University of Fribourg

Bern University of Applied Sciences

Measures to Establish Trust in Internet Voting

Oliver Spycher

Tallinn, September 26th, 2011

Outline

Outline

Benefits and Obstacles in Internet Voting

Offer Internet Voting and hope to

- increase turnout
- facilitate participation of expats
- accelerate tallying and counting
- save ressources
- be modern

Beware of

- restrictive security requirements
- importance of meeting them
- distrust that they are not met

Trust Aspects

Voting procedures need to be accepted among the electorate

Trust regarding

- correctness of result
- secrecy of the ballot

Trust Aspects

Voting procedures need to be accepted among the electorate

Trust regarding

- correctness of result
- secrecy of the ballot
- individual constraints

Outline

Two Classes of Measures

Related to overall security

- Separation of Duty
- Verifiability
- Vote Updating

Related to the concerns of the individual

- Test Elections
- Independent Voting Clients

The foundation: **Transparency** (convince experts, then public), **Evaluation** by recognized standards (to prove thorough assessment)

Transparency

Sound security features are a precondition to trust

Open documents for experts to assess and evaluate:

- Technical requirements, including security concept
- Technical implementation, source code, cryptographic protocol
- Security Gap between requirements and implementation
- Assessment of simplified documentation for average voters

Assessment of simplified documentation to achieve credibility among public

Outline

Selected Measures in 4 Voting Systems

Governmental

- Estonian (national)
- Norwegian (local and municipal)

Non-Governmental

- Helios (from academic research)
- Polyas (from industry)

Separation of Duty

Separate secrecy-critical information and integrity-critical power among multiple entities

Implications

- No need to trust one single entity (computer, site, vendor)
- Trust only in 1 out of many at being reliable and independent

Systems

- Estonian (one site)
- Norwegian, Polyas (two sites)
- Helios (as many sites as specified by the organizer)

Need to expose payoff and limitations!

Verifiability

Allow voters to verify the correctness of the published result

Implications

- No need to trust any entity (computer, site, vendor)
- Verifiability vs. lacking proofs (research ongoing), complaints

Systems

- Estonian (no verifiability)
- Norwegian (cast-as-intended verifiability)
- Polyas (tallied-as-recorded verifiability)
- Helios (verifiability, but only under a strong assumption)

Need to expose payoff and limitations!

Vote Updating

Allow voters to update by i-vote and / or paper vote

Implications

- Side-step vote selling, confusion, individual doubts
- Trust that cast votes reflect free will
- Sound authentication required, act of voting trivialized
- May contradict legal restrictions and traditions

Systems

- employed in Estonian, Norwegian, Helios
- not employed in Polyas

Conclusions

- High security is necessary but not sufficient
- Technology is hard to explain, yet the measures can be explained by analogies
- Involve independent experts at evaluating the correctness and limitations of the explanations
- Each of the 7 measures is employed to some degree by at least one system (also the undiscussed ones)

Conclusions

- High security is necessary but not sufficient
- Technology is hard to explain, yet the measures can be explained by analogies
- Involve independent experts at evaluating the correctness and limitations of the explanations
- Each of the 7 measures is employed to some degree by at least one system (also the undiscussed ones)

The perfectly secure Internet voting system has not yet been invented. Governments need to select the measures according to the concerns in their specific population.

Thank You!

Questions / Remarks

e-voting.bfh.ch and **www.secuso.cased.de**

contacts, papers, reports