App security testing checklist

for Android

In order to excecute the following checks, it is needed to download the following testing guide: https://confluence.securegroup.zone/download/attachments/211946950/MSTG-EN.pdf?version=1&modificationDate=1622559365802&api=v2

Architecture and design

- [ ] All app components are identified and needed.
  Reference points:MSTG-ARCH-1, MSTG-ARCH-7
- [ ] Security controls are enforced not only on the client side, but on the respective remote endpoints.
  Reference points: MSTG-ARCH-2 and MSTG-PLATFORM-2
- [ ] All connected remote services are defined and secured.
  Reference point: Architectural Information
- [ ] Data considered as sensitive in the context of the mobile app is identified.
  (reference point: Identifying Sensitive Data)
- [ ] All app components are has defined business and/or security functions. (reference point: Environmental Information)
- [ ] All security controls have a centralized implementation.
  (reference points: MSTG-ARCH-1, MSTG-ARCH-7)
- [ ] A mechanism for enforcing updates of the mobile app exists.
  (reference point: MSTG-ARCH-9)
- [ ] The app should be complient with privacy laws and regulations.

Data storage

- [ ] System credential storage facilities need to be used to store sensitive data, such as user credentials or cryptographic keys.
  (reference points: MSTG-STORAGE-1 and MSTG-STORAGE-2)
- [ ] No sensitive data is stored outside of the app container or system credential storage.
  (reference points: MSTG-STORAGE-1 and MSTG-STORAGE-2)
- [ ] If sensitive data is still required to be stored locally, it should be encrypted using a key derived from hardware-backed storage which requires authentication.
- [ ] No sensitive data is written to application logs.
  (reference point: MSTG-STORAGE-3)
- [ ] No sensitive data is shared with third parties unless it is a necessary part of the architecture.

(reference point: MSTG-STORAGE-4)

- [ ] The keyboard cache is disabled on text inputs that process sensitive data.
  (reference point: MSTG-STORAGE-5)

- [ ] No sensitive data, such as passwords or pins, is exposed through the user interface.
  (reference point: MSTG-STORAGE-7)

- [ ] No sensitive data is included in backups generated by the mobile operating system.
  (reference point: MSTG-STORAGE-8)

- [ ] The app removes sensitive data from views when moved to the background.
  (reference point: MSTG-STORAGE-9)

- [ ] The app does not hold sensitive data in memory longer than necessary, and memory is cleared explicitly after use.
  (reference point: MSTG-STORAGE-10)

- [ ] The app enforces a minimum device-access-security, such as requiring the user to set a device passcode.
  (reference point: MSTG-STORAGE-11)

- [ ] The app's local storage should be wiped after an excessive number of failed authentication attempts.

Authentication and Session Management

- [ ] If the app provides users access to a remote service, some form of authentication, such as username/password authentication, is performed at the remote endpoint.
  (reference points: MSTG-AUTH-1 and MSTG-STORAGE-11)

- [ ] If stateful session management is used, the remote endpoint uses randomly generated session identifiers to authenticate client requests without sending the user's credentials.
  (reference point: MSTG-AUTH-2)

- [ ] If stateless token-based authentication is used, the server provides a token that has been signed using a secure algorithm.
  (reference point: MSTG-AUTH-3)

- [ ] The remote endpoint terminates the existing session when the user logs out.
  (reference point: MSTG-AUTH-4)

- [ ] A password policy exists and is enforced by the remote endpoint.
  (reference point: MSTG-AUTH-5 and MSTG-AUTH-6)

- [ ] There is a mechanism to protect against the submission of credentials an excessive number of times.
  (reference point: MSTG-AUTH-5 and MSTG-AUTH-6)

- [ ] Sessions are invalidated at the remote endpoint after a predefined period of inactivity and access tokens expire.
  (reference point: MSTG-AUTH-7)

- [ ] Biometric authentication, if any, is not event-bound (i.e. using an API that simply returns "true" or "false"). Instead, it is based on unlocking the keychain/keystore.
  (reference point: MSTG-AUTH-8)

- [ ] Sensitive transactions require step-up authentication.
  (reference points: MSTG-AUTH-9 and MSTG-AUTH-10)

Network Communication

- [ ] Data is encrypted on the network. The secure channel is used consistently throughout the app.
  (reference points: MSTG-NETWORK-1 and MSTG-NETWORK-2)
- [ ] The app verifies the certificate of the remote endpoint when the secure channel is established. Only certificates signed by a trusted CA are accepted.
  (reference point: MSTG-NETWORK-3)
- [ ] The app doesn't rely on a single insecure communication channel (email or SMS) for critical operations, such as enrollments and account recovery.
  (reference point: MSTG-NETWORK-5)

Platform Interactions

- [ ] The app only requests the minimum set of permissions necessary.
  (reference point: MSTG-PLATFORM-1)
- [ ] All inputs from external sources are validated. This includes data received via the UI, IPC mechanisms such as intents, custom URLs, and network sources.
  (reference point: MSTG-PLATFORM-2)
- [ ] The app does not export sensitive functionality via custom URL schemes or IPC mechanisms.
  (reference points: MSTG-PLATFORM-3 and MSTG-PLATFORM-4)
- [ ] JavaScript is disabled in WebViews unless explicitly required.
  (reference point: MSTG-PLATFORM-5)

Code Quality and Build Settings

- [ ] The app is signed with a valid certificate and the private key is properly protected.
  (reference point: MSTG-CODE-1)
- [ ] The app has been built in release mode, with settings appropriate for a release build (e.g. non-debuggable).
  (reference point: MSTG-CODE-2)
- [ ] Debugging code and developer assistance code (e.g. test code, backdoors, hidden settings) have been removed. The app does not log verbose errors or debugging messages.
  (reference point: MSTG-CODE-4)
- [ ] All third-party components used by the mobile app, such as libraries and frameworks, are identified and checked for known vulnerabilities.
  (reference point: MSTG-CODE-5)

- [ ] The app catches and handles possible exceptions.

  (reference point: MSTG-CODE-6)