Trust and Transparency Challenges of E-Voting

Workshop 'Internet Voting: What can Canada learn?
Carleton University, Ottawa, January 26, 2010
Peter Wolf, Technical Manager, International IDEA

The Requirement of Trust

The main challenge concerning transparency for internet voting systems as well as all other e-voting systems without paper trail is that there is no external evidence of the system's correct operation.

This makes a meaningful observation of the voting process very difficult if not impossible.

As a result most systems depend to a large extent on the public trust in them.

Ideally this trust is based on a transparent voting system and process.

The Transparency Challenge

Who needs to be trusted?

First of all voting system vendors, the election administration and their specialists who build, run and maintain the voting systems.

Second, for external control of the voting systems, many countries use some sort of independent auditing or certification process. Specialists of the auditing or certification agencies are granted deep insight into the voting system, and the agencies will issue a certification or confirmation of the system's reliability.

For remote Internet voting there is an additional component outside the control of vendors, election administration and certifying bodies: The client computer. Nobody can know if this computer can be trusted or if it is unreliable because of bad maintenance, viruses, malware, etc.

The public including stakeholders like citizens, parties, observers, NGOs and activists ideally trusts this system and all its actors.

But there will always be some stakeholders that will question the system and want to gain deeper insight. They can be divided into two types:

- Unbiased stakeholders: observers, parties, citizens. Often used to some sort of physical observation of paper based elections. They would like to get similar insight into the electronic process to be convinced.

- Fundamental opponents: often with strong IT security or data protection background. They know how easy it is to manipulate IT systems, are not prepared to trust systems without external evidence. Convincing them is difficult or impossible. They can be very vocal, in extreme cases like the Netherlands even stop electronic voting. Sometimes there is also a fear that they could be source of hacking attacks and use them as means to discredit e-voting systems

What happens when such stakeholders try to get deeper insight into the voting system, ask the election administration for more details?

To some extent information will be made available to them. But at a certain level of detail, often when it comes to accessing the systems' source code, there will be restrictions and access will be denied.

But they can still resort to the certification process. Also here they will be granted some access, like certificates, summary reports. But when they want to access all details of the certification process, like exact requirements, auditing procedures, findings those details will typically not be available to them.

'Top Secret' as in the presentation is of course an exaggeration. 'Trade secret', 'Protection of copyright and intellectual property' is commonly the underlying reason of the secrecy.

Overall the interested public is facing a big black box with some, suspicious looking secrets in it. Sometimes it is then hard to see that this is not some sort of conspiracy, but simply common practice in other parts of the industry:

- For commercial vendors of proprietary software, source codes of usually kept secret to protect the vendors' trade secret. (open source is obviously an alternative here)
- In industrial certification the exact processes are often kept secret to protect the certifying agencies' trade secret of their exact methodology.

For the 'unbiased observers' this black box is frustrating. For fundamental opponents it can even make things easier: Instead of focusing on details they can simply point to the black box as an evident explanation for their skepticism.

Opening the Black Box/Recent European Developments

Two ongoing European projects attempting to 'open the black box' will be interesting to follow:

Regarding source codes many EMBs accept that they have to rely on commercial voting software and services. Many also accept that this naturally means that public access to the voting systems will be limited. But this is not always true.

For the Norwegian internet voting project (first pilot planned for 2011) the EMB is very ambitious about the level of transparency it aims to achieve. “We do not require anybody to trust us, the system will be so transparent that no trust in an institution or company will be required”. It will be interesting to see how the entire project develops.

For now there is one first success: the tender for the internet voting system explicitly requested publication of all source codes. Most major commercial vendors were bidding for the tender. Reportedly they were not happy with the publication requirement, but in the end they were ready to fulfil it.

Maybe an indication of where the vendors are going: a recognition that opening up will be more and more required. In a similar development in the US, Sequoia promised to publish their source codes at the end of 2009.

Still, there are many aspects of an e-voting system that cannot be assessed by source code inspection. These include: is the public code actually the one used in the real voting system, hardware components, the procedures required for securely operating the voting system and also the system’s resilience against insider attacks.

Here meaningful audit and certification procedures play an important role.

But for now there are no common standards for certifying and auditing e-voting systems (like what exactly to certify, how requirements should be specified, what the right detail level for requirements is, how public the certification process should be).

This has been recognized by the Council of Europe and in another interesting development.

The Council of Europe has already adopted a set of standards for e-voting in 2004. As a follow up, discussions about certifying e-voting systems have been initiated last year. Ultimately these discussions should lead to the adoption of guidelines or standards for certifying e-voting systems with Europe wide acceptance.