Information security of the 2016 Philippine automated elections, a case study

Jeffrey Ian C. Dy

Technical Report

RHUL–ISG–2022–4

11 April 2022

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Executive Summary

The Philippines held its first fully automated national and local elections in 2010, after 18 years of deliberation on transitioning from manual counting of ballots. While the 2010 automated elections was a success, some criticisms emerged and points for improvement that were later applied in the 2016 Philippine presidential elections. This research examined the issues surrounding the 2016 automated presidential elections with the aim of recommending improvements for the Philippine Automated Election System (AES) for the next presidential elections in 2022.

To assess the 2016 presidential elections, the research developed and used an Automated Election System Trust Model that included the properties of: (1) voter privacy; (2) uncoercibility / receipt-freeness; (3) individual verifiability; (4) universal verifiability; (5) fairness; (6) data integrity; (7) availability; and (8) non-repudiation. Analysis of 426 log files of Vote Counting Machines (VCM) and Consolidation and Canvassing System (CCS) covering 192 clustered precincts were compared to news clippings, case pleadings, transcripts of the meetings of the JCOC and its Technical Working Group (TWG), and various laws, rules and regulations to create a more holistic picture of the 2016 automated presidential elections. In the scoring, the AES failed in 5 out of 8 properties of the Trust Model. Lack of transparency was seen as the major factor, thereby urging the adoption of a more transparent approach to certification and source code review in evaluating the Philippine AES.

Keywords: Philippines, elections, automated elections, eVoting, electoral fraud, Smartmatic, Commission on Elections.