Usability evaluation methods

Verena Schochlow, Stephan Neumann

Theoretical background

Usability criteria after DIN EN ISO 9241:

- Efficacy
- Efficiency
- Satisfaction

„Why Johnny can't encrypt" (Whitten & Tygar, 1999)→ Usability criteria for security

Security Software is usable if the people who are expected to use it:

1. are reliably made aware of the security tasks they need to perform;
2. are able to figure out how to successfully perform those tasks;
3. don't make dangerous errors; and
4. are sufficiently comfortable with the interface to continue using it.

Methods for usability evaluation

Expert methods:

- Heuristic evaluation
- Usability Checklists
- Cognitive Walkthrough
- …

User studies:

- Laboratory studies
- Questionnaires (e.g. System Usability Scale)
- …

GMX/Mailvelope E2E-Encryption

Cognitive Walkthrough (CW) → Focus on learnability of relevant tasks

Preparation:

- Identification and selection of relevant user tasks
  - Setup
  - Encryption
  - Decryption
- Identification of correct actions to achieve task objective

GMX/Mailvelope E2E-Encryption

Realization:

- Experts (ideally inter-disciplinary) take the perspective of a novice user
- They mentally walk through the identified actions
- Question: „Would a novice user complete the action in the expected way?“ → Why? Why not?

Analysis:

- Successful/ not successful actions
- Identified issues
- Possible Changes/ Recommendations

Application to GMX/Mailvelope E2E-Encryption

- Setup of encrypted communication
  - Information partially provided too late, e.g. use from secure machines after completed setup
  - Lack of definition of terminology, e.g. PGP-encryption, key password
  - Lack of information regarding Mailvelope developers
  - Difference between e2e, De-Mail and “email made in Germany“ not made clear
- Sending encrypted mails

  - Misleading visualization
  - Mislead supported by terms like „confidential“ or “safe” mail

Application to GMX/Mailvelope E2E-Encryption

Decryption of encrypted mail

- Similar procedure to non-encrypted mails
- Clear text visible after entering key password

Main issues:

→Current interface is not sufficiently tailored towards user's mental models

→Misleading terms and small visualization might lead to sending unencrypted mails by accident