**Grantly Tong: Phase 6**

**1. What is your security recommendation? Why did you choose it?**I recommend implementing secure communication using HTTPS to encrypt data exchanged between the app and server, protecting it from interception or tampering. This is essential for safeguarding sensitive user information.

**2. Who does the recommendation benefit (end-user, developer, etc.)?**It benefits end-users by protecting their data and developers by securing the app’s reputation and preventing breaches.

**3. If the recommendation was found somewhere other than the provided checklist, include a link to it.**This recommendation is part of the Android App Security Checklist under secure communication.

**4. When would the recommendation have to be implemented (based on how serious the security risk is)?**It should be implemented early in development to prevent data exposure during testing or release.

**5. Why do you think your project needs your recommendation?**If the app communicates with servers, HTTPS ensures data integrity and protects against unauthorized access, maintaining user trust.

**6. How do you think your recommendation could be applied?**Enable HTTPS on APIs, use SSL/TLS certificates, configure the app to reject HTTP, and verify SSL/TLS certificates on the client side.

**7. How feasible would the implementation be?**This is highly feasible with widely available tools like Retrofit and OkHttp that support HTTPS natively.