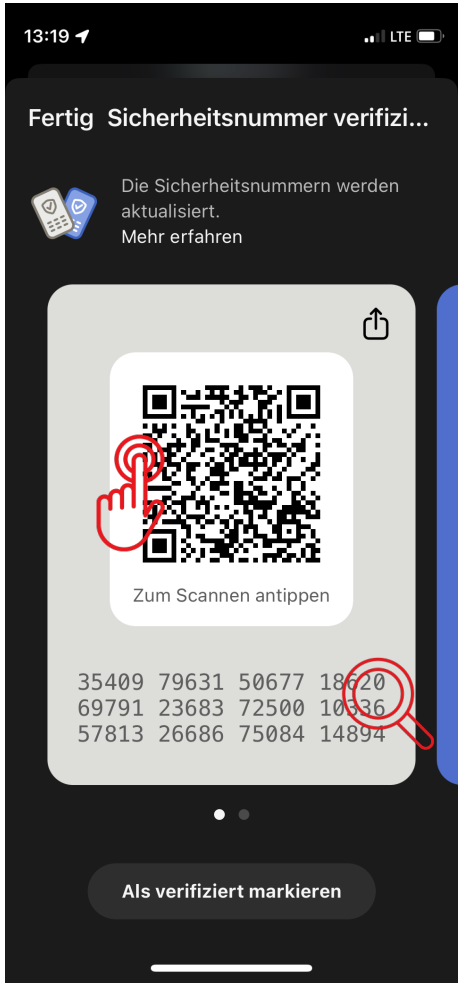
Can Johnny be a whistleblower? A qualitative user study of a social authentication Signal extension in an adversarial scenario

Maximilian Häring[1], Julia Angelika Grohs[1], Eva Tiefenau[2], Matthew Smith[1,2], Christian Tiefenau[1]

[1]: University of Bonn, [2]: Fraunhofer FKIE

CURRENT AUTHENTICATION CEREMONIES

Current Authentication Ceremonies



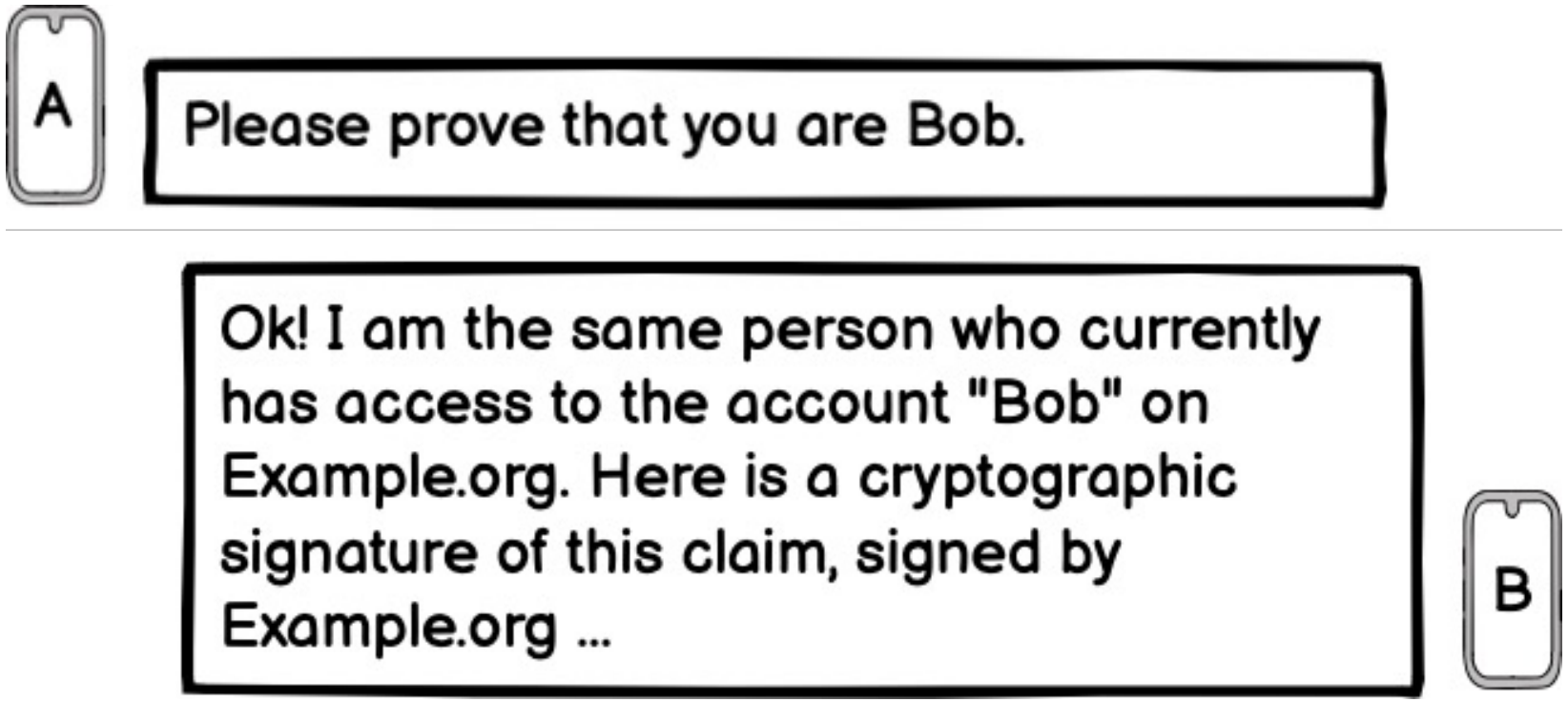
AC = verifying the public key

Behavioural Security Group

UNIVERSITÄT BONN

NEW: SOCIAL AUTHENTICATION

New Authentication Ceremony: Social Authentication



HOW SECURE IS SOCIAL AUTHENTICATION?

Study Design

- Lab study ~1h
- Whistleblower scenario
  - Participant should share files about corruption in the government
- 3 journalists – 3 possible ACs
- No-win scenario: PITM attack
- Compensation: additional money for correct decisions

Journalists

Michael Kobel

Investigativjournalist

Maurerweg 28, 10235 Berlin
Phone: +49 160 92135099
Mail: michael_kobel@newsbody.de

QR-Code
Signal Sicherheitsnummer

QR

Amira Patel

Investigativjournalist

Hallentorstraße 4, 20654 Hamburg
Phone: +49 160 92107646
Mail: amira_patel@newsorg.de

Signal Sicherheitsnummer:
72500 10336 57813 26686
75084 04894

Text

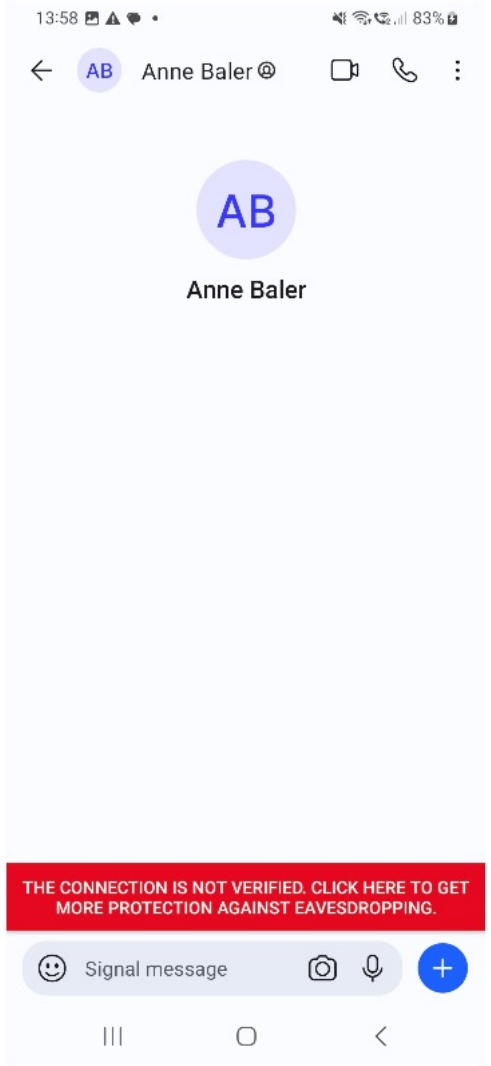
Anne Baler

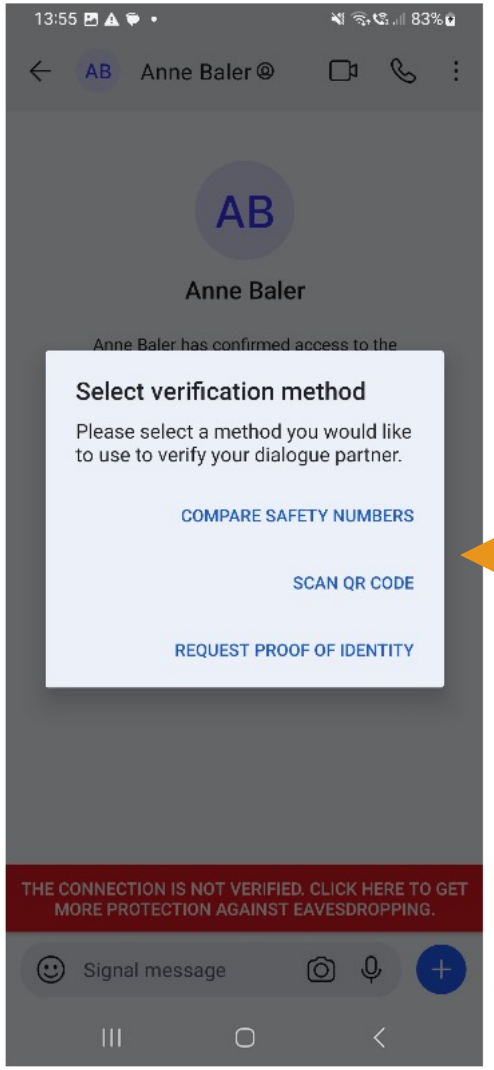
Investigativjournalist

Isarwege 15, 80542 München
Phone: +49 160 92158365
Mail: anne_baler@newsunion.de
Twitter: @AnneBaler
Facebook: Anne_Baler
Instagram: @AnneBaler
LinkedIN: anne-baler-98746524b

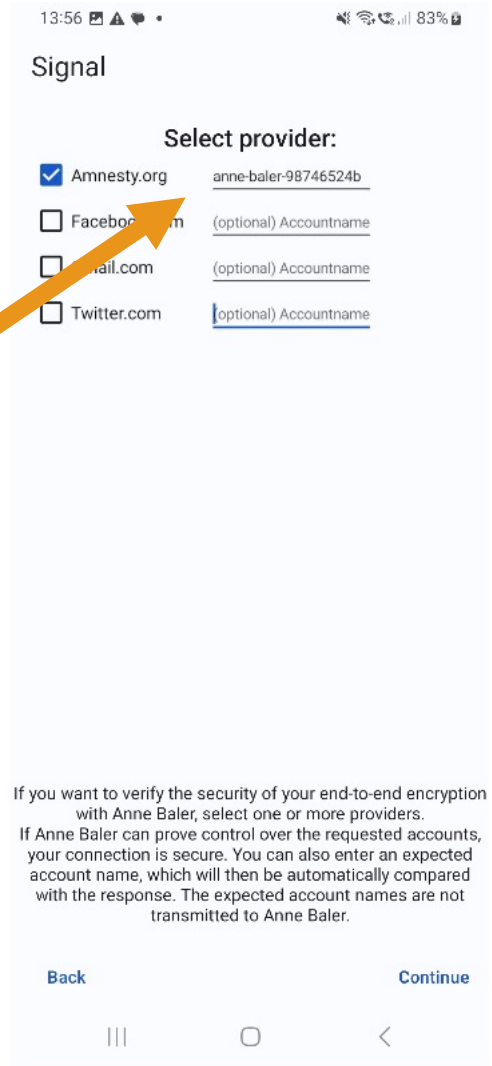
Social Authencation

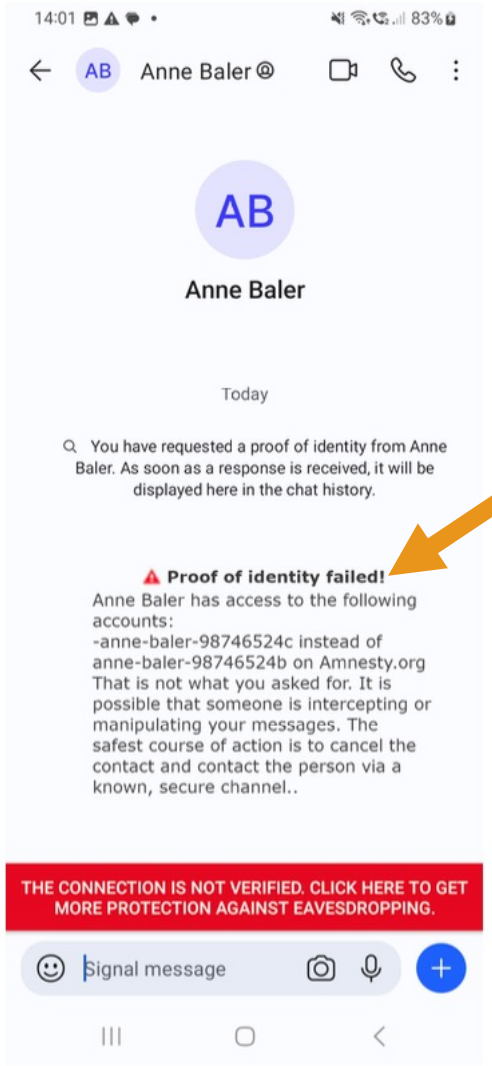
Leading the User to the AC





UI - Social Authentication





RESULTS - HOW SECURE IS SOCIAL AUTHENTICATION?

Results

- 18 participants
- 7 failed the scenario (send the data)
- Themes
  - In-band comparison (4x)
  - Gambling for more compensation (1x)
  - Stress during the study (1x)
  - **Fast-clicking (1x)**

What now?

- Scenario allowed participants to reason and decide
- Social authentication caused less failures then current ACs
- More research is needed on the perception of SA

Behavioural Security Group

Fraunhofer FKIE

UNIVERSITÄT BONN

Any Questions/Comments?

haering@cs.uni-bonn.de