The methodology used by Secarma for mobile application assessments is based upon the OWASP Mobile Application Security Verification Standard (version 0.9.2).

A mobile application assessment will include at least the following checks

1. Threat modelling

a) Enumerate 3rd party components
b) Check them for known vulnerabilities
c) Locate client side validation
d) Ensure remote endpoints verify client is up-to-date

2. Data storage and privacy

a) Appropriate storage of credentials/keys
b) Review log files created by application.
c) Examine data being sent to 3rd parties
d) Cache disabled for sensitive data
e) Screenshots disabled for sensitive data

3. Cryptography assessment

a) Ensure use of secure sources of pseudo random number generation.
b) Check encryption for sensitive information stored locally.

4. Authentication and session management

a) Check server-side controls authentication
b) Check server-side controls session management.
c) Enumerate password policy
d) Verify session is terminated after inactivity.

5. Network communication

a) Assure server side TLS is configured securely.
b) Ensure application will not operate over plain-text at any time.
c) Does app verify the server's certificate?
d) Check for second communication channel for critical operations

6. Environmental interaction requirements

a) Ensure all permissions are necessary
b) Verify input validation of data from all external sources is conducted.
c) Confirm JavaScript is disabled in WebViews unless required.
d) Enumerate list of protocols enabled within WebKit
e) Check for "jailbreaking" detection

7. Code quality/build settings

a) Confirm app is signed with a valid certificate
b) Ensure appl was built in "release mode"
c) Check debugging settings
d) Exception handling analysis

8. Reverse engineering defence analysis

a) Confirm that code obfuscation was used.
b) App detects it is running in a virtual environment
c) App encrypts libraries to prevent trivial analysis

Pre-Requisites

- An application assessment is an easy project to facilitate. The following lists the prerequisites required to facilitate the engagement:
- Access to the application so that it can be installed on our devices.
- Knowledge of required operating system versions or device hardware so we can confirm if we can use our devices.
- While optional providing the source code for the mobile application can significantly improve the quality of the output.