What’s Done Is Not What’s Claimed: Detecting and Interpreting Inconsistencies in App Behaviors

Chang Yue[1,2], Kai Chen[1,2,⋆], Zhixiu Guo[1,2], Jun Dai[3], Xiaoyan Sun[3] and Yi Yang[1,2]

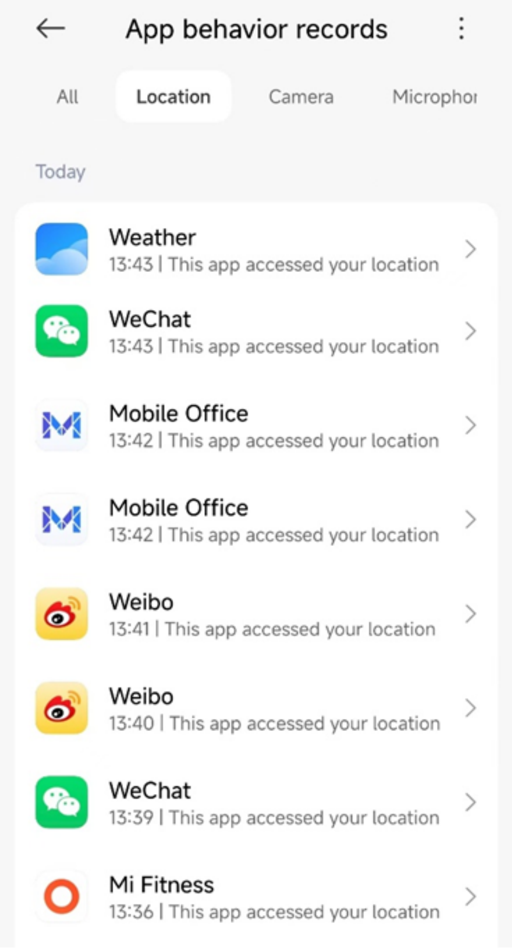
[1]Institute of Information Engineering, Chinese Academy of Sciences, China
[2]School of Cyber Security, University of Chinese Academy of Sciences, China
[3]Department of Computer Science, Worcester Polytechnic Institute, USA
{yuechang,chenkai,yangyi}@iie.ac.cn, gzhixiu@gmail.com, {jdai,xsun7}@wpi.edu

OVERVIEW

- Background
- Motivation
- Method
- Evaluation
- Findings
- Summary

BACKGROUND

Numerous privacy access in mobile apps



App behavior records

All | Location | Camera | Micropho

Today

Weather
13:43 | This app accessed your location

WeChat
13:43 | This app accessed your location

Mobile Office
13:42 | This app accessed your location

Mobile Office
13:42 | This app accessed your location

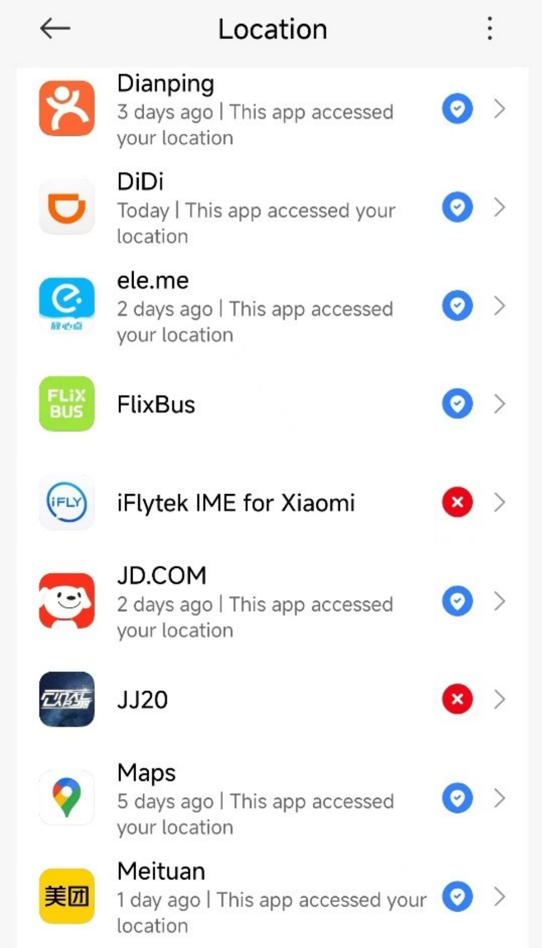
Weibo
13:41 | This app accessed your location

Weibo
13:40 | This app accessed your location

WeChat
13:39 | This app accessed your location

Mi Fitness
13:36 | This app accessed your location

Permission management in mobile system



Location

Dianping ✓
3 days ago | This app accessed your location

DiDi ✓
Today | This app accessed your location

ele.me ✓
2 days ago | This app accessed your location

FlixBus ✓

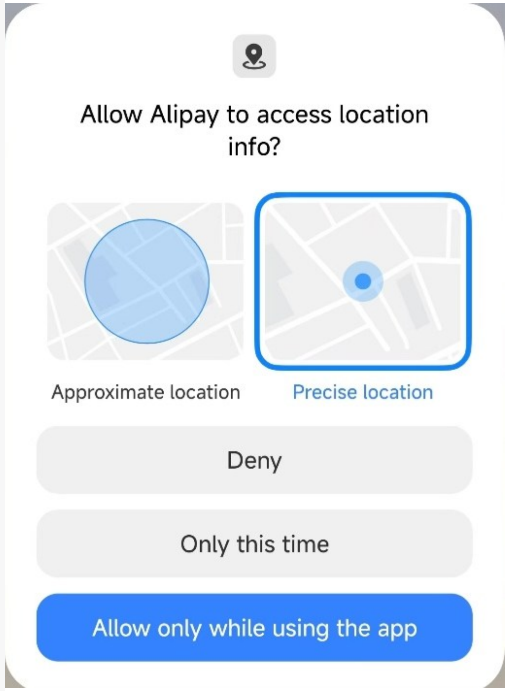
iFlytek IME for Xiaomi ✕

JD.COM ✓
2 days ago | This app accessed your location

JJ20 ✕

Maps ✓
5 days ago | This app accessed your location

Meituan ✓
1 day ago | This app accessed your location



Allow Alipay to access location info?

Approximate location | Precise location

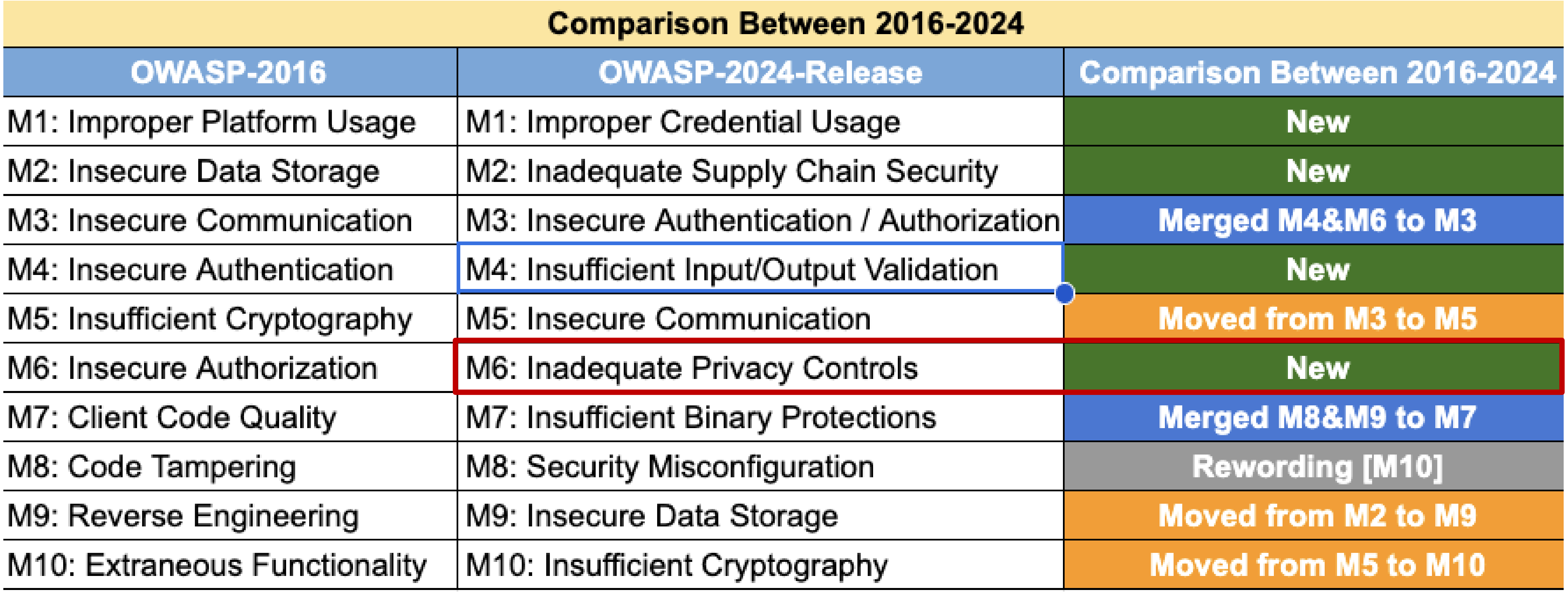
Deny

Only this time

Allow only while using the app

BACKGROUND

- **Privacy leakage remains one of the most critical issues**



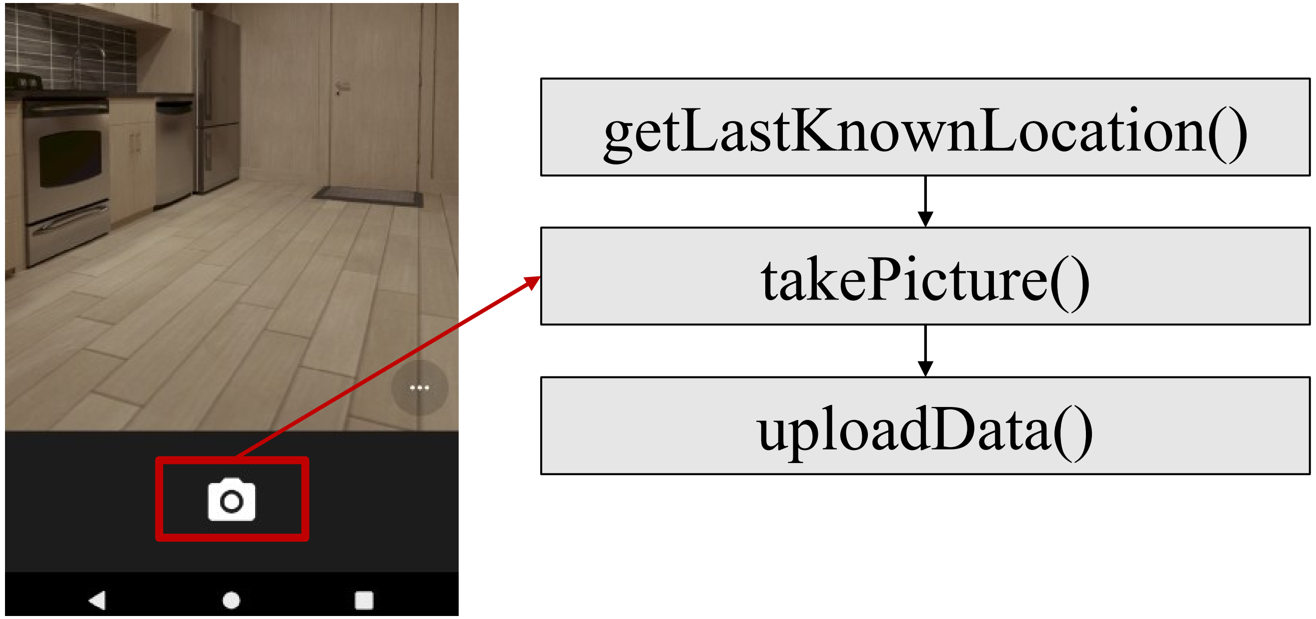
Comparison Between 2016-2024

OWASP-2016	OWASP-2024-Release	Comparison Between 2016-2024
M1: Improper Platform Usage	M1: Improper Credential Usage	New
M2: Insecure Data Storage	M2: Inadequate Supply Chain Security	New
M3: Insecure Communication	M3: Insecure Authentication / Authorization	Merged M4&M6 to M3
M4: Insecure Authentication	M4: Insufficient Input/Output Validation	New
M5: Insufficient Cryptography	M5: Insecure Communication	Moved from M3 to M5
M6: Insecure Authorization	M6: Inadequate Privacy Controls	New
M7: Client Code Quality	M7: Insufficient Binary Protections	Merged M8&M9 to M7
M8: Code Tampering	M8: Security Misconfiguration	Rewording [M10]
M9: Reverse Engineering	M9: Insecure Data Storage	Moved from M2 to M9
M10: Extraneous Functionality	M10: Insufficient Cryptography	Moved from M5 to M10

BACKGROUND

- ➢Users feel difficult to understand why each permission is required

- ➢Apps may perform sensitive behaviors without users' consent



getLastKnownLocation()

takePicture()

uploadData()

The app collects location and upload it to server when taking photos

MOTIVATION

Research questions:

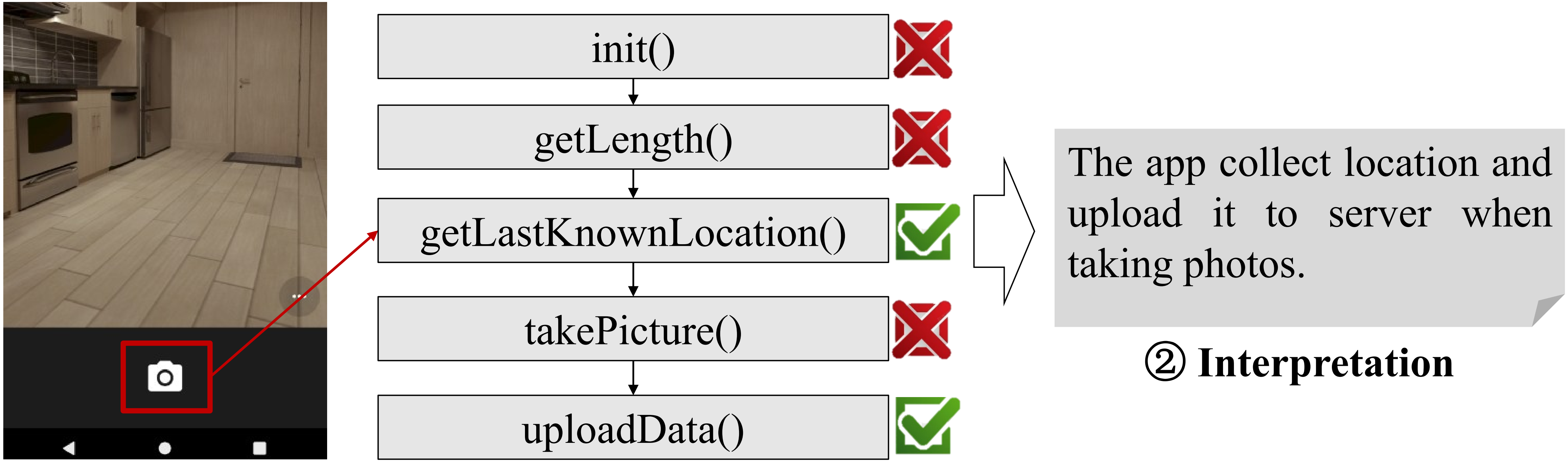
- Do users know the behaviors the app is performing?
  - Does the app notify users about the behaviors it is performing?
  - Does the app notify users about its behaviors consistently with the behaviors it actually performs?

Goals:

- Help app users better understand app behaviors so that they can independently assess the associated risks.

MOTIVATION

- **Inconsistent behaviors.** UI elements do not inform users about the relevant information regarding the behavior being performed.
- **Interpretation.** Present inconsistent behaviors in user-friendly natural language.



init() ✗

getLength() ✗

getLastKnownLocation() ✓

takePicture() ✗

uploadData() ✓

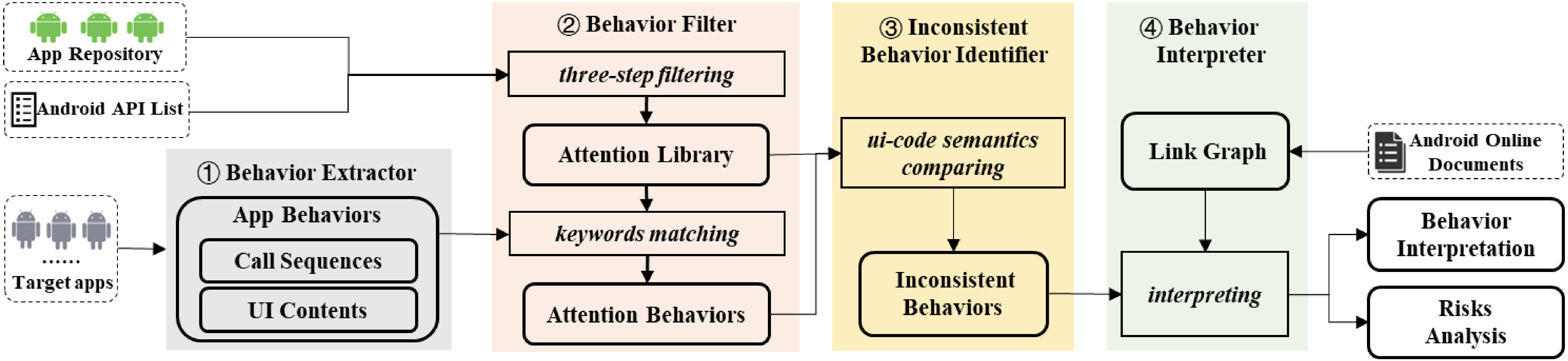
The app collect location and upload it to server when taking photos.

① Inconsistent behaviors

② Interpretation

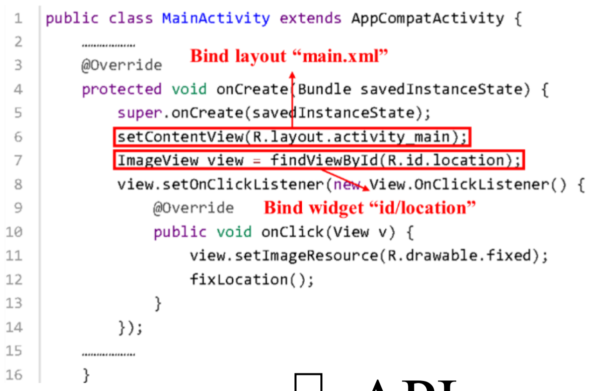
METHOD

- ➢ Inconsistent behaviors extraction based on static analysis
- ➢ Behaviors interpretation using LLMs

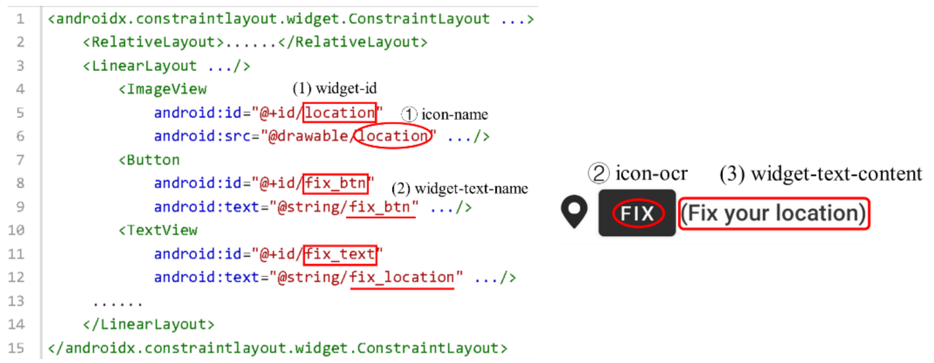


Framework of InconPreter

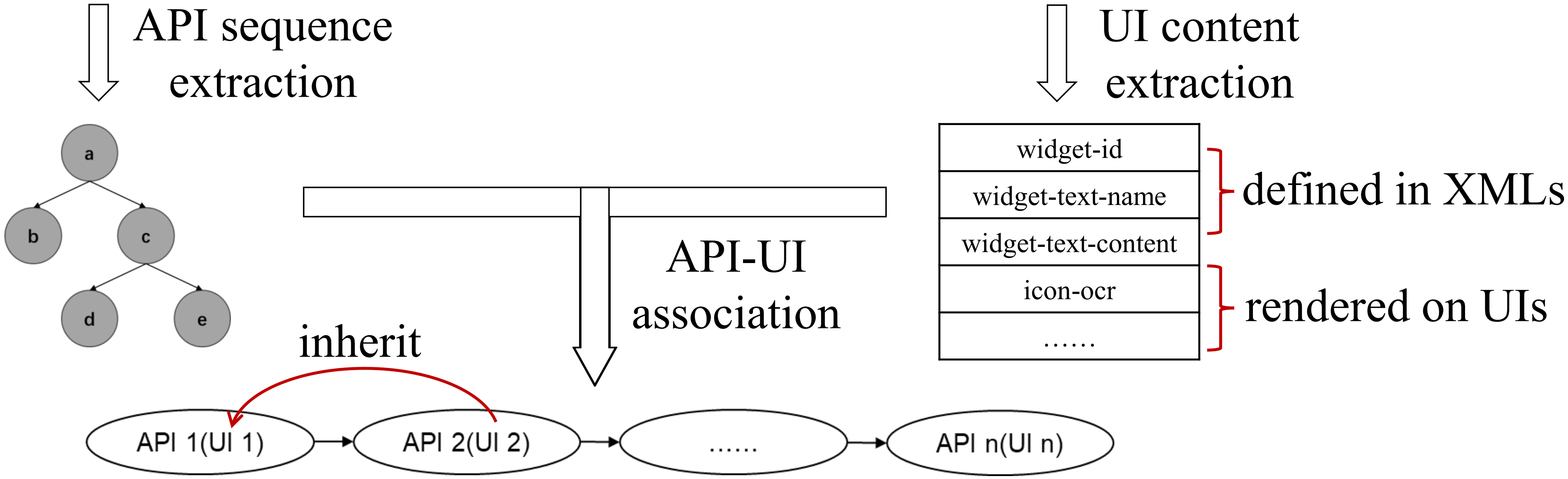
① Behavior Extraction



```
public class MainActivity extends AppCompatActivity {
    ..............
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        ImageView view = findViewById(R.id.location);
        view.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                view.setImageResource(R.drawable.fixed);
                fixLocation();
            }
        });
    ..............
    }
```



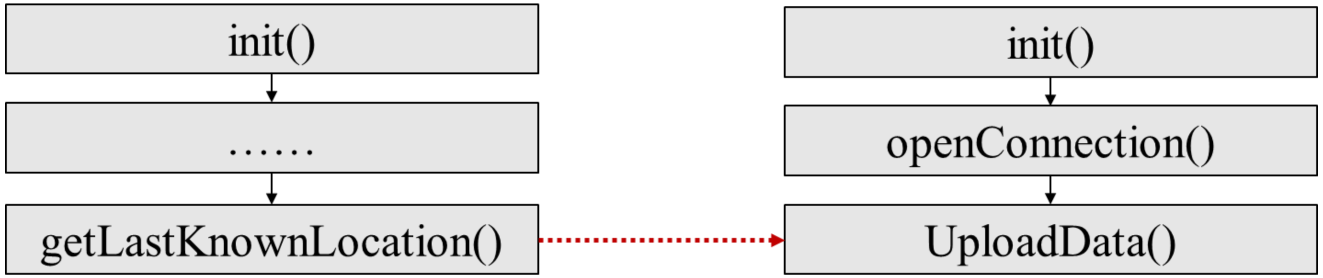
```
<androidx.constraintlayout.widget.ConstraintLayout ...>
    <RelativeLayout>......</RelativeLayout>
    <LinearLayout .../>
        <ImageView
            android:id="@+id/location"
            android:src="@drawable/location" .../>
        <Button
            android:id="@+id/fix_btn"
            android:text="@string/fix_btn" .../>
        <TextView
            android:id="@+id/fix_text"
            android:text="@string/fix_location" .../>
        ......
    </LinearLayout>
</androidx.constraintlayout.widget.ConstraintLayout>
```



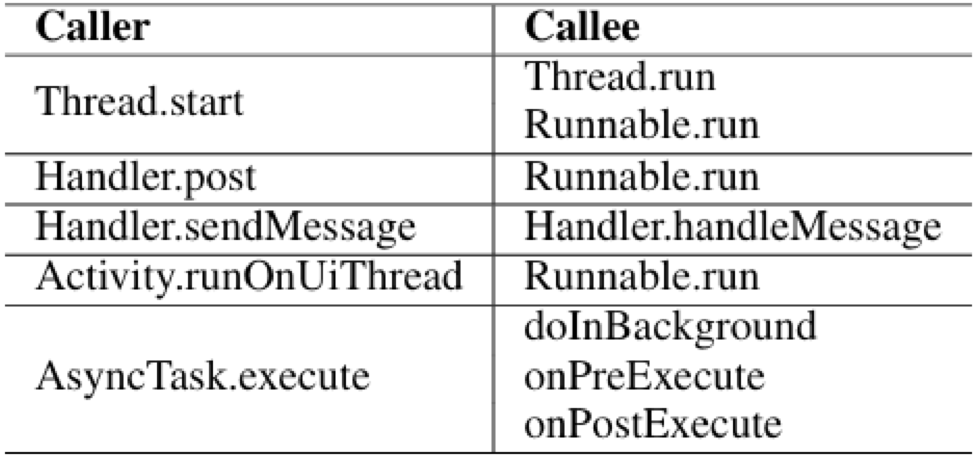
① Behavior Extraction

To ensure the completeness of behaviors：

- Data flow



- Implicit calling



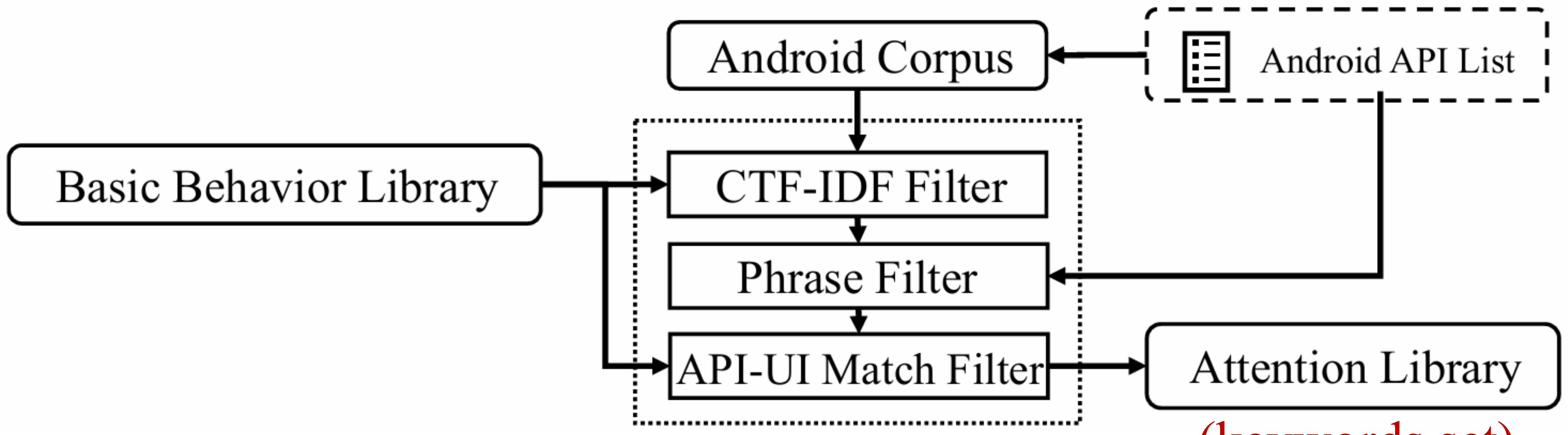
Caller	**Callee**
Thread.start	Thread.run Runnable.run
Handler.post	Runnable.run
Handler.sendMessage	Handler.handleMessage
Activity.runOnUiThread	Runnable.run
AsyncTask.execute	doInBackground onPreExecute onPostExecute

② Behavior Filtering

- In various apps, unimportant words appear more frequently than those related to sensitive resources.

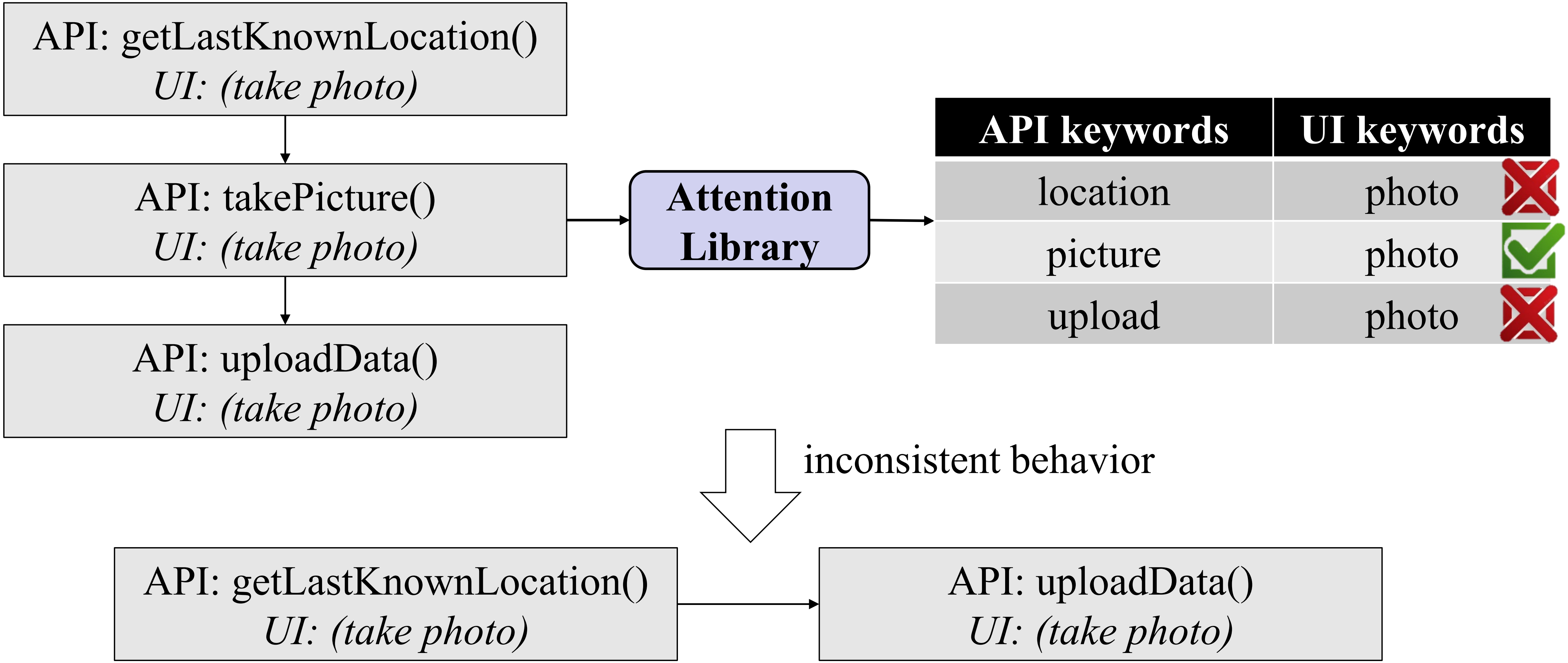
- Words that combine with many other words are not important.

- An API should be important when it is semantically related to its UI elements.



(keywords set)

③ Inconsistent Behavior Identification



API: getLastKnownLocation()
UI: (take photo)

API: takePicture()
UI: (take photo)

API: uploadData()
UI: (take photo)

Attention Library

API keywords	UI keywords	
location	photo	✗
picture	photo	✓
upload	photo	✗

inconsistent behavior

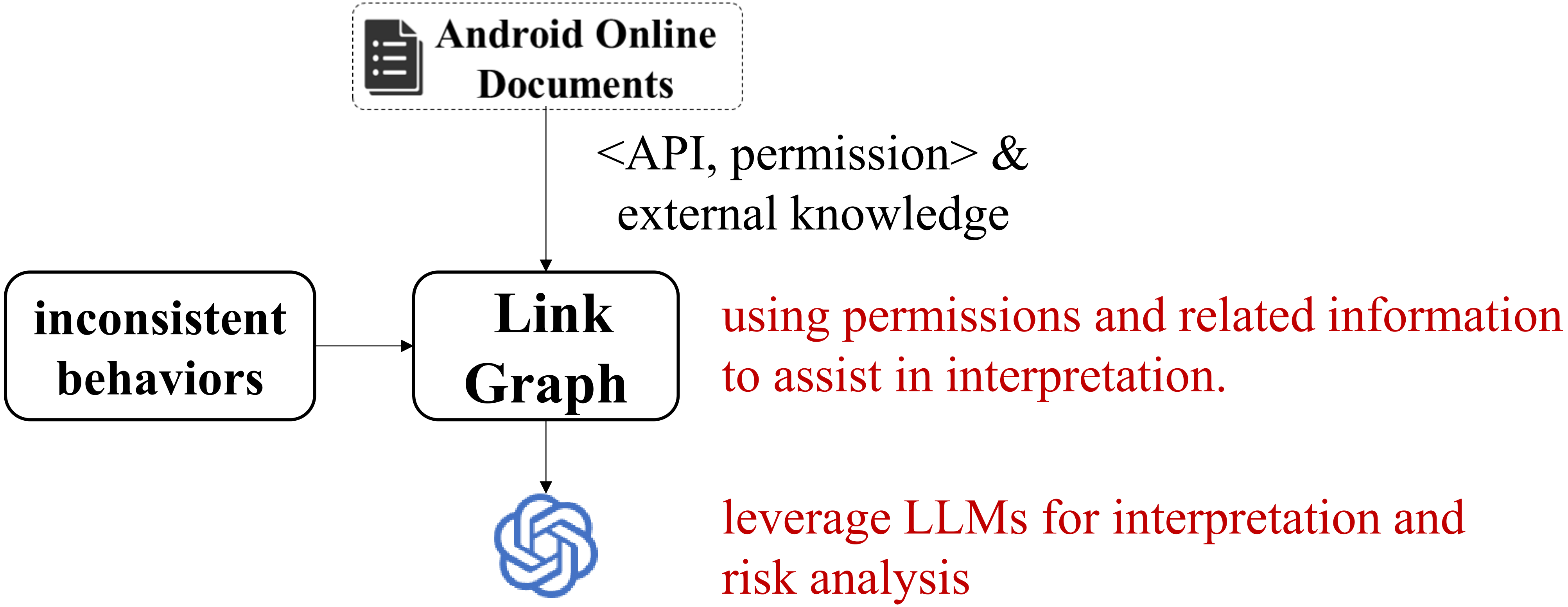
API: getLastKnownLocation()
UI: (take photo)

API: uploadData()
UI: (take photo)

④ Behaviors Interpretation

- APP needs APIs with **specific permissions** to access sensitive data and resources.

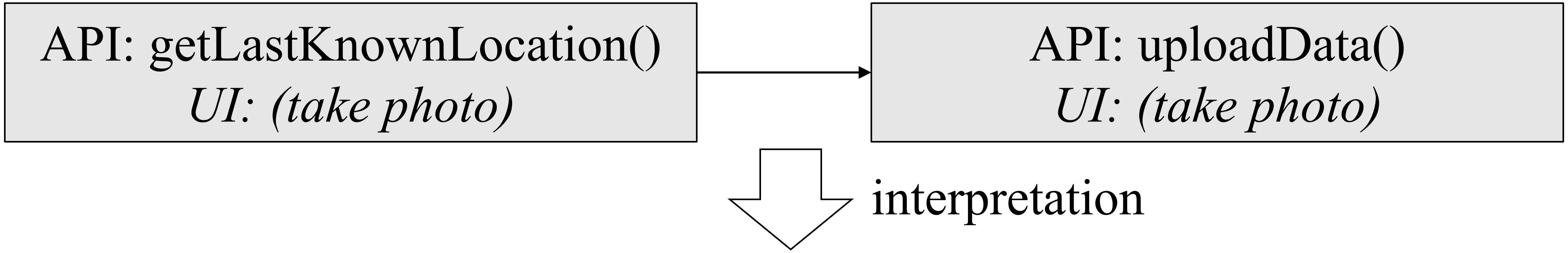
- LLMs perform well in summarization and reasoning tasks.



using permissions and related information to assist in interpretation.

leverage LLMs for interpretation and risk analysis

④ Behaviors Interpretation



API: getLastKnownLocation()
UI: (take photo)

API: uploadData()
UI: (take photo)

interpretation

- **Summary**

When users use a photography app to take a photo, the app unexpectedly accesses location data (ACCESS_FINE_LOCATION) and upload the location to a server (NETWORK).

- **Risky operation:** [ACCESS_FINE_LOCATION, NETWORK]
- **Explanation:**

➢ ACCESS_FINE_LOCATION: While some photography apps may use location data to tag photos with geolocation metadata, this is not essential for the primary function of taking a photo. Accessing precise location data can expose users' real-time location, leading to potential privacy risks if the data is stored or shared without consent.

➢ NETWORK: Network access is not directly required. It could be used for uploading photos or user location. This poses risks of unauthorized data transmission or exposure to network-based attacks.

EVALUATION

Performance in behaviors interpretation

User Study (the highest score is 5)

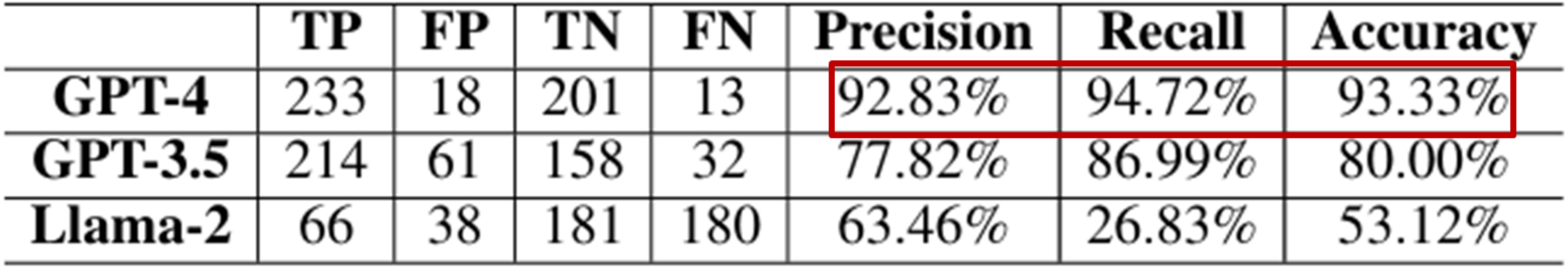
- The interpretation is **easy to understand** (4.07)
- The interpretation is **reasonable** (4.15)
- The interpretation is **helpful** for understanding apps’ behavior (4.12)

EVALUATION

Performance in risky inconsistent behaviors identification

① Comparison between different LLMs on 100 labeled apps

- **GPT-4** performs best in risk analysis



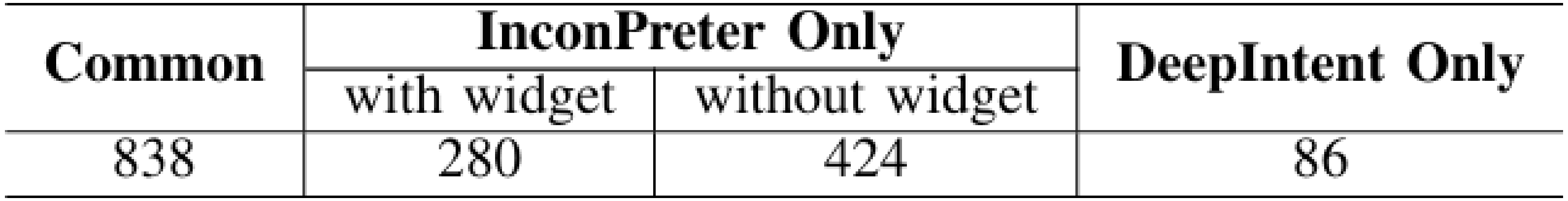
	TP	FP	TN	FN	Precision	Recall	Accuracy
GPT-4	233	18	201	13	92.83%	94.72%	93.33%
GPT-3.5	214	61	158	32	77.82%	86.99%	80.00%
Llama-2	66	38	181	180	63.46%	26.83%	53.12%

EVALUATION

Performance in risky inconsistent behaviors identification

② Comparison with SOTA on 600 labeled apps

- **94.89%** risky inconsistent behaviors identification rate
- **704 more** risky inconsistent behaviors than SOTA



Common	InconPreter Only		DeepIntent Only
	with widget	without widget	
838	280	424	86

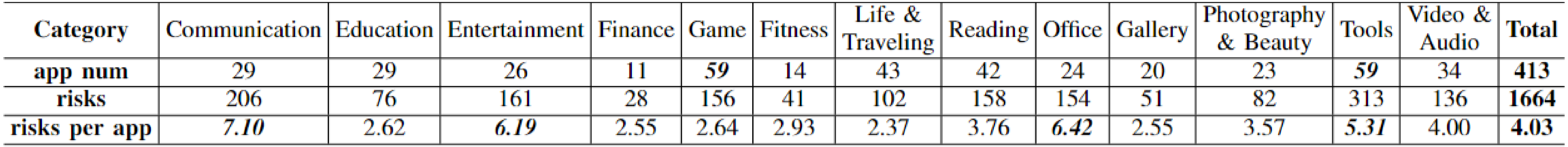
③ On 100 Android Malware Dataset samples

- **94.56%** risky behaviors identification rate
- **27 new** additional risky behaviors

FINDINGS

Distribution of risky inconsistent behaviors

- **413 wild apps** are identified containing **1664 risky inconsistent behaviors**, and these apps **cover all app categories**.
- **89 (21.55%)** apps have downloads **exceeding 1 million**.
- **322 (77.97%)** apps contain **740 self-starting** risky inconsistent behaviors.

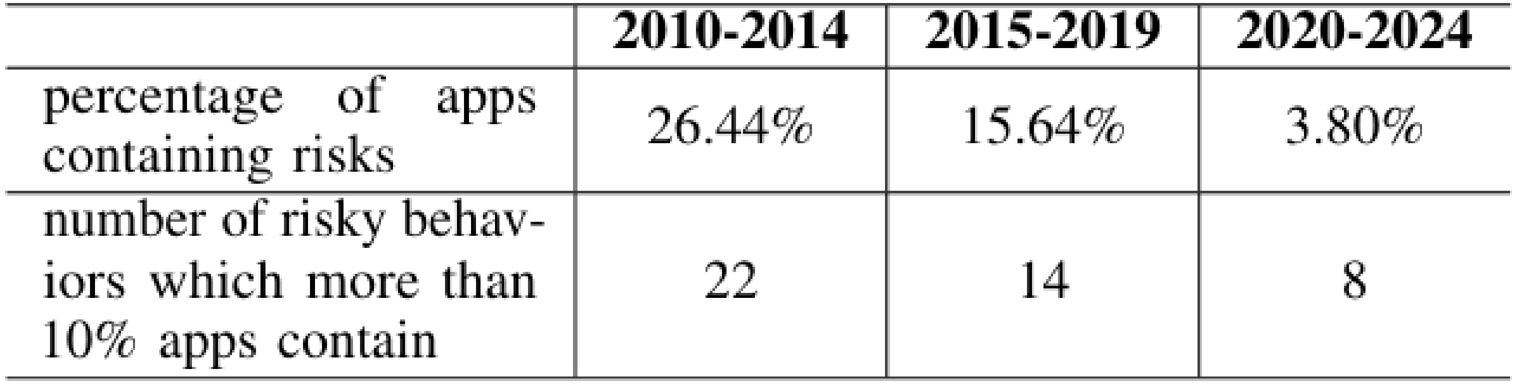


Category	Communication	Education	Entertainment	Finance	Game	Fitness	Life & Traveling	Reading	Office	Gallery	Photography & Beauty	Tools	Video & Audio	Total
app num	29	29	26	11	***59***	14	43	42	24	20	23	***59***	34	**413**
risks	206	76	161	28	156	41	102	158	154	51	82	313	136	**1664**
risks per app	*7.10*	2.62	*6.19*	2.55	2.64	2.93	2.37	3.76	***6.42***	2.55	3.57	***5.31***	4.00	**4.03**

FINDINGS

Evolution of risky inconsistent behaviors between periods

- Due to increasing privacy concerns and stricter market regulations, risky inconsistent behaviors have significantly **decreased**.
- Due to the decreased frequency of phone call usage but increased reliance on online communication, risky behaviors related to **user contact information** have a declining trend, but those associated with **location, Wi-Fi, Bluetooth** show an increasing trend.



	2010-2014	2015-2019	2020-2024
percentage of apps containing risks	26.44%	15.64%	3.80%
number of risky behaviors which more than 10% apps contain	22	14	8

SUMMARY

- Propose InconPreter to **extract and interpret inconsistent behaviors** in apps, enabling users to **better understand what the app is doing** and **independently assess the potential risks**.

- Identify **1,664 risky inconsistent behaviors** from 413 apps, including leakage of location, SMS, and contact information, as well as unauthorized audio recording, etc., **affecting millions of users**.

Thank You

Q &A