

Security in Large-Scale Internet Elections: A Retrospective Analysis of Elections in Estonia, The Netherlands, and Switzerland

Guido Schryen, Eliot Rich

Remote voting through the Internet provides convenience and access to the electorate. At the same time, the security concerns facing any distributed application are magnified when the task is so crucial to democratic society. In addition, some of the electoral process loses transparency when it is encapsulated in information technology. In this paper, we examine the public record of three recent elections that used Internet voting. Our specific goal is to identify any potential flaws that security experts would recognize, but may have not been identified in the rush to implement technology. To do this, we present a multiple exploratory case study, looking at elections conducted between 2006 and 2007 in Estonia, Netherlands, and Switzerland. These elections were selected as particularly interesting and accessible, and each presents its own technical and security challenges. The electoral environment, technical design and process for each election are described, including reconstruction of details which are implied but not specified within the source material.

We found that all three elections warrant significant concern about voter security, verifiability, and transparency. Usability, our fourth area of focus, seems to have been well-addressed in these elections. While our analysis is based on public documents and previously published reports, and therefore lacking access to any confidential materials held by electoral officials, this comparative analysis provides interesting insight and consistent questions across all these cases.

Effective review of Internet voting requires an aggressive stance towards identifying potential security and operational flaws, and we encourage the use of third party reviews with critical technology skills during design, programming, and voting to reduce the changes of failure or fraud that would undermine public confidence.

Index Terms— e-voting, Internet voting, Internet election, security, verifiability, RIES, Estonia, Neuchâte

Manuscript received July 17, 2009.

Guido Schryen is with the International Computer Science Institute, Berkeley, CA 94704 USA (phone: 510-666-2972; fax: 510-666-2956; e-mail: schryen@gmx.net).

Eliot Rich is with the University of Albany, Albany, NY 12222 USA (e-mail: e.rich@albany.edu).