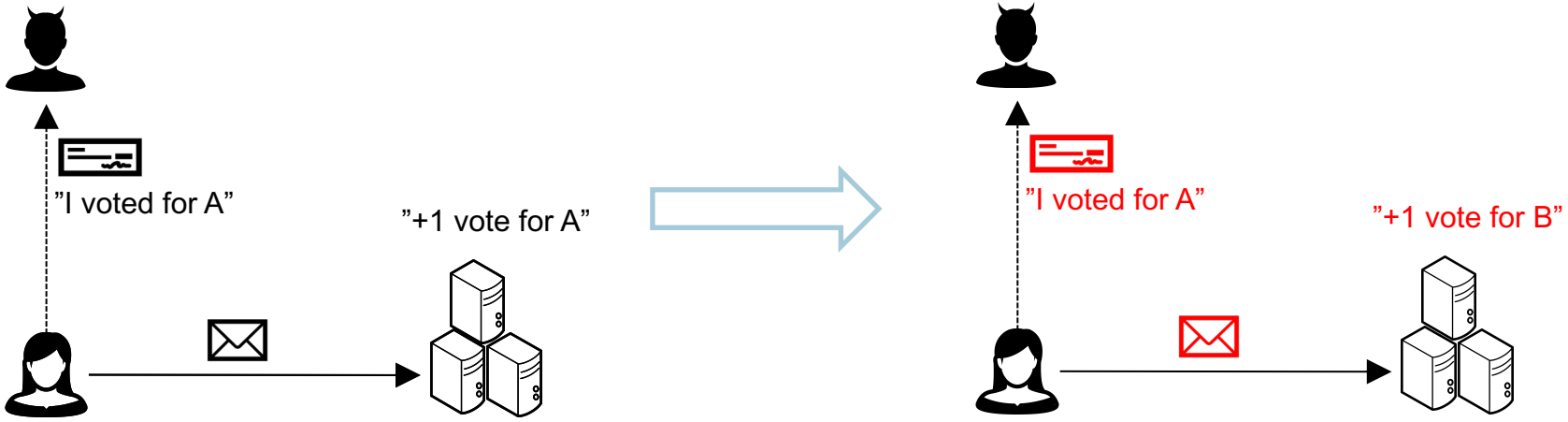
Human Factors in Coercion-Resistant Internet Voting

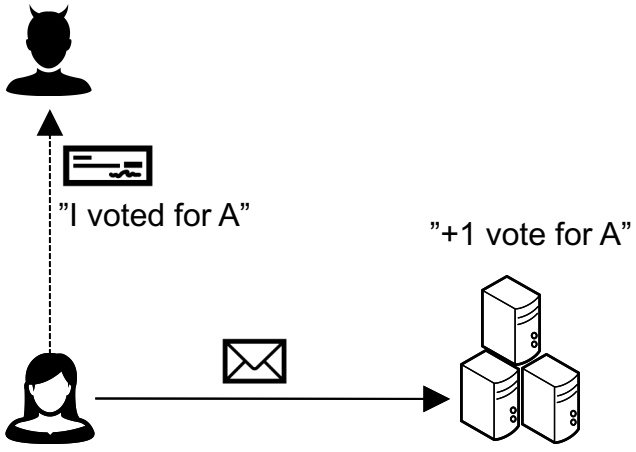
Oksana Kulyk



Coercion in Internet Voting

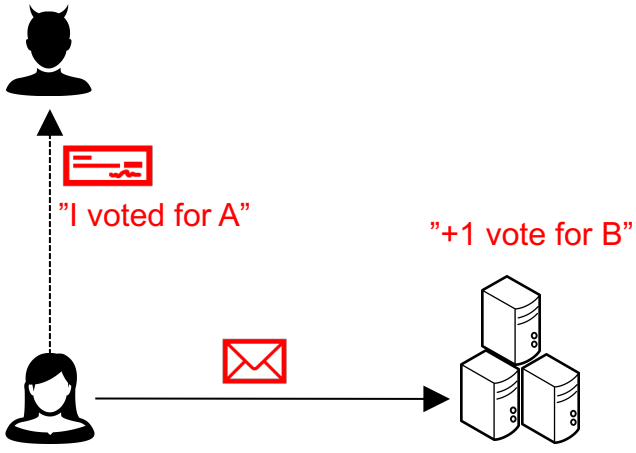
- Internet voting is an unsupervised channel
  - Hard to restrict voter actions (e.g. recording the voting procedure)
  - Hard to monitor the voting environment (e.g. over-the-shoulder adversary)

→ Voter coercion and/or vote buying a real possibility



Coercion in Internet Voting

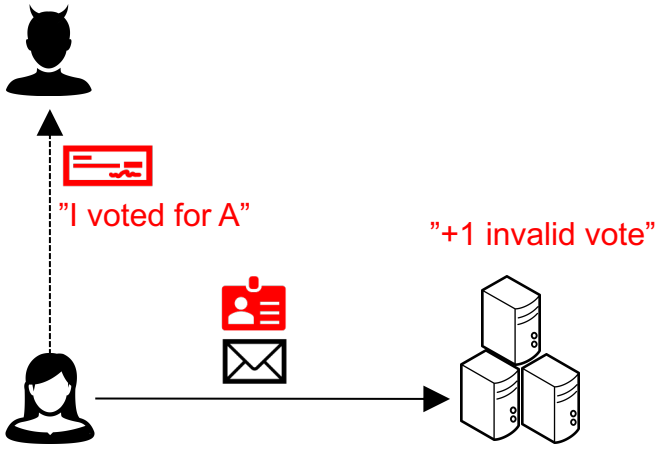
- Solution: schemes with different levels of coercion-resistance incl. receipt-freeness
- Counter-strategy
  - A procedure different from normal vote casting
  - The voter either obeys the coercer or applies a counter-strategy
  - Goal: adversary should not be able to tell whether the voter obeyed or not



Types of Counter-Strategies

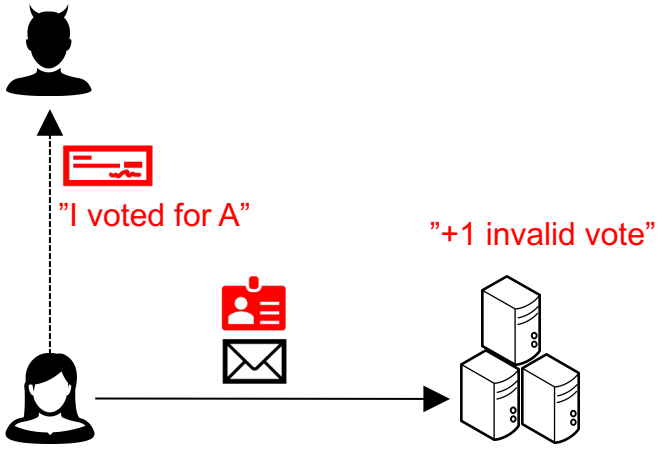
Fake Credentials

- While coerced, the voter authenticates themselves with fake credential
- The votes cast with the fake credential are not tallied
- When left alone, the voter can cast another vote using their real credential
- Adversary cannot distinguish between fake and real credentials



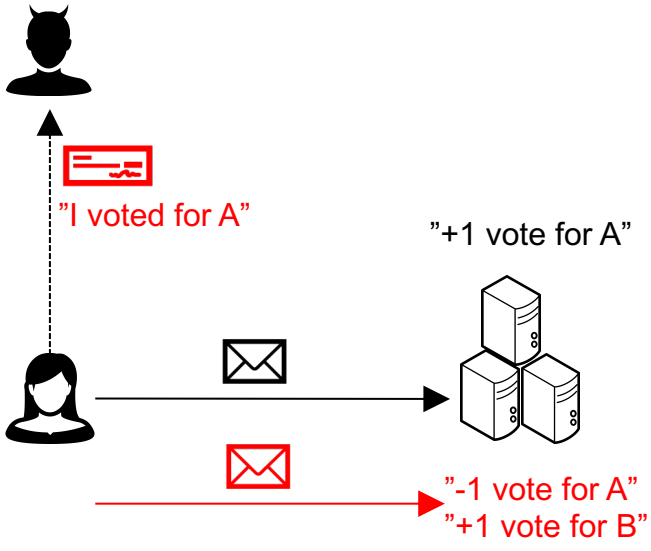
Fake Credentials

- Different level of credential complexity
  - Cryptographic secret keys (256-bit long) [JCJ05]
  - Passwords/passphrases [CH11]
  - 4-character PINs [PS17, NV12]
- Issues
  - Voters must be able to enter the credentials without mistakes
  - Possible mitigations: panic passwords, entering the credential twice → further complication of the procedure
  - Voters must understand how to fake a credential
  - No adversarial observation during credential distribution



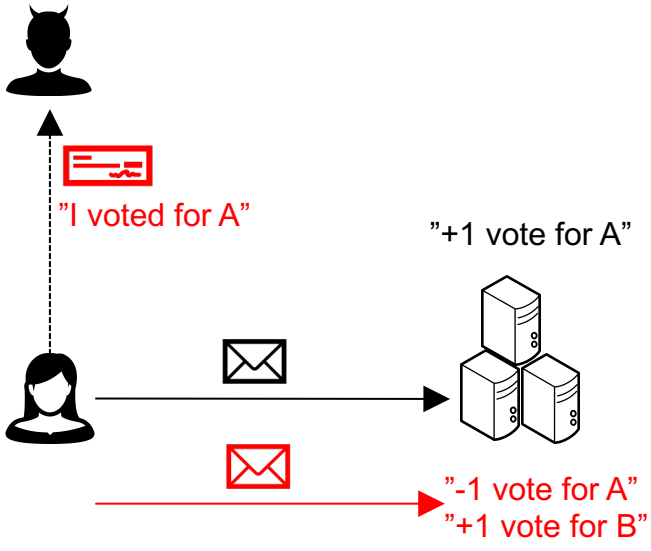
Deniable Vote Updating

- The voter votes as instructed by the adversary
- When left alone, the voter casts another vote overwriting the previous one
- The adversary cannot tell whether a vote has been overwritten



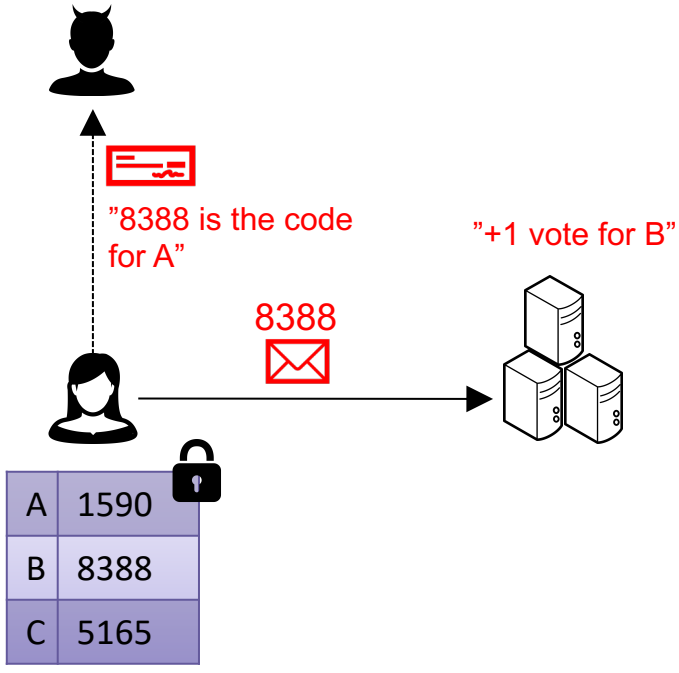
Deniable Vote Updating

- Types of vote updating
  - After coercion: ”Simple” vote updating [LHK11]
  - Either before or after coercion: ”Preliminary” vote updating [KTV15, BKV17]
- Issues
  - Simple vote updating: last-minute coercion works
  - Preliminary vote updating: the voter has to keep track of all the votes they cast or plan to cast in the election
  - Additional voter involvement needed to undo the coercion



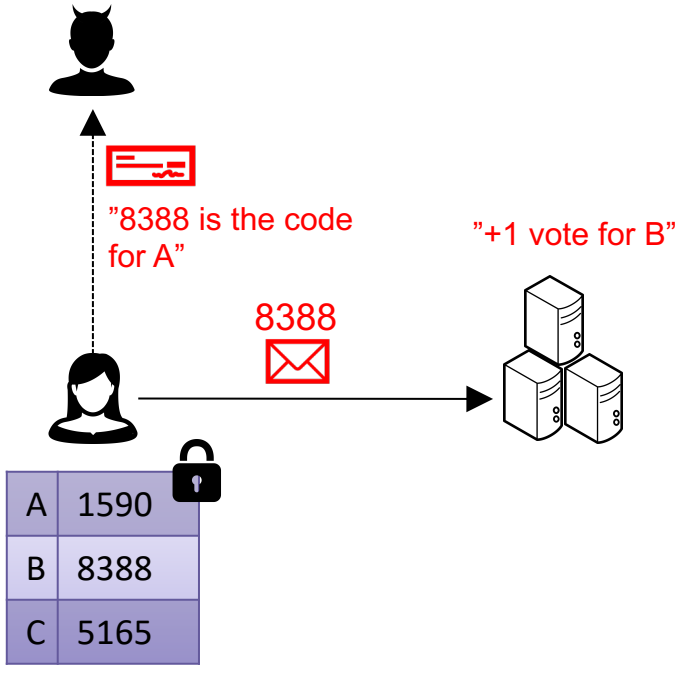
Code Voting

- The voter has a secret unique code assigned to each candidate
- The voter casts a code as their choice
- The adversary does not detect which voting option has been chosen



Code Voting

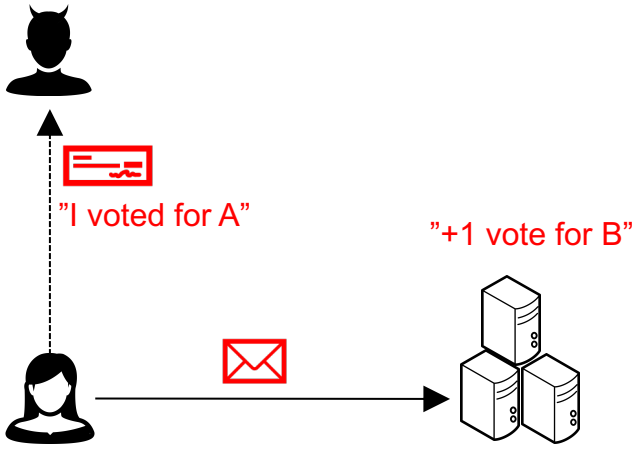
- Types of codes
  - Mobile app with codes [BGS13]
  - Code sheets [RT09]
- Issues
  - No adversarial observation of the app/code sheet
  - Faking code sheets/app output might be needed
  - More codes to fake/remember
  - Voter has to input the code without mistakes



Summary

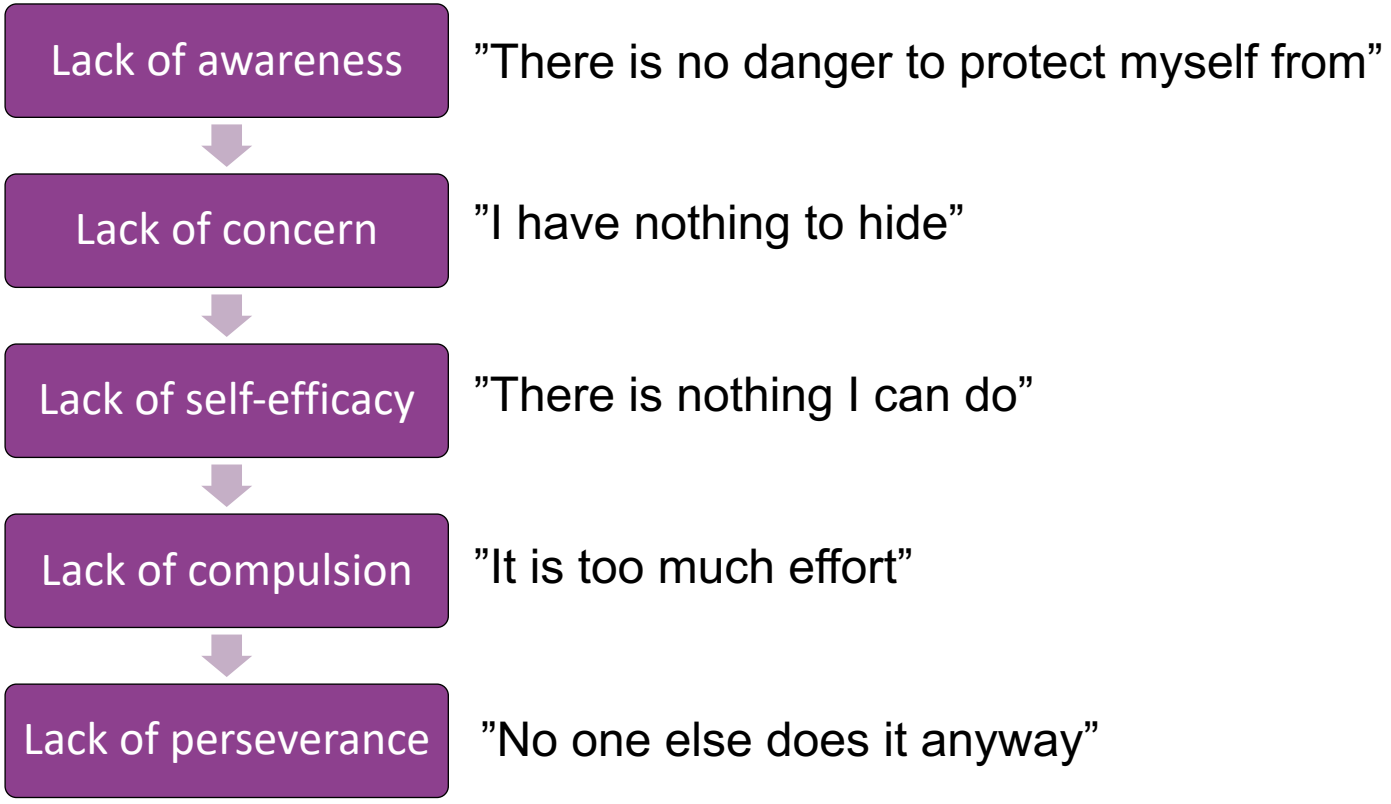
- Capabilities assumed for the voters
  - Being free from coercion/observation at some point
  - Remembering codes/credentials
  - Faking code/credential for the adversary
  - Being able to input codes/credentials correctly
  - Being able to remember and follow the procedure steps
- Are these assumptions realistic?
  - Can the voters apply the counter-strategy, also under stressful conditions?
  - Will they apply the counter-strategy?

→ Insights from related studies might be helpful



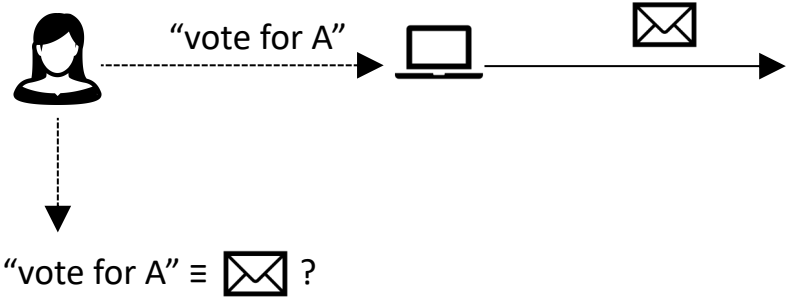
Human Factors Preventing Coercion-Resistance

General Reasons for Insecure Behaviour [VRKE15]

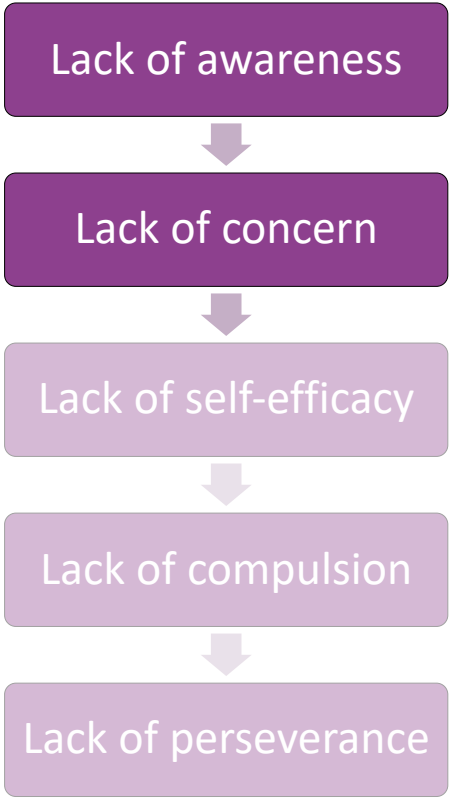


Related Field: Cast-as-Intended Verifiability

- Methods for the voters to verify the correctness of their cast vote
- Issues revealed by existing research
  - Procedure is too complex
  - Voter are not motivated to follow the procedure
  - Voters have misconceptions regarding the procedure
- Mapped into model from [VRKE15] in [KV18]
- Similarity to counter-strategies
  - Voter involvement necessary
  - Complicated procedure
  - No familiarity with the concept

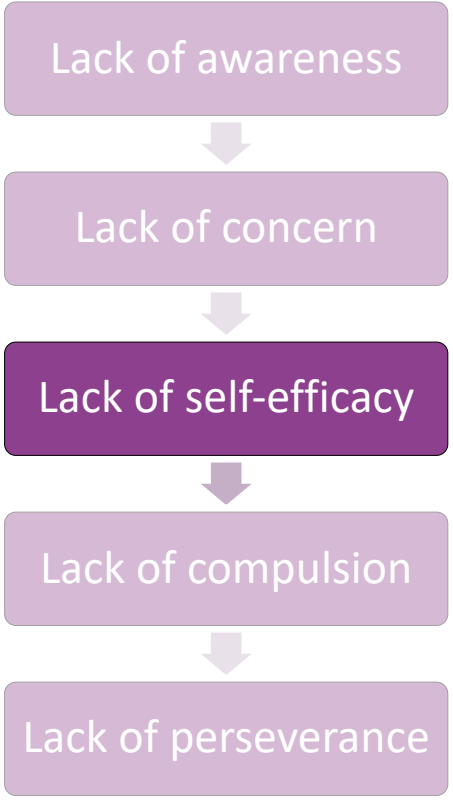


Lack of Awareness & Concern



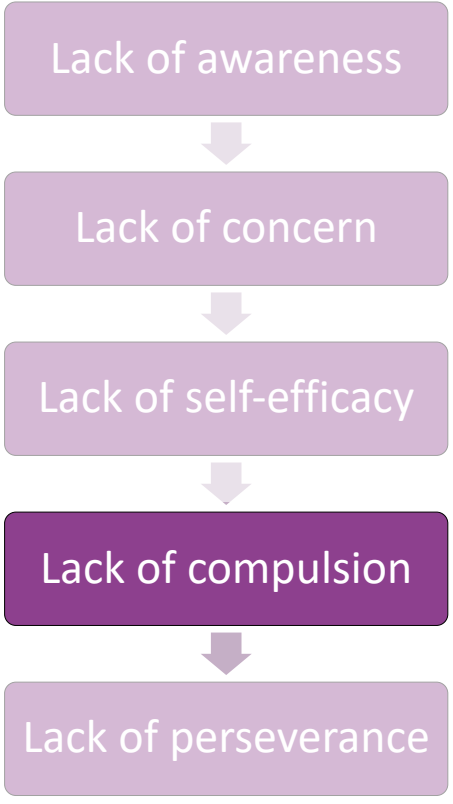
- Verifability
  - Lack of awareness: voters do not know about the risks
  - Lack of concern: hardly applicable
- Coercion resistance
  - Lack of awareness: hardly applicable
  - Lack of concern: hardly applicable

Lack of Self-Efficacy



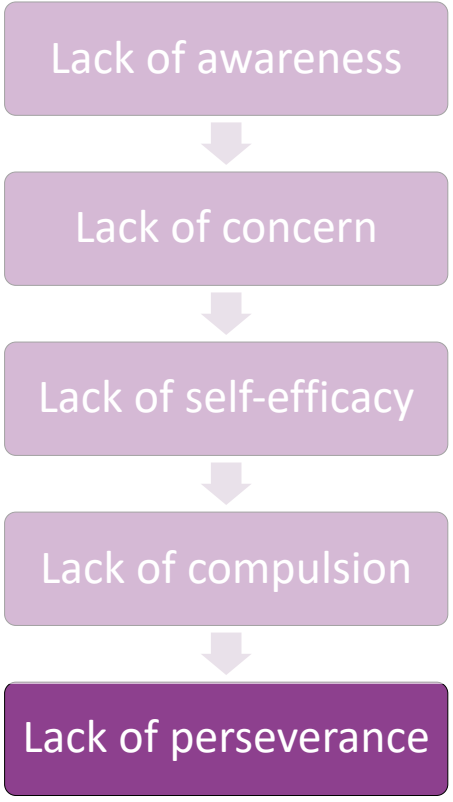
- Verifability
  - Voters don’t know that they can verify
  - Verification procedure is too complicated
  - Voters don’t believe that the verification is actually helpful
- Coercion resistance
  - Voters might not know about the counter-strategies
  - Counter-strategies are complicated
  - Voters might not trust that the counter-strategies help
- Issues specific to coercion resistance
  - Active coercer discouraging from disobeying
  - Risks of applying the counter-strategy incorrectly are higher
  - No system feedback for the voters that could hint the coercer

Lack of Compulsion



- Verifiability
  - Verification requiring too much time
  - Verification process seeming too complicated
- Coercion resistance
  - Counter-strategy requiring too much time and effort
  - Might seem more rational to just obey the coercer/vote buyer

Lack of Perseverance

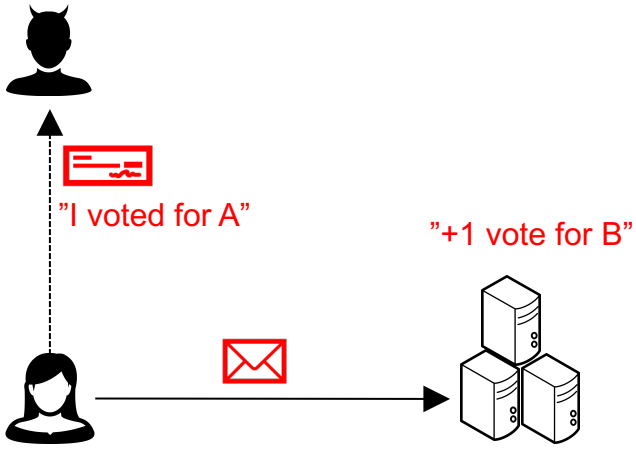


- Verifiability
  - ”Verification is only for experts”
  - ”Only paranoid ones verify”
- Coercion resistance
  - Being actively pressured by the adversary

Open Questions

- Are these issues actually relevant? → empirical studies
- How can these issues be mitigated?
  - Usable implementations of existing schemes
  - Development of new counter-strategies
  - Other measures, e.g. voter education
- Are there other issues?
  - Empirical studies
  - Research into related fields (e.g. privacy protection)
- Which counter-strategy is the most successful?

Thank you!



References (1)

- [BGS13] Backes, M., Gagné, M., & Skoruppa, M. (2013, November). Using mobile device communication to strengthen e-Voting protocols. In Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society (pp. 237-242). ACM.

- [BKV17] Bernhard, D., Kulyk, O., & Volkamer, M. (2017, August). Security proofs for participation privacy, receipt-freeness and ballot privacy for the Helios voting scheme. In Proceedings of the 12th International Conference on Availability, Reliability and Security(p. 1). ACM.

- [CH11] Clark, J., & Hengartner, U. (2011, February). Selections: Internet voting with over-the-shoulder coercion-resistance. In International Conference on Financial Cryptography and Data Security (pp. 47-61). Springer, Berlin, Heidelberg.

- [JCJ05] Juels, A., Catalano, D., & Jakobsson, M. (2005, November). Coercion-resistant electronic elections. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society (pp. 61-70). ACM

References (2)

- [KTV15] Kulyk, O., Teague, V., & Volkamer, M. (2015, September). Extending helios towards private eligibility verifiability. In International Conference on E-Voting and Identity (pp. 57-73). Springer, Cham.

- [KV18] Kulyk, O., & Volkamer, M. (2018). Usability is not Enough: Lessons Learned from'Human Factors in Security'Research for Verifiability. E-Vote-ID 2018, 66.

- [LHK11] Locher, P., Haenni, R., & Koenig, R. E. (2016, February). Coercion-resistant internet voting with everlasting privacy. In International Conference on Financial Cryptography and Data Security (pp. 161-175). Springer, Berlin, Heidelberg.

- [NV12] Neumann, S., & Volkamer, M. (2012, August). Civitas and the real world: problems and solutions from a practical point of view. In 2012 Seventh International Conference on Availability, Reliability and Security (pp. 180-185). IEEE.

- [RT09] Ryan, P. Y., & Teague, V. (2009, April). Pretty good democracy. In International Workshop on Security Protocols (pp. 111-130). Springer, Berlin, Heidelberg.

References (3)

- [PS17] Patachi, Ş., & Schürmann, C. (2017, October). Eos a Universal Verifiable and Coercion Resistant Voting Protocol. In International Joint Conference on Electronic Voting (pp. 210-227). Springer, Cham.

- [VRKE15] Volkamer, M., Renaud, K., Kulyk, O., & Emeröz, S. (2015, September). A socio-technical investigation into smartphone security. In International Workshop on Security and Trust Management (pp. 265-273). Springer, Cham.