REMOTE VOTING SCHEMES: A COMPARATIVE ANALYSIS

October 2007

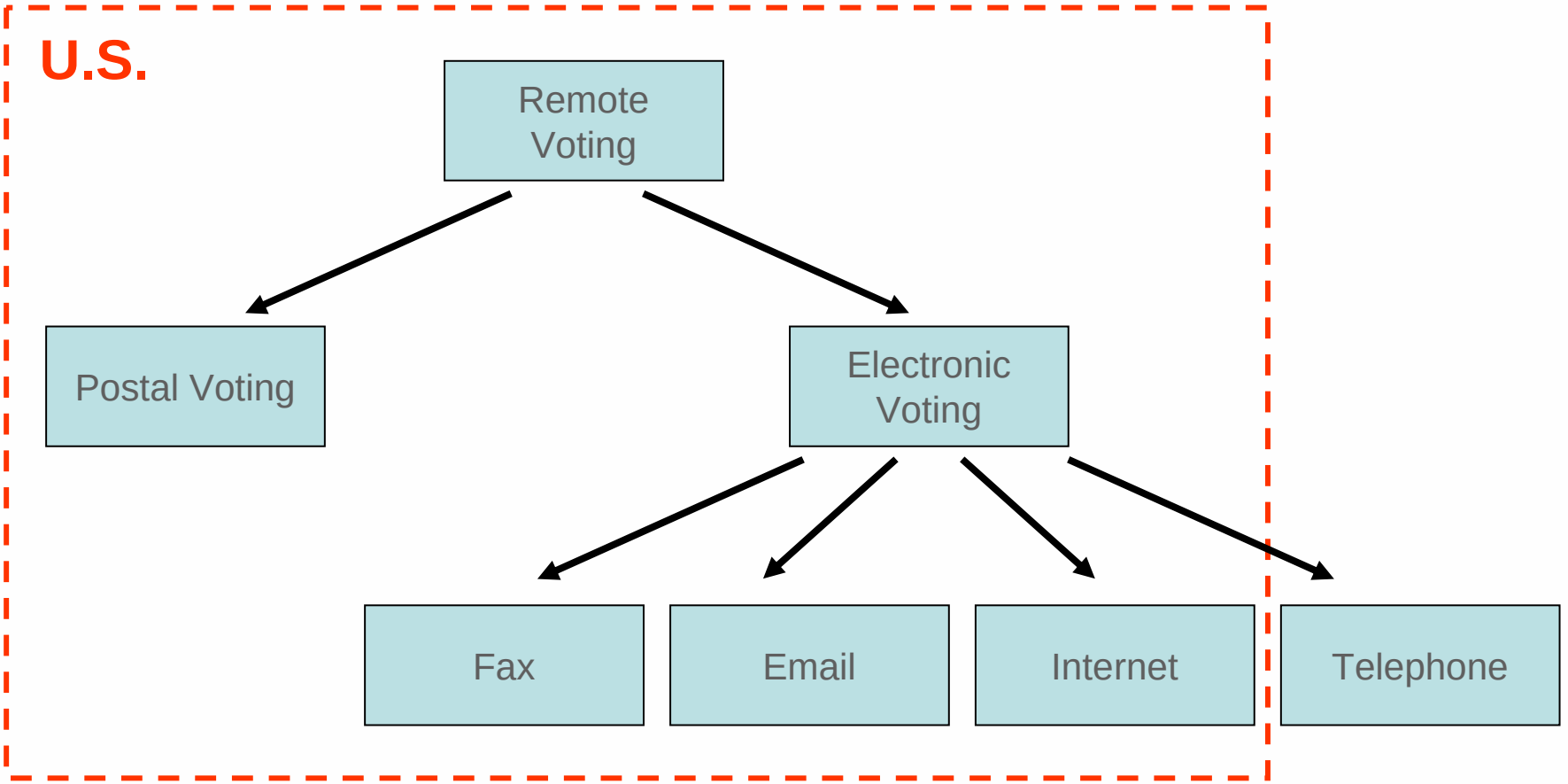
Jordi Puiggali
VP Research & Development
Jordi.Puiggali@scytl.com

scytl
Secure Electronic Voting

Index

- Remote Voting Schemes
  - Postal Voting
  - FAX
  - E-mail
  - Internet
- Evaluation Criteria
  - Security
  - Usability
  - Election Management
- Comparative analysis
- Conclusions

Classification



In our study we only analyzed the remote voting methods currently supported or tested in the United States for overseas voters (UOCAVA).

Postal, fax and email voting

- Postal Voting
  - Method supported by all States of US for UOCAVA voters
  - Main benefits:
    - Allows absentee voters to participate in the Election process
    - Easy to understand for average voters
  - Main drawbacks:
    - Reliability and security of the postal service
- Fax voting
  - Method supported by 24 States of US for UOCAVA voters
  - Main benefits:
    - Solves the uncertain reception issue of postal votes (recommended as contingency channel)
  - Main drawbacks:
    - Voter's privacy: Voters must sign a secrecy waiver
- Email voting
  - Method supported by 7 States of US for UOCAVA voters
  - Main benefits:
    - Partially solves the uncertain reception issue of postal votes (recommended as contingency channel)
  - Main drawbacks:
    - Voter's privacy: Voters must sign a secrecy waiver

Internet voting

- Internet voting
  - Introduced in 2000 for US overseas voters but currently is not supported after the publication of the SERVE Security report.
  - Main benefits:
    - Solves the uncertain reception issue of postal votes
    - Warns voters in case of involuntary errors that can invalidate their votes
    - Facilitates the implementation of cryptographic techniques
  - Main drawbacks:
    - Transparency: the use of electronic means instead of a paper ballot creates the perception of less transparency in the voting process
    - Insecurity of the voter's platforms: personal computers are vulnerable to virus and malware attacks that can manipulate the voter intend or compromise voter's privacy
    - Insecurity of Internet: Internet is a communication channel vulnerable to denial of service attacks that could prevent the participation of voters

Internet voting scheme used in the study:

- We used the cryptographic electronic voting scheme proposed by Andreu Riera
- This scheme has been used in several binding elections: Switzerland, UK, Philippines…

Index

Security evaluation criteria (i)

- Eligibility
  Only authorized voters should be able to vote. In this criteria we evaluated the involuntary impersonation of voters. Voluntary impersonation is considered as part of the coercion and vote buying criteria.
- Privacy
  The voting system has to protect voter privacy, concealing the relation between voter and his/her cast vote, and ensuring that the voter's choice will remain anonymous.
- Integrity
  A voting system has to protect the vote against manipulation once it is cast and until it is counted.
- Voter verifiability - cast as intended
  Voters must have the possibility to check if their votes have been accurately recorded.
- Voter verifiability - counted as cast
  Voters must have the possibility to verify the inclusion of his/her vote in the final tally. Not implemented in traditional elections.

Security evaluation criteria (ii)

- Prevention of intermediate results

  The voting system shall prevent the disclosure of intermediate results before the election is closed.

- Ballot box accuracy

  Protection against the addition of bogus ballots or the elimination of valid ballots (ballot stuffing).

- Coercion and vote buying resistance

  One of the main concerns of remote voting channel is that it facilitates coercion or vote buying. Therefore it is important to verify if the channel facilitates these practices or includes countermeasures to mitigate them.

- Channel reliability

  Availability to detect delivery delays o denial of service attacks in an appropriate timeframe.

Usability evaluation criteria

- Prevention of voting errors

  The voting channel has to prevent involuntary voting errors by voters when casting their votes (e.g., under-voting, over-voting).

- Ease of use

  The voting channel must be easy to use by average voters.

- Accessibility

  Disabled voters have to be allowed to vote with total privacy without the need of assistance from third parties.

Election management evaluation criteria

- Election set-up
  The voting channel has to be suitable to carry out a single election set-up.
- Voting period election management
  The voting channel has to be easy to manage during the voting period.
- Counting process
  It is important that the voting channel does not delay the current counting process.
- Auditing of the election results
  Voting channels must provide means for facilitating the audit of the election to ensure its correct execution.

Index

- Remote Voting Schemes
  - Postal Voting
  - FAX
  - E-mail
  - Internet
- Evaluation Criteria
  - Security
  - Usability
  - Election Management
- Comparative analysis
- Conclusions

Criteria evaluation approach

Criteria evaluation approach:

- Security: Risk Management
- Usability and Election management: requirement fulfillment analysis

Risk management

- Risk assessment: Analysis and evaluation of risks
  - Assumptions for implementing an attack
  - Effort required for exploiting the vulnerability
    Role of the attacker
    Can be targeted or must be widespread?
  - Probability of detection
    Are there any means for detecting such attack?
  - Isolation of the attack
    Is it possible to isolate the attack?
- Risk mitigation:
  - Security controls (countermeasures) available to prevent or mitigate the risks
  - Efficiency of these security controls
  - Risk acceptance based on current postal voting risk acceptance

Security comparative analysis (i)

Comparative factor	Postal Voting	Fax Voting	E-mail Voting	Internet Voting
Eligibility	**Medium** Easy impersonation to cast a vote. Handwritten signatures are difficult to validate accurately or not always validated.	**Low** Easy impersonation to cast a vote. Handwritten signatures are digitalized and therefore easy to tamper with.	**Low** Easy impersonation to cast a vote. Handwritten signatures are digitalized and therefore easy to tamper with.	**High** Te use of strong authentication such as digital certificates, prevents the risk of an involuntary impersonation attack.
Privacy	**Medium** There is a risk that the contents of postal votes could be accessed during their transportation or when the postal envelopes are opened.	**Low** Votes are received without any privacy protection. Voters are required to sign a secrecy waiver.	**Low** Votes are received without any privacy protection. Voters are required to sign a secrecy waiver.	**High** Votes are encrypted before being cast. Cryptographic measures, such as mixing processes, can be implemented to break any connection between vote and voter. Voters can protect their PC's against malware or use secure voting kiosks.
Integrity	**Low** There is no way to prove that the cast vote stays unaltered during the election process.	**Low** There is no way to prove that the cast vote stays unaltered during the election process.	**Low** There is no way to prove that the cast vote stays unaltered during the election process.	**High** Votes can be digitally signed, preventing any manipulation. Furthermore, when using voting receipts, any attempt to delete a vote could be detected by the voter when verifying the receipt.

Security comparative analysis (ii)

Comparative factor	Postal Voting	Fax Voting	E-mail Voting	Internet Voting
Voter verifiability - cast as intended –	**Medium** There are tools to track a vote sent by mail. However, there is no guarantee that the envelope received by the Election Officials contains the same vote cast by the voter.	**Low** There is no guarantee that the Fax vote is received at the destination as it was cast by the voter.	**Low** There is no guarantee that the postal envelope that contains the vote is received at the destination as it was cast by the voter.	**High** A verification process can be implemented as an independent process from the vote selection process in the voting terminal. Votes are protected by cryptographic means after being cast.
Voter verifiability - counted as cast -	**Medium** The voter can verify that his / her ballot is present during the tallying process through a ballot tracker. However, the voter can not verify if the ballot contents are the same selected by him /her.	**Low** The voter does not have any means to individually verify that her cast vote is present during the tallying process.	**Low** The voter does not have any means to individually verify that her cast vote is present during the tallying process.	**High** A voting receipt allows voters to individually verify that their votes are present in the tallying process.
Prevention of intermediate results	**Medium** The contents of the votes and therefore intermediate results could be accessed during transportation.	**Low** Vote contents could be accessed during the transmission. The vote contents are always accessible upon reception.	**Low** Vote contents could be accessed during the transmission. The vote contents are always accessible upon reception.	**High** Votes are encrypted before they are cast. Only the board members can decrypt them at the end of the election.

Security comparative analysis (iii)

Comparative factor	Postal Voting	Fax Voting	E-mail Voting	Internet Voting
Ballot box accuracy	**Medium** It is possible to add bogus ballots without detection. Votes can also be eliminated during transportation. Handwritten signatures can be verified to detect massive fraud.	**Medium** It is possible to add bogus ballots without detection However, the fax numbers of the voters can be audited in order to detect mass fraud.	**Low** It is possible to add bogus ballots. Email addresses can be impersonated. Also emails can be eliminated during transmission.	**High** Each encrypted vote can be digitally signed using a unique voter digital certificate to prevent the addition of bogus votes. Additionally, voting receipts can be provided to voters to allow them to detect the elimination of their votes.
Coercion and vote buying resistance	**Low** Voters can show the selected voting options to third parties before casting their votes, making coercion and vote selling possible.	**Low** Voters can show the selected voting options to third parties before casting their votes, making coercion and vote selling possible.	**Low** Voters can show the selected voting options to third parties before casting their votes, making coercion and vote selling possible.	**Medium** If a voter is coerced with the coercer's presence, he/she can cast a new vote later if multiple-voting is allowed. Alternatively, voting kiosks could help to prevent coercion and vote buying.

Security comparative analysis (iv)

Comparative factor	Postal Voting	Fax Voting	E-mail Voting	Internet Voting
Channel reliability	**Low** This voting channel depends on the reliability of the postal system of the country from which votes are cast. It is not unusual to receive votes after the closing date and voters can not do anything.	**High** Voters realize if their Fax vote has not reached to the election authority. Therefore contingency measures (e.g., try later or use another voting channel) can be used to prevent the lost of their votes.	**Medium** E-mail reception confirmation can be sent to the voter. However the e-mail transmission can be delayed.	**High** Voters realize if their vote has not reached the election authority if an error arises when casting the vote. Therefore contingency measures (e.g., try later or use another voting channel) can be used to prevent the lost of their votes.

Usability comparative analysis (i)

Comparative factor	Postal Voting	Fax Voting	E-mail Voting	Internet Voting
Prevention of voting errors	**Low** Voters cannot be alerted of involuntary voting errors that can invalidate their votes.	**Low** Voters cannot be alerted of involuntary voting errors that can invalidate their votes.	**Medium** Involuntary errors cannot be detected when the vote is being cast. However, votes can be automatically reviewed when received to detect errors. This could be a complex process since it requires some email interchanges with the voter (e.g., sending an email response with the vote status to the voter and wait for voter email confirmation).	**High** The voting application can detect any error during the selection process and notify voters before they cast their final vote. This allows voters to make the appropriate corrections.
Ease of use	**High** Most voters are familiar with paper ballots.	**High** Most voters are familiar with paper ballots.	**Low** Voters usually need to scan their votes and attach the scanned image to emails.	**Medium** Voting terminals can provide an intuitive, easy-to-use voter interface with clear instructions. However, some voters are not familiar with this kind of devices.

Usability comparative analysis (ii)

Comparative factor	Postal Voting	Fax Voting	E-mail Voting	Internet Voting
Accessibility	**Low** Paper ballots possess serious problems to visual impaired and some physically disabled voters. Support of multiple languages can cause privacy issues.	**Low** Paper ballots pose serious problems to visual impaired and some physically disabled voters. Support of multiple languages can cause privacy issues.	**Medium** The use of personal computers facilitates the interaction for disabled voters. However support of casting votes in multiple languages can cause privacy issues.	**High** The use of personal computers facilitates the interaction for disabled voters. Support of multiple languages does not require casting the vote in that language.

Election management comparative analysis (i)

Comparative factor	Postal Voting	Fax Voting	E-mail Voting	Internet Voting
Election set-up	**Low** Setting up an election requires long timeframes to ensure that election materials are received by voters on time.	**Medium** Time frames can be reduced since election materials can be received by fax. However this process could be difficult to automate.	**High** The sending of election materials can be automated by email.	**High** Process can be centralized (e.g., generation of a centralized electoral roll, instructions in a website) without requiring sending any materials to voters.
Voting period election management	**Medium** The management of the postal votes is mostly manual.	**Low** The privacy of the faxed votes must be protected (e.g., introduced in postal envelopes) after being received.	**Medium** The management of the votes could be automated. However email formatting problems could arise (e.g., different scanning resolutions).	**High** The management can be automated. Only the management of the security measures (e.g., management of election cryptographic keys) could add some complexity.
Counting process	**Medium** Votes must be manually counted or Election Officials have to place them into an optical counting device.	**Medium** Votes must be manually counted or Election Officials have to place them in an optical counting device.	**High** Counting process can be automated. However, problems with the internal formatting of votes could arise.	**High** Counting process is automated.

Election management comparative analysis (ii)

Comparative factor	Postal Voting	Fax Voting	E-mail Voting	Internet Voting
Audit of the election results	**Low** There is no guarantee that the cast vote is present during the tallying process. The voting channel (postal service) is practically impossible to audit.	**Low** There is no guarantee that the cast vote is present during the tallying process. Voting channel (land phone) is difficult to audit.	**Low** There is no guarantee that the cast vote is present during the tallying process. Voting channel (mailers, DNS servers, etc.) is difficult to audit.	**High** Voters can individually check the accuracy of the election with their voting receipts. Auditors can audit the voting application.

Index

- Remote Voting Schemes
  - Postal Voting
  - FAX
  - E-mail
  - Internet
- Evaluation Criteria
  - Security
  - Usability
  - Election Management
- Comparative analysis
- Conclusions

Conclusions

- Security
  - Currently accepted U.S. remote voting methods have serious security issues
  - When using appropriate cryptographic voting schemes, the implementation of Internet voting is not posing higher security risks to the voting process
  - Internet voting, based on appropriate cryptographic schemes, can provide better countermeasures for mitigating or preventing remote voting security risks posed by U.S. remote voting methods
- Usability
  - The introduction of Internet voting prevents the involuntary casting of invalid votes and increase the accessibility of the voting process
- Election management
  - Internet voting does not increase the complexity of the election process and improve the election auditability

www.scytl.com