User-Centric Mobile Security Assessment

Wing Lam, Dengfeng Li, Wei Yang, Tao Xie

(University of Illinois at Urbana-Champaign, email: taoxie@illinois.edu)

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 facilitating users to deal with these behaviors.
- Existing techniques lack privacy customization to preserve user privacy at different levels to deliver a private-yet-desirable level of utility efficacy.

Approaches

- 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.

Dynamic Detection of Suspicious Behaviors Assisted by Users

User-assisting behavior abstraction

- Abstract low-level code into high-level behavior descriptions, facilitating users to investigate.
- Dynamically update abstraction functions based on users’ feedback to ensure abstraction efficacy.
- Collect evidence for users to report suspicious apps.
- Complement other techniques (e.g., checking against app’s description).

User-assisting behavior exploration

- During exploration, request users’ intervention when a certain app state cannot be achieved by an automatic event-generation engine.
- Prompt event-generation requests to users such as logging in.

Suspicious-behavior detection

- Allow users to define high-level security/privacy rules to monitor apps.

Analysis on Removal of Unwanted Behaviors

Unwanted-behavior removal

- A general framework, Smar (Systematic Mobile App Repair)
- A suite of repair strategies to repair the 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.

Privacy-Preserving Mobile Utility Apps: A Balancing Act

- Expected behavior: Video game for killing pigs.
- Unexpected behavior: Phone and location used for advertising.

Challenge: balance users’ privacy and utility app’s functionality.

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

A privacy framework

- 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.

This material is based upon work supported by the Maryland Procurement Office under Contract No. H98230-14-C-0141