Challenges of Usable Privacy and Security

2022-05-31

KARLSTAD UNIVERSITY
SWEDEN

Simone Fischer-Hübner

(Recent joint work with Ala Sarah Alaqra, Matthias Beckerle, Jan Eloff, Erik Framner, Bridget Kane, Farzaneh Karegar, Eunice Hammond, Lejla Islami, Thomas Lörunser, Patrick Murmann, John Sören Pettersson, Delphine Reinhardt)
Challenges of Usable PETs:
1. Privacy/Security is usually only a secondary task

Challenges of raising the users’ attention for privacy decisions / consent

Example:
Different types of **affirmative (inter-)actions** may affect user attention **to certain parts of policy information**

Challenges of Usable PETs:
2. Cultural Dimensions of Privacy Preferences / Personas

Hofstede Insight – Country Comparison

Challenges of Usable PETs

3. Perceptions of PETs - Finding suitable metaphors & explanations

Challenge: PETs based on “crypto magic”

- hard to comprehend or trust the privacy functionality
- hard to find real-world analogies as metaphors
- Technical background knowledge may have a negative impact on mental models
Example: Platform for Privacy-Preserving Data Analytics

Evaluation results:

• Homomorphic Encryption:
  Skepticism / Distrust in claims on data analysis of encrypted data

• Homomorphic Encryption & Differential Privacy:
  Mental models may be impacted by knowledge about other security tools

• DP- Misconception triggered by digital-world analogies
  • Examples
    • Knowledge of encryption - > DP is reversible
    • Knowledge of VPNs -> DP = selective disclosure
    • Knowledge of firewalls -> DP = access control


CONCLUSIONS – ADDRESSING CHALLENGES

• Raising user attention to (secondary) privacy policy tasks depends on the information presentation & **modes of interactions**

• **Cultural dimensions** need special considerations for User-Centred Design

• Both real-world & **digital-world analogies** for PETs need to be considered
Thanks!