User-Centric Mobile Security Assessment

Dengfeng Li , Wei Yang, Wing Lam, 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.

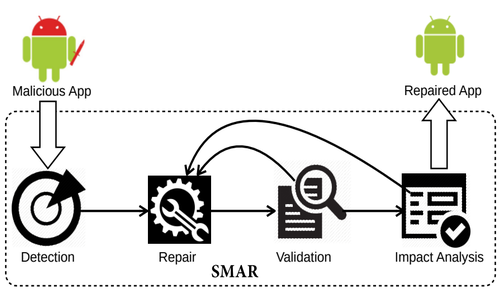
Motivation

- Existing privacy/security analysis techniques lack precision (static analysis) or completeness (dynamic analysis).
- Existing techniques report suspicious behaviors without 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.

Analysis for Removal of Unwanted Behaviors

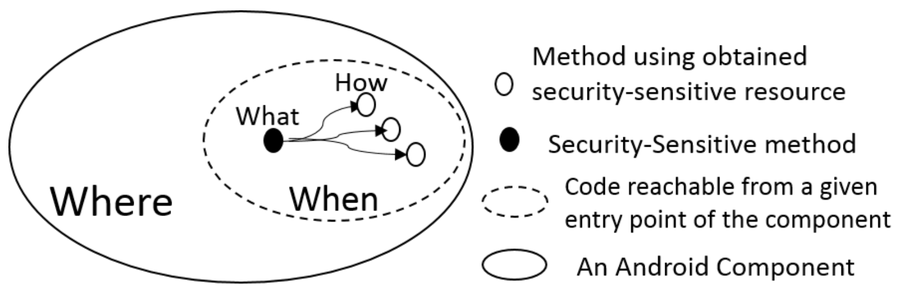
Unwanted-behavior Removal

- 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".



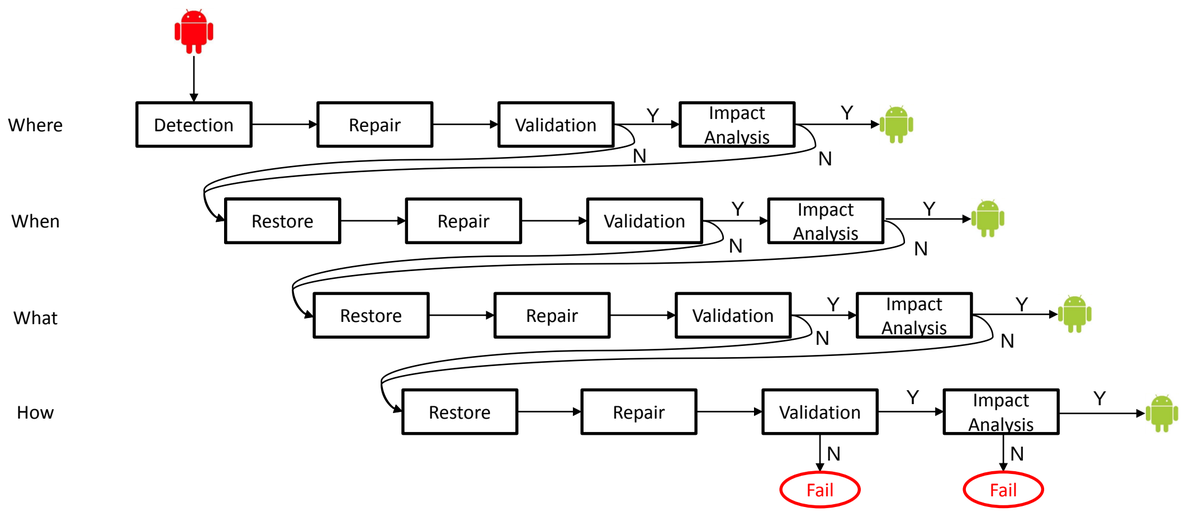
Impact Analysis of Behavior Removal

- 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.



Flexible Choices – Removing Unwanted Behaviors

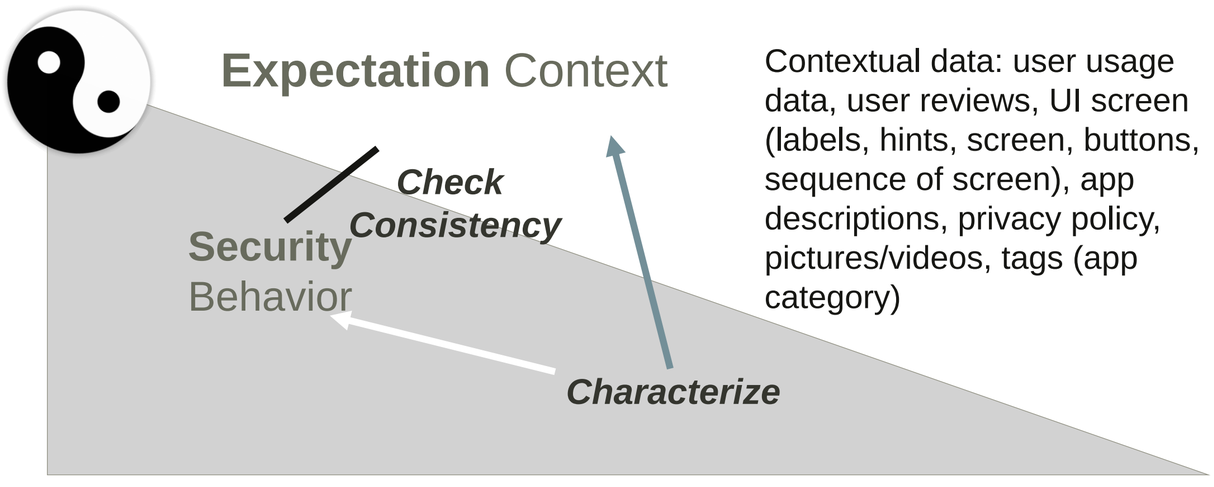
- Users can experience the app without making compromises in privacy/security.
- Users can change configurations after experiencing the app.



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.

Yin-Yang View on Mobile App Security



Goal of Our System:

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

Run-time Inconsistency – Example

•Expectation Context: Movies are loading

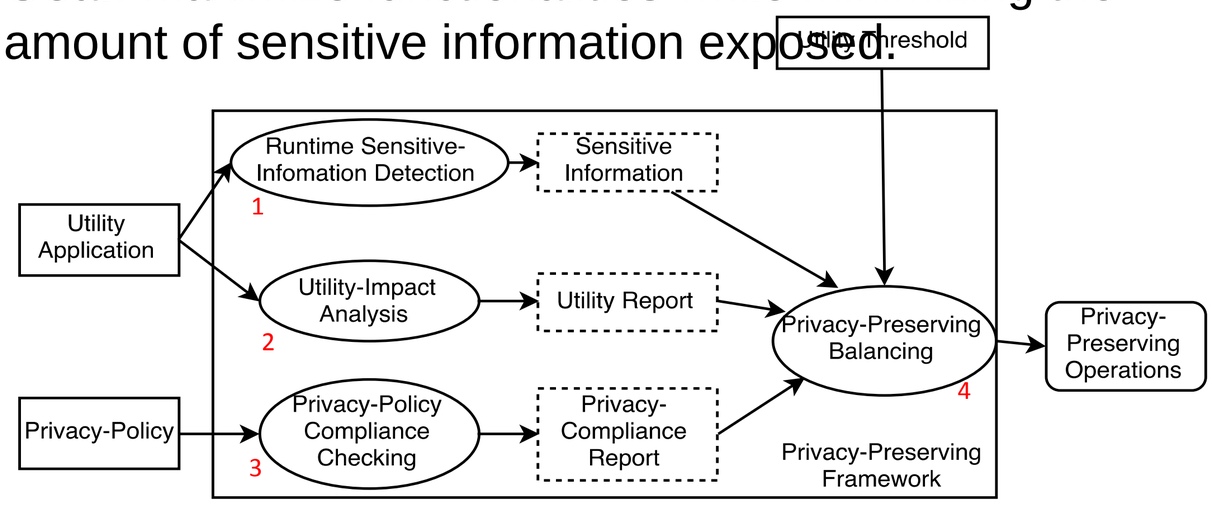

```
POST /get45.php HTTP/1.1
Content-Length: 173
Content-Type: application/x-www-form-urlencoded
Host: d[redacted].jp
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

id=12345&tel=15555215554&data=name%3AContact1%09tel%3A11111111111%09email%3Acontact1%
40domain.com%0Aname%3AContact2%09tel%3A222-222-222222%09email%3Acontact2%40domain.com%
0AHTTP/1.1 200 OK
Date: Thu, 12 Apr 2012 19:12:10 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

- **Unexpected behavior:** Sensitive information (e.g., IMEI, phone #, location) is sent to unknown host

Privacy-Preserving Mobile Utility Apps: A Balancing Act

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.

SCIENCE OF SECURITY
VIRTUAL ORGANIZATION
Funded by the National Security Agency.

INFORMATIONTRUST INSTITUTE

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