Seminar session 3: The Human Factor – Usable Security Case Study

What is Usable Security?

- A field concerned with making the security features of systems easy to undersandd and use. (Nurse et al.)
- ... focuses on the design, evaluation, and implantation of interactive secure systems. (Kainda et al.)
- The study of interaction between humans and computers, or human-computers interaction, specifically as it pertains to information security. (Wikipedia)

Usability:

- Learnability: How easy is it for users to accomplish basic tasks the first time they encounter the design?
- Efficiency: Once users have learned the design, how quickly can they perform tasks?
- Memorablity: When users return to the design after a period of time not using it, how easily can they re-establish proficiency?
- Errors: How many errors do users make, how serve are these errors and how easily can they recover?
- Satisfacation: How pleasant is it to use the design?

Triangle of Security, Functionality and Usability

Identification → Identify the user

Authentification → Authenticate the user is allowed to log-in

Multifactor Authentification

- Something you know: Passwords, patterns, Q&A, recognition
- Something you have: A device, e.g,. smartcard, containing private key; A device with secure connection, e.g., pone; Cookies stored in browser
- Something you are – biometrics: Fingerprint, voice, face, iris, hand,...; Static, dynamic or continuous(e.g., gait)
- Somebody you know: known friends

Passwords were lost/ stolen:

- Login infos by presenting them in public (television, open access ,ect.)
- Breached and sold over the internet
- Ease of brute force based on weak passwords (psychology aspect of common pw)

Discussion: What can we do differently? Different approaches:

1. Biometrics
2. 2FA
3. Facial recognition
4. Iris
5. Fingerprint
6. Voice
7. Smell
8. Ear shape
9. Behavioural (typing, movement, ect.)

Biometrics:

- Information about you, physical or behavioural
- Biometrics can be compromised (e.g Fingerprint)
- Behavioural Biometrics: Thinks you do, you behave, you type, you move...

Exercise:

In small groups choose and research one of the authentication methods listed on the next slide.

- How the method works
- Where does it sit on the security, functionality and usability triangle?
- How difficult is it to spoof your method?
- Are there any privacy implications or concerns associated with the method?
- Does it reduce cognitive load?

- Fingerprint

- Facial recognition: Authentification by characteristic parts of the users face. Was less secure in the past but getting better by evolvement. Office quite good security and it is functional. Good usability (drawbacks by the Covid pandemic and wearing the mask).

- Typing data

- Gait analyisis

- Voice

- Multi-factor authentication: Based on something you know and something you have. Quite good security. But: threats arising from man in the middle attacks and spoofing. General good functionality. Usability disadvantages because of the need of devices, especially for older ages, as well as the need for a running device for authentification. Increase of cognitive load.

Security ranking:

1. MFA
2. Face/Fingerprint (?)
3.
4.
5. Fingerprint/voice (?)
6. Typing data