E-Voting: Risky technology or great improvement?

November 28 2014

On this forthcoming weekend the Australian state election takes place, and in Victoria State they will be using a new e-voting system to improve secrecy, reliability and user-friendliness. But how secure are such systems? And do people trust such systems? These are key questions for Prof. Peter Y A Ryan, e-voting expert at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) from the University of Luxembourg. The technology that will be applied at this weekends state election is based on Ryan's original voting concept called "Pret-a-Voter" that he developed in 2004.

"The new voting system includes mainly two advantages compared to classical ballot systems," says Ryan: "It guarantees ballot privacy and offers an encrypted receipt at the same time, so the voter can verify that his vote was correctly counted. Furthermore it reduces the probability of unwanted invalid votes by using a touchscreen that gives extensive support, for example to handicapped people or people with language issues." Building on Peter Y A Ryan's fundamental contribution, the system is the result of a collaboration between experts from Luxembourg, the University of Surrey (UK), the University of Melbourne (Australia) and the Victorian Electoral Commission.

In recent years, computer scientists, mathematicians, sociologists and psychologists are developing new voting systems that should offer more comfort, less costs, increased turnout of voters plus increased security and trust. Beside the positive aspects of using digital technology to support elections, like the one used in Australia, every technology brings

with it risks of manipulation. "Of course, IT experts are able to make e-voting systems very secure, but they will never be able to reduce the risks to zero. Every electronic system can be hacked, but with smart encrypting, the risk of a manipulation or the loss of secrecy of votes can be minimized", says Ryan, who is specialized on such encrypting mechanisms: "Also pen and paper based elections can be manipulated - so the pros and cons need to wisely be deliberated and systems need to be developed further."

The history of e-voting started in 18th Century with lever machines in the US and moving on through punch cards, optical scan and touch screen machines. Similar technological experiments have been conducted in Europe and beyond. Some countries have experimented and even introduced internet voting, notable Estonia. All of these have been shown to be vulnerable to attack, often large-scale and virtually undetectable.

The crypto/security community have made significant strides in the last decade or so in designing schemes with remarkable security properties. In the past few years we are starting to see implementations of these designs trialled for real elections, notably the upcoming elections in Victoria State. "Arguably such systems provide much stronger assurances of integrity and secrecy of the votes than conventional, pen and paper hand counting," adds Ryan: "The challenge remains however to convince the various stakeholders, politicians, election officials, voters, of their trustworthiness. The arguments are subtle and involve some understanding of the properties of cryptographic primitives, so the challenge remains to convey sufficient understanding and instill confidence."