Technical requirements for internet-based voting

Mark D. Ryan
University of Birmingham, UK

m.d.ryan@bham.ac.uk

IET Roundtables, 2019

Correctness

- Each vote should be correctly recorded and counted.
- Only eligible votes should be included (i.e., ballot stuffing is impossible).
- The outcome of the election should be correctly computed.

Verifiability

- Any voter can independently check her vote has been correctly recorded and counted.
- Any observer can independently verify that only eligible votes have been included.
- Any observer can independently check the declared outcome.

Vote secrecy, and incoercibility

- Nobody can see how I voted.
- Incoercibility: Nobody can see how I voted even if I cooperate with them.
- "Everlasting privacy": Nobody can see how I voted even if there are advances in cryptanalysis or computing.

Usability

- Intuitive, natural interface, for voting and for verifying
- Vote-and-go (single episode)
- The way the system works, including the way it achieves verifiability and secrecy properties, is understandable and intuitive to the voter.

Software and hardware independence

- The set of components of the system that a voter/observer is required to trust ("TCB") is the empty set.
- Undetected incorrectness in any of the utilised sw or hw should not result in undetectable error in the result

	Estonia	Helios	Achievable
Verifiability			
individual	Chk. on oth. dev.	Indirect	🟩
eligibility	No	No	🟩
universal	No	Yes	🟩
Secrecy			
plain	Attempted	Yes	🟩
incoercibility	Attempted	No	🟧
everlasting	Bal. not publ.	Bal. publ.	🟧
Usability			
intuitive	Yes	OK	🟩
vote & go	Yes	Yes	🟩
understandable	Somewhat	Somewhat	🟥
Sw & hw independence			
verifiability TCB	Empty	Client	🟩
secrecy TCB	Authorities	Client	🟧