PKC + MPC + Internet Voting implies "Secret Endorsements" or How Politicians can keep their Friends

Yvo Desmedt Pyrros Chaidos

University of Texas at Dallas University College London, UK

August 21, 2012

Yvo Desmedt did this research while at University College London. Pyrros Chaidos was supported by an EPSRC scholarship (EP/G037264/1 – Security Science DTC).

Vote Copying, Bug or Feature?

Cortier and Smyth used ballot copying to attack voter privacy: by re-casting a person's vote enough times, the result can be influenced so as to reveal the original vote.

- But isn't influencing the result the point of voting?
- Is there a way to make ballot copying beneficial?

Vote copying as a Feature

What if Alice wants Bob to copy her vote, such that Alice does not know whether Bob actually did or not.

- Last year (rump session, see ESORICS 2012) we announced copying protocol protocols that are unmodified Helios 3.0 specific.
- Provided Public Key Cryptography is used, protections against the copying attack (e.g. using non-malleable encryption) will not work: MPC can be used to construct blinded copies.

Using Ballot Copying (simple)

Offering a ballot for blind copying can be "safer" than a public endrorsement in many cases:

- Endorsing candidates from a different party (Joe Lieberman, Don Young).
- Mayor (former UK prime minister) stated that Murdoch did pressure him. Later prime ministers of the UK stated they were not. So, with so many politicians (likely) lying, we might want to trust the ones we believe do not!

Using Ballot Copying (simple)

- Workplace situations are tougher: candidates may be colleagues or higher-ups.
- Controversial vs “safe” candidates.

Using Ballot Copying (general)

Ballot copying can also change how endorsements are made and used.

- A group of people could use MPC or a modified voting protocol to produce a secretly endorsed ballot rather than issue public endorsements (tally remains secret)!

Using Ballot Copying (general)

Ballot copying can also change how endorsements are made and used.

- A group of people could use MPC or a modified voting protocol to produce a secretly endorsed ballot rather than issue public endorsements (tally remains secret)!
- For multi-seat elections a voter might wish to allocate different fractions of his ballot to different endorsements.

  e.g. 3 seat election: 2 votes copied from the Wall Street Journal (WSJ) secretly endorsed candidate, 1 votes copied from the Sierra Club secretly endorsed candidate.

Using Ballot Copying (general)

Ballot copying can also change how endorsements are made and used.

- A group of people could use MPC or a modified voting protocol to produce a secretly endorsed ballot rather than issue public endorsements (tally remains secret)!
- For multi-seat elections a voter might wish to allocate different fractions of his ballot to different endorsements.

  e.g. 3 seat election: 2 votes copied from the Wall Street Journal (WSJ) secretly endorsed candidate, 1 votes copied from the Sierra Club.
- If there aren't enough seats he might wish to assign a probability of actually using each endorsement.

  e.g. 1 seat election: with 60% probability: the vote copied from WSJ secret endorsement, and with 40% probability the vote copied from the Sierra Club.

Using Ballot Copying (general)(cont.)

- Mix & Match of the previous methods. e.g. 2 seat election: first vote copied from the WSJ endorsement ballot, second vote 20%: copied from WSJ (second candidate), 80%: copied from the Sierra Club.

Caveat: Many groups in the world are implementing MPC. How efficient/inefficient is above today?

Open Problems and Impact

Secret endorsements are a new feature, which was impossible to implement in paper voting systems.

- Internet voting is very different from e-booth voting!
- What functionality do we want from Internet-voting?
- What other unintented features have we missed?
- Which paper-voting concepts break on the internet?

Open Problems and Impact (cont.)

- Human aspects of security are being considered, but what about the impact of MPC on our society?
- What else from our paper society cannot be faithfully copied?

Acknowledgements and credit

- Josh Benaloh and Niels Ferguson for their discussions.
- Bulens et al. for simultaneously considering vote copying as a form of delegation.