Software Improvements Pty Ltd

Telephone Voting Solution

Electoral Commission ACT

Key Security Issues Overview

1 June 2020

The System

The Telephone Voting Solution (TVS) for the 2020 ACT Legislative Assembly Election enables voting via telephone for those community members who have difficulty presenting at a polling place, including the Blind and Vision-Impaired.

The TVS incorporates controls and processes designed to protect the vote, and the integrity of the voting process.

The TVS will be subjected to all of the security principles that would apply to any other voting methods available for the same election, and will undergo its own IRAP Assessment[1] in conjunction with upgraded eVACS® electronic voting system, currently in use by Elections ACT.

Physical Security

The TVS comprises two servers: an IVR server and a telephone voting server.

The system's two servers will be located at either SSICT premises in Canberra, or an ISM-certified external hosting facility.

The system will be protected by a certified firewall, with a number of approvals required to access the system.

More specifically, the system will;

- Rely on telecommunications provider enabled security on the telephony within the public telephone network.
- provide IVR (interactive voice response) verification in a way that preserves vote secrecy (e.g. protecting against a decrypted vote being linked to a voter).
- be configurable to limit server access to a specific range of Session Initiation Protocol (SIP) and Internet Protocol (IP) addresses.
- for secure telephony communication with the telecommunications provider, utilise Transport Layer Security (TLS) where available.
- for secure web service communication between the two servers, utilise https (TLS 1.2).
- ensure audio file updates are only available to authorised users.

Authentication of voters

All voters using the TVS will require completion of a registration process, where they will be formally identified and issued with personal access credentials.

The system will authenticate the elector as a registered telephone voter against these credentials, and collect their telephone voting preferences.. A web service Session Token is used to link the voting credential to the voting preferences, and this Session Token is only active for the length of the web service communication session. Committing the vote also deletes the voting session token.

Threats of cyber-attack

---

[1] https://acsc.gov.au/publications/irap/IRAP_Policy_and_Procedures.pdf)

The vote data is collected via telephone and stored in a controlled environment, where the threat of a cyber-attack or denial-of-service is minimised. A malicious attempt at hacking the system would need to be made via an interruption to the public telephone service.

Encryption

Communications between different components of the telephone voting system are encrypted through use of HTTPS (via TLS1.2). Votes are encrypted together for export via a password protected encrypted container on USBs.

Cast-as-Intended

(Individual Verifiability)

A complete list of voter preference selections is returned (played) to the voter once they have completed voting, allowing voter to check and confirm that their encrypted preference information was received by the server correctly, and contains their selected voting options.

Vote Correctness

The voting server verifies that the voter preferences stored during a voting session match with the order of preferences obtained by re-running the key presses made by the voter during their voting session.

The automatic sequential numbering of preferences ensures that a voter submits either a blank informal vote or a valid vote.

Vote Secrecy

The use of voting credentials as a voter verification method provides authentication of voters without ongoing reliance on access to electoral rolls. Additionally, the use of a Session Token to link the voter and their preferences (through an encrypted web service) removes any link between the voter and their vote once the voting session ends.

Context

Of note is the following extract from the "Report on the Security of the iVote System" by Roger Wilkins AO, dated May 2018, which has relevance to all of Australia's Electoral Commissions;

> *"Electoral commissions should always bear in mind that the ultimate arbiter of election results is a court. In designing systems for elections, including internet voting, electoral commissions therefore need to have the sort of evidence that would enable a court to conclude that the system produces a reliable outcome and, if a problem has occurred, its effect has been identified. Their test should be: would a court say that this system is fair and reasonable? Can we demonstrate that to the satisfaction of a court?"*

Author

Software Improvements Pty Ltd
May 2020