MASVS-PRIVACY

mas.owasp.org

Closed for comments on the 30th of November 2023. Thank you for contributing!

- The OWASP MAS team -

Introduction

Mobile applications frequently access sensitive user data to deliver their core functionalities. This data ranges from personally identifiable information (PII), health metrics, location data, to device identifiers. Mobile devices are a constant companion to users, always connected, and equipped with numerous sensors—including cameras, microphones, GPS and BLE—that generate data capable of inferring user behavior and even identifying individuals. The landscape is further complicated by advanced tracking techniques, the integration of third-party SDKs, and a heightened awareness of privacy issues among users and regulators. As a response, there's a growing trend towards on-device processing to keep user data localized and more secure.

It's crucial to protect this data both to gain the trust of users and to comply with global privacy regulations, such as the General Data Protection Regulation (GDPR) in Europe, the Children's Online Privacy Protection Rule (COPPA) and the California Consumer Privacy Act (CCPA) in the U.S., and similar legislation being considered by governments and regulators around the world.

With data becoming a valuable asset for many businesses, apps frequently incorporate third-party tools, such as Software Development Kits (SDKs), to analyze user activity or display ads. These tools can sometimes collect and share data with other companies, often without the clear knowledge or consent of the user. Beyond that, many of these third-party tools monetize the collected data by building services on top of it. They can also create separate data intelligence offerings, such as analytics databases, further enriching their own ecosystem at the expense of user privacy.

While making sure the app handles data securely—ensuring its confidentiality, integrity, and availability—is a basic step for an effective data protection strategy (addressed by other categories of the current OWASP Mobile Application Security Verification Standard (MASVS) such as MASVS-STORAGE, MASVS-CRYPTO, or MASVS-NETWORKING), it's distinct from the broader concept of data privacy. Data security focuses on safeguarding data from unauthorized access, while data privacy emphasizes the rights of users and how data is collected, processed, stored, and shared. This category takes the OWASP MASVS a step further, looking deeper into the challenges of adding privacy features in mobile apps. It's designed to guide developers and analysts in making sure data is used, stored, and shared in a way that respects user privacy and conforms to best practices. It does so by following a “privacy by design and by default” approach, accentuating core principles like data minimization, unlinkability, transparency, and intervenability.

Scope

The main goal of MASVS-PRIVACY is to provide a baseline for user privacy. It is not intended to cover all aspects of user privacy, especially when other standards and regulations such as ENISA or the GDPR already do that. We focus on the app itself, looking at what can be tested using information that's publicly available or found within the app through methods like static or dynamic analysis.

While some associated tests can be automated, others necessitate manual intervention due to the nuanced nature of privacy. For example, if an app collects data that it didn't mention in the app store or its privacy policy, it takes careful manual checking to spot this.

Note on "Data Collection and Sharing"

For the MASTG tests, we treat "Collect" and "Share" in a unified manner. This means that whether the app is sending data to another server or transferring it to another app on the device, we view it as data that's potentially leaving the user's control. Validating what happens to the data on remote endpoints is challenging and often not feasible due to access restrictions and the dynamic nature of server-side operations. Therefore, this issue is outside of the scope of the MASVS.

Important Disclaimer

MASVS-PRIVACY is not intended to serve as an exhaustive or exclusive reference. While it provides valuable guidance on app-centric privacy considerations, it should never replace comprehensive assessments, such as a Data Protection Impact Assessment (DPIA) mandated by the General Data Protection Regulation (GDPR) or other pertinent legal and regulatory frameworks. Stakeholders are strongly advised to undertake a holistic approach to privacy, integrating MASVS-PRIVACY insights with broader assessments to ensure comprehensive data protection compliance. Given the specialized nature of privacy regulations and the complexity of data protection, these assessments are best conducted by privacy experts rather than security experts.

References & Related work:

- OWASP MASTG - Mobile App User Privacy Protection
- General Data Protection Regulation (GDPR)
- Children's Online Privacy Protection Rule (COPPA)
- California Consumer Privacy Act (CCPA)
- ENISA - Privacy and data protection in mobile applications
- IEEE - Engineering Privacy in Smartphone Apps: A Technical Guideline Catalog for App Developers
- Google - Privacy best practices
- Google - Provide information for Google Play's Data safety section
- Apple - User privacy and data use
- Apple - App privacy details on the App Store

Controls

MASVS-PRIVACY-1

The app minimizes access to sensitive data and resources.

Apps should only request access to the data they absolutely need for their functionality and always with informed consent from the user. This control ensures that apps practice data minimization and restricts access control, reducing the potential impact of data breaches or leaks.

Furthermore, apps should share data with third parties only when necessary, and this should include enforcing that third-party SDKs operate based on user consent, not by default or without it. Apps should prevent third-party SDKs from ignoring consent signals or from collecting data before consent is confirmed.

Additionally, apps should be aware of the 'supply chain' of SDKs they incorporate, ensuring that no data is unnecessarily passed down their chain of dependencies. This end-to-end responsibility for data aligns with recent SBOM regulatory requirements, making apps more accountable for their data practices.

MASVS-PRIVACY-2

The app prevents identification of the user.

Protecting user identity is crucial. This control emphasizes the use of unlinkability techniques like data abstraction, anonymization and pseudonymization to prevent user identification and tracking.

Another key aspect addressed by this control is to establish technical barriers when employing complex 'fingerprint-like' signals (e.g. device IDs, IP addresses, behavioral patterns) for specific purposes. For instance, a fingerprint used for fraud detection should be isolated and not repurposed for audience measurement in an analytics SDK. This ensures that each data stream serves its intended function without risking user privacy.

MASVS-PRIVACY-3

The app is transparent about data collection and usage.

Users have the right to know how their data is being used. This control ensures that apps provide clear information about data collection, storage, and sharing practices, including any behavior a user wouldn't reasonably expect, such as background data collection. Apps should also adhere to platform guidelines on data declarations.

MASVS-PRIVACY-4

The app offers user control over their data.

Users should have control over their data. This control ensures that apps provide mechanisms for users to manage, delete, and modify their data, and change privacy settings as needed (e.g. to revoke consent). Additionally, apps should re-prompt for consent and update their transparency disclosures when they require more data than initially specified.

Tests

In privacy testing, much like with security, the specific context and use case play a big role. While some tests might not show an outright violation, they're designed to provide clear and relevant evidence. This ensures that a reviewer can make a well-informed decision about potential issues.

A prerequisite for privacy testing with the MASTG, is to clearly identify data considered sensitive in the context of the mobile app and to understand how both the first-party and any third-party partners utilize each type of data. For instance, if your app gathers an email address for user authentication and to tailor their experience, that touches on both App Functionality and Product Personalization. To get a clearer picture of these nuances, it's a good idea to refer to resources like Apple's App Privacy Details and Google Play's Data Usage Guidelines.

MASVS-PRIVACY-1: The app minimizes access to sensitive data and resources.

- Validate Data Access Scope
  Description: Ensure the app only accesses data essential for its functionality.
    - Ensure metadata with data protection relevance is removed when using device sensors (e.g. camera, microphone).
    - Erase personal data as soon as its purpose is fulfilled.

- Permission Management
  Description: Ensure only necessary permissions are requested when they are really needed.
    - Review permissions required by the app.
    - Review permissions required by third-party libraries and SDKs.
    - Use privacy-friendly APIs provided by the platform as alternatives to permissions (e.g. use the Photo Picker API instead of the storage permission; when pairing a device with BLE don’t ask for location; if location is needed, ask for coarse location).
    - Avoid platform-signed permissions when possible.
    - Confirm permissions are requested contextually (e.g., accessing the camera when taking a photo) and not just at app startup.
        - E.g. list permissions requested at app startup vs later.
        - Trace APIs that require permission usage. If possible, trace when the app accesses protected resources (from the OS side), the same way that the Privacy Dashboard an android and the Privacy Report does on iOS.
    - Check if permissions are revoked when no longer needed.

MASVS-PRIVACY-2: The app prevents identification of the user.

- Anonymization and Pseudonymisation Measures
  Description: Ensure techniques like anonymisation and pseudonymisation are implemented to prevent user identification.
    - Stripping data of any direct identifiers, such as user ID or name, before server-side collection.
    - Manipulating data to break the linkage and prevent re-linkage to real-world identities.
    - Check for use of Private (Information) Retrieval protocols and OHTTP (Oblivious HTTP).

- Identifier Management Review
  Description: Avoid using identifiers that are unique, or probabilistically unique. Instead, opt for identifiers that can be reset, except for user safety purposes when there are no alternative methods available. If you use advertising IDs, make sure they are only used for advertising purposes.
    - Only use an advertising ID for user profiling or ad-serving use cases.
    - For non-ad-serving use cases, use a privately stored globally-unique ID (GUID), which is app-scoped.
    - Check for identifiers generated using device or network data for the purpose of uniquely identifying a device.
    - Use the secure settings Android ID (SSAID) to share state between the apps that you own without requiring the user to sign in to an account (Android).

MASVS-PRIVACY-3: The app is transparent about data collection and usage.

- Consent Management and User Awareness
  Description: Obtain explicit user consent before accessing sensors or local data.
    - Check for informative notifications or prompts.
    - Review purpose strings explaining data access needs.

- Data Collection and Sharing
  Description: Ensure sensitive data isn't shared with third parties unless necessary and users are informed both from the app and third-party code.
    - Ensure adherence to platform guidelines on data declarations.
    - Review data sent to app servers.
    - Review data sent to trackers.
    - Prevent data exchange between apps unless explicitly specified or chosen by the user.
    - Ensure local data processing mechanisms are prioritized (e.g. iOS on-device processing or Android On-Device Machine Learning and Private Compute Services).
    - Provide the user with a list of each third party with whom information about the user is shared, identify the categories of data shared with each third party, and provide links to those parties.

- Privacy Policy Validation
  Description: Ensure a privacy policy is provided.
  - Check if a URL for the app's privacy policy is provided in the app store and the app itself.
  - Check that users are informed about data flow, third-party sharing, protection measures, and their data rights.
  - Check privacy policy declarations and compare with app actual behavior.

- App Store Declaration Consistency
  Description: Compare store declarations with the app's privacy policy and actual behavior.
  - Check store declarations and compare with privacy policy.
  - Check store declarations and compare with app actual behavior.

MASVS-PRIVACY-4: The app offers user control over their data.

- Data Management Mechanisms
  Description: Ensure mechanisms are in place for users to delete all their data and modify privacy settings with granularity.
  - Offer mechanisms to delete all user data.
  - Allow users to modify privacy settings with granularity and revert to default settings.

MAS-P - Baseline Privacy Profile

The MAS-P profile establishes a foundational set of practices mobile apps should comply with to safeguard users' personally identifiable information (PII) and ensure compliance with prevailing data protection regulations.

MAS-P serves as a baseline for privacy and is intended to work cohesively, and in some cases even overlap, with other OWASP MAS profiles, such as MAS-L1 and MAS-L2, ensuring a holistic approach to both security and privacy.