Seminar session 2: The Human Factor – Exploring usability design options

Overview:

- Introduction to usable security
  - ➔ Security features
  - ➔ Usability
  - ➔ Typical issues
- Guidance on usable security
- Examples
  - ➔ Passwords
  - ➔ Graphical passwords

What is usable security:

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

Security Features:

- Integrity → Trustworthy of the informations.
- Availability → Availability to be able to get the informations when these are needed.
- Confidentiality → Ensuring informations are only access able to allowed users.

= Security

Usability:

Security + Human computer interaction = Usable security

Usability → is a central concept of HCI, which considers how easy a system is to use.

- 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?
- Memorability: 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?

- Satisfaction: How pleasant is it to use the design?

Discussion:

Do you think that the idea of making security more usable is important?

- If the system is too secure then user experience could be bad.
- If something is not usable people will by pass to get things done
- Security can close convenience gaps for users, e.g. passwords and a lack of single sign on encourages users to write passwords down.

Balancing of:

- Security
- Functionality
- Usability

Discussion:

Examples of technology that exhibit all three of these areas?

- Google search page, contains input validation (e.g. XSS, SQL injection), served HTTPS
- Gmail –log in with 2FA, usable and functionality

What the problems with security?

- Security interfaces tend to be too confusing and clumsy
- Security is usually a secondary goal (and therefore users are unmotivated)
- Strain on users to remember several security settings, configurations and passwords
- Task workload and increasing complexity of security of security systems and interfaces
- Abundance of technical terminology
- Forcing uniformed security decisions on users

General guidance:

- Reduce cognitive load associated with cybersecurity system activities
- Make security state visible, and security functionality visible and accessible
- Give informative and useful feedback on security operations
- Design such that security does not reduce performance

- Give guidance on what tasks users need to perform and where necessary, provide recommendations support
- Reduce the use of technical and security-specific terms and jargon
- Provide help, advice and documentation

Online Accounts:

- 2007 survey by Microsoft: 26 online accounts, 6.5 passwords, 3.9 sites per password
- 2015 research by Dashlane: 118 online accounts registered to one email
- 2017 research by Last Pass: 119 passwords in their online vault

Why do we use passwords:

-" Since the dawn of the electronic age, the computer password has been a trusted guardian of secrets large and small. For many people, obtaining their own password became a rite of initiation into computer culture itself. Now, growing numbers of security experts feel that the password in its common form is too old an unsophisticated for the job."

Discussion:

Why do we use passwords?

- They're easy to implement and to authenticate
- They're really well understood
- They maintain basic security and should go some way to ensuring CIA
- A cheapest means of authentication
- Unintrusive to the user

Guidance for a good password:

- Make them memorable
- Ensure your password is hard to guess
- Use a mixture of symbols, letters and number
- You don't need to worry about using symbols
- Substitute numbers for letters e.g. 3 for e
- Make sure passwords are at least 8 characters long?
- Make sure passwords are at least 16 characters long?
- Never use dictionary words
- Use three random words
- Use a passphrase containing a number of dictionary words
- Never use personal details such as pet's name, children's name or your birthday

Disscussion:

Why do you think there are limits to the length of a password?

- Prevent brute force password. The shorter the passwords easier it is to guess
- Database considerations
- Special characters make no major impact on pw security, the length is the most important factor

Discussion:

What are the alternatives to using passwords?

- Fingerprint
- Facerecognition

Graphical Passwords:

- Use a picture and declare points to klick on for authentication
- In theory a good attempt/solution
- But: Images are processed in our brains quite similar, that leads to the problem, that choosen spots of an image are easy to guess.

Two Factor Authentication (2FA):

- Closest thing to have to enhancing security
- Drawbacks: You need to have the device with you

Questions:

- So for that first essay that first submission, you are looking at three potential human related things that could cause security problems.
- issues that might come out because of humans involved in the system.
- we're not looking at the mitigation now we're just looking at identifying the potential issues that could be caused by humans.

I also have a question on that, I mean are we talking about individually human factors are we talking about group of. → yep both anything goes, I think the important thing is to the justification that you give for the human factors that you've identified and The reasoning behind it, because i'm of the opinion that most things are in scope and it's just having a trader so.