PORI
HONG KONG PUBLIC OPINION RESEARCH INSTITUTE
香 港 民 意 研 究 所

Tel 電話: (852) 3844 3111
Fax 傳真: (852) 3705 3361
Website 網址: https://www.pori.hk
Address 地址: 3rd Floor, SPA Centre, 53-55 Lockhart Road, Wanchai, Hong Kong
香港灣仔駱克道 53-55 號恆澤商業大廈 3 樓

香港民意研究所（研究所，PORI）有關普及投票系統資訊安全之聲明

2020 年 7 月 17 日

香港民意研究所謹代表普及投票系統的資訊科技顧問小組，向公眾闡述有關系統的資訊安全，以及說明過去幾天與系統保安相關的事故。

普及投票系統設計以安全及保密作首要考慮，只收集最低限度的個人資料，包括香港身分證的最後四碼、發出日期及出生日期，以作核實身份、防止重覆投票之用。為防止洩露個人資料，系統不會以明文傳送任何資料。所有個人資料均先以單向密碼雜湊處理，再進行端對端加密，然後以 QR Code 形式傳送至票站設備。票站設備鑰匙只能解密指定資料作核實身份之用，核實身份後再傳送已加密的選票資料至伺服器。進行點票時，伺服器的資料會經加密網絡下載，以 USB 隨身碟轉移至離線電腦上進行解密及點票。為避免遭黑客經互聯網入侵，電子點票系統與互聯網完全隔絕，並且移除或停用了不必要的硬件。點票所使用的解密鑰匙經由多名人員妥善保存於不同地點，整個點票系統包括離線電腦，均獨立於研究所辦公室的電腦系統。

有關初選系統的技術規格可參考研究所早前公佈之 GitHub 連結，稍後技術團隊亦將開放源碼，希望可以為各公民團隊所用，並協助繼續發展系統。開放源碼亦可以讓任何人士均可審視程式碼，將來再使用系統時，協助儘早指出並堵塞任何可能存在的保安漏洞。

我們當初已經假設可能會有其他組織（包括政府）監控通訊網絡或入侵電腦。不過作為一個民間組織，在有限的資源下要作出防禦的難度甚高；所以我們從投票系統設計中已設置多重保安，保證系統洩漏個人資料的可能性極低。簡而言之，電子投票系統有三個重要部分需要重點保護：

- 離線處理的電腦和物理環境要保證安全
- 解密鑰匙需要妥善的離線保護
- 每個票站均需設有一組獨立的加密鑰匙和密碼，以防止大規模資料洩露

PORI
HONG KONG PUBLIC OPINION RESEARCH INSTITUTE
香 港 民 意 研 究 所

Tel 電話: (852) 3844 3111
Fax 傳真: (852) 3705 3361
Website 網址: https://www.pori.hk
Address 地址: 3rd Floor, SPA Centre, 53-55 Lockhart Road, Wanchai, Hong Kong
香港灣仔駱克道 53-55 號恆澤商業大廈 3 樓

就我們所知，在整個初選的運作當中，電子投票系統之各個部份均正常運行，點票過程亦在研究所以及資訊科技顧問小組的監察下進行。另外紙張點票的流程與環境也是重要一環，不過相對獨立於電子投票，我們不在此詳述。

所有原始資料，包括個人資料及解密鑰匙均已在點票完成後銷毀；包括:

- 刪除伺服器上的投票檔案資料庫及其所有備份
- 所有曾經儲存解密鑰匙及投票檔案的 USB 以重覆寫入方式刪除
- 兩部曾經儲存少量紙張點票資料的手提電腦硬碟以重覆寫入方式刪除

研究所僅保存不含個人資料之統計數據作日後各方研究之用，統計數據已被加密及封存，待九月立法會選舉後公開。

最後，我們也希望藉此向公眾解釋及交代較早前發生兩件與資訊保安相關的事故：

一、電子點票結果提前被傳媒披露

研究所仍在調查事件，顧問小組暫不認為與投票系統有關。據我們了解，當晚系統點票完畢，點票結果經視像會議讀出，並由研究所職員紀錄於 Google Spreadsheet 及文件中以供內部使用。文件只紀錄有關點票結果，並不存在任何選民的個人資料。至於是次處理文件的方式是否存在瑕疵，令黑客有機可乘或資料被流出，則有待進一步跟進調查。

我們再一次強調，投票資料及解密鑰匙均為離線處理，據我們所悉並無外洩。

二、上週五晚間研究所曾被警方搜查，系統需重設加密鑰匙

當晚顧問小組得悉，其中一部被警方搜查的電腦儲存了所有票站加密鑰匙及密碼。雖然警方保證資料並不會用於調查以外之用途，但鑑於我們無法保證所有票站的加密鑰匙及密碼均能妥善保密，謹慎起見，星期五當晚即決定使用新的離線電腦重設所有加密鑰匙，並安排將離線電腦及解密鑰匙，交由保密人員於安全地點保管。此措施導致：

- 週六的票站需要延遲開始
- Android 投票 App 無法使用，用戶只可透過網頁版投票 (iPhone 投票 App 因未通過 Apple 的審查，仍維持網頁版投票)

帶來不便，還望體諒。

我們會繼續秉持對資訊保安的最高要求，保障個人資料安全，希望繼續協助香港人在安全的環境下表達意見。

PORI
HONG KONG PUBLIC OPINION RESEARCH INSTITUTE
香 港 民 意 研 究 所

Tel 電話: (852) 3844 3111
Fax 傳真: (852) 3705 3361
Website 網址: https://www.pori.hk
Address 地址: 3rd Floor, SPA Centre, 53-55 Lockhart Road, Wanchai, Hong Kong
香港灣仔駱克道 53-55 號恆澤商業大廈 3 樓

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:

PORI
HONG KONG PUBLIC OPINION RESEARCH INSTITUTE
香 港 民 意 研 究 所

Tel 電話: (852) 3844 3111
Fax 傳真: (852) 3705 3361
Website 網址: https://www.pori.hk
Address 地址: 3rd Floor, SPA Centre, 53-55 Lockhart Road, Wanchai, Hong Kong
香港灣仔駱克道 53-55 號恆澤商業大廈 3 樓

- 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.

PORI
HONG KONG PUBLIC OPINION RESEARCH INSTITUTE
香 港 民 意 研 究 所

Tel 電話: (852) 3844 3111
Fax 傳真: (852) 3705 3361
Website 網址: https://www.pori.hk
Address 地址: 3rd Floor, SPA Centre, 53-55 Lockhart Road, Wanchai, Hong Kong
香港灣仔駱克道 53-55 號恆澤商業大廈 3 樓

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.