IT Security 2024/2025

Exercise Sheet 14

– Web Authentication Schemes –

Melina Hoffmann

Publication: 23.01.2024
Deadline: 29.01.2024 10:00

Lightning Survey ⚡

Exercise 1 (eID Fraud Scenarios, 1.5 points)**.** For each of the following short scenarios, describe concisely (1-2 sentences each) and precisely at which step of the online authentication process as described in the lecture the malicious or fraudulent action is detected. You can assume that all other parts of the eID system are benign and work as specified. If you make further assumptions, please state them together with your answer. Submit everything in `eid-fraud.txt`.

a) A pickpocket has obtained the government-issued identification card (*Personalausweis*) of somebody else and tries to use it to open a bank account in the original card holder's name.

b) A fraudster has forged a government-issued identification card (*Personalausweis*) including the integrated chip for an entirely fake identity and tries to obtain a SIM card in the name of this fake identity.

c) A malicious actor wants to obtain personal data from various citizens. The malicious actor has replicated a government service website and has lured a citizen onto the spoofed website, who has now started an eID authentication process on the spoofed website.

Exercise 2 (sPACE-Attack, 3.5 points)**.** Research the sPACE attack (CVE-2024–23674) on the German eID scheme and answer the following questions. State all of your corresponding sources and write your solution into `space.txt`.

a) What is the goal of the attack? (max. 2 sentences)

b) Where in the eID system and processes lies the exploited vulnerability? (max. 3 sentences)

c) Which requirements need to be fulfilled by the attacker and on the user's side for a successful attack? (max. 3 sentences)

d) Describe the sequence of steps for the attack. (max. 15 sentences)

e) When and by whom was this attack made public? (1 sentence)

f) What was the public response of the BSI (Federal Office for Information Security) to this attack, especially with regards to the assessment of the severity and recommended actions for citizens to protect themselves? (max. 2 sentences)

Exercise 3 (User Agent Header, 2 points)**.** For each of the following User Agent strings, briefly state which information about the browser can be inferred from each component of the string. State all of your corresponding sources and write your solution into `user-agent.txt`.

a) Mozilla/5.0 (Android 4.4; Mobile; rv:70.0) Gecko/70.0 Firefox/70.0

b) Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36

Exercise 4 (Web Audio API, 3 points)**.** Research how the Web Audio API can be used for browser fingerprinting and answer the following questions into `web-audio.txt`. State all of your corresponding sources.

a) Describe the browser component(s) used in fingerprinting via the Web Audio API. (max. 3 sentences)

b) How is an audio fingerprint generated? (max. 10 sentences)

c) Why can these fingerprints vary between browsers? (max. 5 sentences)