**1.0: Introduction and System Overview**

**徽标, 图标

描述已自动生成**

The mobile banking application under security evaluation is “Maybank MAE”. MAE is a mobile banking application offered by Maybank. MAE serves as a secure and user-friendly application for customers to effortlessly access their financial services through mobile devices. The app’s purpose is to enable customers to manage their finances while on the road by providing functions like checking account balances, moving money, paying bills, and more.

The MAE mobile banking application comprises several components. It relies on Backend Servers responsible for managing accounts, processing transactions, and handling client requests. The database component plays a crucial role by securely storing user information, account details, and transaction records. To ensure safe communication between the bank's servers and the app, communication interfaces are employed.

Encryption plays an important role in ensuring the confidentiality of sensitive client data, including account numbers and transactional information (NIST, 2021). By preventing unauthorized changes or manipulation of data during storage or transmission, encryption also contributes significantly to maintaining data integrity (NIST, 2021). Authentication methods serve to permit only authorized users to access the MAE Maybank system, reducing the risk of unauthorized access attempts and enhancing overall system availability (NIST, 2021).

**2.0: Security Requirement Analysis**

**2.1 Vulnerabilities found in the System**

MAE is vulnerable to mobile app vulnerabilities, like many other mobile applications. These include possible vulnerabilities like virus attacks, code errors, and data leaks (Rouse, 2021).

Data Security Risks are yet another serious vulnerability. Since MAE handles sensitive customer financial data and personal information, it may be subject to cyberattacks and data breaches (Statt, 2021).

Additionally, authentication weaknesses were identified as a potential vulnerability. Passwords that are simple to guess might expose user accounts to unauthorized access if user authentication measures were weak or compromised (Rouse, 2021).

**2.2 Severity of Problem**

Careless handling of sensitive customer data can lead to significant financial losses, damage to the bank's reputation, and potential legal consequences (NIST, 2021). To mitigate this risk, it is essential to implement robust data protection measures. This includes encrypting data both in transit and at rest, and regularly conducting audits of data access to ensure its security.

Neglecting the evolving threat landscape can leave the bank vulnerable to a wide range of cyber threats (Burbidge, 2021). It is crucial to establish effective threat detection techniques and real-time monitoring to swiftly identify and mitigate emerging threats. Early threat identification and response are critical to prevent data breaches, financial losses, and reputational harm.

Weaknesses in user access control systems can lead to unauthorized access, potentially resulting in data breaches and fraudulent activities (NIST, 2021). It also can lead to unauthorized transactions, data leakage, and system compromise. MAE should implement Role-Based Access Control (RBAC) methods, which ensures that users are only granted access to resources and actions relevant to their roles.

Violating local and industry-specific regulations can have severe consequences, including substantial fines, loss of public trust, and legal actions (PCI Security Standards Council, 2021). To safeguard its reputation and legal standing, the bank must prioritize strict adherence to these regulations.

**3.0 Encryption and Authentication Evaluation**

**3.1 Encryption Methods Evaluation**

Some encryption methods are available for securing MAE. One of the effective methods is **symmetric encryption**, such as AES-256. Symmetric encryption is well-suited for safeguarding data at rest, such as customer account information. It offers the advantages of speed and simplicity, requiring only one key for both encryption and decryption processes (Schneier, 2015).

MAE can be secured by **asymmetric encryption** methods like RSA or ECC by ensuring secure communication. Asymmetric encryption uses a pair of keys, one for encryption and one for decryption (Paar & Pelzl, 2010). This approach enhances the security of transactions and interactions within MAE.

**3.1.1 Symmetric Encryption**

The Advanced Encryption Standard, also known as AES, is a commonly used symmetric encryption algorithm. User account information and other data that is stored at rest in MAE can be protected using it. The choice of symmetric encryption algorithm, such as the Advanced Encryption Standard (AES-256), ensures that sensitive customer data remains confidential (NIST, 2001).

**3.1.2 Asymmetric Encryption**

RSA (Rivest–Shamir–Adleman) or ECC (Elliptic Curve Cryptography) can be employed for secure communication within MAE. While ECC offers good security with lower key lengths, RSA is well renowned for its dependability in key exchange and digital signatures (Menezes et al., 2017).

**3.1.3 Key Management Practices**

To protect client data, effective key management practices are essential for MAE, including secure key generation, storage, distribution, and rotation. For example, MAE should employ Hardware Security Modules (HSMs) to securely store and manage encryption keys, reducing the risk of unauthorized access (Stallings, 2017).

**3.1.4 Encryption Codes**

The process of converting plaintext data into ciphertext relies heavily on encryption codes, as those applied to AES encryption. To preserve the security of sensitive client information in the context of MAE, encryption codes are used. For instance, encryption codes are employed to protect user credentials and transaction information from potential risks when a user signs into their MAE account or completes a financial transaction (Schneier, 2015).

**3.1.5 Comparison of Strengths, Weaknesses, and Practical Considerations**

Symmetric Encryption, such as AES-256, has several strengths. It is fast and efficient, ideal for encrypting data at rest like customer account information. To comply with the security requirement of data sensitivity, its primary key must be securely managed to avoid unauthorized access (NIST, 2021). However, symmetric encryption may fail to meet the security requirement of data integrity, as it utilizes the same key for both encryption and decryption (Schneier, 2015).

Asymmetric Encryption, such as RSA or ECC, excels at secure communication, which is in line with the requirement to safeguard data while it is being transmitted (Paar & Pelzl, 2010). Data integrity and secrecy are guaranteed by its two-key system, which uses one key for encryption and another for decryption. However, it is computationally demanding, which could have an impact on the MAE app's performance (NIST, 2021). Future concerns posed by quantum computing may also affect it (Shor, 2016).

**3.2 Authentication Methods Evaluation**

There are authentication methods applicable to MAE. One of the methods is **multi-factor authentication (MFA).** MFA works highly effectively to reduce the danger of unauthorized access, protect sensitive financial data, and stop fraudulent transactions. Many MFA methods, including utilizing mobile apps or biometric information, are simple to use and demand nothing from consumers, improving the overall mobile banking experience. MFA is a scalable solution that is used extensively in online financial services.

**Biometric authentication** is also applicable to MAE, such as fingerprint or facial identification offers strong security measures (Jain et al., 2016). To retain efficacy, MAE should take precautions against potential vulnerabilities like spoofing and keep up with changes in biometric security. The total mobile banking experience is improved by users' excellent usability and convenience with biometric authentication (Jain et al., 2016).

**3.2.1 Trade-offs between security and user experience**

MAE should consider implementing a multi-tiered authentication approach. For routine activities, users can benefit from convenient methods like biometrics. MAE can request stronger authentication, such as 2FA, from users during high-risk transactions or sensitive account activity.

**4.0 Recommendations and Implementation**

**4.1 Recommended encryption and authentication methods**

AES-256 encryption is recommended to be used, which is well known for its high level of security and robustness, to secure critical data inside the MAE app (NIST, 2021). MAE may consider about adding routine key rotation and tightening key management procedures to further improve the encryption method (Schneier, 2015). This would guarantee that, even if a key were compromised, the potential harm would be reduced.

For enhancing security, MAE is recommended to implement Multi-Factor Authentication (MFA) for user access, which has been shown to significantly reduce the risk of unauthorized access (NIST, 2021). MAE could explore adaptive authentication techniques that evaluate risk variables and modify authentication requirements as necessary to further enhance MFA (Choudhary et al., 2019).

**4.2 Challenges and Risks**

One of the key challenges facing MAE is the establishment of robust **key management practices** tailored to financial transactions due to its extensive handling of sensitive financial data. The risks associated with inadequate key management practices are significant, making it essential for MAE to employ industry-standard techniques.

While partnering with reputable **Certificate Authorities (CAs)** is crucial for maintaining trustworthiness, managing SSL/TLS certificates for a sizable user base poses a complex challenge for MAE. The risk here lies in the possibility that users may encounter security alerts or face difficulties accessing the app securely if SSL/TLS certificates are not renewed as scheduled.

Configuring and consistently maintaining **secure communication protocols** like TLS is of paramount importance to safeguard user data during transactions in MAE. Ensuring that both the client and server components use the latest and most secure TLS versions and cipher suites is a significant challenge. The potential risk associated with improper TLS settings in MAE is the exposure of sensitive financial information to threats.

Balancing strong security with a seamless user experience is a challenge for MAE, especially considering the minimal performance impact of encryption and decryption processes, particularly during high-traffic periods. The risk lies in the possibility that poorly optimized encryption in MAE could frustrate users by causing slow transaction processing or unresponsiveness.

**5. Conclusion**

**5.1 Key findings**

In the security evaluation of MAE, encryption emerged as a fundamental safeguard for data in transit and at rest, effectively thwarting unauthorized access and data breaches (NIST, 2021). Data security was greatly improved by employing effective key management procedures that minimized the danger of key disclosure (Smith, 2020). To manage users and ensure proper access, role-based access control (RBAC) was shown to be essential (NIST, 2021). The sensitivity of customer financial data highlighted the necessity for strong protection that adhered to industry standards and regulations (PCI Security Standards Council, 2021).

**5.2 Monitoring and maintenance**

There are several steps can be taken to maintain the MAE’s security posture in the face of constantly changing threats. Regular security audits and penetration testing can assist in locating vulnerabilities that require immediate attention (Verizon, 2021). Further enhancing the entire security posture is regular staff and customer education on security best practices (Verizon, 2021). MAE could perform user authentication, which continuously enhance user authentication for security and user experience balance.

**5.3 Learning outcomes / reflection**

This security evaluation underlines the crucial functions of authentication and encryption in the security of mobile banking. It is crucial to continuously monitor dangers and adapt to them. Vigilance, adherence to best practices, and user education will allow MAE to continue to offer a secure and reliable banking experience even as the threat landscape changes. In conclusion, maintaining MAE's security and credibility depends on protecting data, abiding by laws, and staying ahead of threats.