Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System

Filip Zagorski and Richard T. Carback and David Chaum and Jeremy Clark and Aleksander Essex and Poorvi L. Vora

Abstract: We propose and implement a cryptographically end-to-end verifiable (E2E) remote voting system for absentee voters and report on its deployment in a binding municipal election in Takoma Park, Maryland. Remotegrity is a hybrid mail/internet extension to the Scantegrity in-person voting system, enabling secure, electronic return of vote-by-mail ballots. It provides voters with the ability to detect unauthorized modifications to their cast ballots made by either malicious client software or a corrupt election authority—two threats not previously studied in combination. Not only can the voter detect such changes, they can prove it to a third party without giving up ballot secrecy.

Category / Keywords: applications / election schemes

Publication Info: The 11th International Conference on Applied Cryptography and Network Security (ACNS 2013)

Date: received 12 Apr 2013, last revised 15 Apr 2013

Contact author: clark at scs carleton ca

Note: This paper extends the version appearing at ACNS 2013 with an appendix.

Version: 20130415:145812 (All versions of this report)