Peer Response 1

Hi George,

Thank you for your submission to this discussion. It is a thorough view on the A07 OWASP Top 10 weakness. Both flowcharts are thought-through, and clear and demonstrate the critical decision points at which a weakness may be introduced in the process. Below is some further feedback on the password flowchart particularly.

For the sake of clarity, I would begin the first block as, “User commences registration” to ensure clarity that registration can only be successful once a sufficiently secure password is used. I would additionally break down the specific features that define a “strong password”, such as – does it contain numbers, does it contain special characters, is it at least 8 characters long – and split the decision on re-used password separately, as a re-used password would require the user to have registered already.

A critical step that also is becoming more critical is the use of Multi-Factor Authentication (MFA). For low-risk applications this may be tedious, but for organisations, this is a non-negotiable. More work is required to make the MFA setup and usage process more user-friendly and increase positive perceptions of the need of MFA (Das et al., 2020), therefore as such, adding more steps and decisions in the flowchart may hinder user experience. A balance must be obtained.

On the second flowchart, a positive decision is immediately made upon entering valid credentials, however a secure login does not terminate here. It is important to validate the device the user is logging in from, and manage sessions to ensure they expire and

may not be reused by an attacker, as described in the Common Weakness Enumeration (CWE)-613: Insufficient Session Expiration.

Thank you again for this submission, it has given me considerations of my own submission and has highlighted how complex authentication is, beyond just setting a strong password.

References:

Das, S., Wang, B., Kim, A. & Camp, L.J. (2020) MFA is A Necessary Chore!: Exploring User Mental Models of Multi-Factor Authentication Technologies. In *HICSS* (1-10).