Abstract

Apple’s app privacy labels aim to help users easily understand an app’s privacy practices. However, misleading labels can trick privacy-aware consumers into data-intensive apps, diminishing the labels’ credibility. Lalaine is the first systematic study to evaluate the consistency of data-flow to privacy labels, analyzing 5,102 iOS apps to assess the extent of label non-compliance and its implications.

Contribution

Lalaine - the first large-scale and comprehensive study for privacy label compliance.

A formalized consistency model

An end-to-end detection tool

Root causes analysis & cases study

Apple’s Stance on Privacy: A Paradigm Shift – Privacy Label

Apple's app privacy labels aim to help users easily understand an app’s privacy practices. However, misleading labels can trick privacy-aware consumers into data-intensive apps, diminishing the labels’ credibility. Lalaine is the first systematic study to evaluate the consistency of data-flow to privacy labels, analyzing 5,102 iOS apps to assess the extent of label non-compliance and its implications.

Consistency Model

• Data protection principles: data minimization, purpose limitation
• Consistency model: a type of policy language to facilitate automatic compliance check.

Design & Implementation

Apple Store

Apple’s Stance on Privacy: A Paradigm Shift – Privacy Label

Apple’s app privacy labels aim to help users easily understand an app’s privacy practices. However, misleading labels can trick privacy-aware consumers into data-intensive apps, diminishing the labels’ credibility. Lalaine is the first systematic study to evaluate the consistency of data-flow to privacy labels, analyzing 5,102 iOS apps to assess the extent of label non-compliance and its implications.

Consistency Model

• Data protection principles: data minimization, purpose limitation
• Consistency model: a type of policy language to facilitate automatic compliance check.

Take aways

Pervasive non-compliance app

• The privacy label non-compliance in iOS apps is prevalent, with a serious impact on credible and transparent disclosure of app privacy practices.
• The root causes of privacy label non-compliance are diverse.
• We are reporting all findings (non-compliant privacy labels) to Apple.

Recommendations for Stakeholders

• Apple: A comprehensive ontology of sensitive data items/sensitive API
• SDK Vendors: improve data transparency and guidance accuracy for privacy labels.
• App Developer: sanitize SDKs to understand their data practices.

Apple’s stance on privacy: A paradigm shift – Privacy label

Apple’s Stance on Privacy: A Paradigm Shift – Privacy label

Apple’s app privacy labels aim to help users easily understand an app’s privacy practices. However, misleading labels can trick privacy-aware consumers into data-intensive apps, diminishing the labels’ credibility. Lalaine is the first systematic study to evaluate the consistency of data-flow to privacy labels, analyzing 5,102 iOS apps to assess the extent of label non-compliance and its implications.

Consistency Model

• Data protection principles: data minimization, purpose limitation
• Consistency model: a type of policy language to facilitate automatic compliance check.

Take aways

Pervasive non-compliance app

• The privacy label non-compliance in iOS apps is prevalent, with a serious impact on credible and transparent disclosure of app privacy practices.
• The root causes of privacy label non-compliance are diverse.
• We are reporting all findings (non-compliant privacy labels) to Apple.

Recommendations for Stakeholders

• Apple: A comprehensive ontology of sensitive data items/sensitive API
• SDK Vendors: improve data transparency and guidance accuracy for privacy labels.
• App Developer: sanitize SDKs to understand their data practices.