Electronic voting: An analysis of the safety critical issues

The subject of electronic vote tabulation involves a unique combination of technological, computational, engineering and sociological problems that produce a set of constraints upon the systems used for ballot entry and vote counting. Using a computer introduces universal vulnerabilities to privacy, accuracy, and security in elections. Ireland and other European countries have begun initiatives to convert all or part of their voting to electronic balloting systems. Europe appears to be rushing ahead to deploy computer voting technologies with serious sociological and technological downsides, such as lack of auditability, and increased opportunities for vote selling, monitoring, coercion, and denial of service attacks.

Previous work has identified the various types of voting systems already in operation; the constraints under which they are required to operate; and the numerous checks and balances that need to be provided for accuracy and integrity. We propose extending this work to examine new types of voting systems based on projected evolution of current communication technologies; and to construct a formal, mathematical model of the e-voting *problem*.

The main hypothesis is that electronic voting merits a mathematical treatment - through the construction of formal models, using state-of-the-art techniques in computer science and software engineering. The main aim of the proposed research is to demonstrate that no e-voting system can be considered 'safe' until the requirements of these systems are better defined; and to develop a method for supporting the implementation and deployment of safe e-voting systems, based on formal requirements models.

The research strategy is to: 1) examine a number of already deployed e-voting systems and to perform risk analysis on them failing to meet their requirements, 2) demonstrate that using formal methods for engineering the software in such systems can reduce certain risks, 3) develop a generic, extensible set of formal methods, techniques and tools that can be used in the implementation of new e-voting systems, based on evolving communication technologies, and 4) validate the theoretical models through development of a novel remote electronic voting system that is proven to be correct with repsect to a set of well-defined safety requirements.

The project will follow the standard approach to applying formal methods to software engineering problems: there will be an iterative cycle where theoretical models are evolved through validation against real, concrete implementations. It is likely that the project will adopt object oriented modeling techniques, in order to support compositional analysis of our models at all levels of abstraction.

The project will be supported by the TASS research group at NUI Maynooth. This group has exisiting collaborations with DCU (Ireland), Nancy (France) and Clemson (USA) in the area of applied formal methods and safety critical systems. The TASS research group also has a history of industrial collaboration with telecommunication companies (such as BT and France Telecom).

Travel to France and USA (to further the collaborations) would benefit the research in the early stages of the project.