Improving Mobile Application Security via Bridging User Expectations and Application Behaviors

Wei Yang
Univ. of Illinois

Xusheng Xiao **Rahul Pandita** **William Enck**
NC State Univ.

Tao Xie
Univ. of Illinois

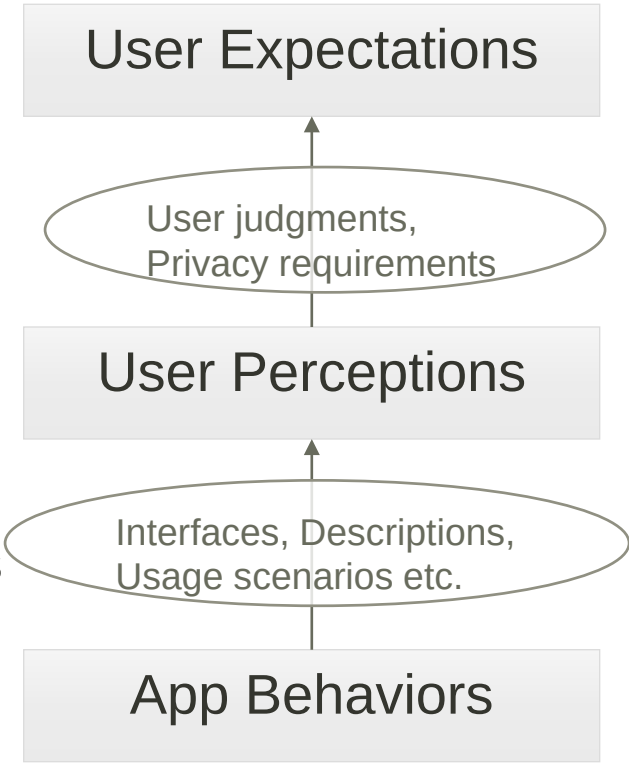
UNIVERSITY OF ILLINOIS
AT URBANA-CHAMPAIGN

illinois.edu

User Expectations and App Behaviors

- **User expectations** are reflected via **user perceptions** of **app behaviors** (in combination with user judgments)

- There are ***gaps*** btw. user perceptions and application behaviors
  - Some application behaviors may be user imperceptible, or contradict w/ user perceptions
  - The user may not be able to make right judgments based on perceived information

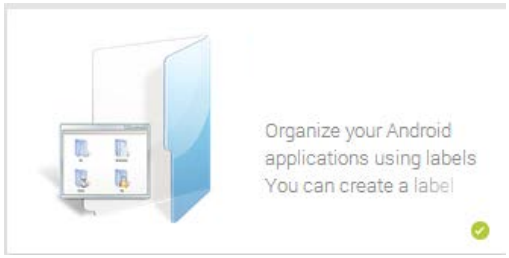


WHYPER: Automated Risk Assessment

[Pandita et al. USENIX Security'13]

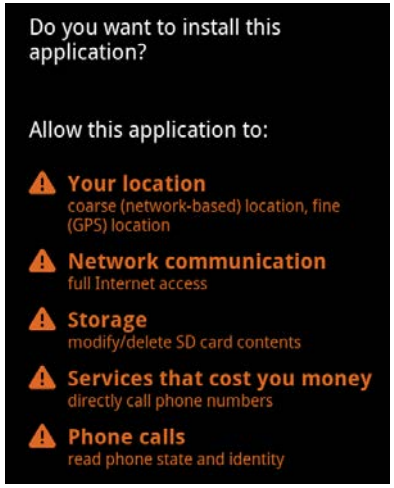
- User Perceptions: **App Description**
- App Behaviors: **Permission Request/Use**
- A framework using NLP techniques to construct traceability between a sentence in app description ←→ a permission of an app

App Description



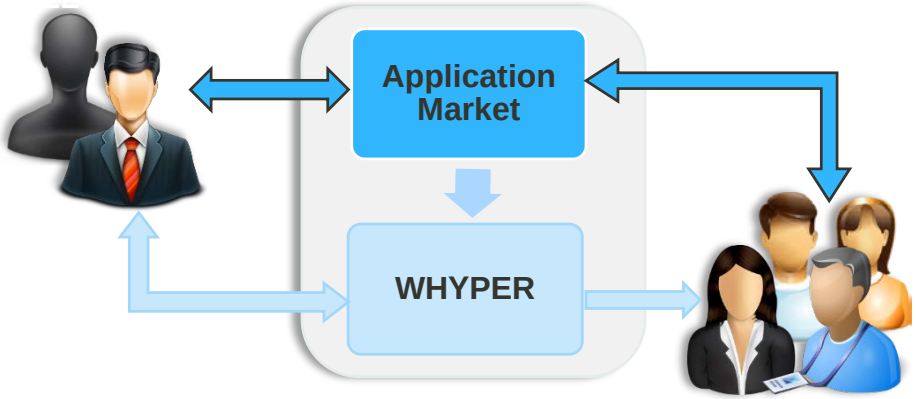
Links

Permission List



WHYPER Use Cases

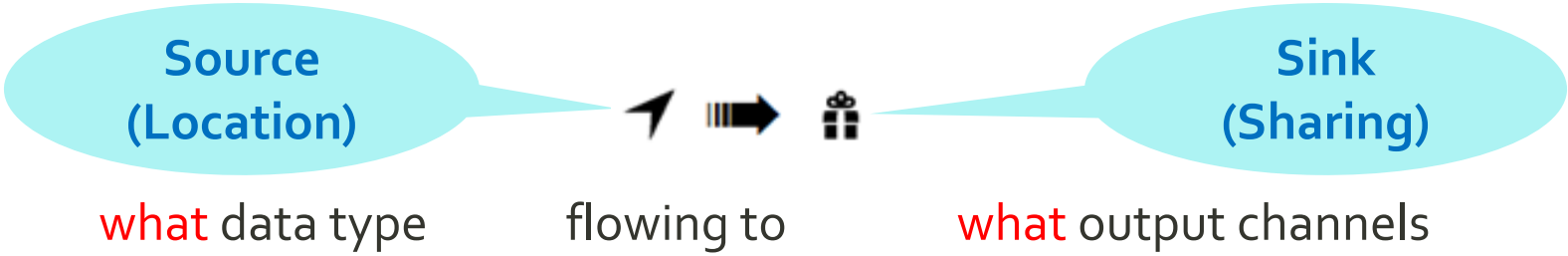
- Enhance user experience while installing apps
- Enforce functionality disclosure on developers
- Complement program analysis to ensure more appropriate justifications



User-Aware Privacy Control

[Xiao et al. ASE'12]

- User Perceptions: **Inspected Outgoing Info**
- App Behaviors: **Info Flows**



- User-awareness of **shared data instances** at **runtime** monitored sink via user inspection

Escaping/Tampering Flows

- Notify users of potential information leak
  - escaping flows – info may flow to output channels (e.g., network sockets) where users cannot inspect
  - tampering flows – info may be tampered before the info is presented to users for inspection