mobidev   mobidev.biz   contact@mobidev.biz   ☎ +1 916 243 0946 (USA/Canada)

Andrew Makarov,
Solution Architect and iOS/Android Group Leader at MobiDev

LINKEDIN

Security should be a fundamental consideration from the very beginning. This involves embedding security principles throughout the development lifecycle to anticipate potential risks and design solutions that effectively mitigate threats. By integrating security from the start, you can create more resilient applications that are better equipped to withstand attacks.

Mobile Application Security Checklist

□	**ARCHITECTURE & DESIGN:**	• Design apps with security in mind from the start. • Follow security principles like Least Privilege and Defense in Depth. • Use secure APIs with OAuth2 or JWT for authentication. • Regularly update and rotate API keys or tokens. • Minimize permissions requested and use secure app signing.
□	**AUTHENTICATION & AUTHORIZATION:**	• Perform authentication and authorization on the server-side. • Require strong passwords and implement multi-factor authentication (MFA). • Use platform-specific secure storage for passwords and tokens. • Re-authenticate users for sensitive operations.
□	**DATA STORAGE & PRIVACY:**	• Encrypt sensitive data both at rest and in transit. • Store data securely using platform APIs. • Minimize the storage and retention of Personally Identifiable Information (PII). • Obtain user consent before collecting or using PII.
□	**NETWORK COMMUNICATION:**	• Always use HTTPS for secure communication. • Avoid overriding SSL certificate validation. • Use certificate pinning to prevent man-in-the-middle attacks. • Encrypt data even when using SSL.
□	**USER INTERFACE:**	• Mask sensitive information on UI fields. • Notify users about security-related activities. • Validate and sanitize all user inputs and outputs.
□	**CODE QUALITY:**	• Conduct regular code reviews with a focus on security. • Use static analysis tools to identify vulnerabilities. • Keep libraries and dependencies updated.
□	**APPLICATION INTEGRITY:**	• Disable debugging in production. • Implement code obfuscation and integrity checks.
□	**TESTING:**	• Perform penetration testing to identify vulnerabilities. • Use automated testing to verify security controls. • Ensure security features do not compromise usability.
□	**POST-DEPLOYMENT:**	• Have an incident response plan in place. • Plan for regular updates and patches. • Use monitoring and analytics to detect threats in real-time. • Conduct periodic system audits.

MobiDev can help you with:

- Providing the software audit to identify risks and vulnerabilities in code and infrastructure.
- Creating a comprehensive tech strategy for your current or new product, prioritizing the security of your application.
- Ensuring secure mobile application development by assigning a dedicated development team or augmenting your team with Middle & Senior level mobile app engineers.