Classifying Privacy and Verifiability Requirements for Electronic Voting

Lucie Langer, Axel Schmidt, Melanie Volkamer, Johannes Buchmann
CASED
Technische Universität Darmstadt
{langer, axel, buchmann}@cdc.informatik.tu-darmstadt.de, volkamer@cased.de

Voter privacy and verifiability are fundamental security concepts for electronic voting. Existing literature on electronic voting provides many definitions and interpretations of these concepts, both informal and formal. While the informal definitions are often vague and imprecise, the formal definitions tend to be very complex and restricted in their scope as they are usually tailored for specific scenarios and assume particular attack models. Moreover, some of the existing interpretations are contradictory.

This paper provides informal, yet precise definitions of anonymity, receipt-freeness and coercion-resistance and identifies different levels of individual and universal verifiability. The definitions are informal enough to be understood by readers without detailed technical knowledge in order to allow for an interdisciplinary discussion, and yet precise enough to capture any logical relations. We also analyze the relations between the requirements and their different levels and investigate whether specific combinations are impossible.

The overarching goal of this paper is to make a first step towards providing a compilation of the different levels which are conceivable for implementing the e-voting security requirements in practice. An according compilation allows to customize the security requirements for elections of different significance, for instance political elections vs. elections in associations.