

## **Introduction**

Breaches in the digital world have harmed and inconvenienced companies in recent times due to remiss cybersecurity (Bach-Nutman, 2020). However, the non-profit organisation Open Worldwide Application Security Project (OWASP) was established in order to enhance software defense (Poston, 2020). OWASP lists 10 Web Application Security Risks on their website. For this collaborative discussion, I have decided to select the weakness introduced in 2021, “A04:2021 - Insecure Design”.

## **Rationale**

According to OWASP (N.D.a), Insecure Design is when designs are either useless or absent, and there is an apparent lack of sophisticated safeguards from targeted cyberattacks. This security risk was selected since I still login to websites and programmes that ask multiple security questions as a means of verification. In order to present through a flowchart where vulnerabilities can arise, a UML activity diagram was utilised. Abbas et al. (2021) states that activity diagrams usually present how systems work. Figure 1 presents how an attacker can correctly respond to security questions after stealing the digital identity of a user, and eventually gain access to the system.

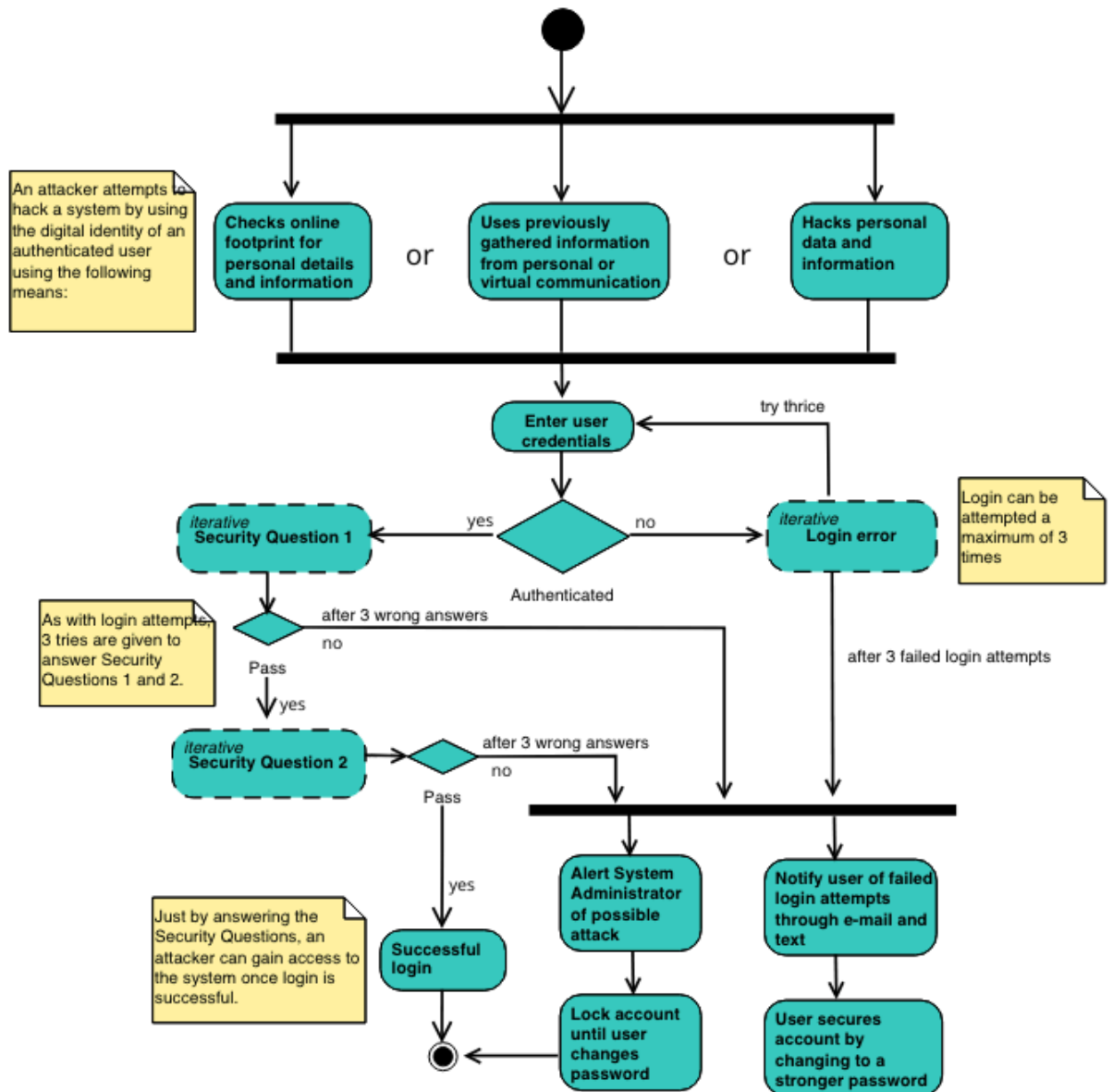


Figure 1: UML Activity Diagram presenting steps that can possibly lead to  
A04:2021-Insecure Design weakness

## **Conclusion**

I have always considered security questions to be an extra protection during sign ins, especially as they are the verifiers needed in my banking apps and e-mails. On the contrary, Grassi et al. (2017) asserts that questions requiring precise facts as responses must never be asked for authentication, as emphasised in the National Institute of Standards and Technology (NIST) 800-63B Digital Identity Guidelines. Fortunately, I now know that even these seemingly very personal questions can be answered by persistent attackers. In order to keep the security of systems and web applications more up-to-date and standardised, application of the proactive protocol “C6: Implement Digital Identity” is recommended. OWASP (N.D.b) informs us that NIST 800-63b has streamlined authentication into three levels— First is Passwords, Second is Multi-Factor Authentication, and Last is Cryptographic Based Authentication.

## References:

Abbas, M., Rioboo, R., Ben-Yelles, C-B. & Snook, C.F. (2021) Formal modeling and verification of UML Activity Diagrams (UAD) with FoCaLiZe. *Journal of Systems Architecture* 114(101911): 1-14. DOI: <https://doi.org/10.1016/j.sysarc.2020.101911>.

Bach-Nutman, M. (2020) Understanding the Top 10 OWASP Vulnerabilities. *arXiv:2012.09960*. DOI: <https://doi.org/10.48550/arXiv.2012.09960>.

Grassi, P.A., Fenton, J.L., Newton, E.M., Perlner, R.A., Regenscheid, A.R., Burr, W.E., Richer, J.P., Lefkovitz, N.B., Danker, J.M., Choong, Y-Y., Greene, K.K. & Theofanos, M.F. (2017) *NIST Special Publication 800-63B: Digital Identity Guidelines*. DOI: <https://doi.org/10.6028/NIST.SP.800-63b>.

OWASP (N.D.a). A04 Insecure Design - OWASP Top 10:2021. Available from: [https://owasp.org/Top10/A04\\_2021-Insecure\\_Design/](https://owasp.org/Top10/A04_2021-Insecure_Design/) [Accessed 15 March 2024].

OWASP (N.D.b) OWASP Top Ten Proactive Controls 2018 | C6: Implement Digital Identity. Available from <https://owasp.org/www-project-proactive-controls/v3/en/c6-digital-identity> [Accessed 15 March 2024].

Poston, H. (2020) Mapping the OWASP Top Ten to Blockchain. *Procedia Computer Science* (177): 613-617. DOI: <https://doi.org/10.1016/j.procs.2020.10.087>.