Clash Attacks on the Verifiability of E-Voting Systems

Ralf Küsters Tomasz Truderung
Andreas Vogt
University of Trier, Germany
{kuesters,truderung,vogt}@uni-trier.de

Abstract

Verifiability is a central property of modern e-voting systems. Intuitively, verifiability means that voters can check that their votes were actually counted and that the published result of the election is correct, even if the voting machines/authorities are (partially) untrusted.

In this talk, we raise awareness of a simple attack, which we call a clash attack, on the verifiability of e-voting systems. The main idea behind this attack is that voting machines manage to provide different voters with the same receipt. As a result, the voting authorities can safely replace ballots by new ballots, and by this, manipulate the election without being detected.

This attack does not seem to have attracted much attention in the literature. Even though the attack is quite simple, we show that, under reasonable trust assumptions, it applies to several e-voting systems that have been designed to provide verifiability. In particular, we show that it applies to the prominent ThreeBallot and VAV voting systems as well as to two e-voting systems that have been deployed in real elections: the Wombat Voting system and a variant of the Helios voting system.

We discuss countermeasures for each of these systems and for (various variants of) Helios provide a formal analysis based on a rigorous definition of verifiability. More precisely, our analysis of Helios is with respect to the more general and in the area of e-voting often overlooked notion of accountability.

This work has appeared at S&P 2012. The talk will be given by Ralf Küsters.