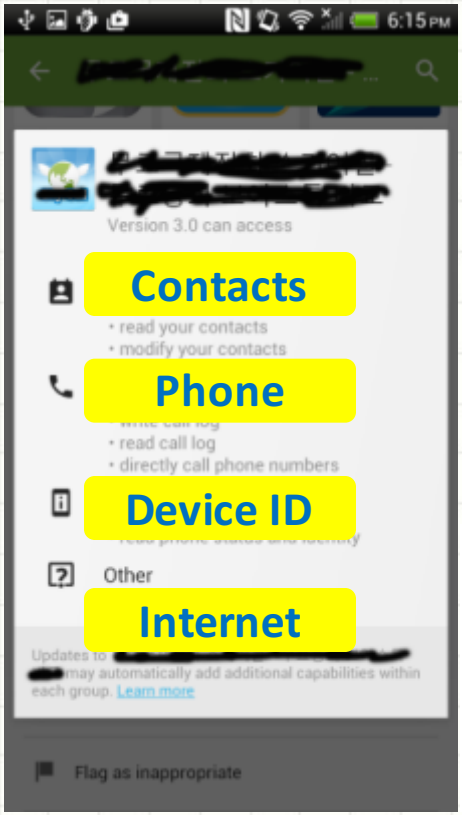
Towards Automatic Generation of Security-Centric Descriptions for Android Apps

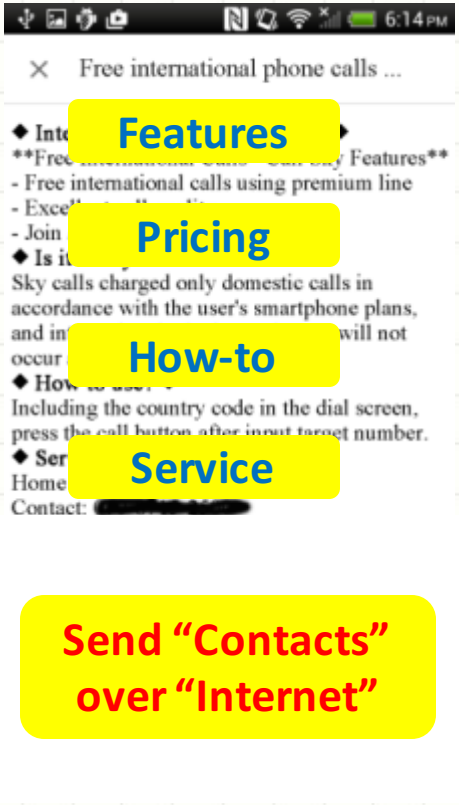
Mu Zhang (NEC Labs)
Yue Duan (Syracuse Univ.)
Qian Feng (Syracuse Univ.)
Heng Yin (Syracuse Univ.)

Motivation: Limitation of App Descriptions

Permissions:

1) **Hard to read.** *Felt et al. (SOUPS'12)*
2) **Insufficient to tell "HOW"**



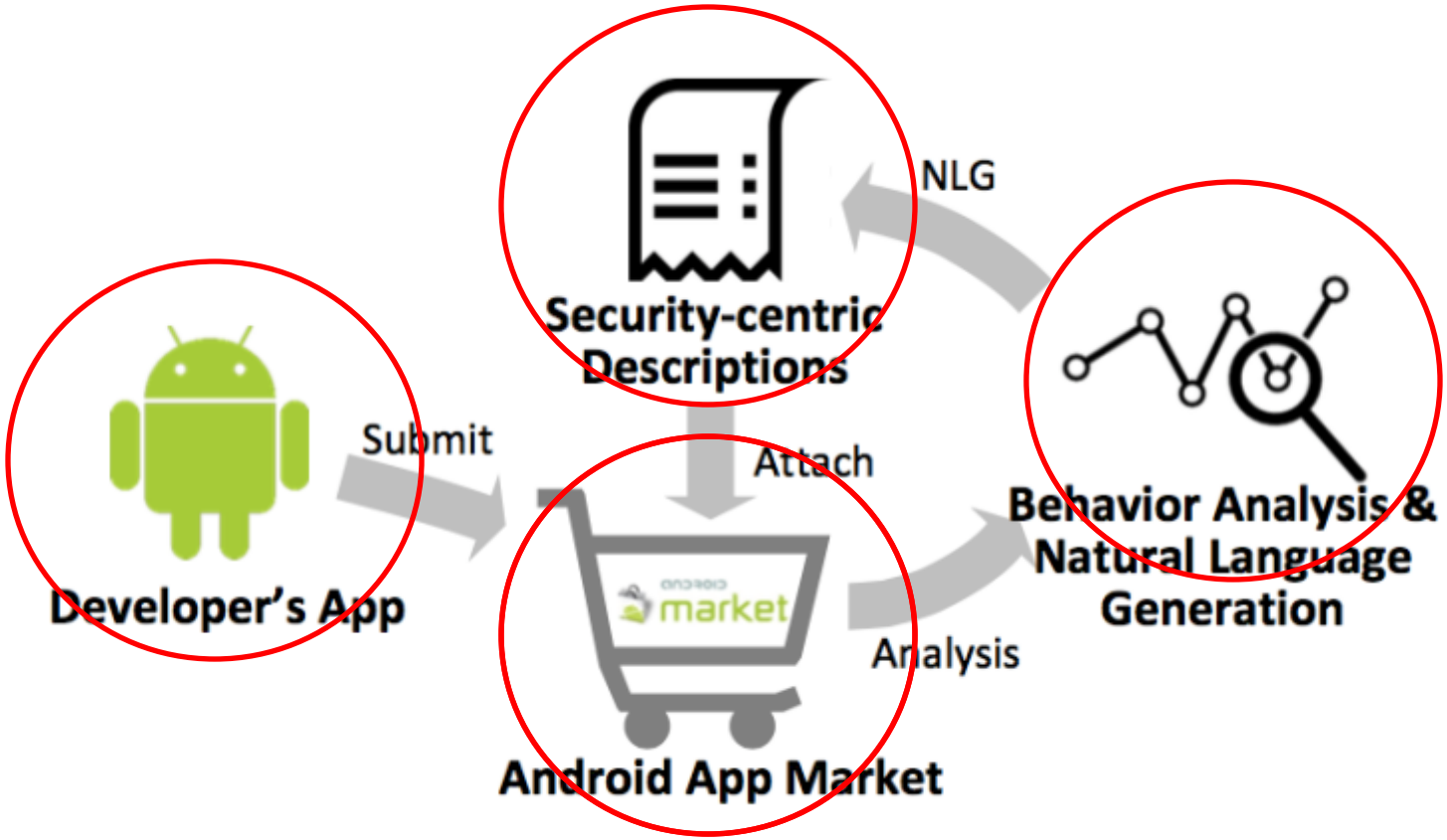


Send "Contacts" over "Internet"

Textual Desc.: Not really about security.
WHYPER (Security'13)
AutoCog (CCS'14)

What an app claims to do **vs.** **What the app actually does**

DESCRIBEME: Automatically Deriving Textual Descriptions from Android Program Code



Existing Work: Automated Java Program Summarization

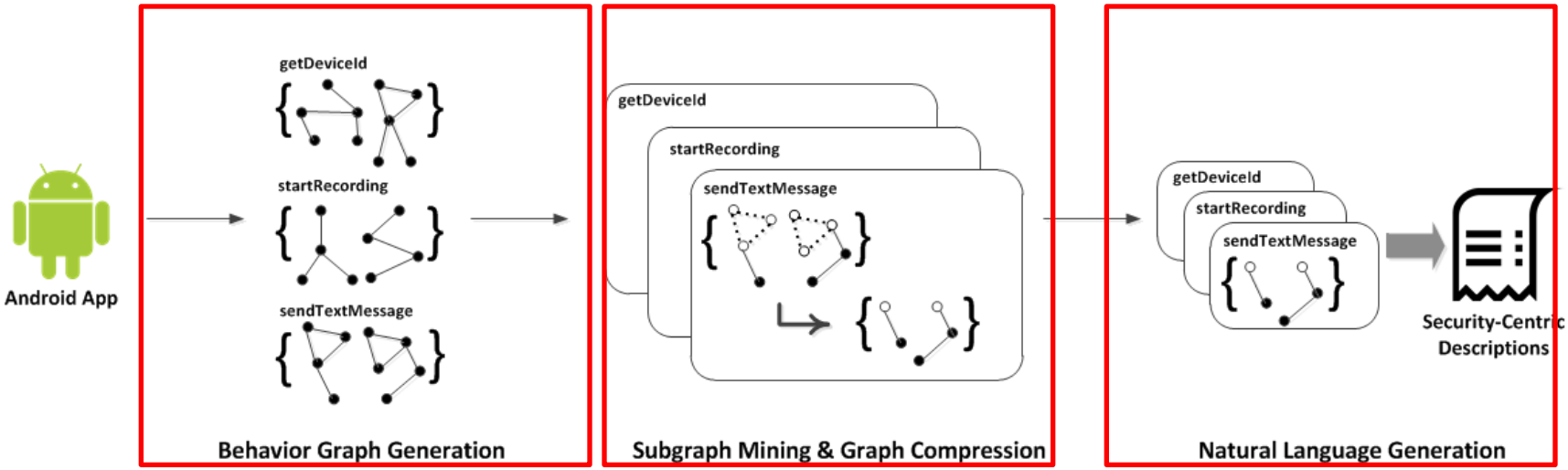
- In Software Engineering Context
  - **Java Methods** (*ASE'10*)
  - **Method Parameters** (*ICPC'11*)
  - **Classes** (*ICPC'13*)
  - **Conditional Statements** (*ASE'10*)
  - **Algorithmic Structure** (*ICSE'11*)
- We are dealing with a **DIFFERENT** problem

	Existing Work	DescribeMe
Purpose	Review legacy code	Understand security risks

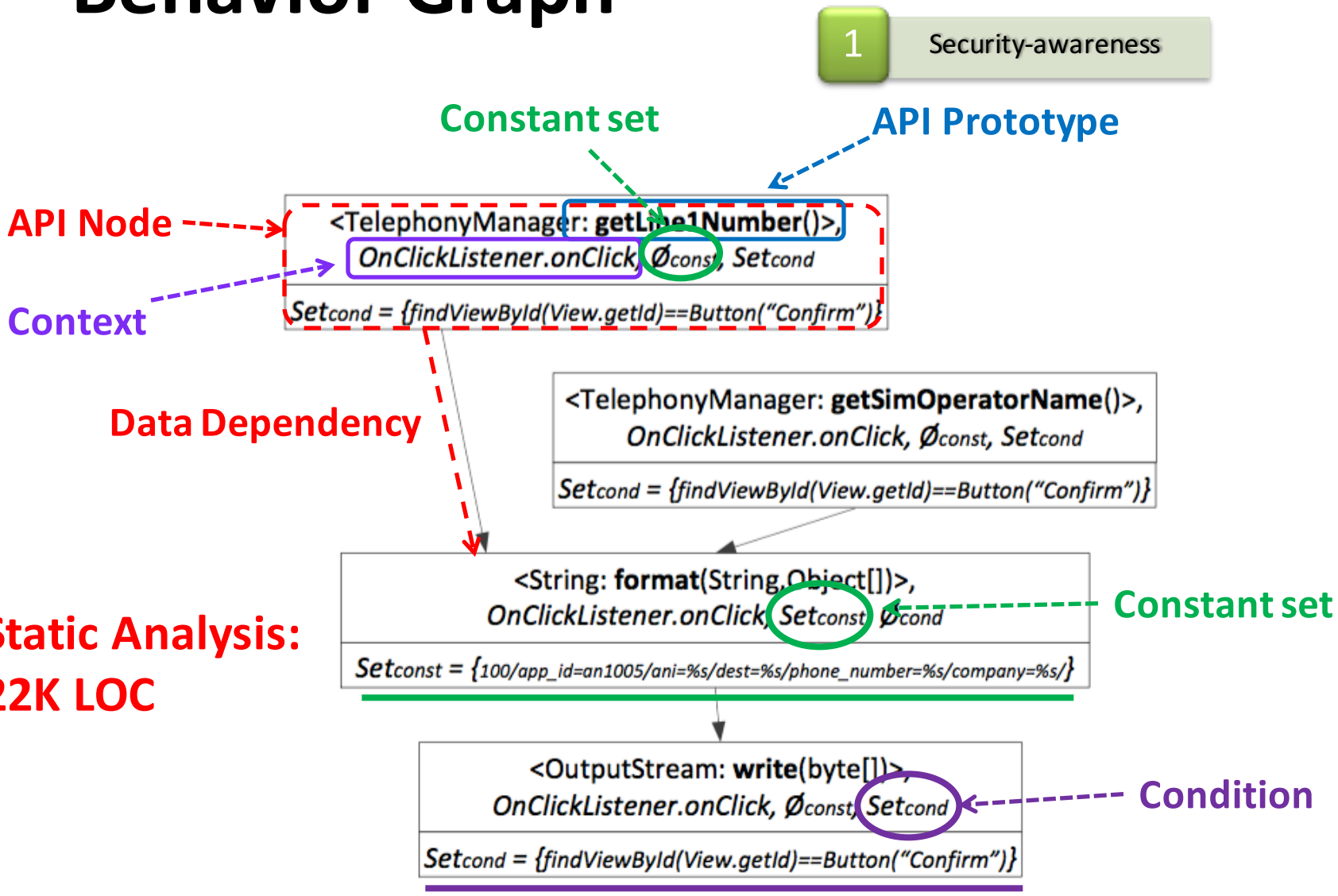
Challenges & Requirements

1. Security-awareness
2. Conciseness
3. Human-understandability

Approach Overview



Behavior Graph



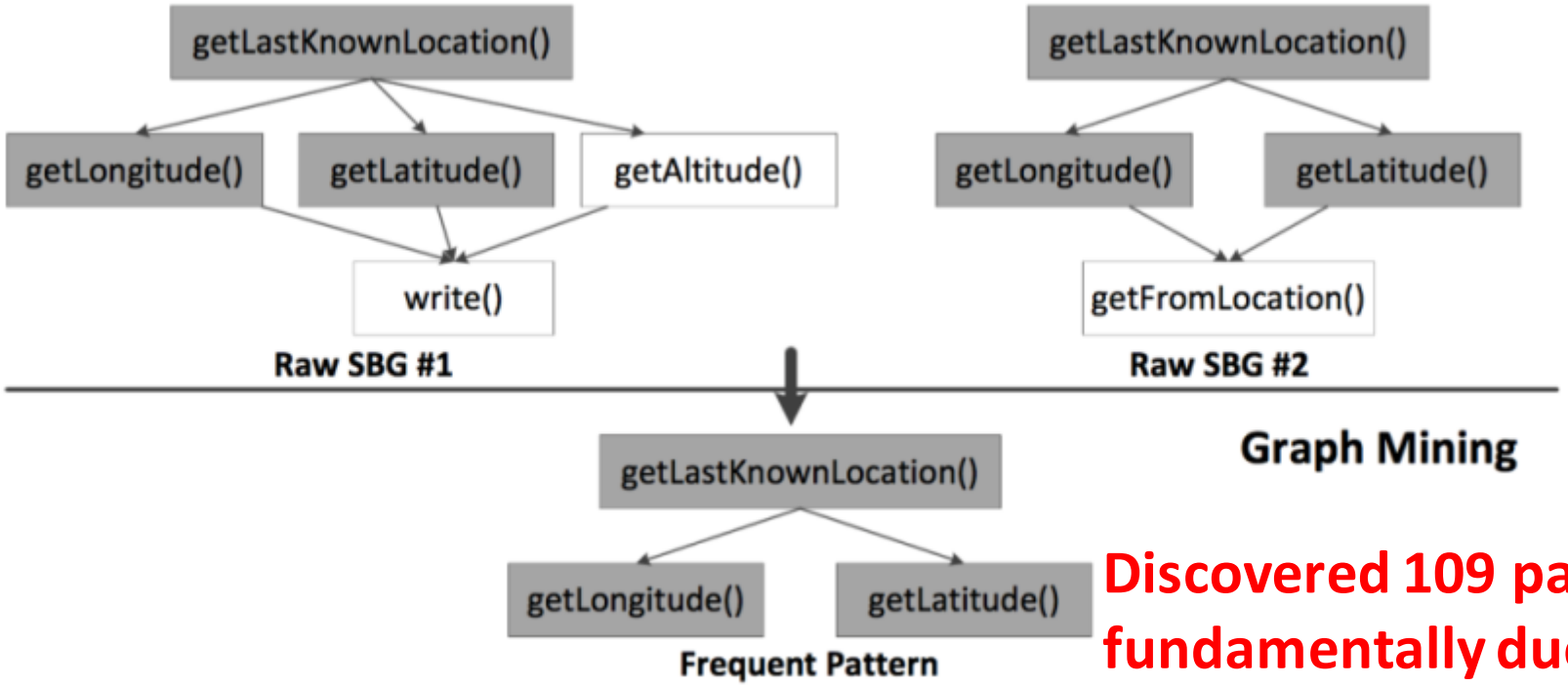
Condition Analysis

3 Human-understandability

- Extract only **user-aware** conditions
  - **User Interface**
  - **Device Status**
  - **Natural Environment**
- Present **simple logic** to users
  - **Equation/Inequation**

Our condition analysis is focused only on the conditions that users can observe and evaluate.

Subgraph Mining



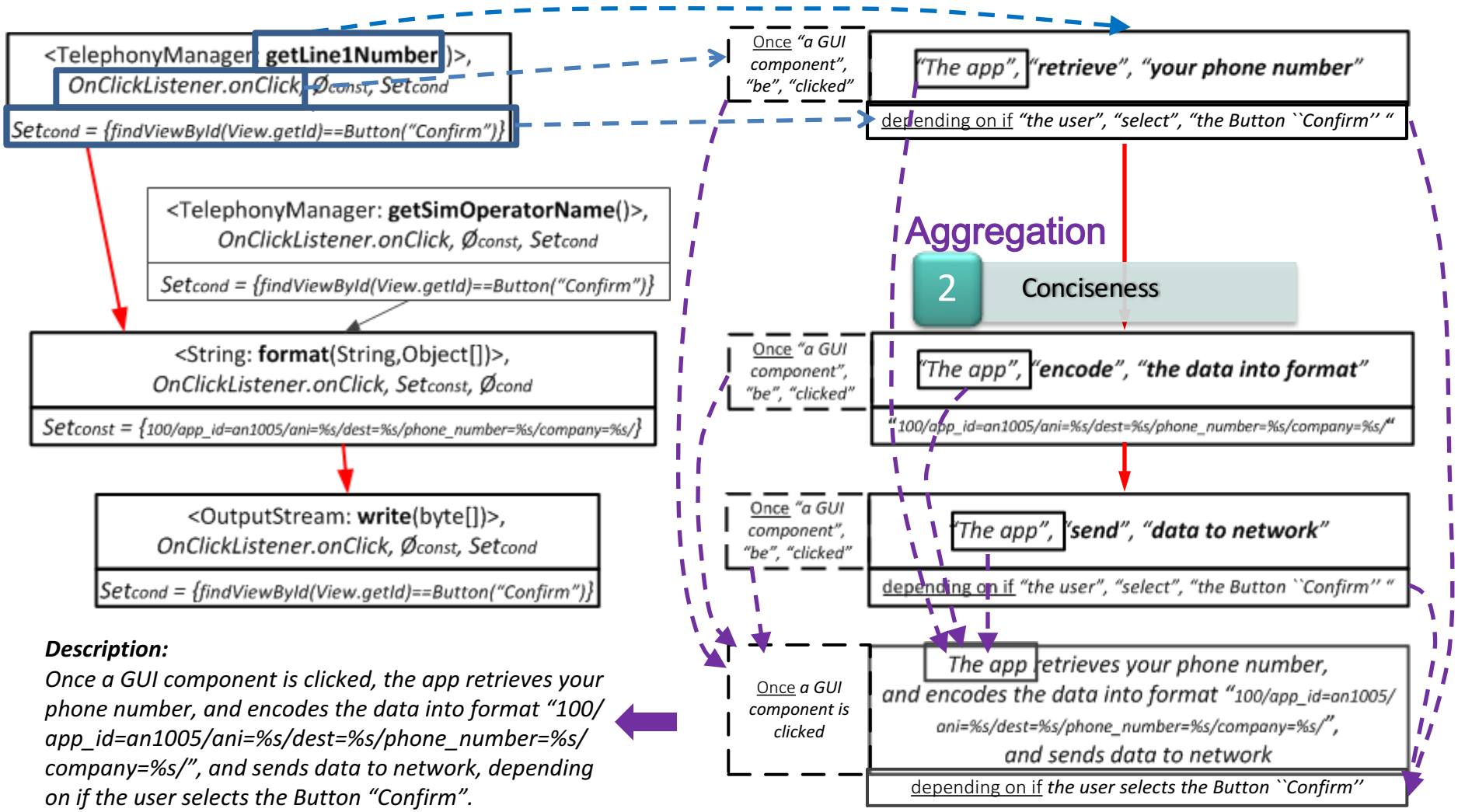
Discovered 109 patterns fundamentally due to design patterns in Android apps.

Graph Compression: Replace the subgraphs with single nodes

2 Conciseness

3 Human-understandability

Natural Language Generation



Description:

Once a GUI component is clicked, the app retrieves your phone number, and encodes the data into format "100/app_id=an1005/ani=%s/dest=%s/phone_number=%s/company=%s/", and sends data to network, depending on if the user selects the Button "Confirm".

EVALUATION: Correctness

Question 1: Is generated description correct?

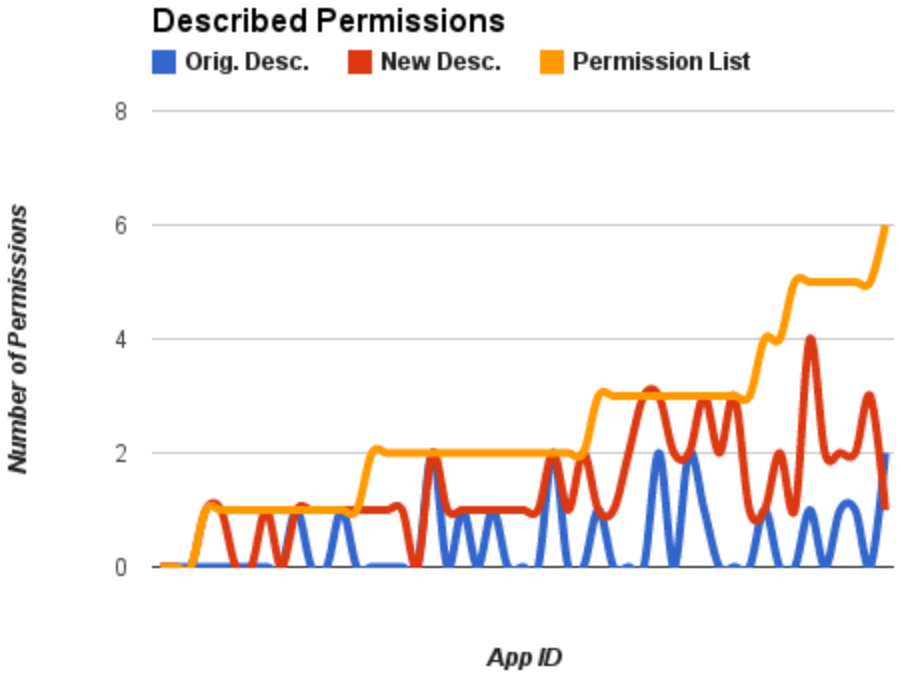
Run DESCRIBEME over DroidBench

Total #	Correct	Missing Desc.	False Statement
65	55	6	4

1. Points-to Analysis
2. Exception handling
3. Reflection

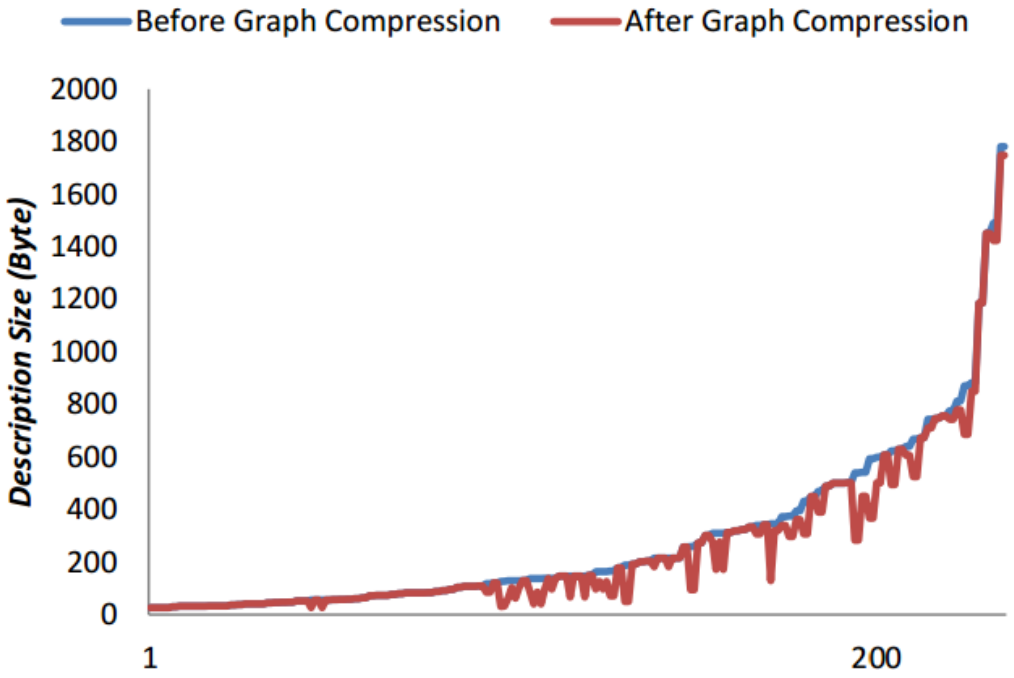
EVALUATION: Security-Awareness

Question 2: Developer's descriptions cannot faithfully reflect the usage of permissions. Can we do better?



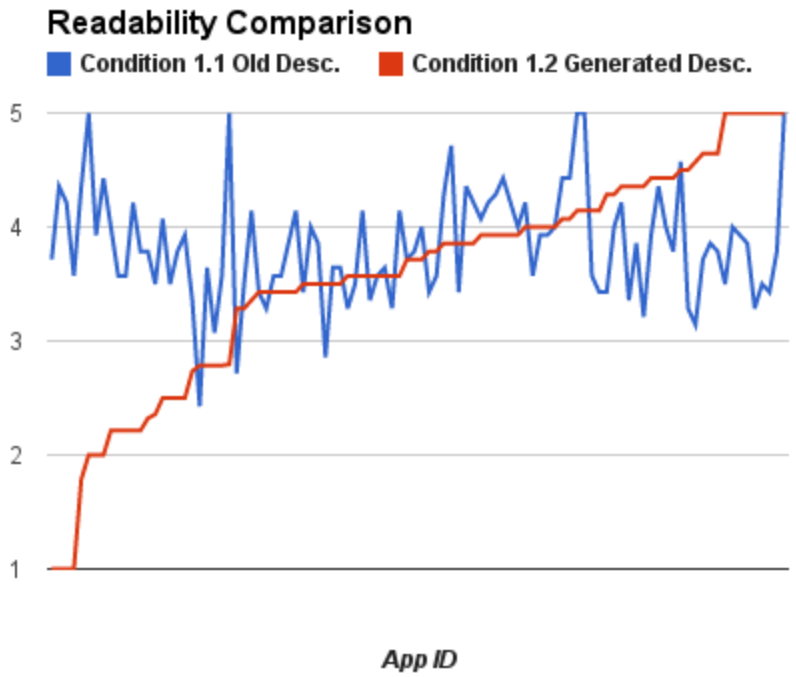
EVALUATION: Improvement of Conciseness

Question 3: Is subgraph mining effective?



EVALUATION: Readability

Question 4: Can average users read the machine generated descriptions?



EVALUATION: Human-Understandability

Question 5: Can our descriptions help users avoid risks?

App Download Rate	w/ old desc.	w/ new desc.
Malware		
Privacy-breaching		
Clean		

Conclusion

- We propose a novel technique that **automatically describes security-related app behaviors** to the end users in natural language.
- We implement **DESCRIBEME** which combines **program analysis, subgraph mining and natural language generation** to create security-centric, concise and human-readable descriptions.

Related Work

[1] Sridhara et al., Towards Automatically Generating Summary Comments for Java Methods, in ASE'10.

[2] Buse et al., Automatically Documenting Program Changes, in ASE'10.

[3] Sridhara et al., Automatically Detecting and Describing High Level Actions Within Methods, in ICSE'11.

[4] Sridhara et al., Generating Parameter Comments and Integrating with Method Summaries, in ICPC'11.

[5] Moreno et al., Automatic Generation of Natural Language Summaries for Java Classes, in ICPC'13.

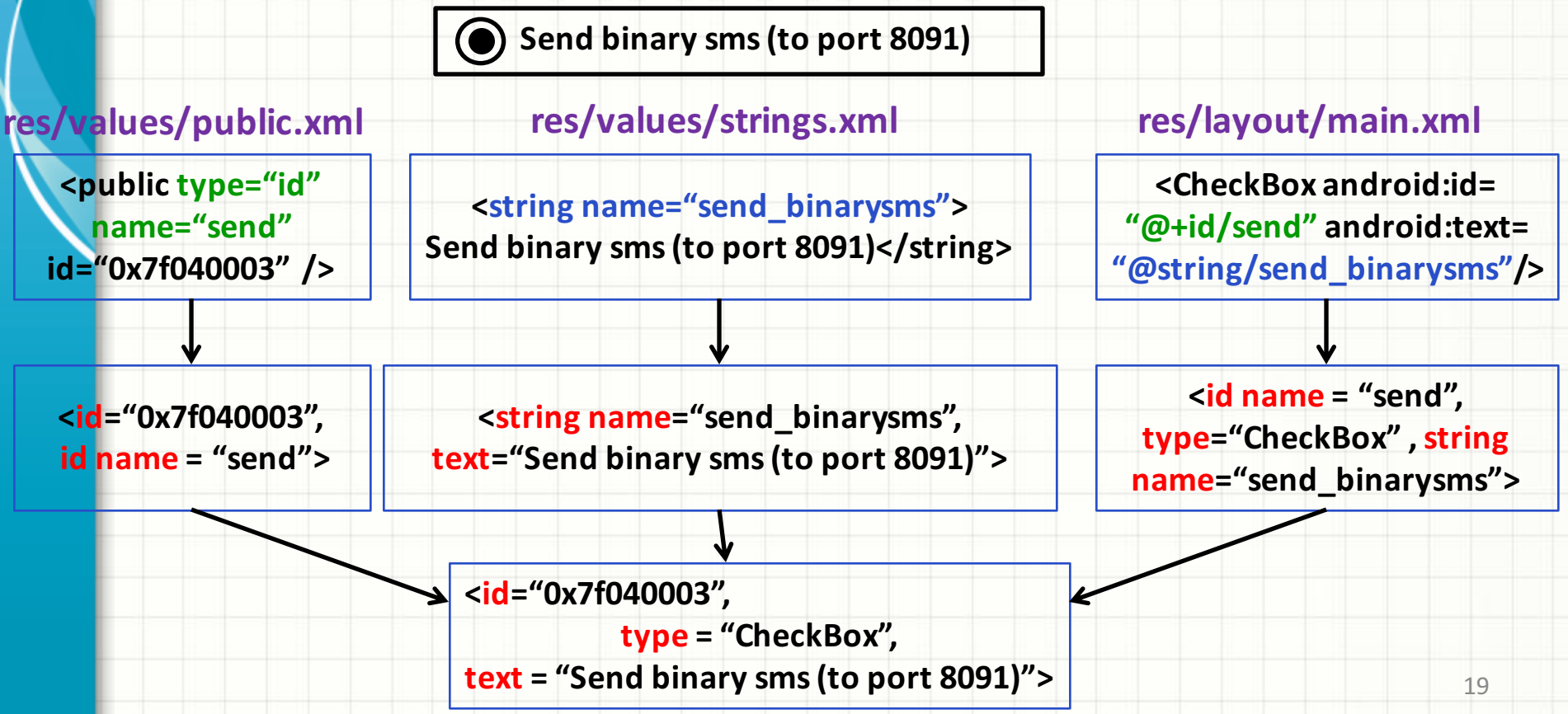
[6] Pandita et al., WHYPER: Towards Automating Risk Assessment of Mobile Applications, in USENIX Security'13

[7] Qu et al., AutoCog: Measuring the Description-to-permission Fidelity in Android Applications

Thank You!

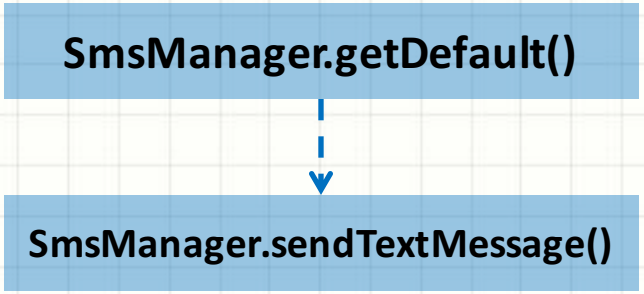
UI-related Triggering Conditions

- **UI Analysis:**
  - to correlate what the user sees to what the app does

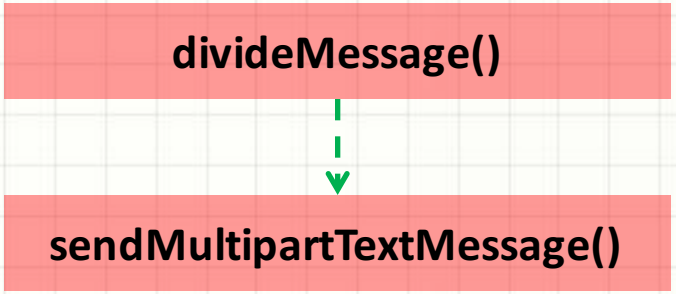


Subgraph Mining

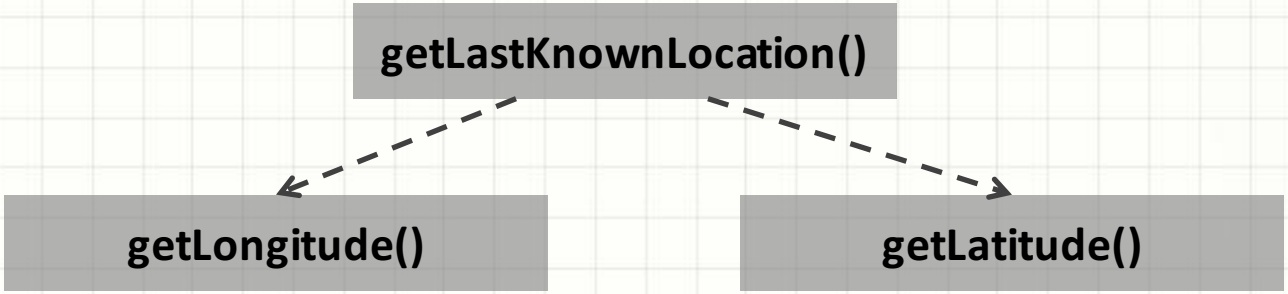
1. Singleton Retrieval



2. Workflow



3. Hierarchical Data



Description Model

3 Human-understandability

- 3-tuple for APIs
  - createFromPdu(): {“**the app**”, “**retrieve**”, “**incoming SMS message**”}
- **Manually modeling 306 APIs and 103 patterns**
- Guideline for Word Selection
  - **Straightforward**
  - **Distinguishable**
  - Counterexamples:

    “Blow into the mic to extinguish the flame like a real candle”

    “You can now turn recordings into ringtones”