WOOLLEMIA INFOSEC

Case Study

Comprehensive Mobile Security Assessment for a Native Android & iOS Banking Application

Industry	Digital Banking & Fintech
Application Type	Native Android (Kotlin) and iOS (Swift) Consumer Banking Applications
Assessment Type	Comprehensive Mobile Application Security Assessment
Technology Landscape	Native Android & iOS Apps, Biometric Authentication, Local Data Storage, Certificate Pinning, Backend REST APIs
Core Services Delivered	Static & Dynamic Application Analysis, Local Data Storage Review, Platform Security Control Testing, API Communication Security Review, Reverse Engineering & Tamper Resistance Testing, Authentication & Session Security Review

Executive Summary

Mobile banking applications operate in one of the most hostile environments in modern software: a device the organization does not control, running alongside untrusted applications, and vulnerable to physical access, rooting, jailbreaking, and reverse engineering. Ensuring these applications protect customer credentials, financial data, and transaction integrity requires assessment techniques specific to the mobile platform.

A digital banking provider engaged Woollemia Infosec to conduct a comprehensive Mobile Security Assessment of its native Android and iOS consumer banking applications ahead of a major release introducing biometric authentication and expanded payment features. The organization wanted independent assurance that both platform versions of its application were resilient against device-level threats, reverse engineering, and insecure data handling.

Woollemia Infosec performed a structured assessment covering static and dynamic application analysis, local data storage security, platform-specific security control implementation, API communication security, and resistance to reverse engineering and tampering, across both the Android and iOS applications.

The assessment enabled the client to remediate critical local data protection and tamper-resistance gaps ahead of launch, strengthening customer trust in its mobile banking experience.

Client Overview

The client offers a digital-first banking experience through native Android and iOS applications, enabling customers to view account balances, transfer funds, pay bills, manage cards, and authenticate using biometric credentials. Both applications communicate with shared backend banking APIs supporting transaction processing, account management, and identity verification.

As the organization prepared to introduce biometric authentication and additional payment capabilities, it recognized the need for an independent, platform-aware security assessment covering both native application codebases.

Business Challenge

The client needed assurance that sensitive data, including session tokens, cached account information, and biometric authentication artifacts, was not insecurely stored on the device in a way that could be extracted by an attacker with physical or malware-based access.

The organization also required validation that its applications could detect and appropriately respond to rooted or jailbroken devices, and that reverse engineering the application binaries would not reveal hardcoded secrets, internal API structures, or bypassable security logic.

Because both applications shared common backend services but were built as fully native codebases in Kotlin and Swift, the client wanted a consistent security evaluation applied to both platforms, accounting for platform-specific security mechanisms and common implementation pitfalls unique to each.

Any weakness allowing session hijacking, credential extraction, or transaction manipulation could directly translate into financial fraud and regulatory exposure for a banking application.

Our Understanding

Woollemia Infosec recognized that securing a native banking application requires evaluating the application binary itself, its runtime behavior on real devices, its use of platform security features, and its communication with backend services as an integrated whole rather than isolated components.

Our team understood that Android and iOS present meaningfully different security models, storage mechanisms, and common developer mistakes, and that a credible mobile assessment must apply platform-specific testing techniques to each application rather than a single generic checklist.

Our Solution

Static Application Analysis

Our consultants performed static analysis of both the Android APK and iOS IPA binaries, reviewing decompiled and disassembled code for hardcoded credentials, API keys, insecure cryptographic implementations, and logic that could reveal internal application behavior.

Dynamic Application Analysis

The applications were tested at runtime on both rooted Android devices and jailbroken iOS devices, observing application behavior, in-memory data handling, and interaction with backend services under active manipulation.

Local Data Storage Security Review

Our team reviewed how each application stored session tokens, cached account data, and biometric authentication references, validating use of platform-appropriate secure storage mechanisms such as the Android Keystore and iOS Keychain rather than insecure local storage or shared preferences.

Platform Security Control Testing

The assessment validated implementation of root and jailbreak detection, certificate pinning, anti-debugging protections, and secure biometric authentication integration using platform-native APIs on each operating system.

API Communication Security Review

Our consultants intercepted and analyzed traffic between each application and its backend banking APIs, testing for certificate pinning bypass, insecure transport configurations, and inconsistent authorization enforcement between the mobile clients and backend services.

Reverse Engineering and Tamper Resistance Testing

The engagement evaluated each application's resistance to reverse engineering and runtime tampering, including code obfuscation effectiveness, binary protection mechanisms, and the ability to bypass client-side security checks through instrumentation frameworks.

Authentication and Session Security Review

Our team reviewed the end-to-end authentication flow including biometric enrollment, fallback authentication, session token issuance, and token lifecycle management across both platforms to confirm consistent security behavior.

Manual Validation and Reporting

Every finding was manually validated on physical Android and iOS devices, with platform-specific proof-of-concept demonstrations, followed by a comprehensive technical report and executive summary covering both applications, mapped to the OWASP Mobile Application Security Verification Standard.

Business Value Delivered

The Mobile Security Assessment gave the client platform-specific visibility into real device-level risks affecting both its Android and iOS banking applications, going well beyond what static scanning tools alone could identify.

The engagement strengthened the organization's confidence in protecting customer credentials and financial data on both major mobile platforms, ahead of introducing biometric authentication and expanded payment features.

By addressing local storage, tamper resistance, and API communication gaps before launch, the client reduced fraud risk and strengthened its regulatory readiness for its mobile banking channel.

Why Woollemia Infosec

Woollemia Infosec delivers platform-aware mobile security assessments covering native Android and iOS applications, combining deep expertise in mobile reverse engineering, platform security architecture, and secure mobile development practices.

Our consultants apply testing techniques specific to each mobile platform, ensuring that Android and iOS applications receive an equally rigorous, appropriately tailored assessment rather than a single generic mobile checklist.

Conclusion

This representative engagement demonstrates Woollemia Infosec's ability to perform comprehensive Mobile Security Assessments across native Android and iOS applications handling sensitive financial data.

By evaluating local data storage, platform security controls, API communication, and tamper resistance, we helped the client establish a stronger security foundation for its mobile banking channel across both major platforms.