2

Review Your Choices: When ConfirmationPages Break Ballot Secrecy in OnlineElections

James Brunet , Athanasios Demetri Pananos , and Aleksander Essex(B)  
Western University, London, Canada  
{jbrunet8,apananos,aessex}uwo.ca

Brief Description of the Topic

Ballot secrecy in online elections is studied for active attacks, but passive attacks on message lengths are less explored. Volkamer and Krimmer's requirement for e-voting protocol messages raises concerns. The study tested if ballot confirmation pages leak voter selection information, with Montreal-based Simply Voting being the only vendor with publicly accessible demonstrations.[1]

The system involves ballot-casting, verification, and review processes, but potential side-channel attacks, such as length-based attacks on voter selections, have been observed in the Voatz system.[2] Voatz's system allows explicit, uncompressed candidate names, while Simply Voting uses fixed-length IDs. The length and value of a candidate's name can affect confirmation page size and potentially leak information under certain conditions.

SwissPost and Neuvote systems avoid transmitting confirmation pages over the internet by generating them on the client side in JavaScript. This prevents network activity and no correlation between candidate name length and network response length. To mitigate length-based fingerprinting attacks, padding is added to ensure a fixed response length. However, this method has limitations and could slow page load times. Simply Voting has implemented a mitigation by adding random padding bytes to their ballot confirmation pages, resulting in a 25% accuracy in prediction strategies. Ballot secrecy headers can be compromised when a voter abstains, resulting in unique TLS record lengths.

Conclusions of the Paper

In a real-world mayoral election, a model based on network-observed TLS record length of voters' vote confirmation page predicted the chosen candidate with 83% accuracy. In complex ballots, it outperformed random guessing. However, limited information could be collected for significant subgroups of ballots. This performance discrepancy is unlikely to be explained by sample variation, according to validation. It is difficult to obtain voter demos, and firms should not require lengthy internal considerations to answer to requests. The industry should follow Simply Voting's lead and provide free demos.

Critical Opinion of the Paper

This paper explores the issue of ballot secrecy in online voting settings, highlighting the potential for exploitation by network observers. A novel attack on encrypted ballot confirmation pages was demonstrated in a recent Canadian mayoral race .A testing system was developed, consisting of a Client Application and a Server Application, to simulate an online voting system. The system simulates an election where voters can vote for one or more offices, with each ballot representing an actual HTTP request. In reality, a voter's choice correlates with the TLS record length of the ballot confirmation page.

SwissPost and Neuvote systems are better because avoid transmitting confirmation pages over the internet by generating them on the client side in JavaScript.There is no Internet activity ,no correlation between candidate. Padding is used to length-based fingerprinting attacks, however it has disadvantages such as huge response size and content reliance. A solution could be to display candidate names as fixed-length images.

1. Cardillo, A., Akinyokun, N., Essex, A.: Online voting in Ontario municipal elections: a conflict of legal principles and technology? In: Krimmer, R., et al. (eds.)E-Vote-ID 2019. LNCS, vol. 11759, pp. 67–82. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-30625-0\_5
2. Specter, M.A., Koppel, J., Weitzner, D.: The ballot is busted before the blockchain:a security analysis of Voatz, the first internet voting application used in US. Federalelections. In: 29th USENIX Security Symposium (USENIX Security 2020), pp. 1535–1553 (2020)

Citation /Reference: Use **APA** format

Brunet, J., Pananos, A. D., & Essex, A. (2022, September). Review Your Choices: When Confirmation Pages Break Ballot Secrecy in Online Elections. In *International Joint Conference on Electronic Voting* (pp. 36-52). Cham: Springer International Publishing.‏