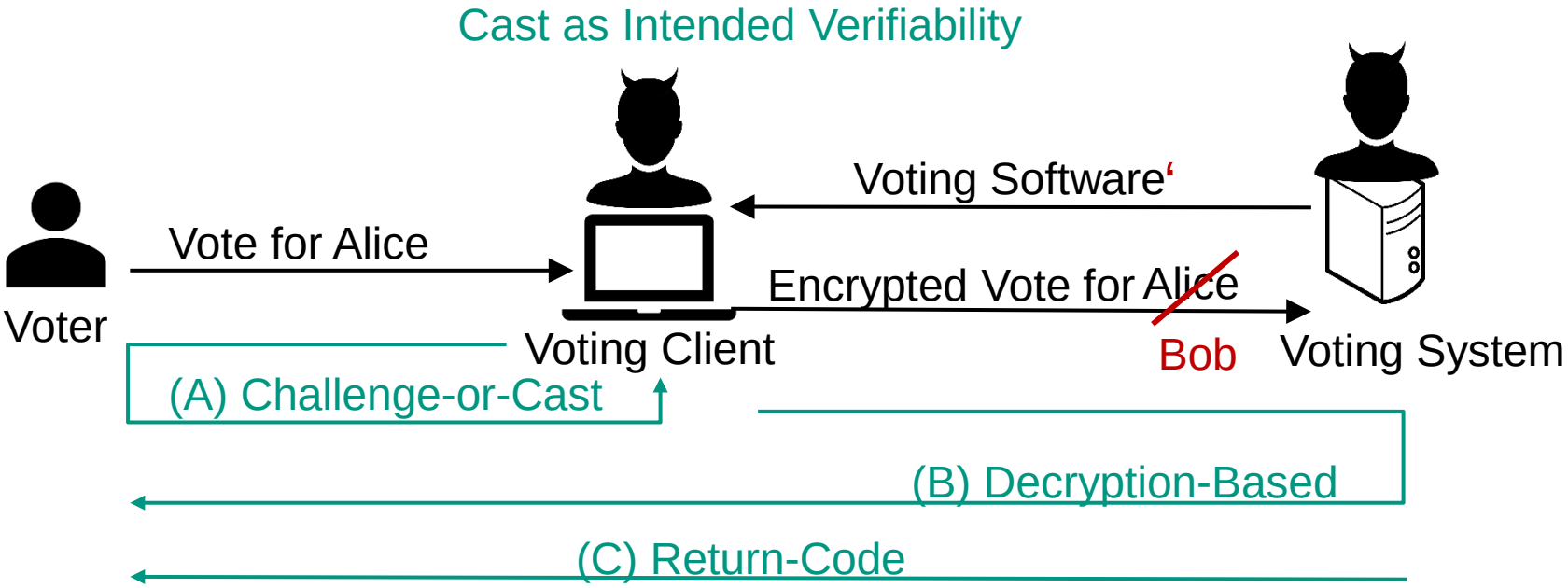
Usability is not Enough!

Lessons Learned from 'Human Factors in Security' Research for Verifiability

Oksana Kulyk, Melanie Volkamer

KOMPETENZZENTRUM FÜR ANGEWANDTE SICHERHEITSTECHNOLOGIE (KASTEL)
FORSCHUNGSGRUPPE SECURITY · USABILITY · SOCIETY (SECUSO)

Motivation



- For privacy reasons: Task cannot be delegated
- Assumptions for ‘manipulations will be detected’ are needed
  - Voters actually attempt to verify
  - Voters can perform the verifiability process
- These two assumptions also hold in presence of an adversary who aims to prevent voters from verifying (= stronger adversary)

Available Research Results

Regarding “Voters actually attempt to verify”

- Mental models on verifiability → Misconceptions
  - Not necessary due to trust in the selected system
  - Should be done by election observers / don’t want to be involved
  - Being scared that the vote privacy can be violated
  - Safeguard against own mistakes

Regarding “Voters can perform the verifiability process”

- Usability ….
  - … in user studies
  - … in terms of people’s ability to verify in case they are asked to do so
  - … in terms of people being able to detect simulated attacks

Research Questions

Assumptions for ‘manipulations will be detected’ are needed

- Voters actually attempt to verify
- Voters can perform the verifiability process

These two assumptions also hold in presence of an adversary who aims to prevent voters from verifying (= stronger adversary)

- What else may influence voters’ likelihood to actually verify?
- What can such a stronger adversary do to prevent the voter from verifying?

Influencing Factors – Methodology

- Human factors in security/privacy research
  - Similar challenges: What keeps people from applying security /privacy measures?
  - Several influencing factors were identified through qualitative studies in various application areas

- Our approach: Identify those that might be applicable for our context

Influencing Factors – Results

- Lack of risk awareness (known from available e-voting specific results)
- Lack of concern
  - “not being important enough”, “nothing bad can happen”
  - Voters device is not manipulated
  - “My individual vote does not has a big influence / does not matter much”
- Lack of self-efficacy
  - “too complicated”, “not effective against big players”
  - Voters might consider verifying as too complicated
  - Voters might consider it as being in-effective in case e.g. eligibility verifiability is not addressed in the voting system / due to strong trust assumptions
- Lack of compulsion
  - “takes too much time”, “is too expensive”
  - Not applicable as elections don’t happen that often (?)
  - Applicable due to their mental model of logging in, select, cast, done

Stronger Adversary – Methodology

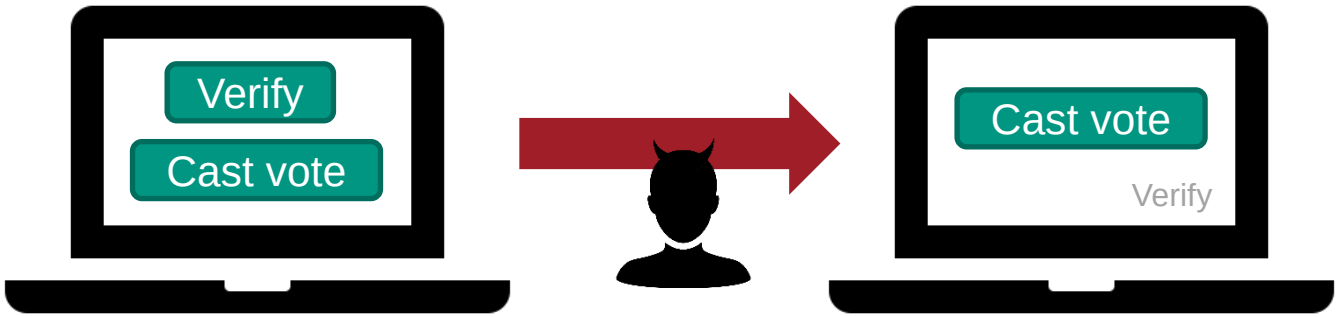
- The assumptions also hold in presence of an adversary who aims to prevent voters from verifying (= stronger adversary

- Human factors in security/privacy research
  - Social engineering attacks
  - ‚Manipulate' users intention to behave securely

- Our approach: Identify approaches social engineers use and which could be applied for our context

Stronger Adversary – Results

- Communicating that verifying is not necessary using trustworthy looking channels
  - Depending on the approach
    - Communicating that verifying puts vote privacy at risk
    - Offering to verify for them / offering the verifying software
- Modifying the design of the UI (while still looking professional)
  - To make it difficult to find the option to verify at all
  - To make it difficult to verify



Stronger Adversary – Results

- Communicating that verifying is not necessary using trustworthy looking channels
  - Depending on the approach
    - Communicating that verifying puts vote privacy at risk
    - Offering to verify for them / offering the verifying software
- Modifying the design of the UI (while still looking professional)
  - To make it difficult to find the option to verify at all
  - To make it difficult to verify
  - Explain that verifiability is currently not available / not necessary / already performed /…

Conclusion: Usability is not enough

- But also ensure …
  - … voters are motivated and not afraid to verify
  - … voters understand what to do to verify in order to detect relevant UI modifications
  - … voters are aware of potential fake messages

- How??
  - Better understand voters attitude towards verifiability
  - Better understand for a concrete system and setting what a ‘stronger’ adversary could do
  - Develop corresponding awareness campaigns to address identified misconceptions and raise awareness for potential attack vectors

- For the references see: TUT Press or https://eprint.iacr.org/2018/683