Collaborative Discussion 1 – Peer Response 1 – Kingsley Onyeemeosi

Thank you Kingsely for your well argued post.
Regarding the limited login attempts, I see a dilemma in which to find oneself.

On the one hand, limited login attempts offer effective protection against brute forece attacks by computer calculations. On the other hand, the medical staff needs access at all times and a doctor accidentally enters the password incorrectly several times under high stress. If this happens and an admin has to release the account before trying to log in again, this can endanger the health of patients.The question therefore arises as to how a secure password can theoretically be designed.

A four-digit numeric PIN has 10^4 = 10,000 possible combinations. For passwords with uppercase and lowercase letters, digits and the ten special characters, there are already a number of possibilities with 4 digits of 72^4 = 26,873,856(Wood, 1977).

This is a massive increase in the possibilities, but assuming that computers can, on average, perform more than 4 billion calculations per second, it can determine such a password within 72^4/4,000,000,000 = 0.0067 seconds.

With a password with 10 digits, the calculation time in this example increases to 72^10/4,000,000,000 = 9.359… * 10^9 seconds or (72^10/4,000,000,000 * 31,556,926 = 29.6) 29.6 years. That is already an acceptable amount of time in terms of security.

With a password with 11 digits, the calculation time for the theoretical approach is already 72^11/4,000,000,000 * 31,556,926 = 2,135 years. This is a satisfactory length theoretically and from a human life perspective.

At this point, however, the theoretical limitations must be addressed. When looking at all possible password combinations were included, including passwords that only consist of ones, for example. These combinations can also generate words or names. Another decisive factor is the computing power of the computer. As early as 2016, supercomputers were able to carry out 100 * 10^15 calculations per second(Fu et al. 2016). The 11-digit password in the consideration would be determined by such a computer within 72^11/8 * 10^15 = 2,695 seconds or 45 minutes. This shows that with increasing computer performance, the password length must increase in order to make brute force attacks unattractive.

References:

Wood H. (1977)Computer Science & Technology: The Use of Passwords for Controlled Access to Computer Resources. Department of Commerce, National Bureau of Standards, Institute for Computer Sciences and Technology. Available from: https://play.google.com/store/books/details?id=xNI1Ab60YPYC&rdid=book-xNI1Ab60YPYC&rdot=1 [Accessed: 16.11.2021]

Fu, H., Liao, J., Yang, J., Wang, L., Song, Z.,Huang, X.,Yang, C., Xue, W., Liu, F., Qiao, F., Zhao, W., Yin, X., Hou, C., Zhang, C., Ge, W., Zhang, J., Wang, Y., Zhou, C., & Yang, G. *(2016)* The Sunway TaihuLight supercomputer: system and applications. *Sci. China Inf. Sci.* 59:072001. Available from: https://link.springer.com/article/10.1007/s11432-016-5588-7#citeas [Accessed: 16.11.2021]