Research Paper – 4

Mobile Security

Name:

1) Rutvik Gandhi (8809972)
2) Preet Mali (8838251)

Course Code: INFO8190

Section - 2

Professor: Himani Gandhi

- Considering kind of reliance, we have with our smartphones and mobile apps both today and in the future, it means a large amount of critical information is floating about, accessible to cybercriminals. Knowing that, mobile app developers need to do everything they can to protect their users and clients.

A) Research Secure best practices for Mobile app development. List and briefly describe two of these best practices. (2.5 Marks)

Ans.

1) Secure Data Transmission:

Make sure that every piece of information sent between the servers and the mobile app is secured. This is especially crucial when handling sensitive data, such financial information, personal information, and login passwords. To encrypt data in transit, use secure communication protocols like HTTPS (SSL/TLS).

Tips for Implementation:

- For all connections between the mobile application and backend servers, use HTTPS.
- Use robust encryption techniques and make sure they are updated to fix flaws.
- Sensitive information should not be transmitted over URLs as they might be recorded in several locations.

2) Code Obfuscation and App Hardening:

Description: To make it harder for attackers to reverse engineer the application, code obfuscation is changing the code into a more complicated and challenging-to-understand version. App hardening refers to methods that make it more difficult for hackers to decipher and alter the binary code of the application.

Implementation Advice:

- To make it more difficult for reverse engineers to decipher the logic of the application, rename variables, methods, and classes in the source code using code obfuscation tools.

- Use anti-reverse engineering strategies like code packaging and detection of code tampering.
- Update the program often to add additional hardening and obfuscation layers and keep ahead of emerging threats.

B) Describe how you would implement these two practices in an app. (2.5Marks)

Ans.

1) Secure Data transmission:

Steps in Implementation:

- **For network requests, use HTTPS:**

- Make that the app only uses the HTTPS protocol rather than HTTP for all network queries. The majority of contemporary frameworks and libraries include simple-to-use options or procedures for turning on HTTPS.

- **SSL/TLS Certificate Pinning:**

- In order to improve communication security, use SSL/TLS certificate pinning. By ensuring that the application only interacts with servers that have pre-defined, particular SSL certificates, this lowers the possibility of man-in-the-middle attacks.

2) Code Obfuscation and App Hardening:

Steps in Implementation:

- **Include Tools for Code Obfuscation:**

- During the construction phase, use code obfuscation tools like Swift Shield for iOS or ProGuard for Android. By renaming variables, classes, and methods, these technologies make it more difficult for attackers to decipher the logic through simple code analysis.

- **Put Code Tampering Detection into Practice:**

- Incorporate measures for detecting code tampering to determine whether the application has been altered or tampered with. This might include utilizing libraries made specifically for this purpose, integrity checks, or checksum verification.

By protecting data transfer and increasing the difficulty of possible attackers trying to reverse engineer and tamper with the app's code, putting these procedures into practice helps improve the security of your mobile application. To remain abreast of emerging threats, these security measures must be routinely updated and reviewed.

2. The most important requirement to allowing secure mobile devices is to have a solution in place to authenticate the users of those devices.

A) Research and describe two methods of mobile device user authentication other than just using username and password. (2.5 Marks)

Ans.

1) Biometric Authentication:

- Biometric authentication is the process of authenticating an individual's identification by their distinct biological traits. Facial recognition, iris scanning, voice recognition, and fingerprint recognition are examples of common biometric techniques. Because biometric traits are exclusive to each person and challenging to duplicate, they offer a more easy and safe method of user authentication.
- **Put into Practice:**

- Fingerprint Recognition: Fingerprint scanners are a common feature on contemporary cellphones. During device setup, the user registers their fingerprint; future authentication entails comparing the submitted fingerprint to the one that is saved.
- Facial Recognition: Facial characteristics are captured and analyzed by front-facing cameras. During setup, the user's face is taken, and the saved template is compared with the real-time facial characteristics for subsequent authentication.
- Iris Scanning: Some gadgets scan a user's iris for distinctive patterns using infrared light. High precision and security are offered by iris scanning.
- Voice Recognition: Voice recognition uses an individual's distinctive vocal features to analyze them and can be utilized for authentication. On the other hand, accuracy-affecting environmental circumstances could make it less likely.

2) Multi-Factor Authentication (MFA):

- Multi-Factor Authentication (MFA) requires users to present many forms of identity before providing access, hence adding an additional layer of protection. Generally, the components may be divided into three categories: biometric data; something you have (a physical device or token); and something you know (password or PIN).
- Put into Practice:

- 2FA, or two-factor authentication: Users of 2FA, a popular MFA protocol, must supply two distinct forms of authentication. For instance, the user could receive a one-time code on their registered mobile device after providing a password, which they have to enter to finish the authentication process.
- Biometric + PIN: Adding a personal identification number (PIN) to a biometric technique enhances security. In addition to providing the biometric scan (which they are required to do)
- Tokens or Smart Cards: In business environments, users could get tokens or smart cards that provide temporary codes. The temporary code functions as an extra authentication factor, and these actual gadgets function as something the user owns.

By introducing additional levels of difficulty beyond the conventional username and password techniques, the use of biometric authentication or multi-factor authentication greatly increases the security of mobile devices. These techniques are especially good at limiting the hazards connected with compromised or stolen credentials and preventing unwanted access.

B) Describe in a few sentences, which one of these two mobile device user authentication methods you feel is better, and why. (2.5 Marks)

Ans.

The relative merits of biometric authentication over multi-factor authentication (MFA) are contingent upon the particular security requirements and user experience factors. But generally speaking, MFA is seen as a more reliable method of protecting mobile devices. Although biometric authentication provides robust user identification and ease, it may have drawbacks due to the possibility of biometric data breach or false positives. Nevertheless, MFA adds an extra degree of protection that is less dependent on a single point of attack by combining many authentication elements (such as a password and a physical device). Because of this, it is a flexible and adaptive solution that strikes a balance between security and user ease, making it the go-to option in settings where a higher level of assurance is required.

Reference:

1) Timbó, R. (2023, September 20). *Top 10 practices for mobile application development for 2023*. RSS. https://www.revelo.com/blog/best-practices-for-mobile-application-development
2) *Mobile app development: 10 best practices in 2023 to follow*. KMS Solutions Blog. (n.d.). https://blog.kms-solutions.asia/10-mobile-app-development-best-practices
3) ThoughtSpot, T. (2023, May 2). *15 mobile app Design Best Practices: 2023*. https://www.thoughtspot.com/data-trends/best-practices/mobile-app-design-best-practices
4) Ian Blair Ian is the CEO and Co-Founder of BuildFire. He's a visionary leader and tech-driven strategist running a team and platform that powers 10. (2020, August 24). *17 top mobile app best practices during development*. BuildFire. https://buildfire.com/top-mobile-development-practices/
5) Contributor, T. (2023, July 7). *What is mobile authentication?: Definition from TechTarget*. Security. https://www.techtarget.com/searchsecurity/definition/mobile-authentication
6) Twilio. (2021, November 30). *What is mobile authentication?: Twilio*. Twilio Blog. https://www.twilio.com/blog/mobile-authentication
7) Authentication for mobile devices: Types & effectiveness - study.com. (n.d.). https://study.com/academy/lesson/authentication-for-mobile-devices-types-effectiveness.html
8) User authentication on mobile devices: Approaches, threats and trends. (n.d.-b). https://mosis.eecs.utk.edu/publications/wang2020user.pdf