Objective

- Understand how users respond to security warnings reported by malware detection tools, and design techniques to facilitate user assistance.
- Understand how users respond to privacy statements accompanying apps and design techniques to facilitate user assistance.

Motivation

- Existing privacy/security analysis techniques lack precision (static analysis) or completeness (dynamic analysis).
- Existing techniques report suspicious behaviors without involving users to deal with these behaviors.
- Existing techniques lack privacy customizations to preserve user privacy at different levels to deliver a private yet user-desirable level of utility efficacy.
- Incorporate user assistance for app exploration and abnormal-behavior detection.
- Support user validation of malicious-app candidates via program-repair techniques.
- Sanitize users' app usage data to balance between privacy preservation and utility efficacy.

Yin-Yang View on Mobile App Security

- To comprehensively characterize expectation contexts and security behaviors, and check their consistency.

Analysis for Removal of Unwanted Behaviors

Unwanted-behavior Removal

- A general framework, SMAR (Systematic Mobile App Repair)
- SMAR is a suite of strategies to repair apps at all four levels: "where", "when", "what", "how".

Impact Analysis of Behavior Removal

- Identify isolated components of the app, and provide assurance that the app functionalities residing in other components remain unaffected.
- Perform change impact analysis for functionalities within isolated components.

Goal of Our System:

- To comprehensively characterize expectation contexts and security behaviors, and check their consistency.

Flexible Choices – Removing Unwanted Behaviors

- Users can experience the app without making compromises in privacy/security.
- Users can change configurations after experiencing the app.

Challenge: balance users’ privacy and the app’s functionalities.

Goal: maximize functionalities while minimizing the amount of sensitive information exposed.

Solution: a privacy framework to

- Leverage dynamic UI rendering, geometrical layout analysis, and NLP to identify sensitive input fields.
- Anonymize each input, and dynamically measure its impact on the functionalities of an app.
- Conduct analysis to verify against declared privacy policy.
- Analyze privacy specification and app functionality.