Privacy and Technology - Exercise 4, 12/13 December 2023

Usable Authentication

1) Password strength checking

This task should practically illustrate how users choose compliant but insecure passwords and the divergence between theoretical and practical brute force resistance.

Human factors impact on password security. Take a public passwords dataset (e.g. rockyou.txt, uploaded in PANDA) and filter out the passwords that were created according to the policy [A-Za-z0-9@#$%^&+=] with at least 9 characters. You are free in choosing the technique, e.g. with Python regex using Jupyter Notebook.

Tasks:

- Compute the entropy, $H = \log_2 N^L$
- How long does an attacker need to break the password via brute force? (Theoretically, according to the computed entropy)
- Look at the subset of the password (e.g., first 10 or 20) in your Jupyter Notebook
- Use zxcvbn to compare the "real" strength of these passwords to the theoretical entropy
- What can you say about password strength and usability?

2) Usability testing of a password manager

In this task you will conduct an expert usability test of a password manager. The goal is that they learn to apply the methodology and the results should illustrate the usability limitations of a security technology. The password manager could be KeePass (recommended by the BSI and the university)

Process:

i) Read about Nielsen's heuristics

ii) Work in groups to identify usability problems based on the heuristics

iii) Create a final report with your findings by creating a list of usability problems (see slides)