**Security Recommendation Review: Mobile App Project Phase 6**

Group 6

Jayden L, Honglei C, Parth A, Prabal S

**Security Recommendation**

Our recommendation to implement a custom SSL/TLS security provider refers to the integration of a custom implementation for handling Secure Sockets Layer (SSL) and Transport Layer Security (TLS) connections within the app. This custom provider replaces or enhances the default system provider, such as OpenSSL, which comes with the Android device.

We chose this because a custom security provider can allow a app to control its SSL/TLS connections, reducing reliance on potentially vulnerable system providers. This helps in avoiding known security risks associated with default providers and ensures better protection for sensitive user data.

**Recommendation Benefit**

End Users:

Provides a custom security provider, their data transmission between the app and servers will become more secure. This directly enhances their privacy and protects their sensitive information, such as login credentials and personal data.

Developers:

The recommendation also benefits developers by providing them with more control and flexibility over the app's security. Developers can also customize the security provider the way they want to fit the app's specific requirements, which will ensure optimal security without relying on default system providers.

Stakeholders and Investors:

An app's success and financial stability are less likely to be impacted by security issues when it is secure and has a custom security provider. It gives users peace of mind that the app is taking the appropriate precautions to protect user data, which can be important in luring and keeping investors.

Companies and Businesses:

Implementing a custom security provider enhances the app's reputation for security and reliability. This can lead to increased user trust and retention, which are crucial for the success of the app. Additionally, it helps mitigate the risk of data breaches or security incidents that could harm the company's reputation.

**Recommendation Source**

The recommendation to use a custom security provider is based on industry best practices for Android app security. More details can be found in the Android Developers documentation:

Android Developers - Security Provider:

<https://developer.android.com/privacy-and-security/security-gms-provider>

**When would the recommendation have to be implemented**

The recommendation should be implemented during the development phase of the mobile app project, as it addresses a critical aspect of security. The sooner it's implemented, the better, to mitigate potential security risks from the beginning. Waiting later on can increase more risk and troubleshooting that will have to be involved.

**Why our project needs our recommendation:**

Data Transmission Security:

Our app fetches audio files from remote servers. When these audio files are transmitted over the internet, they are encrypted to protect user privacy. Implementing a custom security provider ensures that these audio files are transmitted securely using HTTPS, preventing potential eavesdropping or tampering of the audio data during transmission.

User Privacy:

Music players often involve user data, such as personalized playlists and account information. A custom security provider ensures that user data transmitted between the app and servers is encrypted, safeguarding sensitive information from unauthorized access. Implementing a custom security provider reflects a commitment to security and user trust. Users are more likely to trust an app that takes measures to secure their data, leading to increased user satisfaction and app reputation.

**How the Recommendation Could Be Applied:**

By the Integration with Expo Audio API, we can add SSL/TLS Support by integrating a custom SSL/TLS library with the Expo Audio API. This will ensure that audio files are fetched and transmitted securely over HTTPS.

As well as implementing certificate pinning within the custom security provider. This involves obtaining the public key hashes of the server's SSL certificate(s) for the audio files. Including these public key hashes in your app's network security configuration to specify which certificates to trust.

We can also add feasibility by implementing a custom security provider with certificate pinning is feasible for your music player app, especially since it involves handling audio files securely. The integration will require adding the necessary libraries and configuration, but it is a common practice in secure app development.

**How feasible is it?**

With the availability of libraries, ease of integration with Expo Audio API, straightforward configuration for certificate pinning, testing/debugging tools, community support, and alignment with best practices, the implementation of a custom security provider with certificate pinning for our music player application is feasible.