

A Statement from Hong Kong Public Opinion Research Institute (PORI) on the Information Security of the PopVote System

17 July 2020

On behalf of the PopVote IT Advisory Group, PORI would like to brief the public on the information security of the system and the security related incidents in the past few days.

PopVote system is designed with security and confidentiality as the primary concerns and only collects minimal personal data. The last four digits of the HKID, the date of issue and date of birth are used for identity verification and to prevent repeated voting. To prevent leakage of personal information, no information is transmitted in plain text. All personal data are first one-way cryptographically hashed, then end-to-end encrypted, and then transmitted to polling station device by QR Code. The private key of the polling station device can only decrypt the specified data for identity verification, and then send the encrypted ballot data to the server after identity verification. During ballot counting, the server data was downloaded from the encrypted network and transferred to the air-gap computer via USB flash drive for decryption. To prevent hacking from the Internet, the air-gap computer running the electronic ballot counting system was completely offline from the Internet and unnecessary hardware were removed or disabled. The decryption keys used in the ballot counting were securely kept in different locations by multiple personnel. The system was independent from the computer systems in PORI's offices.

The technical specifications of the preliminary election system can be found on the GitHub link that PORI has previously announced, and the technical team will also open sources the software as soon as it is ready. We open source the software in the hope that it can be reused by others in the civil society, and help continue developing the system. Open source will also allow anyone to review the code, help identify and fix any potential problems when using the system again in the future.

We assumed that there would be attacks from other organisations, including the government against this system. As a civil organisation, it is very difficult to defend against the threats with only limited resources. Therefore, the system adopts a security by design principle, and multiple layers of security measures are in place to ensure that the likelihood of personal data leakage from the system is extremely low. In short, there are three key components of the electronic voting system that need to be protected:

- The air-gap computer and physical environment must be secure.
- The end-to-end encryption key requires proper offline protection.
- A separate set of encryption keys and passwords are required for each station to prevent large-scale data leakage.

To the best of our knowledge, all parts of the electronic voting system have been operating normally throughout the primary election operation. The ballot counting was done under the supervision of PORI and the IT Advisory Group. The process and environment of the paper counting was also an important part of the process, but as it is not covered by the electronic ballot counting, so we do not go into detail here.

All original data, including personal information and decryption keys, were destroyed after the completion of the count, including:

- Deleting the database of voting files on the server and all its backups.
- All USBs that have ever stored decryption keys and voting files are securely deleted by overwrites multiple times.
- Erasure of two laptop hard drives that had stored small amounts of paper counting data by overwrites multiple times.

PORI will only keep statistics that do not contain personal data for future research purposes. The statistics will be encrypted and sealed for disclosure after the Legislative Council election in September.

Finally, we would also like to take this opportunity to explain to the public and account for two recent information security related incidents.

1. Early disclosure of e-counting results by the media

PORI is still investigating the incident and the IT Advisory Group does not believe it is related to the voting system. As far as we understand it, the system finished counting that night and the results were read out via video conferencing and recorded by PORI staff at the end of the night. It is stored on Google Spreadsheets and documents for internal use. The documents only recorded the polling results and did not contain any personal information of the voters. Whether there are any flaws in the way the documents were handled this time which could be exploited by hackers or information was leaked is subject to further investigation.

Once again, we emphasize that the voting data and decryption keys are handled offline and have not been compromised as far as we know.

2. Last Friday night, PORI was raided by the police, and the system encryption keys were regenerated.

That night, the IT Advisory Group was informed that one of the computers searched by the Police stored the encryption keys and passwords of all the polling stations. Although the police assured us that the information would not be used for any purpose other than investigation, we cannot guarantee the secrecy of encryption keys and passwords of all the polling stations at this point.

On Friday night, the decision was made to use a new air-gap computer to regenerate all the encryption keys. The air-gap computer and decryption keys are kept in a secure location by confidential personnel. This measure results in:

- Delayed start for Saturday's station.
- The Android Voting App is not available and users can only vote via the webpage (iPhone Voting App will remain the webpage as it has not been approved by Apple).

We apologize for the inconvenience this may cause.

We will continue to uphold the highest standards of information security to protect personal data and hope to continue to help Hong Kong people to express their views in a secure environment.