Best Practices in Internet Voting

Jordi Puiggalí, Jesús Chóliz, Sandra Guasch

Scytl Secure Electronic Voting
Tuset 20, 1-7, 08006 Barcelona, Spain
{name.lastname}@scytl.com

I. Introduction

Now a day, governments are using alternative voting channels such as postal, fax, or electronic voting to allow voters to cast their votes remotely. For instance, in USA, the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) [1] and Military and Overseas Voter Empowerment (MOVE) Act [2] are focused on providing to military and overseas voters means to exercise their right to vote remotely.

When choosing a specific scheme for remote voting, it is important to evaluate the security of the system by taking into account its security risks. The security measures implemented by the system must be identified and their effectiveness on mitigating these risks evaluated. Moreover, it must be ensured that these security measures are designed and implemented properly, evaluating if the measures properly address the security issues. If they are not implemented in a proper way, the security level provided drops dramatically. For instance, the fact that a voting platform is using a cryptographic mechanism does not ensure that this is properly implemented.

This paper is focused on evaluating Internet Remote Voting security measures that can be applied to mitigate the risks of remote voting. This can be used as reference when evaluating the best practices applied when designing and implementing these security measures. To evaluate their effectiveness, we used postal voting as reference.

The paper is organized as follows: in section II we introduce some basic security risks of remote voting, in section III, some security considerations used when implementing security measures in an Internet Remote Voting scheme are presented; in section IV we evaluate how the security measures effectively mitigate the introduced security risks using postal voting as reference, and the paper concludes in section V.

II. Security Risks of Remote Voting

In this section, we define general security risks of remote voting without considering a specific voting channel. They idea is to use them as reference for comparing different remote voting channels independently of the technology used by the channel.

The risks that we will use as reference are:

- **Unauthorized voters casting votes:** non-eligible voters could try to cast a vote for a specific election. The voting channel must provide a robust way to remotely identify voters.
- **Voter impersonation:** a voter or an attacker could try to cast a vote on behalf another person. The voting channel must provide a robust way to detect any impersonation attempt.
- **Ballot stuffing:** an attacker can try to add in the ballot box votes from voters that did not participate in the voting process. The voting channel must prevent the acceptance of votes that have not been cast by their intended voters.
- **Voter privacy compromise:** an attacker could break the voter privacy, identifying the voter with her voting options and, thereby, breaking the vote secrecy. The voting system must ensure that the voter's intent remains secret during the voting and counting phases.
- **Voter coercion and vote buying:** one person or organization could buy or force a voter to vote for specific voting options. The voting channel must prevent a voter from proving to a third party in an irrefutable way her voting intent.
- **Vote modification:** vote contents could be modified to change the election results. The voting system must detect any manipulation of valid cast votes.
- **Vote deletion:** an attacker could try to delete valid votes from the ballot box. The ballot box must be protected against unauthorized changes.
- **Publication of non-authorized intermediate results:** the intermediate results could be disclosed before the election is closed, influencing those voters that have not exercised their right to vote yet. The voting system has to preserve the secrecy of the cast votes until the tally process to prevent any partial results disclosures.
- **Voter distrust:** a voter does not have any means for verifying the correct reception and count of her vote. Therefore, the voter could have a negative feeling about the voting process. The voting platform must allow the voter to check if the vote has been correctly received at its destination, and if it has been present in the tallying process.

- **Election boycott-denial of service:** an attacker could disrupt the availability of the voting channel by performing a denial of service attack. The voting platform must detect the eventual congestion of the election services in order to react against them as soon as possible, e.g. by using contingency channels.
- **Inaccurate auditability:** not enough election traceability or easy to tamper with audit data may allow attackers to hide any unauthorized behavior. The voting channel should provide means to implement an accurate audit process and to detect any manipulation of the audit data.

III. Security considerations when implementing security measures in Internet Remote Voting schemes

When evaluating an Internet Voting platform, it is important to evaluate the efficiency of the measures implemented to manage the security risks. In this section we will introduce some security methods implemented in voting platforms and evaluate their efficiency on achieving the security objectives demanded in a secure election. These measures will be used in this paper to evaluate the risk mitigation of remote voting platforms.

Authentication methods: one important issue in Internet voting is how voter identity can be proved in a remote way. A usual approach consists on providing a username and a password to the voter at the time of registration, and request for them at the time of casting the vote, to ensure the identity of the voter. Following this approach, the username / password values have to be stored in the voting server in order to verify the identity of the voter. Therefore, in case an external attacker gains access to it, these credentials could be stolen from or modified in this server, in order to impersonate valid voters. Moreover, these credentials are vulnerable to eavesdropping attacks that intercept the passwords when submitted. Alternative proposals consist on using strong authentication methods, such as one-time passwords or digital certificates. One-time passwords prevent the re-use of intercepted credentials, since the authentication information sent (password) changes each time the voter is authenticated. The most robust solution for voter authentication is the use of digital certificates, since it provides, in addition to access authentication, data authentication: by digitally signing her vote, the voter can demonstrate that she is the owner of a specific vote. When this approach is used, the vote is encrypted before being signed. Otherwise, the digital signature could be used to correlate voters with votes. In case voters do not have digital certificates (e.g. an electronic ID card), a key roaming mechanism can be used to provide digital certificates to voters when casting their votes. The digital certificate would be protected by a PIN or password known by the voter. This password is not stored in a remote database and therefore cannot be accessed to impersonate the voter.

Vote encryption: in an e-voting platform, votes are vulnerable to eavesdropping practices during their transmission and storage. Therefore, vote encryption at the time of vote casting is of paramount importance to preserve vote secrecy. Some voting platforms implement vote encryption at the network transmission level, using SSL connections between the voter PC and the voting server. However, SSL encryption falls short to protect end-to-end voter privacy, since the vote is not encrypted when leaving the transmission channel: the vote is received at the voting server in clear text. Therefore, any attacker that gains access to the server system could access to the clear-text vote information and break the voter privacy. To solve this issue, it is strongly recommended to use data level encryption of votes, such as encrypting the votes using an election public key. That way, any attack at voting server level will not compromise voter privacy, since votes leaving the voting channel are still encrypted. The protection of the election private key is further discussed in a later section.

Vote integrity: cast votes are vulnerable from being tampered with by attackers that gain access to the voting system. As mentioned in previously sections, an efficient approach to prevent vote manipulation after casting a vote is to digitally sign it after encryption. Alternatively, votes can be protected by applying a cryptographic MAC function (e.g., an HMAC function) and send this value as an integrity proof of the vote. However, this measure has some security risks, since the key used to calculate the MAC function must be also known by the voting server to validate the vote integrity. Therefore, an attacker who gained access to the voting server could generate valid integrity proofs of modified votes. Digital signatures issued by voters do not have this problem. Moreover, digital signatures can be used for both integrity verification and identification purposes. In addition to digital signatures, advanced cryptographic techniques, such as zero-knowledge proofs of origin [3], can be used to ensure that the encrypted vote has been recorded as cast by the voter. The digital signatures and zero-knowledge proofs can

be stored jointly with the votes in the digital ballot box, in order to ensure their integrity until the moment of vote decryption

Protection of the election private key: as mentioned before, the election private key is aimed to protect voters privacy and intermediate results secrecy. Usually, asymmetric encryption algorithms are used: votes are encrypted using a public key, and they can only be decrypted using the corresponding private key. To prevent that an individual person could decrypt the votes, this key must be protected using a separation of duties approach. A recommended practice consists on splitting the key in several shares using threshold cryptography algorithms, and to give one share to each Electoral Board member. That way, a minimum number of Electoral Board members must collaborate to recover the election private key and decrypt the votes. It is of paramount importance to use a threshold scheme to prevent that the loss of one share could prevent the decryption of the votes.

Anonymizing votes before decryption: most voting platforms directly decrypt the votes at the end of the election. However, if the decryption is done straight forward, it could be possible to correlate clear text votes with encrypted ones and, therefore, to original voters. It is critical to break the correlation between clear text votes from the original casting order. The most efficient methods are based on Mixnets, where votes are shuffled and decrypted/encrypted several times before obtaining the vote contents; and the homomorphic tally, where the election result is obtained without decrypting the individual votes, but decrypting the result of operating the encrypted votes. Other methods (such as randomizing votes while stored) could not fully guarantee that there is no link between votes and voting order.

Individual and Universal verification methods: one of the major concerns of remote voting in general is the lack of means for the voter to verify the correct reception and count of her vote. The introduction of remote electronic voting can provide to the voters some means to individually verify the voting process, providing more confidence and detecting possible attacks. The verification process can be split in two methods: cast as intended and counted as cast verification.

The cast as intended verification consists on ensuring that the vote received by the voting server contains the voting options originally selected by the voter. For instance, it can be used to detect if the voter computer has any malware that is changing her voting options before encryption. One way to perform this verification consists on calculating special codes (commonly called Return Codes) using the encrypted vote received at the voting server, and returning them to the voter. The voter will in turn use a special Voting Card issued for the election to verify that the received Return Codes are those assigned to the voting options she has chosen. Since the Return Codes are calculated using a secret key only known by the voting server, an attacker cannot deliver forged Return Codes to the voter without being detected.

The counted as cast verification consists on ensuring that the vote cast by the voter is included in the final tally. This verification detects manipulation or deletion of cast votes. One method to ensure that the vote has reached the counting phase is to deliver to the voter a receipt with a random identifier. If this random identifier can only be retrieved from the encrypted and tallied votes, a voter can then verify that her vote has been included in the tally. It is of paramount importance that these random identifiers cannot be correlated with clear text votes. Otherwise, the Voting Receipt could be used for vote buying or coercion practices. This measure must be complemented with the universal verification of the decryption process. Universal verification should allow auditors and observers to verify in an irrefutable way that the decrypted votes represent the contents of the encrypted ones. In other words, that the decryption process did not manipulate the results. This can be achieved using advance cryptographic techniques.

Traceability and Auditability: traceability is essential for an Internet voting platform: logs or proofs generated by the different modules can be used to detect and react against real-time attacks or malfunctions, as well as ensuring the reliability of the election results. All the sensitive operations performed in the voting platform modules have to be registered in logs, taking care of not registering information that can compromise voters' privacy. In order to prevent an attacker from deleting or modifying these logs (to hide any attack), they can be cryptographically protected, in such a way that a specific log cannot be deleted without detection. Also, critical processes such as vote decryption should be designed to provide cryptographic proofs of correct performance, so an auditor can verify that the election results actually correspond to the values of the votes cast by the voters. It is recommended the use advanced cryptographic techniques to audit the correct performance of these processes. Therefore, both auditors and voters can participate in the audit

process (universal verifiability), increasing also the voter confidence.

IV. Risk Mitigation in Remote Voting

Depending on the approach used for implementing a remote electronic voting platform, security risks are managed in most efficient way. Therefore, the analysis on how these risks are properly mitigated is of paramount importance when taking a decision of implementing a remote electronic voting process. Several studies and reports discussing the risks and countermeasures of specific schemes for remote voting have been presented [4], [5], highlighting the main differences between postal voting, fax voting, e-mail voting and Internet voting. However, these analyses are mainly focused on comparing how the risks are managed by the different remote voting channels.

In this section, we compare how different remote electronic voting platform approaches manage the security risks present in remote voting. To this end, we will use as reference the security risks introduced at the beginning of this paper. In addition, to evaluate the risk mitigation efficiency of each approach, we will use as reference how similar risks are addressed in postal voting.

- **Unauthorized voters casting votes, voter impersonation and ballot stuffing.**
  - **Internet Voting with strong authentication:** *Mitigation Level: High.* Voters are protected from reply attacks and only votes digitally signed by valid voters are accepted.
  - **Internet Voting with password-based authentication:** *Mitigation Level: Low.* Voters are vulnerable to credential stealing attacks. Ballot stuffing is possible.
  - **Postal Voting:** *Mitigation Level: Low.* Voter handwritten signatures are difficult to validate or not always validated. Ballot stuffing is possible.
- **Voter privacy compromise.**
  - **Internet Voting with data-level encryption:** *Mitigation Level: High.* Votes are encrypted before being cast. Cryptographic measures can be implemented to break any connection between vote and voter (such as vote shuffling processes before decryption).
  - **Internet Voting with network-level encryption (SSL):** *Mitigation Level: Low.* Votes are only protected during their transmission and contents could be accessed at voting server.
  - **Postal Voting:** *Mitigation Level: Medium*. Votes are stored in envelopes containing the names of the voters. Votes can be intercepted to access to their contents before they are received by election officials.
- **Voter coercion and vote buying.**
  - **Internet Voting with multiple-voting:** *Mitigation Level: Medium.* If a voter is coerced, she can cast a new vote later.
  - **Internet Voting with kiosk:** *Mitigation Level: High.* Vote is cast in a controlled environment as traditional elections.
  - **Postal Voting:** *Mitigation Level: Low.* Voters can show the selected voting options to third parties before casting their votes.
- **Vote modification.**
  - **Internet Voting with voter digital signatures:** *Mitigation Level: High.* Only valid voters can digitally sign votes.
  - **Internet Voting with server digital signatures:** *Mitigation Level: Medium.* Votes can be manipulated before being digitally signed by the server.
  - **Internet Voting with MAC digital signatures:** *Mitigation Level: Low***.** Integrity proofs can be forged in case of getting access to the voting server.
  - **Postal Voting:** *Mitigation Level: Low.* There is no way to detect that the cast vote has been modified.
- **Vote deletion.**
  - **Internet Voting with cryptographic voting receipts:** *Mitigation Level: High.* Voting receipts allow voters to detect the elimination of their votes.
  - **Internet Voting with standard voting receipts:** *Mitigation Level: Low.* Voting receipts only allow voters to know that the server received the vote.
  - **Postal Voting:** *Mitigation Level: Low.* It is possible to eliminate or delay valid votes without detection.
- **Publication of non-authorized intermediate results.**
  - **Internet Voting with data-level encryption:** *Mitigation Level: High.* Only the Electoral Board members can decrypt the votes at the end of the election. Secret sharing techniques can be used to ensure separation of duties when decrypting.
  - **Internet Voting with network-level encryption (SSL):** *Mitigation Level: Low.*

Intermediate results could be obtained from clear-text votes received in the voting server.

- **Postal Voting:** *Mitigation Level: Medium.* Votes could be intercepted during transportation.

- **Voter distrust.**
  - **Internet Voting with cryptographic verification methods:** *Mitigation Level: High.* The use of individual and universal verification methods, allows voters and auditors to verify the correct behavior of the voting platform.
  - **Internet Voting without verification methods:** *Mitigation Level: Low.* Voters have to trust the voting platform, since they have no evidence of the correct recording and counting of their votes.
  - **Postal Voting:** *Mitigation Level: Low.* There is no guarantee that the vote is received and counted by Election Officials.
- **Election boycott-denial of service.**
  - **Internet Voting:** *Mitigation Level: Medium.* Despite remote e-voting is vulnerable to DoS attacks, the advantage is that voters and election managers can detect this behavior and apply corrective measures to reduce the impact (e.g., vote using an alternative channel or server).
  - **Postal Voting:** *Mitigation Level: Medium.* DoS attacks (e.g., delivery delays) are impossible to detect and, therefore, are more effective than previous ones. The difference is that these are more difficult to implement.
- **Inaccurate auditability.**
  - **Internet Voting with cryptographic audit means:** *Mitigation Level: High.* The use of individual and universal audit means facilitates to audit the real behavior of the voting platform. Using immutable logs ensures that audit processes are based on reliable audit data.
  - **Internet Voting with standard audit means:** *Mitigation Level: Low.* Audit process is based on standard log information that could be tampered with.
  - **Postal Voting:** *Mitigation Level: Low.* Audit means only cover part of the voting channel.

V. Conclusions

In this paper, we have presented the security risks of a remote voting platform, and introduced some recommendations of security measures that must be considered when evaluating the security of an e-voting platform. To show the impact of some of these measures, we evaluated how they can mitigate some of the security risks of remote voting. In this evaluation we also considered the efficiency of Internet voting platforms implementing more standard security measures and also postal voting.

The main conclusion is that the use of cryptographic mechanisms does not always increase the security of the voting platform if they are not properly implemented.

References

[1] UOCAVA law online:
http://www.fvap.gov/resources/media/uocavalaw.pdf

[2] MOVE Act is Subtitle H of H.R. 2647:
http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.2647:

[3] Jakobsson, M. *A practical mix*. In K. Nyberg, editor, EUROCRYPT '98, pages 448-461. Springer-Verlag, 1998. LNCS No. 1403.

[4] Puiggalí, J. and Morales-Rocha, V. 2007. Remote voting schemes: a comparative analysis. In *Proceedings of the 1st international Conference on E-Voting and Identity* (Bochum, Germany, October 04 - 05, 2007). A. Alkassar and M. Volkamer, Eds. Lecture Notes In Computer Science. Springer-Verlag, Berlin, Heidelberg, 16-28.

[5] Regenscheid, A. and Hastings, N. 2008. A Threat Analysis on UOCAVA Voting Systems. NIST.