From:	Carol Boughton
To:	Spence, Rohan
Cc:	Clive Boughton
Subject:	HPE CM: Security issues for the ACTEC telephony (IVR) Platform
Date:	Thursday, 4 April 2019 9:23:06 PM

Ro

Last week you asked the question about the security of IVR voting. Below are some comments provided by our partners.

Regards

Carol

Security and IVR/Telephone Voting for ACTEC

An Interactive Voice Response (IVR) in an election context could perform a number of functions, but is commonly associated with registration processes, voting options provided for absentee or remote voters, and improved accessibility for voters with disabilities.

Certain security aspects of these systems are set out in the Australian Telephone Voting Standard issued by the Electoral Council of Australia (section 10)[i]. However these are more to do with the security and privacy requirements, rather than methods used to ensure compliance with those requirements

Generally, a telephone voting system will be subjected to all of the security principles that would apply at a polling place, such as anonymity and secrecy of the vote, and security of transmission of the votes for counting. The IVR servers would mirror the eVACS® system in terms of presentation of stored data.

The IVR servers (minimum of two) would be a standalone system either physically located within an ACSC[ii] certified high level security environment (such as the Vault hosting facility in Canberra), or co-located with other appropriate vote storage physical infrastructure (e.g. with the Election Server).

A system located within the proposed high level security environment at Vault would be protected by Vault's certified firewall, with a number of access approvals required before access to the system is granted.

The IVR system stores votes in an eVACS® generated server which then uploads to the Election Server for counting, just like votes from polling places and scanning. The storage media will have been encrypted.

We are proposing that the IVR platform undergoes its own IRAP Assessment[iii] in conjunction with eVACS®.

Security associated with the PSTN (Public Switched Telephone Network)

The IVR encrypts all communications within its control (and within the hosting facility) via the Secure Real-Time Protocol (SRTP).

Transmission issues: Telephone voting via the PSTN means that voters may initiate a call from various devices (home analogue/digital landline, business extension or mobile phone) and as such the levels of security available will also vary. For example, the 4G network in Australia provides encryption of mobile phone calls to base stations, but not end to end.

Where telephone voting for government elections is available (e.g. some jurisdictions in Australia), the possibility of unlawful interference with calls over the PSTN is considered an acceptable risk, while ensuring compliance with Australian Government Information Security

Manual guidelines for communications systems (Telephone Systems). [iv]

More specifically, the IVR system could:

- provide IVR 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 SIP and IP addresses.
- for external (web service) communication, utilise https / TLS 1.2.
- ensure file modification is only available to authorised users, with the file system locked down otherwise.
  where Voice / Speech Recognition is required, carry out processing on the IVR servers with no external dependencies.

References:

i.https://www.ecanz.gov.au/sites/default/files/telephone-voting-standard.pdf?v=1526004880

ii https://vaultcloud.com.au/why-vault/secure/

iii Information Security Registered Assessors Program (IRAP) see
https://acsc.gov.au/publications/irap/IRAP_Policy_and_Procedures.pdf

iv https://acsc.gov.au/publications/ism/ISM_10_Guidelines_for_Communications_Systems.pdf

---

Dr Carol Boughton
Managing Director
Software Improvements Pty Ltd
Ph: [redacted]
Mobile: [redacted]
www.softimp.com.au
