University of Fribourg

Bern University of Applied Sciences

Swiss Federal Chancellery

Measures to Establish Trust in Internet Voting

Oliver Spycher

Bratislava, September 27th, 2011

Outline

Requirements and Threats

Introduction to the Measures

Selected Measures in Practice

Outline

Requirements and Threats

Introduction to the Measures

Selected Measures in Practice

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

Some Desirable Properties

- **Correctness**: The published result reflects the electorates' intensions correctly
  - → one-voter-one-vote, only eligible voters
  - → no stuffing, deletion, altering
  - → reliable tallying
  - → no pressure
- **Secrecy of the ballot**
- **Fairness**: No premature results obtainable
- **Receipt-freeness / coercion-resistance**: no advantage for proving how one voted

Some Problems Specific to Internet Voting

- **Scalability of attacks**
- **Choice of operator**
- **Sound authentication**
- **Insecure computers, insecure Internet**

Outline

Requirements and Threats

Introduction to the Measures

Selected Measures in Practice

Selection of Measures, there are more..

Related to overall security

- Separation of Duty, Verifiability, Vote Updating

Related to the concerns of the individual

- Test Elections, Independent Voting Clients

Selection of Measures, there are more..

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
- Evaluation by recognized standards

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

Requirements and Threats

Introduction to the Measures

Selected Measures in Practice

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

The perfectly secure Internet voting system has not yet been invented.

Governments need to select the measures according to the concerns specific to their context.

Internet Voting in Switzerland

- **>95% of votes through postal mail**
- **Up to 4 non-election voting sessions per year**
- **Cantons in charge of implementing political rights**
  → 3 systems, currently 13 of 26 cantons, expats strong driving force
- **Currently in pilot phase**
  → by fed. law: expats plus max. 10% / 20% of citizens
- **Political ambitions to increase, but security first**
  → minimal common security criteria currently being established

- http://www.bk.admin.ch/themen/pore/evoting/

Thank You!

Questions / Remarks

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

contacts, papers, reports