

Dependable E-Voting Systems

Professor Peter Ryan
(peter.ryan@newcastle.ac.uk)

Newcastle University
Centre for Software Reliability, UK

Confidence in voting systems has been badly shaken in recent years, in particular in the wake of the 2000 and 2004 US elections, but also by the many reports of elections throughout the world whose accuracy and probity has been questioned.

Researchers have been pursuing the goal of high assurance, verifiable voting schemes. A number of schemes have emerged in the last few years that are reaching a sufficient level of maturity for them to be seriously considered for deployment in real elections and referenda.

The problem with most existing voting technologies is that voters (and election officials) have to place a high degree of trust in the underlying technology, software etc. The challenge is to provide voting systems that enable voters to confirm that their vote is accurately included in the count whilst not providing them any way to prove to a third party how they voted. Furthermore, this should be achieved without the voter needing to place any trust in officials, software or hardware.

In this tutorial I will describe the requirements of such schemes and the challenges that achieving them pose. Having laid the ground by outlining the various cryptographic primitives that are required And threats that need to be countered, I will then present the Pret a Voter scheme.