Paving the way for electoral reform

Ben Smyth and Mark Ryan

Formal Verification and Security Group,
School of Computer Science,
University of Birmingham

May 19, 2010

Electronic voting systems are being introduced, or trialled, in several countries to provide more efficient voting procedures with an increased level of security. However, current deployment has resulted in catastrophic failure due to unrealistic trust assumptions. In particular, the trustworthiness of hardware/software and election officials has been assumed. In practice, it is very difficult to establish this level of trust and thus systems are vulnerable to attack. Our research into election verifiability overcomes these problems and paves the way for the deployment of dependable electronic voting systems.

A major difference between electronic and traditional paper-based elections is the lack of transparency. In the current paper-based UK system it is possible to observe the whole election process from ballot casting to tallying, and we rely upon robustness characteristics of the physical world; such as the impossibility of altering the markings on a paper ballot sealed inside a locked ballot box. By comparison, it is not possible to observe the electronic operations performed on data, accordingly computer systems may alter voting records in a way that cannot be detected by voters or election observers.

The concept of election verifiability has emerged in the academic literature to address this problem. It allows voters and election observers to verify that votes have been recorded, tallied and declared correctly; in a manner independent from the hardware and software running the election. Three aspects of verifiability are considered:

- *Individual verifiability:* a voter can check that her own vote is included in the election outcome.
- *Universal verifiability:* anyone can check that the election outcome corresponds to the votes cast.
- *Eligibility verifiability:* anyone can check that each vote in the election outcome was cast by a uniquely registered voter.

This research delivers a framework to evaluate the verifiability of electronic voting protocols.

The work has been successfully trialled with respect to two electronic voting protocols which have been implemented and deployed. In particular, the Helios 2.0 protocol was evaluated. This protocol was used in March 2009 to elect the president of the Catholic University of Louvain, Belgium, in an election that had 25,000 eligible voters. This demonstrates the suitability of the framework for analysing real world election systems. Finally, this research forms a foundation for the development of an electronic voting system which provides an assurance of integral elections, ultimately restoring confidence in the UK electoral system.

This brief is based on: Kremer, S., Ryan, M., & Smyth, B. (2010) *Election verifiability in electronic voting protocols*. Technical Report CSR-10-06, University of Birmingham, UK. Available from `http://www.bensmyth.com/publications/10tech/`

For further work on electronic voting please refer to: `http://www.cs.bham.ac.uk/go/security`