channels

Subliminal channels of the type identified by Karlof et al, are not a problem for Prêt à Voter. This is due mainly to the rather special and, to our knowledge unique, 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. This can be done ahead of time without needing to know the vote value. In Prêt à Voter, the ballot forms are generated in advance and allocated randomly to voters. Hence, the cryptographic commitments are made before any linkage to voter identities or vote choices are established.

Regarding semantic subliminal channels, suitable implementation should ensure that, for a given ballot form and vote choice, the digital representation in a Prêt à Voter receipt is unique, i.e., the onion value and the index value indicating the chosen cell on the LH column. Hence, there should be no possibility of a semantic subliminal channel.

Like the Chaum scheme, Prêt à Voter "Classic", [6], uses deterministic cryptographic algorithms. In fact, in both schemes, all the tellers' operations can be made deterministic: encryption and decryption are deterministic and the tellers can be required to post batches of transformed ballot receipts in lexical order at each stage, thus eliminating random subliminal channels. It is not clear whether this is really necessary, as the tellers do not have access to any privacy sensitive information.

5.2 Social Engineering Attacks

In Prêt à Voter, the voter does not engage in a multi-step protocol with the device so there is little scope for any social engineering-style attacks.

It is worth noting that in Prêt à Voter, the analogue of the "cut-and-choose" element of the Chaum or Neff schemes is performed by independent auditing authorities who check a random selection of the ballot forms. This removes the need for a "cut-and-choose" step in the voter's phase of the protocol, as the authority commits to the crypto material on the ballot forms ahead of the election. A random selection of these are checked by the auditors for well-formedness. This can be done before, during and after (on unused, left-over forms) the election period. Assuming that they pass the checks, audited forms are destroyed. Forms that fail the checks would be retained for forensic purposes.

Prêt à Voter also allows the possibility of voters performing random checks on the ballot forms in addition to checks performed by auditors. This is more in the spirit of arranging for the trust to reside solely in the voters themselves. Care has to be taken, however, to avoid introducing other vulnerabilities, such as the possibility of checking ballot forms that have been used to cast votes.

5.3 Denial of Service

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, any (significant) failures or corruption will be detected, but we still have to address the issue of error handling and recovery.

A possible enhancement of Prêt à Voter, detailed in [24], 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 all the unpleasantness of 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.

In [20], it is suggested that an encrypted VVPAT [15]-style mechanism be incorporated. 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.

We emphasise that this is actually quite different to the conventional notion of VVPAT that generates a paper audit trail of unencrypted ballot slips. The

conventional form of VVPAT suffers from a number of privacy problems. For example, if the trail retains the order of votes cast, receipts could be linked to voters by comparing the order in which votes are cast with that of voters entering the booth. Also, any mismatch between the voter's choice and the paper audit record can be difficult to resolve without compromising the voter's privacy.

Where encrypted receipts are recorded, these problems disappear. Note that, due to the encrypted form of the receipts, it is possible for monitors to verify a vote as it is cast, in addition to the voter checking. Any discrepancies can be resolved without loss of voter privacy. We will henceforth refer to such a mechanism as *Verified Encrypted Paper Audit Trail* (VEPAT).

5.4 Discarded Receipts

As with the Chaum and Neff schemes, carelessly discarded receipts could be a problem in Prêt à Voter, as this could indicate which receipts will not be checked by voters on the WBB [11]. Malicious parties could delete or alter the corresponding receipts, confident that the voters will not check them on the WBB.

Aside from voter education [11], a possible mitigation is, again, to invoke a VEPAT mechanism, as described above. Independent observers could check the correspondence between the VEPAT and the contents of the WBB. This has the added advantage in that less reliance need be placed on the votes' diligence in checking their receipts on the WBB.

5.5 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 [11].

Voters should thus be provided with devices capable of verifying the digital signatures. Such devices could be provided by various independent organisations, such as the Electoral Commission, etc. Similar measures could be utilised for Prêt à Voter.

Given 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.

5.6 Insecure Web Bulletin Board

Like the Chaum and Neff schemes and indeed many cryptographic voting schemes, Prêt à Voter relies on a secure WBB to allow voter and verifiability. In a possible attack, the WBB arranges for the voter to see a correct record of her ballot receipt, which, in collusion with the mix-net, has been deleted or altered. As a result, the voter could mistakenly believe that her vote has been accurately counted [11].

However, we note that suggested mitigations, such as robust data storage and allowing only authorised write access to the WBB [11] are still vulnerable to corruption. The challenge is provide a trusted path from the WBB to the voter. The problem of implementing secure web bulletin boards is the subject of ongoing research in the cryptographic voting community.

6 Further Vulnerabilities

In this section, we discuss other possible vulnerabilities not identified in [11], and suggest appropriate mitigation strategies.

6.1 Doll Matching Attack

This vulnerability is specific to the Chaum scheme and is not identified in [11]. Each of the layers that combine to reveal the ballot image have to carry a pair of "dolls", analogues of our "onions", one for each layer. It is essential that these are identical between the layers. The voter is required to check that values on the two layers match. Failure to do this could allow the device to construct fake receipts without detection. It might seem difficult to produce a fake "doll" that alters the vote value whilst differing from the real "doll" in a way that is visually almost imperceptible. This would be analogous to finding (approximate) collisions of a cryptographic hash function. Nevertheless, this should still be considered a potential vulnerability.

A counter-measure is to ensure that visual matching of the dolls is as easy to perform as possible. Thus, for example, the dolls might be encoded aligned bar codes on the two layers. Any mismatch would then show up as a misalignment of the bars.

6.2 Undermining Public Confidence in the Secrecy of Encrypted Receipts

Another potential attack against schemes employing encrypted receipts, is as follows. The Mafia (falsely) 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. For instance, a coercer might urge voters to submit their receipts, claiming that the "correctness"' of the choice would be checked. Some reward, such as entry into a lottery, would be offered for receipts that passed the supposed checks.

Countering such a psychological attack, other than by voter education, could be difficult.

6.3 Side-Channel Attacks

Karlof et al do not discuss the possibility of the vote-capture devices leaking the voters choices via side-channels, e.g., hidden wires, wireless-enabled devices, etc.

This may be because they are regarded as inevitable. In fact, in the case of Prêt à Voter, such channels are not, in fact, a problem.

As explained earlier, the voter's choice does not need to be communicated to the device in order to obtain the encoding of this choice in the receipt. Hence, even if such channels existed, they could not be exploited to leak information from the booth device.

However, the potential for other kinds of side-channels still exists: hidden cameras, "invisible" dots on the receipts etc.

6.4 Kleptographic Channel Attacks

The current version of Prêt à Voter is, however, vulnerable to kleptographic channels, another form of subliminal channel. These were orginally described by Young and Yung [25] and their relevance to voting schemes identified by Gogolewski et al [9]. In the case of Prêt à Voter, the idea is that the authority creating the ballot forms would 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 certain keyed hash applied to the onion value would carry information about the corresponding candidate order. Clearly this would require a significant amount of searching in the seed space and computation, but the resulting selection of seeds would appear random to anyone not knowing the coding strategy and secret hash key.

It is fairly straightforward 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 [24] describes such a mechanism, in which several trustees create proto-ballot forms in a kind of pre-mix. The resulting proto-ballot forms have two distinct onions encrypting the same seed value. The seed value, and hence candidate list, can be extracted from one of these on demand to reveal the full ballot form. Full details can be found in [24].

7 Prêt à Voter Specific Vulnerabilities

Our analysis of Prêt à Voter revealed other possible vulnerabilities that are specific to the scheme. We discuss them and suggest possible mitigations.

7.1 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.

Particularly vulnerable are election systems in which, as in the UK, the ballot forms are a controlled resource: on registration, voters are given one ballot form and they are observed to cast this before existing the polling station. The voter is then under duress to cast the form marked by the coercer and to retain the fresh form that they are provided with when they register. The procedures arguably make it harder for the coercer to initialise the attack. However, a determined attacker would certainly find a way, for example by bribing an official, or placing a fake form in the ballot box. Once the attack is initialised, the procedure works in the coercer's favour.

A possible counter-measure is to make ballot forms freely available in the polling stations, as, for example, in French elections. Voter identity is checked when casting a vote rather than at the time of collecting a ballot form. Thus, as it is not certain that a marked form was actually used to cast a vote, the motivation for the attack is undermined.

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. The counter-measure above does not work as cast receipts are posted to a publicly-verifiable WBB, so allowing the coercer to confirm whether or not the designated ballot form was actually used.

7.2 Mitigation

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 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.

Steps would need to be taken to ensure that the scratch strips cannot be scanned with some device to read the concealed onions. This has reportedly been done using the laser photo-acoustic effect. See [8] for details. Although expense and technical know-how would be required on the part of the attacker, it should still be considered a possible threat.

A rather different counter-measure is to return to an on-demand creation of ballot forms, e.g. printing in the booths. The scheme for the distributed generation of encrypted ballot forms of [24] could be used here. 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 [22].

7.3 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.

A possible solution is to arrange for the ballot form material to be constructed in a distributed fashion, in such a way as to ensure that no single entity knows the association of onions and candidate lists. As noted previously, up until the time of casting a vote, it is not necessary for the voter to see the onion. One could thus devise a scheme in which the onion and candidate list are never exposed simultaneously.

We now outline a simple scheme for distributed construction of "scratch card" style ballot forms. It is based on onions encrypted using El Gamal, or a similar randomised encryption algorithm. The ballot form material is generated by a number of ballot clerks. The first clerk generates a large quantity of onions, which then enter a re-encryption pre-mix involving the other clerks. The last clerk collects the resulting permuted, random onions and, for each one, produces two re-encryptions. These paired onions are now printed onto ballot forms, one at the bottom of the LH column, the other on the bottom of the RH column. A proto-ballot form is shown below:

	7rJ94K
jH89Gq	

These two onions should correspond to the same candidate list. The RH onion is now concealed with a scratch strip.

These are now shuffled and passed to a final clerk who then dispatches the visible, LH onions to the tellers. The tellers send back the corresponding candidate list which is now printed in the LH column and the LH onion is removed. This results in ballot forms similar to those proposed in Section 4, but with the onion value concealed by a scratch strip.

Note that no single entity now knows the association of onion and scratch strip. Strictly speaking, the last two clerks acting in collusion could form the association, but the scheme can be elaborated to raise the collusion threshold. Interestingly, we note also that, even though these two clerks in collusion know the onion/candidate list association, they cannot prove this knowledge to a third party as they do not know the necessary crypto seeds used to compute the onion values. Ballot forms can be randomly audited as before.

Alternatively, the pre-mix approach of [24] alluded to earlier as a counter to kleptographic attacks, would also be effective here to eliminate the authority knowledge problem.

7.4 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 left-hand strip in the presence of an official, preferably in some 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.

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 have to be carefully evaluated, and run counter to the "trust nobody and nothing" philosophy of voter-verifiable schemes.

Another 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.

7.5 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 [6]. 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 mitigate 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. Alternatively, an authorisation code could be introduced on the LH strip that would be destroyed at the time of casting.

8 Conclusions

In this paper, we have performed a threat analysis of the Prêt à Voter scheme. In particular, we have extended the analysis of Karlof et al with some further systems based vulnerabilities not identified in [11], and considered the applicability of these vulnerabilities to the Prêt à Voter scheme.

Prêt à Voter has proved to be remarkably resilient to these vulnerabilities, many of which stem from voter interaction with devices and generation of entropy at the time of voting. However, Prêt à Voter, is potentially prey to chain voting attacks, which do not apply to schemes in which the crypto material is generated on demand. In fact, as we have discussed, this attack is particularly virulent in the context of voter-verifiable schemes with pre-prepared ballot forms and Web Bulletin Boards. Wherever such threats apply to Prêt à Voter, counter-measures have been suggested.

As with any secure system, voting schemes require great care in their design and evaluation, not only of the cryptographic core, but also of the surrounding system. This analysis has provided valuable insight into the way forward for Prêt à Voter, and some enhancements have been suggested. It has also underlined the need for adequate error-handling and recovery strategies, and that a VPEAT style mechanism would be highly desirable.

The analysis presented here, as with the analysis of Karlof et al, does not of course constitute an exhaustive, systematic, identification of all the system-based threats to Prêt à Voter. 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 crypto voting systems. Here, we explore the space of possible failure modes and adversary capabilities, which will enable us to build a threat model.

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

Finally, we conclude that, provided that, in addition to a formal analysis of the core, technical system, socio-technical considerations are incorporated into the design and evaluation phases, there is every reason to suppose that cryptographic schemes of this kind can provide trustworthy, verifiable elections.

Acknowledgements

The authors would like to thank Michael Clarkson, David Chaum, Michael Jackson, Steve Kremer, Andy Neff, Andrey Povyakalo, Mark Ryan and Luca Vigano for fruitful discussions and DSTL and the EPSRC DIRC project for partial funding of this work.

References

1. Votehere, `http://www.votehere.net/default.php`
2. The trouble with technology. The Economist, September 16 (2004)
3. Bannet, J., Price, W., Rudys, A., Singer, J., Wallach, D.: Hack-a-vote: Security issues with electronic voting systems. IEEE Security and Privacy 2(1) (January/ February 2004)

4. Bryans, J., Ryan, P.Y.A.: A dependability analysis of the chaum voting scheme. Technical Report CS-TR-809, University of Newcastle upon Tyne (2003)
5. Chaum, D.: Secret-ballot receipts: True voter-verifiable elections. IEEE Security and Privacy 2(1), 38–47 (2004)
6. Chaum, D., Ryan, P.Y.A., Schneider, S.: A practical, voter-verifiable election scheme. In: di Vimercati, S.d.C., Syverson, P.F., Gollmann, D. (eds.) ESORICS 2005. LNCS, vol. 3679, pp. 118–139. Springer, Heidelberg (2005)
7. Fujioka, A., Okamoto, T., Ohta, K.: A practical secret voting scheme for large scale elections. In: Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, pp. 244–251. ACM, New York (1992)
8. Gerck, E.: Instant lottery cards too, re: reading pins in 'secure' mailers without opening them (2005), http://www.mail-archive.com/cryptography
9. Gogolewski, M., Klonowski, M., Kubiak, P., Kutylowski, M., Lauks, A., Zagorski, F.: Kleptographic attacks on e-election schemes with receipts. In: Müller, G. (ed.) ETRICS 2006. LNCS, vol. 3995, pp. 494–508. Springer, Heidelberg (2006)
10. Jones, D.W.: A brief illustrated history of voting (2003), http://www.cs.uiowa.edo/~jones/voting/pictures
11. Karlof, C., Sastry, N., Wagner, D.: Cryptographic voting protocols: A systems perspective. In: USENIX Security Symposium (2005)
12. Kohno, T., Stubblefield, A., Rubin, A.D., Wallach, D.S.: Analysis of an electronic voting system. In: Symposium on Security and Privacy. IEEE, Los Alamitos (2004)
13. Kremer, S., Ryan, M.: Analysis of an electronic voting protocol in the applied pi-calculus. In: Sagiv, M. (ed.) ESOP 2005. LNCS, vol. 3444, pp. 186–200. Springer, Heidelberg (2005)
14. Lauer, T.W.: The risk of e-voting. Electronic Journal of e-Government 2(3) (December 2004)
15. Mercuri, R.: A better ballot box? IEEE Spectrum Online (October 2002)
16. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1994)
17. Neff, A.: A verifiable secret shuffle and its application to e-voting. In: Conference on Computer and Communications Security, pp. 116–125. ACM, New York (2001)
18. Neff, A.: Practical high certainty intent verification for encrypted votes (2004), http://www.votehere.net/documentation/vhti
19. Neff, A.: Verifiable mixing (shuffling) of el-gamal pairs (2004), http://www.votehere.net/documentation/vhti
20. Randell, B., Ryan, P.Y.A.: Voting technologies and trust. IEEE Security & Privacy (2005) (to appear)
21. Ryan, P.Y.A.: Towards a dependability case for the chaum voting scheme. In: DIMACS Workshop on Electronic Voting – Theory and Practice (2004)
22. Ryan, P.Y.A.: Putting the human back in voting protocols. In: Christianson, B. (ed.) Security Protocols 2006. LNCS, vol. 5087, pp. 20–25. Springer, Heidelberg (2009)
23. Ryan, P.Y.A., Peacock, T.: Prêt à voter: a systems perspective. Technical Report CS-TR-929, University of Newcastle upon Tyne (2005)
24. Ryan, P.Y.A., Schneider, S.A.: Prêt à voter with re-encryption mixes. Technical Report CS-TR-956, University of Newcastle upon Tyne (2006)
25. Young, A., Yung, M.: The dark side of "Black-box" cryptography, or: Should we trust capstone? In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 89–103. Springer, Heidelberg (1996)