Securing Elections, Trust by Verify!

Keynote By

Prof. Dr. Peter Y.A. Ryan

Full Professor of Applied Security at the University of Luxembourg, Head of the APSIA group, SnT

We frequently hear of the result of an election being contested (usually by the losers for some reason). Like justice, democracy should not only be done but seen to be done. Ideally an election should provide proof of the announced outcome, and such proof should be compelling to all right-minded folk. Achieving such transparency while guaranteeing the secrecy of the votes is immensely challenging, arguably one of the greatest challenges facing the information security community. Assurance of accuracy and privacy should be achieved with minimal trust assumptions and against a spectrum of powerful adversaries, from a spouse to a hostile nation state. Such adversaries go beyond what is usually studied in the information security literature as they may interact with the voters issuing instruction and demanding that they reveal private information such as passwords, credentials etc. Furthermore, any voting system should be supremely usable and understandable by the electorate at large.

Note also that voting is not confined to democratic processes, it is also widespread in many digital technologies, for example Single, Secret Leader Elections are central to many crypto technologies.

In this talk I will outline attempts to steer a course between these contending requirements, from primitive technologies of the Ancient Greeks, through a menagerie of technologies used in the US to the latest advances using the power of modern cryptography.