Risk Assessment

This report will analyze two significant threats in the NCA system based on the risk assessment procedure discussed in lectures 4 and 5.

1 Unauthorized Disclosure of Confidential information

Design Assumption: NCA stores users' confidential information, for example, plate number, phone number and driver information.

Threat Description: An attacker may implement a Structured Query Language (SQL) injection attack against the database to gain unauthorised access to users' confidential data. This information can then be utilised to conduct an advanced deception campaign. For example, an attacker may impersonate an NCA employee to deceive users and steal financial resources. Alternatively, the attacker may exploit the compromised database to manipulate records and illicitly generate profits via external means, for example, by providing a service that the user can pay less money to the attacker instead of NCA.

Threat Category: Combined Threats (Social Engineering and Database Attack)

Attack Intend: Attackers would aim to have financial requirements. Because the UK Inflation Rate has increased to 10.7% [1]. If users intend to pay less from the NCA, then attackers can profit through this process.

STRIDE Model: The system demonstrates security weaknesses in three categories: Spoofing, where attackers exploit users' confidential data for unauthorized impersonation of NCA personnel; Tampering, with adversaries capable of injecting and altering data within the system; and Information Disclosure, arising from the unauthorized acquisition and potential misuse of sensitive information by malicious entities.

Assessment of Likelihood: Likely

Justification of Likelihood: From [2], over 33% web application vulnerabilities of 2022 were SQL injection; it was the most dangerous attack in 2021 from the record of [3].

Assessment of Impact: Bad

Justification of Impact: A successful execution of an SQL injection attack grants the attacker unauthorized access to the database, enabling them to perform operations such as reading, updating, deleting, and inserting records [4]. From the report of [5], TalkTalk suffered a data breach in October 2015, prompting customers to change their email and online account credentials. Due to the security incident, the company subsequently recorded a £400,000 fine.

Vulenability Control: Attackers can compromise a database and manipulate data by injecting SQL through user input fields [6]. They may also carry out Denial of Service (DoS) attacks to exploit vulnerabilities and escalate their privileges within the system [6].

Countermeasures: Implement the SQLand framework to enable developers to generate queries using randomized instructions, enhancing query security [6]. NCA should also conduct regular black-box testing to identify potential vulnerabilities in the system and address them proactively [6].

2 Incorrect User in the System

Design Assumption: NCA requires employees to use push-based Multi-Factor Authentication (MFA) to enhance overall security when accessing their work email accounts. By implementing MFA, the NCA reduces the likelihood of unauthorized access, as it requires multiple verification forms for successful authentication.

Threat Description: Attackers may use MFA bombing attacks to bother the target employee with multiple authentication requests, causing the employee to select "Accept" out of frustration. The attacker can then impersonate the NCA employee.

Threat Category: Social Engineering

Attack Intend: Attacker would send phishing emails to the target employee's colleagues to gain higher access to the system.

STRIDE Model: The threat exposes vulnerabilities in three STRIDE categories: Spoofing because the attacker impersonates the target employee; Information Disclosure because unauthorised access and dissemination of sensitive data are possible; and Elevation of Privilege because the attacker can send phishing emails to expand unauthorised access.

Assessment of Likelihood: not very likely

Justification of Likelihood: From 2020 to 2022, 40,942 MFA Bombing Attacks were identified [7]. In the case of Microsoft users, approximately 1% inadvertently accepted these authentication requests without acknowledging them [7].

Assessment of Impact: bad

Justification of Impact: Uber has been attacked with the MFA bombing attacks, and the data has been breached in its network by hacker group Lapsus$, and the attacker has access to the company's working tools [8].

Vulenability Control: Attackers may exploit MFA fatigue by repeatedly sending push notifications to users, prompting them to perform the same behaviour recognition tasks [9]. As a result, users may approve these requests out of frustration, giving attackers an opportunity to take over their accounts [9]. And man-in-the-middle (MitM) attack also can be performed in the MFA if it is a one-time password to SMS.

Countermeasures: From [10] suggested implementing Single Sign-On (SSO) for users, allowing them to authenticate once and access multiple applications and services without re-authentication. This reduces user fatigue and increases attentiveness when receiving messages from MFA apps. Also, behaviour authentication would perform better than the one-time password [8].

References

[1] BBC News. Uk inflation rate calculator: How much are prices rising for you?, Sep 2022. Accessed: 2023-05-06.

[2] Sujay Vailshery. Most common web application critical risks 2020, 2023. Accessed: 2023-05-06.

[3] M. Hasan, A. Al-Maliki, and N. Jasim. Review of sql injection attacks: Detection, to enhance the security of the website from client-side attacks. *Int. J. Nonlinear Anal. Appl*, 13:2008–6822, 2022.

[4] A. Sadeghian, M. Zamani, and S. Ibrahim. Sql injection is still alive: A study on sql injection signature evasion techniques. 2013.

[5] Sponsored. A major threat to business: Sql injection attack, 2022.

[6] William G Halfond, Jeremy Viegas, Alessandro Orso, et al. A classification of sql-injection attacks and countermeasures. In *Proceedings of the IEEE international symposium on secure software engineering*, volume 1, pages 13–15. IEEE, 2006.

[7] speditor. The rise of mfa fatigue attacks, 2022. Accessed: 2023-05-06.

[8] J.V. Writer. Uber: Lapsus$ targeted external contractor with mfa bombing attack, Sep 2022. Accessed: 2023-05-06.

[9] Khaled Zaky and Dean H Saxe. Multi-factor authentication. *IDPro Body of Knowledge*, 1(10), 2022.

[10] BeyondTrust. Mfa fatigue attack: Definitions best practices. n.d.