Collaborative Discussion 1: UML flowchart – Peer Response

1. **Response to Adesola:**

Hi Adesola,

Reading your analysis of cryptographic failures was enlightening. Here is my detailed analysis of your post with explanations and comments:

You effectively highlight the significance of cryptographic failures as a security concern in web applications. You describe what they are and provide examples to illustrate potential scenarios. This helps me understand the importance of addressing this vulnerability.

Despite the points of misinterpretation mentioned by Dr Cathryn, your decision to use an activity diagram to analyse cryptography weaknesses was great and completely understandable. The flow of actions, choices, and interactions within a system is best represented using activity diagrams (Lucidchart, N.D.). Due to my inability to draw ideal diagrams, I can only point out a few problems with yours. However, based on Muller & Meucci (2014) theories, the diagram's capacity to depict parallel actions is a strong point because cryptographic weaknesses can occur along several paths.

The advantages of using an activity diagram efficiently could be discussed. As Farooq (2022) noted, the diagram can graphically depict the weaknesses and mistakes in the process by concentrating on the decisions and activities that result in cryptographic failures. This illustration can assist in spotting potential flaws, giving security teams and engineers a better understanding of the failures.

Your analysis is well-organised and demonstrates that you have a solid grasp of the subject. You did an excellent job of explaining the idea of cryptographic failures, their possible causes, and the significance of dealing with them, and the choice of an activity

diagram is appropriate, considering its ability to visualise the process and decisions that can lead to vulnerabilities.

You can further strengthen your analysis by considering the impact and consequences. For instance, in Ali's (2023) research, he explained the potential implications of cryptographic failures, including data breaches, a decline in trust, problems with law and compliance, and intellectual property theft.

References:

Lucidchart (N.D.). *UML Activity Diagram Tutorial*. [online] Lucidchart. Available at: https://www.lucidchart.com/pages/uml-activity-diagram.

Muller, A. & Meucci, M. (2014). *4.0 Testing Guide Frontispiece*. Available at: https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf.

Farooq, A. (2022). *Threat modelling with UML for cybersecurity risk management in OT-IT integrated infrastructures*. [online] Available at: https://core.ac.uk/download/pdf/521288263.pdf [Accessed 18 Aug. 2023].

Ali, Z. (2023). *Cryptographic Failures: Understanding the Pitfalls and Impact*. [online] Available at: https://www.linkedin.com/pulse/cryptographic-failures-understanding-pitfalls-impact-zahid-ali/ [Accessed 18 Aug. 2023].

2. Response to Sebastien:

Hi Sebastien,

Your initial post highlights several important aspects of the insecure design and implementation of Application Programming Interfaces (APIs). My thoughts on each of the main points are:

Importance of APIs and Security Concerns:

APIs are crucial for online and mobile applications but are also a prime target for attackers. While they enhance functionality and interoperability, security must be a top priority to protect sensitive data and processes (Amazon Web Services, 2023).

RESTful APIs and Vulnerabilities:

RESTful APIs are crucial for modern app designs but can reveal vulnerabilities if not securely designed and deployed. This can lead to unauthorised access or the exposure of private information (Yasar, N.D.).

OWASP API Security Top 10:

It is a good idea to mention the OWASP API Security Top 10. Developers should focus on the OWASP API Security Top 10 to prioritise security efforts. BOLA is a standard API security concern (OWASP, 2019).

BOLA Illustration:

Inadequate access controls in the Broken Object Level Authorization (BOLA) example resulted in unauthorised access to patient profiles in a healthcare application. This shows the importance of proper permission procedures to prevent such attacks (Barahona, 2022).

Uber APIs Security Incident:

The 2019 Uber API security incident exposed sensitive data and authentication tokens, which could lead to an account takeover. This shows that even large businesses can fall victim to API-related vulnerabilities (Shkedy, 2021).

Consequences of Insecure APIs:

Your statement about the potential consequences of insecure APIs is accurate. Insecure APIs can lead to financial losses and damage to reputation. Platform trust is lost when data is not protected, reducing user engagement and adoption (Bignell, 2023).

User Behaviour After Data Breaches:

The reference to the study by Strzelecki & Rizun (2022) adds depth to your post. It is essential to understand that data breaches resulting from insecure APIs can have a lasting impact on user behaviour. Users affected by breaches may abandon platforms due to security, privacy, and trust concerns.

References:

Amazon Web Services (2023). *What is an API? - API Beginner's Guide - AWS*. [online] Amazon Web Services, Inc. Available at: https://aws.amazon.com/what-is/api/.

Yasar, K. (N.D.). *What is API security? Definition from WhatIs.com.* [online] Available at: https://www.techtarget.com/searchapparchitecture/definition/API-security.

OWASP (2019). *OWASP API Security - Top 10 | OWASP*. [online] owasp.org. Available at: https://owasp.org/www-project-api-security/.

Barahona, D. (2022). *What is Broken Object Level Authorization (BOLA) and How to Fix It | APIsec*. [online] Available at: https://www.apisec.ai/blog/broken-object-level-authorization.

Shkedy, I (2021). *The Uber API Authorization Vulnerability*. [online] Available at: https://www.traceable.ai/blog-post/the-uber-api-authorization-vulnerability.

Bignell, F. (2023). *Salt Security Finds API Security Threats on the Rise as Nearly 1 in 5 Have Suffered a Breach*. [online] The Fintech Times. Available at: https://thefintechtimes.com/salt-security-finds-api-security-threats-on-the-rise-as-nearly-1-in-5-have-suffered-a-breach/ [Accessed 20 Aug. 2023].

Strzelecki, A. & Rizun, M. (2022). Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping. *Sustainability*, [online] 14(10), pp.1–17. Available at: https://ideas.repec.org/a/gam/jsusta/v14y2022i10p5866-d814030.html [Accessed 20 Aug. 2023].