Collaborative Discussion 1: UML flowchart

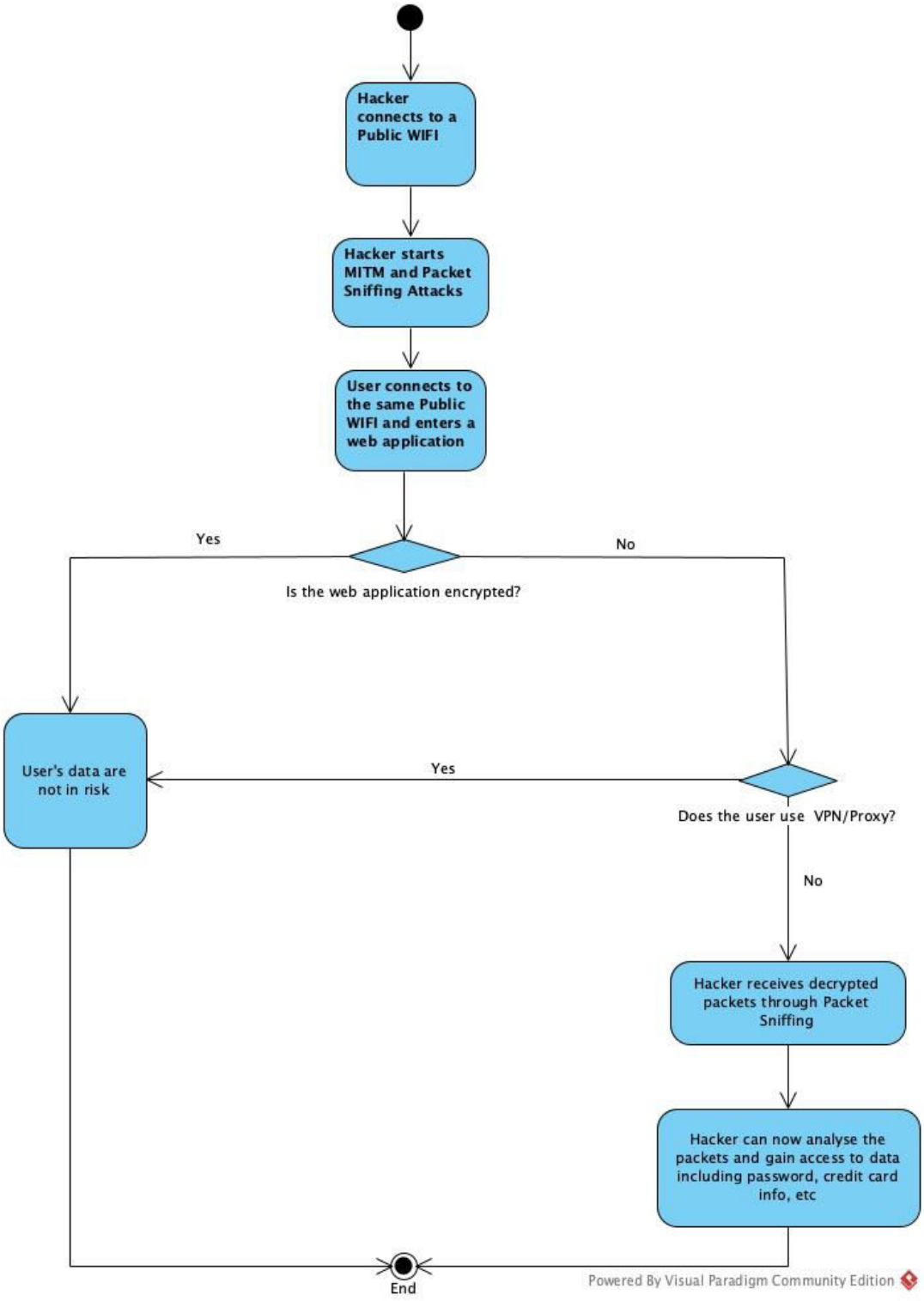
The Open Web Application Security Project (OWASP) is a non-profit foundation aiming to recognise and improve the security of software (OWASP, n.d). It is supported by tens of thousands of members, educational institutes, and more. It provides tools and resources to improve any software developed, it organises and provides training and has an active community for developers interested in improving security (OWASP, n.d).

OWASP has developed a document called “OWASP Top Ten” where it represents the most serious security risks of web applications.

A common critical security risk that affects all kinds of web applications is the A3 – Sensitive Data Exposure. Data Exposure can occur when the web application does not have proper encryption (e.g., HTML, TLS, SSL), resulting in decrypted data flow through the network. Additionally, storing data in decrypted databases can result in an immense data leak. Apart from the obvious risk of creating opportunities for data leaks, APIs without proper encryption do not comply with the EU GDPR and can result in hefty fines (OWASP, n.d).

In order to mitigate the risk of Sensitive Data Exposure, developers should:

a) Create encrypted and safe databases where only strictly necessary data will be stored. Storing additional non-required data puts further data at risk, but also it does not comply with the GDPR, since the regulation strictly allows only required data to be processed (GDPR, 2016)
b) Deploy HTTPS, TLS or SSL encryption protocols to secure data flowing within the network (e.g., from a computer connected to a public WIFI to the server of the web application).


Hacker connects to a Public WIFI
Hacker starts MITM and Packet Sniffing Attacks
User connects to the same Public WIFI and enters a web application
Yes
No
Is the web application encrypted?
User's data are not in risk
Yes
Does the user use VPN/Proxy?
No
Hacker receives decrypted packets through Packet Sniffing
Hacker can now analyse the packets and gain access to data including password, credit card info, etc
End
Powered By Visual Paradigm Community Edition

References:

EUR-Lex (n.d.) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 21 July 2021].

OWASP (n.d) A3:2017-Sensitive Data Exposure Available from: https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure [Accessed 21 July 2021].

OWASP (n.d) OWASP Top Ten Available from: https://owasp.org/www-project-top-ten/ [Accessed 21 July 2021].

OWASP (n.d) Who is the OWASP Foundation? Available from: https://owasp.org [Accessed 21 July 2021].