

Leaking the Privacy of Groups and More:

Understanding Privacy Risks of Cross-App Content Sharing in Mobile Ecosystem

Jiangrong Wu¹, Yuhong Nan^{1*}, Luyi Xing², Jiatao Cheng¹,
Zimin Lin³, Zibin Zheng¹, Min Yang⁴

Sun Yat-sen University¹, Indiana University Bloomington², Alibaba Group³, Fudan University⁴



中山大學
SUN YAT-SEN UNIVERSITY



INDIANA
UNIVERSITY

Alibaba Group
阿里巴巴集团



復旦大學
FUDAN UNIVERSITY

Background: Cross-App Content Sharing



■ Example: News sharing from Tencent News to WeChat.



like



Comment



collect



share

What are the early symptoms of HIV infection? What tests should be done?



Guizhou Disease Control
2023-11-04 17:52:00 Published on the official account of the Guizhou Provincial Center for Disease Control and Prevention in Guizhou

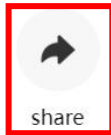


AIDS (Acquired Immunodeficiency Syndrome, AIDS) is a serious immune system disease caused by Human Immunodeficiency Virus (HIV). In the first few weeks after HIV infection, many infected people may not experience any symptoms, or the symptoms may be very mild and easily ignored. This period is called the "acute HIV infection period." Some people may experience symptoms such as fever, sore throat, swollen lymph nodes, and fatigue, similar to those of a common cold. Red or purple spots, rashes, or eczema may appear on the skin; headache, and muscle and joint pain. These early symptoms may resolve on their own after a few weeks, leading the infected person to believe they have recovered, while the virus is still quietly destroying the immune system in the body.

Background: Cross-App Content Sharing



1. Alice (**sharer**) clicks the share button in Tencent News (**source app**)



What are the early symptoms of HIV infection? What tests should be done?



Guizhou Disease Control
2023-11-04 17:52:00 Published on the official account of the Guizhou Provincial Center for Disease Control and Prevention in Guizhou

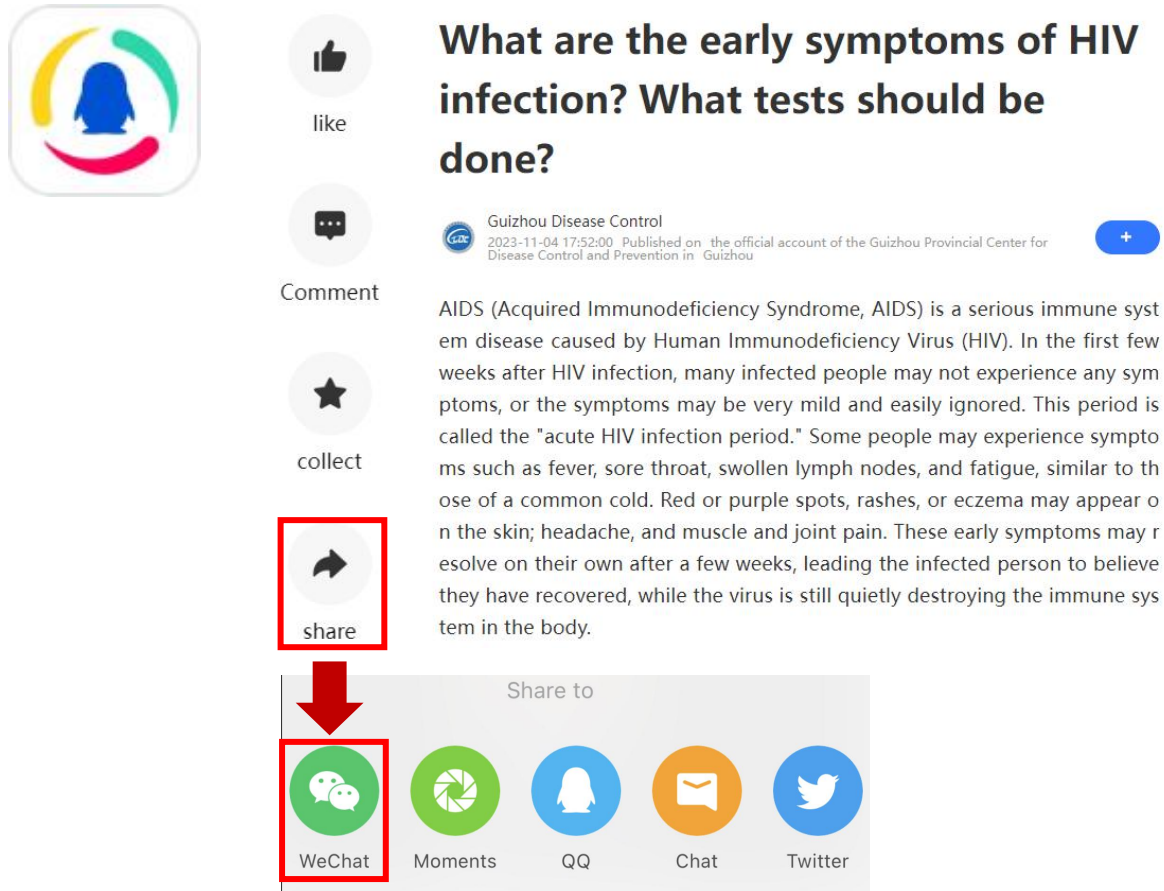


AIDS (Acquired Immunodeficiency Syndrome, AIDS) is a serious immune system disease caused by Human Immunodeficiency Virus (HIV). In the first few weeks after HIV infection, many infected people may not experience any symptoms, or the symptoms may be very mild and easily ignored. This period is called the "acute HIV infection period." Some people may experience symptoms such as fever, sore throat, swollen lymph nodes, and fatigue, similar to those of a common cold. Red or purple spots, rashes, or eczema may appear on the skin; headache, and muscle and joint pain. These early symptoms may resolve on their own after a few weeks, leading the infected person to believe they have recovered, while the virus is still quietly destroying the immune system in the body.

Background: Cross-App Content Sharing



1. Alice (**sharer**) clicks the share button in Tencent News (**source app**)

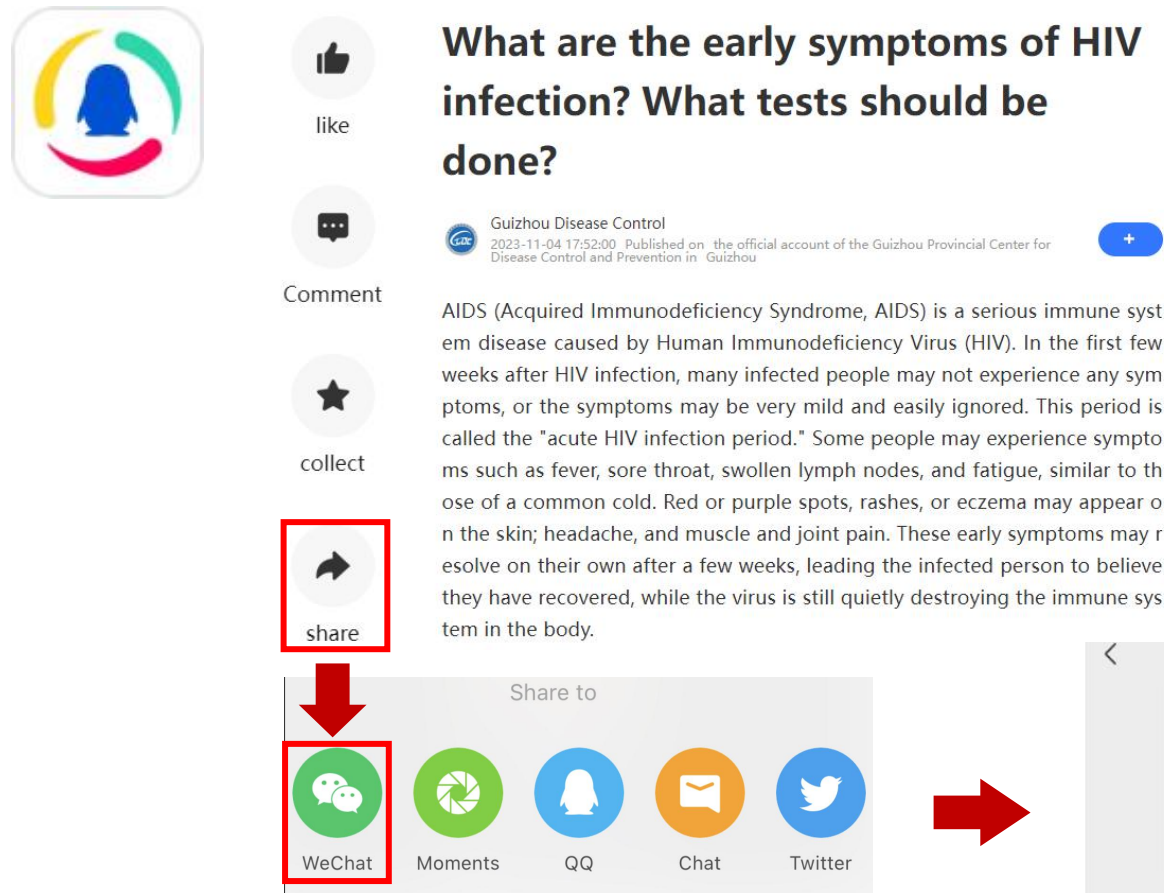


2. Alice (**sharer**) selects WeChat from the list of available targets

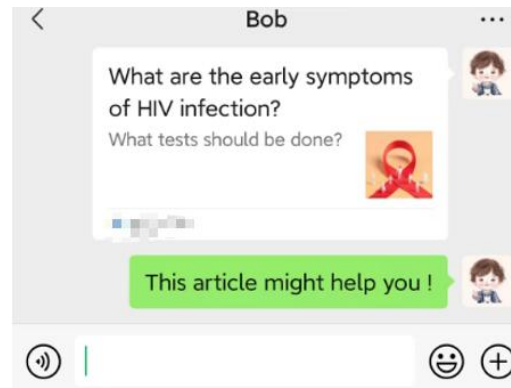
Background: Cross-App Content Sharing



1. Alice (**sharer**) clicks the share button in Tencent News (**source app**)



2. Alice (**sharer**) selects WeChat from the list of available targets

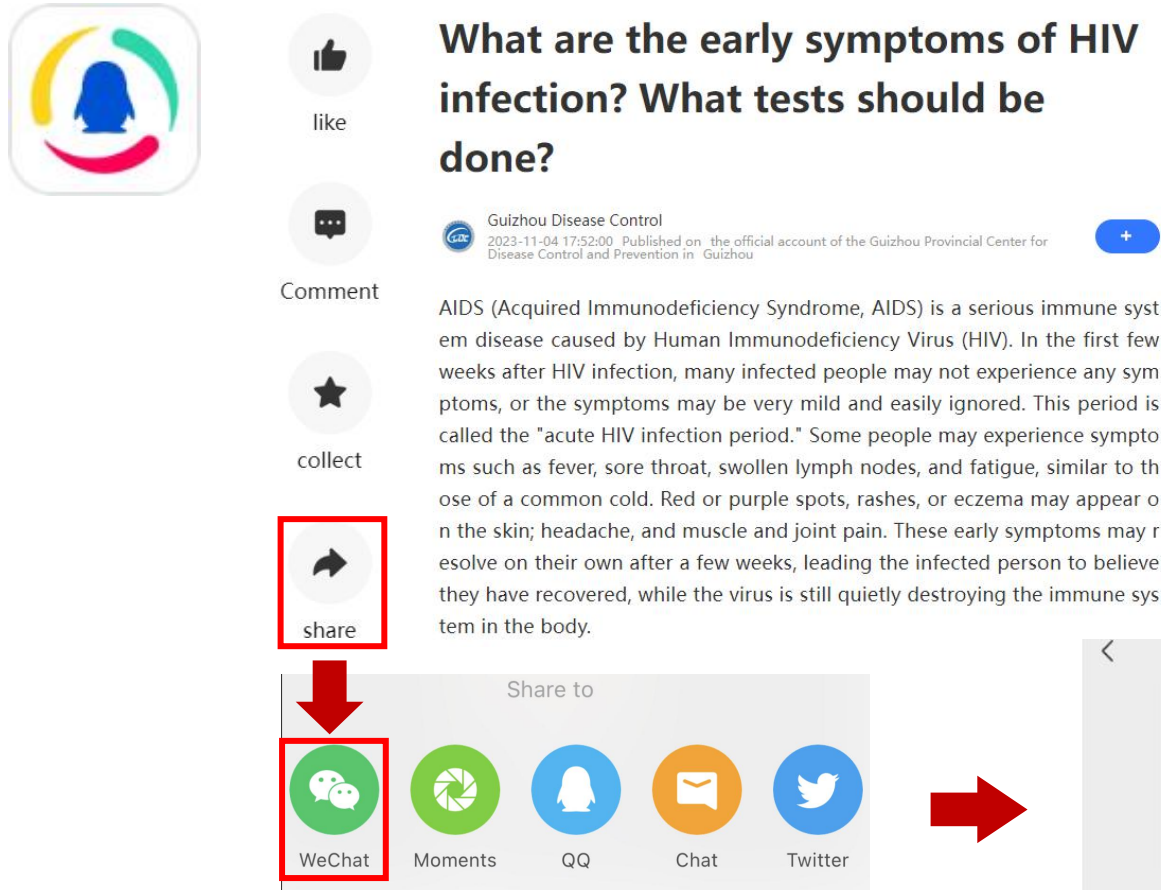


3. Content delivered to Bob (**sharee**) in WeChat

Background: Cross-App Content Sharing







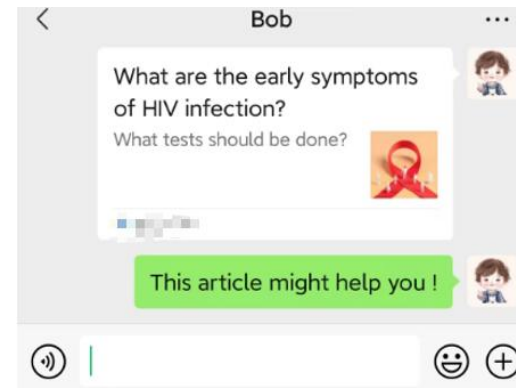
1. Alice (**sharer**) clicks the share button in Tencent News (**source app**)



2. Alice (**sharer**) selects WeChat from the list of available targets

Terminologies:

- **sharer: Alice** 
- **sharee: Bob** 
- **source app: Tencent News** 
- **target app: WeChat** 



3. Content delivered to Bob (**sharee**) in WeChat

Background



■ Prior research on privacy leaks (mobile ecosystem)

- Data processing within an **individual app**
 - User tag Spoofing [UTSFuzzer-Sec23]
 - Privacy risks in IoT Companion Apps [IoTProfiler-Sec23]
- Privacy leakage across **multiple apps** [IccTA-ICSE15]
 - Regular privacy data types: IMEI, Location, etc.
 - System-level IPC channel (Inter-component-communication, ICC)

[UTSFuzzer-Sec23] Li S, Yang Z, Yang G, et al. Notice the imposter! a study on user tag spoofing attack in mobile apps[C]//32nd USENIX Security Symposium (USENIX Security 23). 2023: 5485-5501.

[IoTProfiler-Sec23] Nan Y, Wang X, Xing L, et al. Are You Spying on Me?{Large-Scale} Analysis on {IoT} Data Exposure through Companion Apps[C]//32nd USENIX Security Symposium (USENIX Security 23). 2023: 6665-6682.

[IccTA-ICSE15] L. Li et al., "IccTA: Detecting Inter-Component Privacy Leaks in Android Apps," 2015 IEEE/ACM 37th IEEE International Conference on Software Engineering, Florence, Italy, 2015, pp. 280-291, doi: 10.1109/ICSE.2015.48.

Background



■ Prior research on privacy leaks (mobile ecosystem)

- Data processing within an **individual app**
 - User tag Spoofing [UTSFuzzer-Sec23]
 - Privacy risks in IoT Companion Apps [IoTProfiler-Sec23]
- Privacy leakage across **multiple apps** [IccTA-ICSE15]
 - Regular privacy data types: IMEI, Location, etc.
 - System-level IPC channel (Inter-component-communication, ICC)

■ Our work

- **Cross-app content sharing scenario (CRACS)**

[UTSFuzzer-Sec23] Li S, Yang Z, Yang G, et al. Notice the imposter! a study on user tag spoofing attack in mobile apps[C]//32nd USENIX Security Symposium (USENIX Security 23). 2023: 5485-5501.

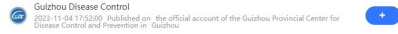
[IoTProfiler-Sec23] Nan Y, Wang X, Xing L, et al. Are You Spying on Me?{Large-Scale} Analysis on {IoT} Data Exposure through Companion Apps[C]//32nd USENIX Security Symposium (USENIX Security 23). 2023: 6665-6682.

[IccTA-ICSE15] L. Li et al., "IccTA: Detecting Inter-Component Privacy Leaks in Android Apps," 2015 IEEE/ACM 37th IEEE International Conference on Software Engineering, Florence, Italy, 2015, pp. 280-291, doi: 10.1109/ICSE.2015.48.

Motivation Example



What are the early symptoms of HIV infection? What tests should be done?



AIDS (Acquired Immunodeficiency Syndrome, AIDS) is a serious immune system disease caused by Human Immunodeficiency Virus (HIV). In the first few weeks after HIV infection, many infected people may not experience any symptoms, or the symptoms may be very mild and easily ignored. This period is called the "acute HIV infection period." Some people may experience symptoms such as fever, sore throat, swollen lymph nodes, and fatigue, similar to those of a common cold. Red or purple spots, rashes, or eczema may appear on the skin; headache, and muscle and joint pain. These early symptoms may resolve on their own after a few weeks, leading the infected person to believe they have recovered, while the virus is still quietly destroying the immune system in the body.



https://view.***.com/article?news_id=20231104A0730U00&uid=8****M&...

The essence of shared content -> **URL**



CRACS is essentially the transmission of URLs across two different apps

Motivation Example



What are the early symptoms of HIV infection? What tests should be done?

Guizhou Disease Control
2023-11-04 17:32:00 Published on the official account of the Guizhou Provincial Center for Disease Control and Prevention in Guizhou

AIDS (Acquired Immunodeficiency Syndrome, AIDS) is a serious immune system disease caused by Human Immunodeficiency Virus (HIV). In the first few weeks after HIV infection, many infected people may not experience any symptoms, or the symptoms may be very mild and easily ignored. This period is called the "acute HIV infection period." Some people may experience symptoms such as fever, sore throat, swollen lymph nodes, and fatigue, similar to those of a common cold. Red or purple spots, rashes, or eczema may appear on the skin; headache, and muscle and joint pain. These early symptoms may resolve on their own after a few weeks, leading the infected person to believe they have recovered, while the virus is still quietly destroying the immune system in the body.



`https://view.***.com/article?news_id=20231104A0730U00&uid=8*****M&...`

The essence of shared content -> **URL**



CRACS is essentially the transmission of URLs across two different apps

General
Data
Protection
Regulation

California
Consumer
Privacy
Act

China's data
protection law,
PIPL

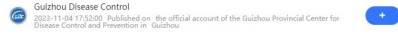
Data minimization:

- The process of **CRACS** should only transmit essential data necessary for accessing the content.

Motivation Example



What are the early symptoms of HIV infection? What tests should be done?



AIDS (Acquired Immunodeficiency Syndrome, AIDS) is a serious immune system disease caused by Human Immunodeficiency Virus (HIV). In the first few weeks after HIV infection, many infected people may not experience any symptoms, or the symptoms may be very mild and easily ignored. This period is called the "acute HIV infection period." Some people may experience symptoms such as fever, sore throat, swollen lymph nodes, and fatigue, similar to those of a common cold. Red or purple spots, rashes, or eczema may appear on the skin; headache, and muscle and joint pain. These early symptoms may resolve on their own after a few weeks, leading the infected person to believe they have recovered, while the virus is still quietly destroying the immune system in the body.



```
https://view.***.com/article?news_id=20231104A0730U00&uid=8*****M&...
```

The essence of shared content -> **URL**



CRACS is essentially the transmission of URLs across two different apps

General
Data
Protection
Regulation

California
Consumer
Privacy
Act

China's data
protection law,
PIPL

Data minimization:

- The process of **CRACS** should only transmit essential data necessary for accessing the content.

Privacy expectations:

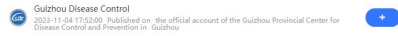
Sending the minimal resources pointing to the shared content to the sharee (**news_id**).



Motivation Example



What are the early symptoms of HIV infection? What tests should be done?



AIDS (Acquired Immunodeficiency Syndrome, AIDS) is a serious immune system disease caused by Human Immunodeficiency Virus (HIV). In the first few weeks after HIV infection, many infected people may not experience any symptoms, or the symptoms may be very mild and easily ignored. This period is called the "acute HIV infection period." Some people may experience symptoms such as fever, sore throat, swollen lymph nodes, and fatigue, similar to those of a common cold. Red or purple spots, rashes, or eczema may appear on the skin; headache, and muscle and joint pain. These early symptoms may resolve on their own after a few weeks, leading the infected person to believe they have recovered, while the virus is still quietly destroying the immune system in the body.

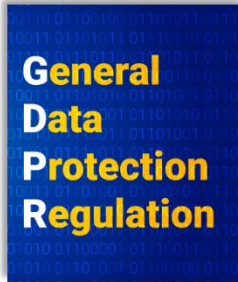


`https://view.***.com/article?news_id=20231104A0730U00&uid=8****M&...`

The essence of shared content is **URL**



CRACS is essentially the transmission of URLs across two different apps



Data minimization:

- The process of **CRACS** should only transmit essential data necessary for accessing the content.

Privacy expectations:

Sending the minimal resources pointing to the shared content to the sharee (**news_id**).



However, the app exposes user id (**uid**) in news sharing





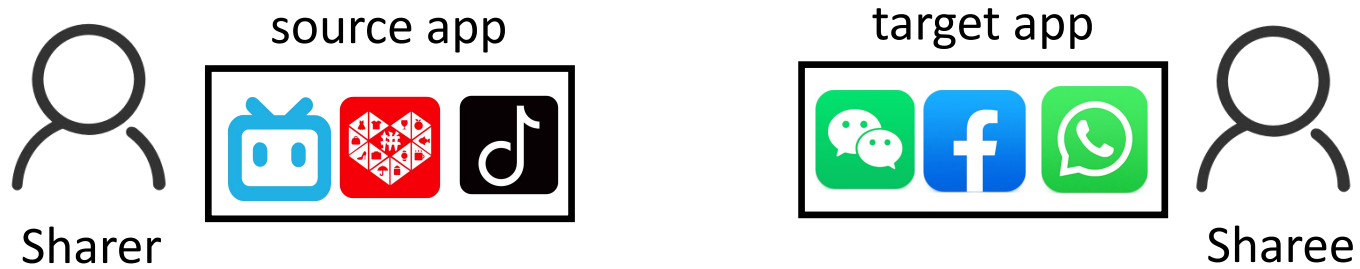
Key research questions

- What are the possible privacy threats in **CRACS**?
- What are users' perceptions and responses regarding such privacy risks?
- How prevalent do such data practices exist in the current mobile ecosystem?

Privacy Threats



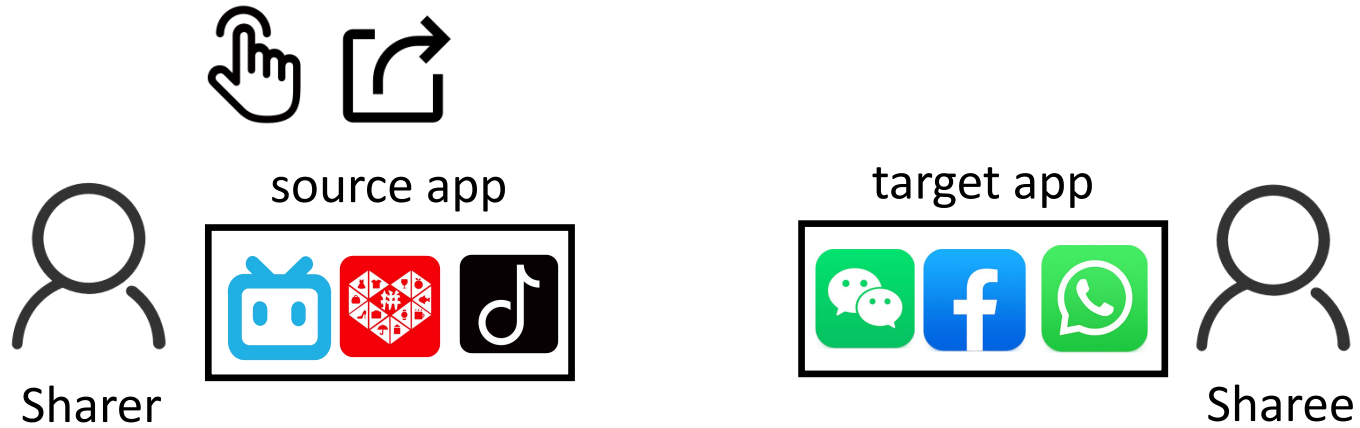
1. Sharing Behavior Tracking (SBT)



Privacy Threats



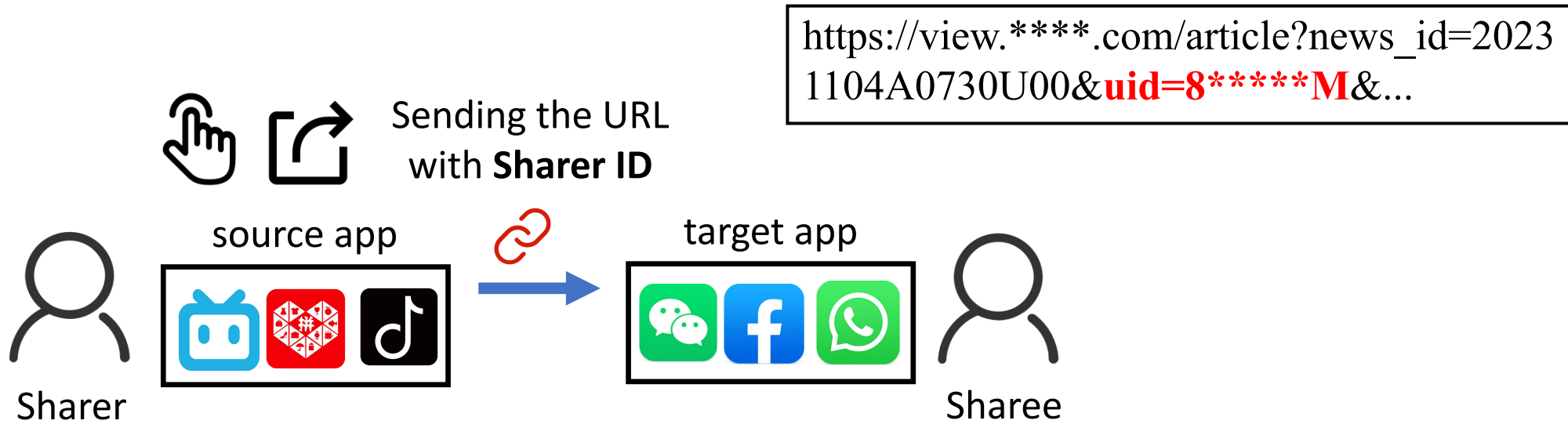
1. Sharing Behavior Tracking (SBT)



Privacy Threats



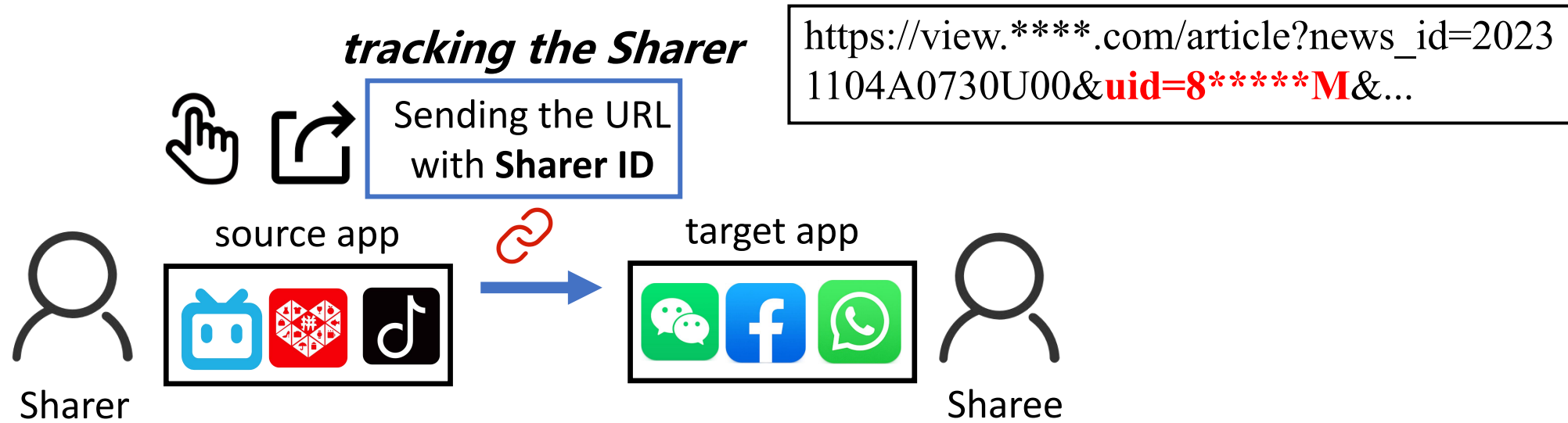
1. Sharing Behavior Tracking (SBT)



Privacy Threats



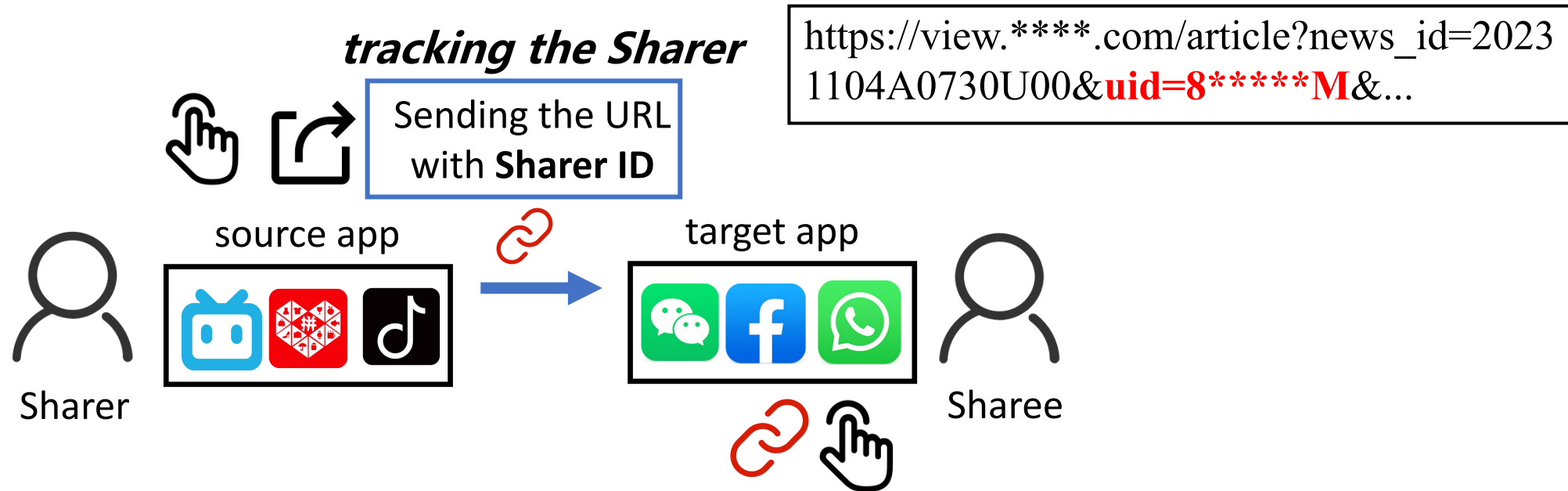
1. Sharing Behavior Tracking (SBT)



Privacy Threats



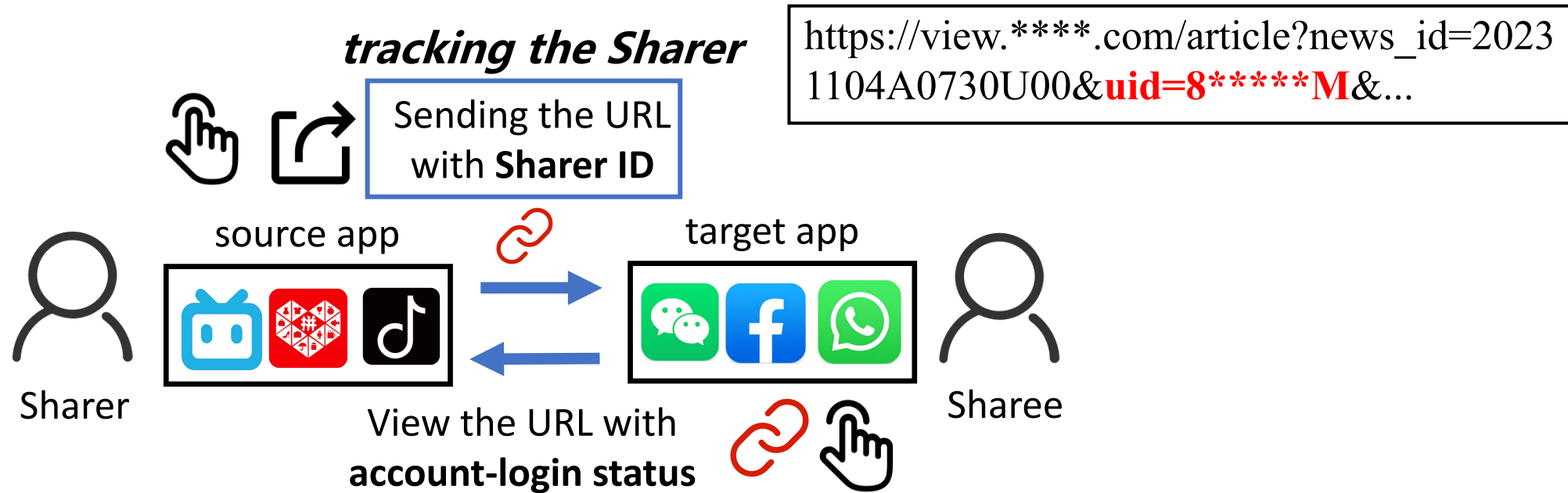
1. Sharing Behavior Tracking (SBT)



Privacy Threats



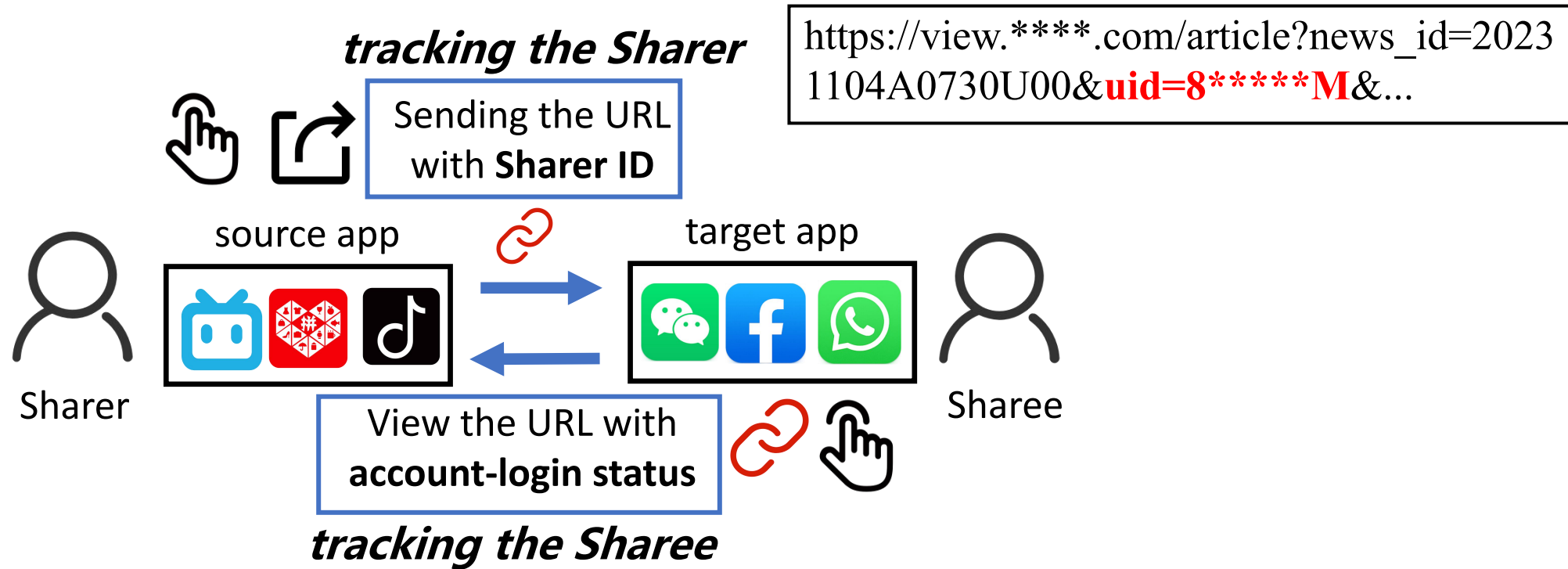
1. Sharing Behavior Tracking (SBT)



Privacy Threats



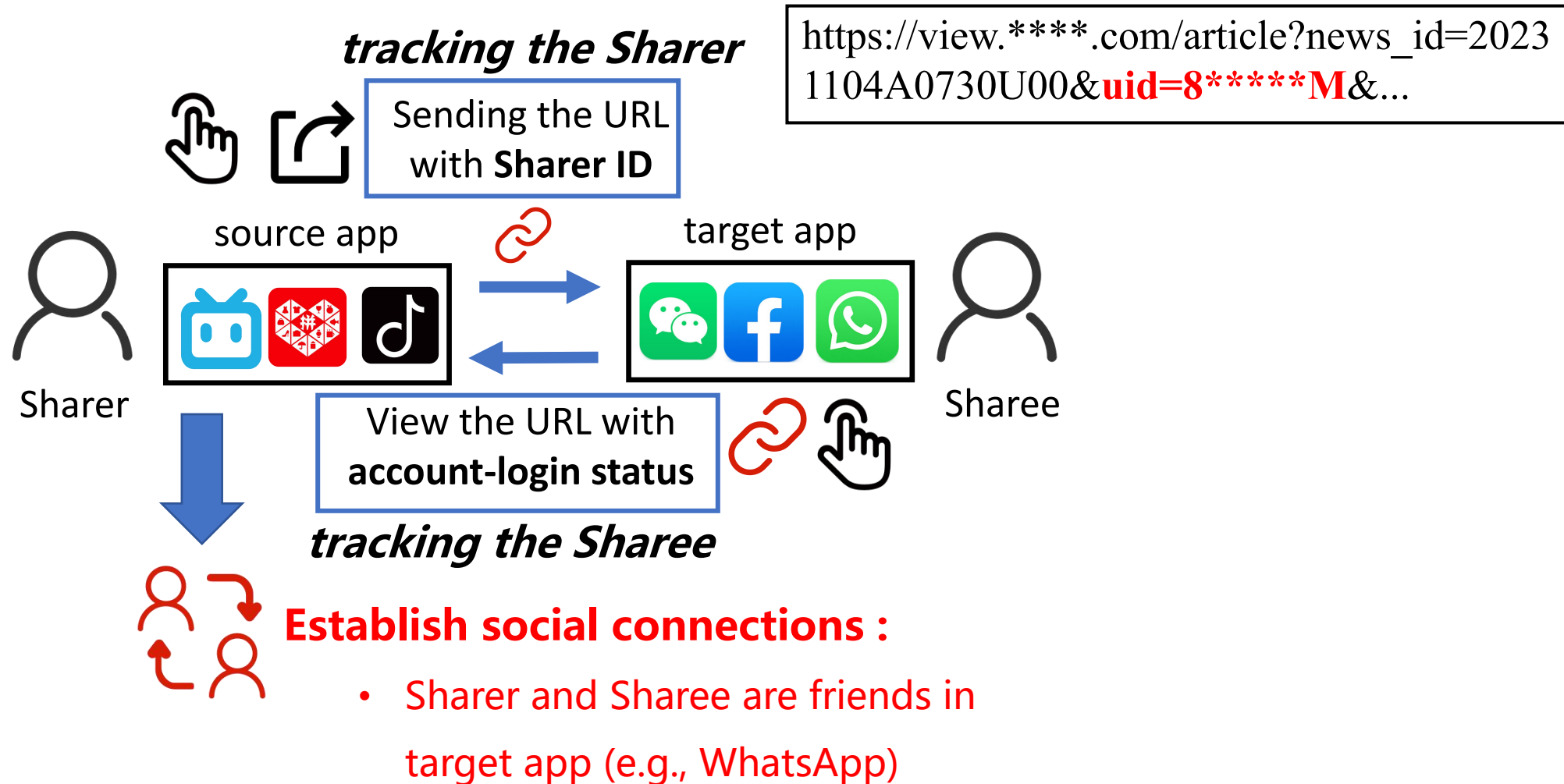
1. Sharing Behavior Tracking (SBT)



Privacy Threats



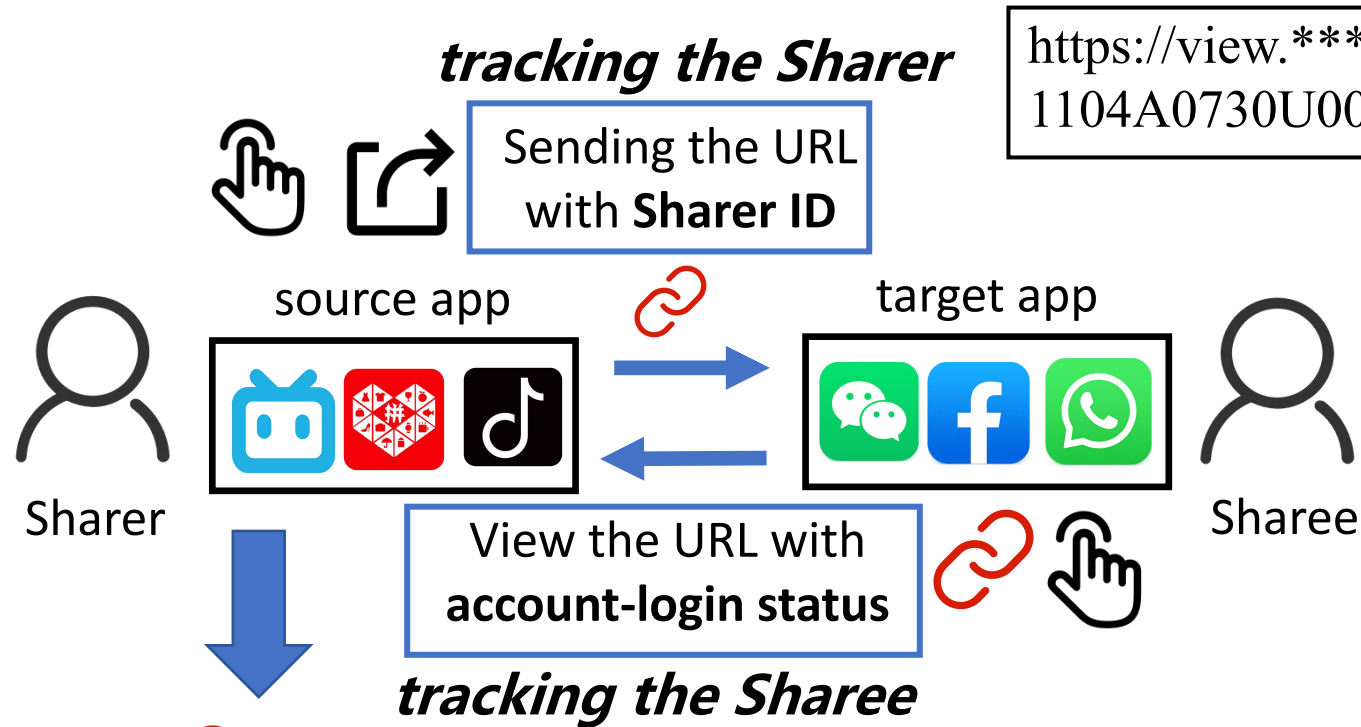
1. Sharing Behavior Tracking (SBT)



Privacy Threats

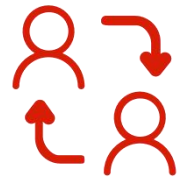


1. Sharing Behavior Tracking (SBT)



Social relationship is important

- Similar to contact list
 - **App must access it via user permission**



Establish social connections :

- Sharer and Sharee are friends in target app (e.g., WhatsApp)

Privacy Threats



2. Sharing Data Interception (SDI)

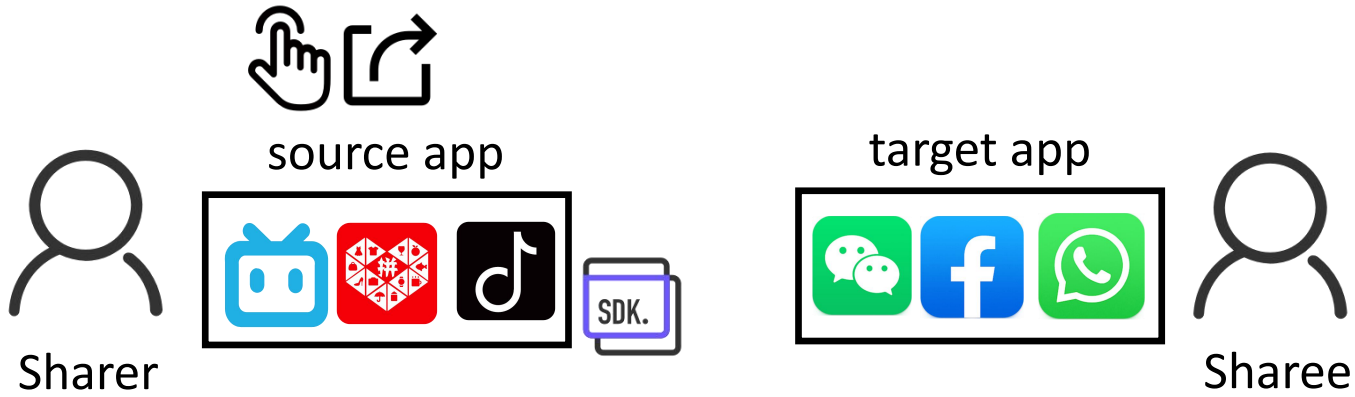


```
public static void shareToPlatform (shareEntity) {  
  
    SNSManager.share2WeChat (shareEntity);  
  
    ShareResultAPI.shareResult (shareEntity);  
    ...  
}
```

Privacy Threats



2. Sharing Data Interception (SDI)

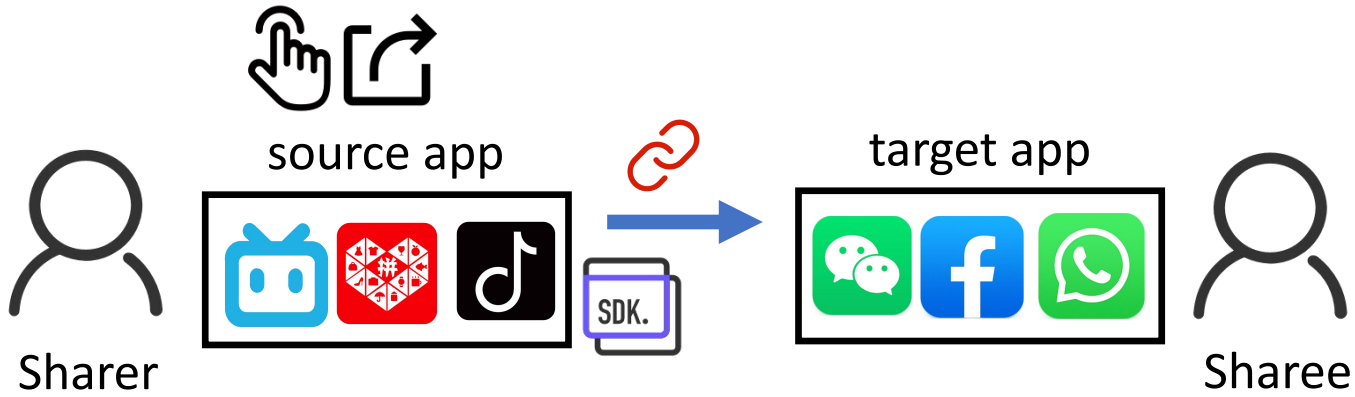


```
public static void shareToPlatform (shareEntity) {  
  
    SNSManager.share2WeChat (shareEntity);  
  
    ShareResultAPI.shareResult (shareEntity);  
    ...  
}
```


Privacy Threats



2. Sharing Data Interception (SDI)

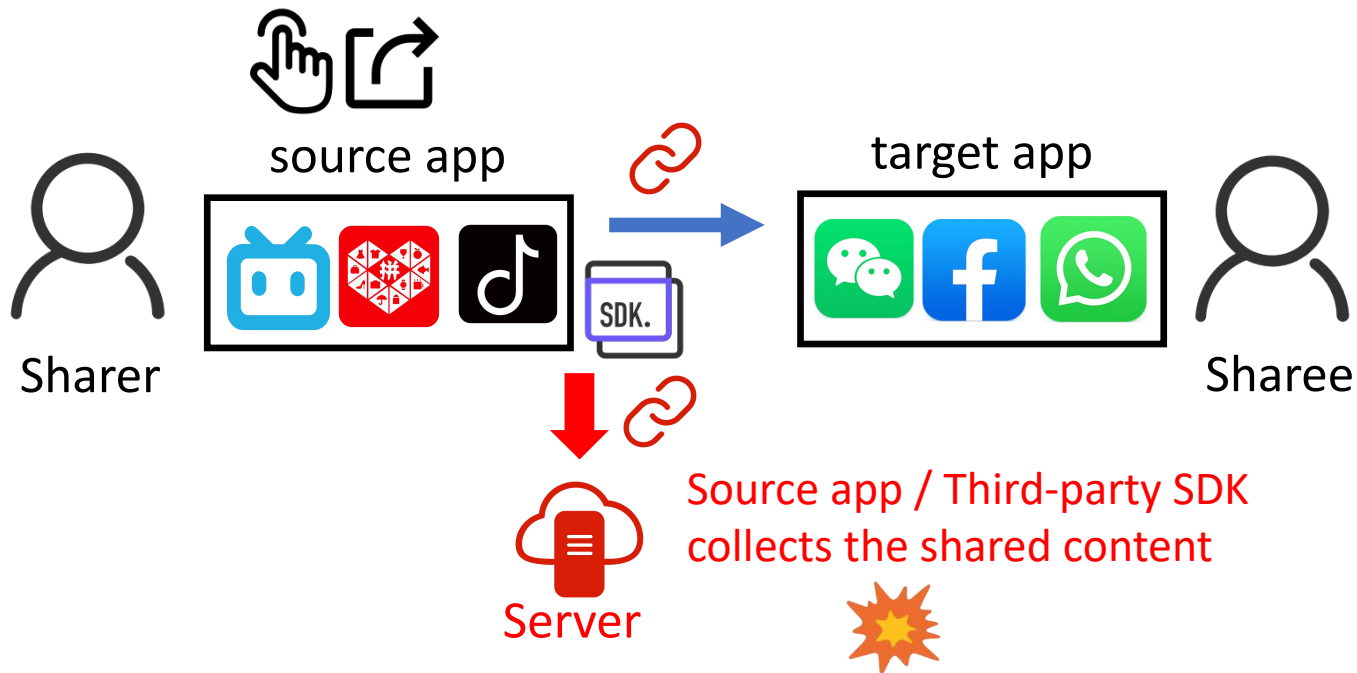


```
public static void shareToPlatform (shareEntity) {  
  
    Send content to WeChat (Necessary)  
    SNSManager.share2WeChat (shareEntity);  
  
    ShareResultAPI.shareResult (shareEntity);  
    ...  
}
```

Privacy Threats



2. Sharing Data Interception (SDI)

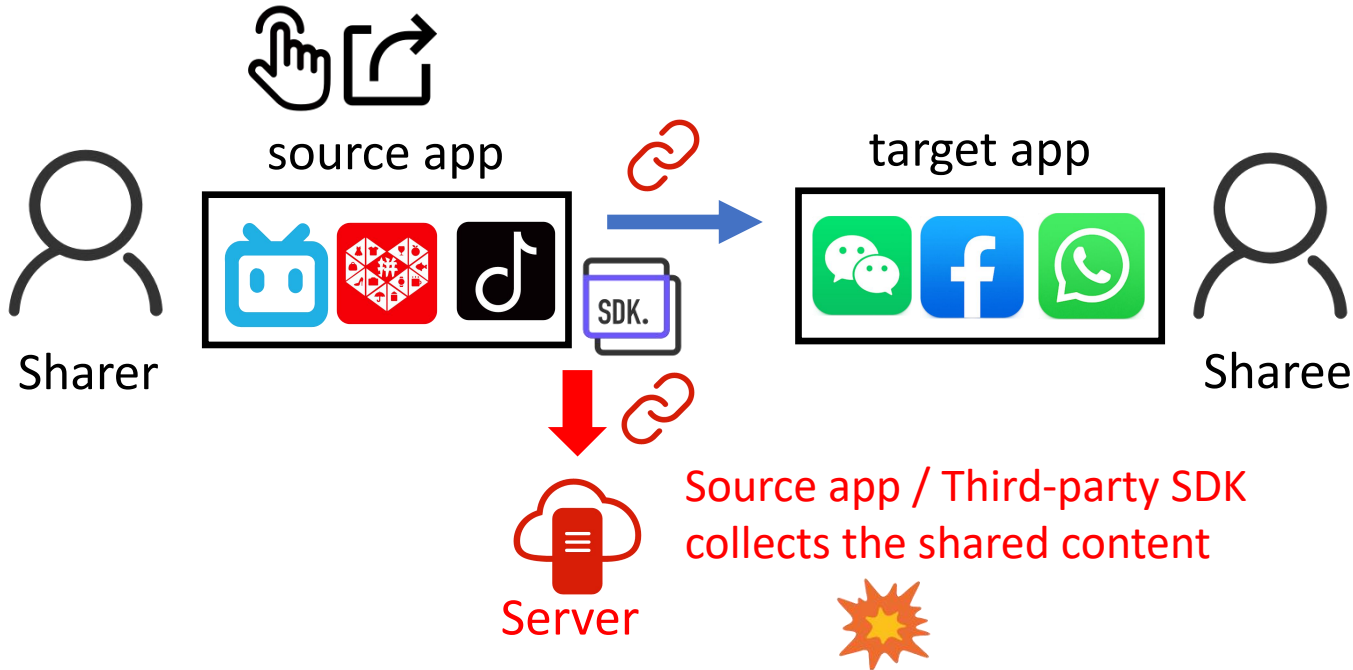


```
public static void shareToPlatform (shareEntity) {  
  
    Send content to WeChat (Necessary)  
    SNSManager.share2WeChat (shareEntity);  
  
    Send the content to Server (Unnecessary)  
    ShareResultAPI.shareResult (shareEntity);  
    ...  
}
```

Privacy Threats



2. Sharing Data Interception (SDI)



```
public static void shareToPlatform (shareEntity) {  
  
    Send content to WeChat (Necessary)  
    SNSManager.share2WeChat (shareEntity);  
  
    Send the content to Server (Unnecessary)  
    ShareResultAPI.shareResult (shareEntity);  
    ...  
}
```

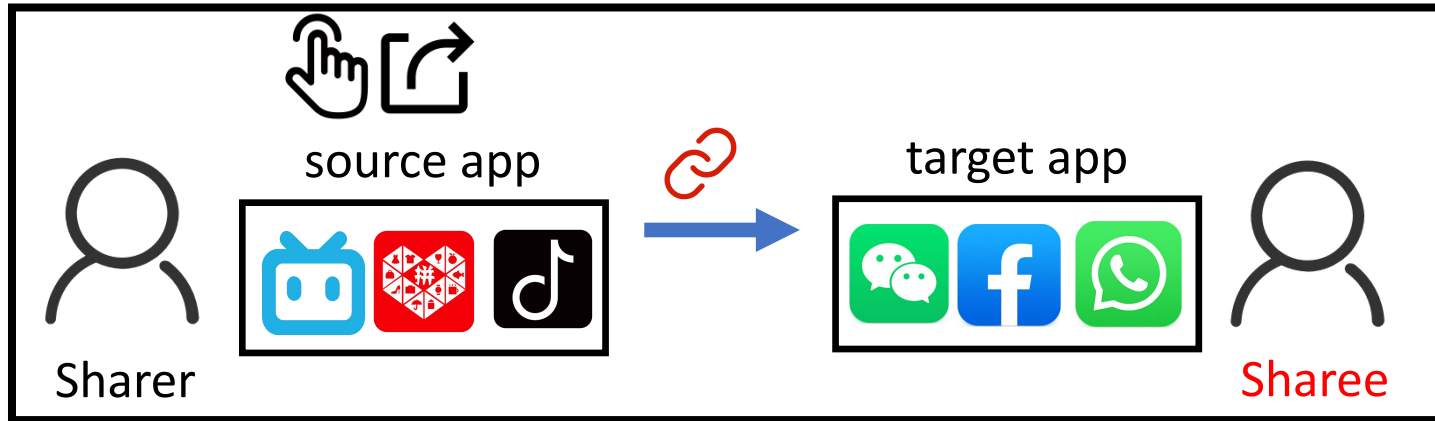
- **Violation of least privilege :**

Interception logic is fundamentally not necessary for **CRACS**, as **CRACS** is done locally without network accessing

Privacy Threats



3. Sharer Data Exposure (SDE)



After **sharee** accesses the shared content URL

3. Sharer Data Exposure (SDE)

`https://www.x*****.com/discovery/item/65018cee0000000015008456?appid=611*****1e7`

- ① **Sharee** extracts the URL of the content and get the **Sharer ID**

3. Sharer Data Exposure (SDE)

`https://www.x*****.com/discovery/item/65018cee0000000015008456?appuid=611*****1e7`



`https://www.x*****.com/user/profile/611*****1e7`

① **Sharee** extracts the URL of the content and get the **Sharer ID**

② **Sharee** builds the **Sharer** homepage URL

Privacy Threats



3. Sharer Data Exposure (SDE)

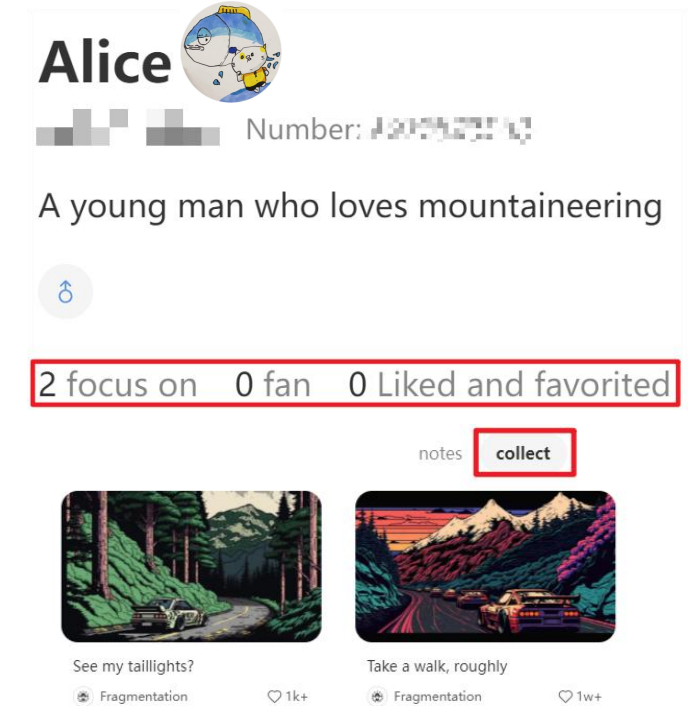
https://www.x*****.com/discovery/item/65018cee0000000015008456?appuid=611*****1e7

① **Sharee** extracts the URL of the content and get the **Sharer ID**



https://www.x*****.com/user/profile/611*****1e7

② **Sharee** builds the **Sharer** homepage URL



③ **Sharee** can access the user profile through homepage URL and monitor the **Sharer**

Privacy Implications



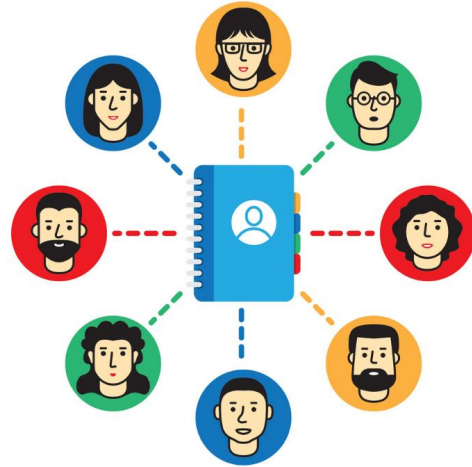
User profile leakage

- Political inclination
- Diseases history
- Interests



Social relationship leakage

- Friends
- Family
- Special groups



Privacy Implications



User profile leakage

- Political inclination
- Diseases history
- Interests



Social relationship leakage

- Friends
- Family
- Special groups

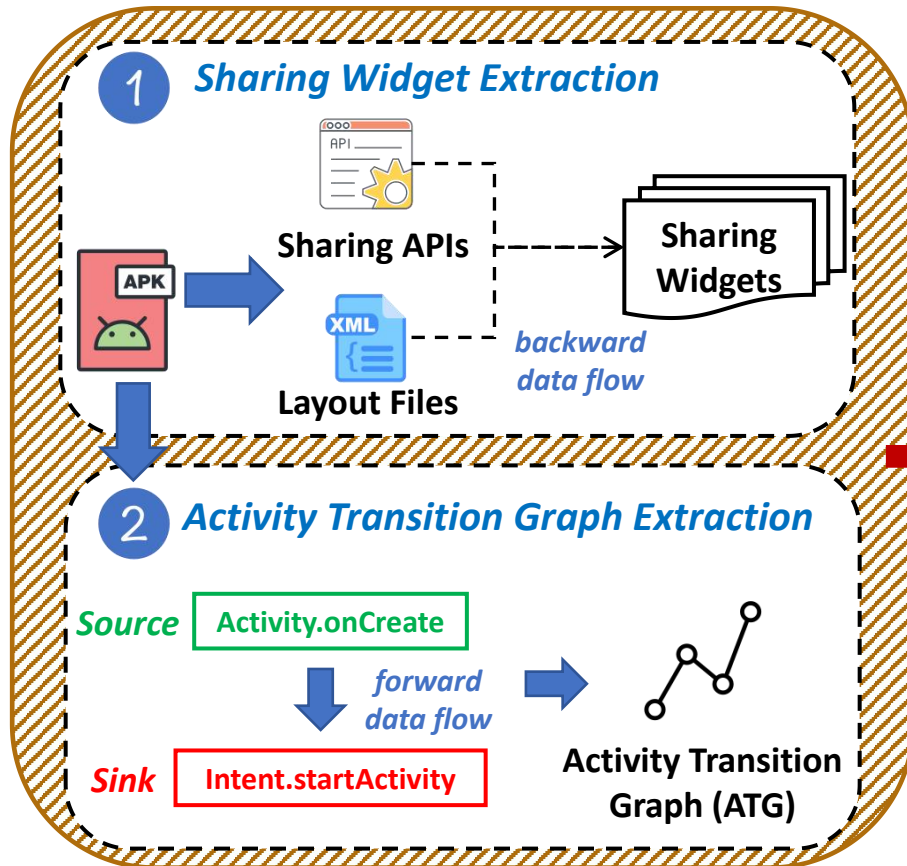


Adversary can identify
different groups of users and their portrait

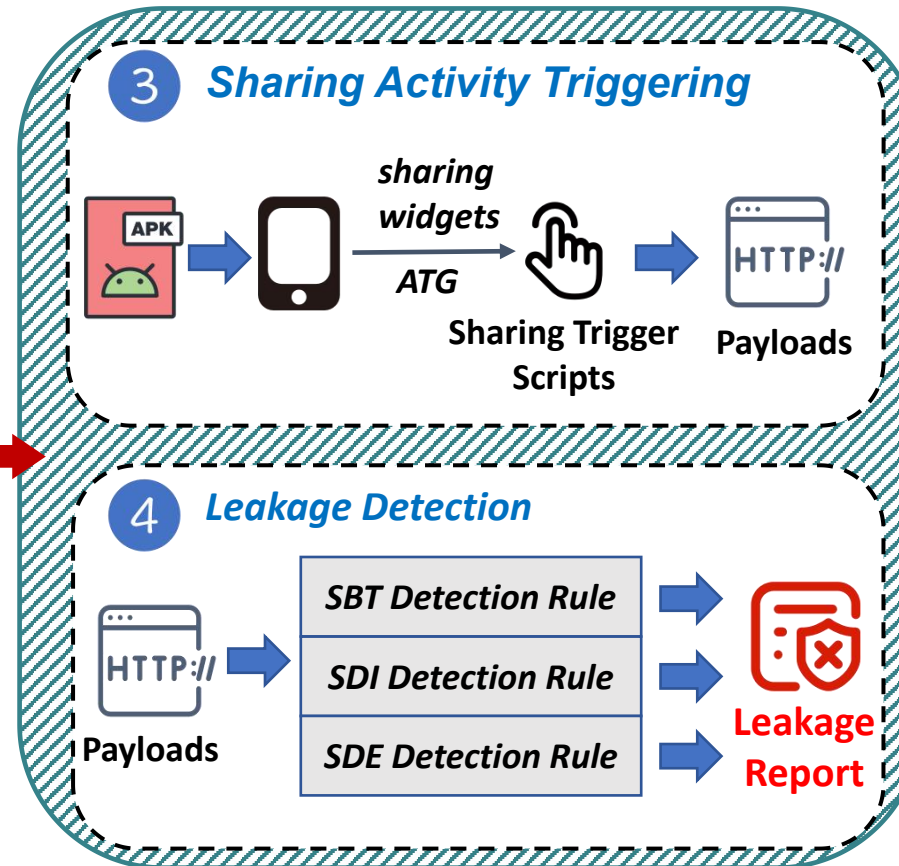
Analyzing CRACS Data Practices in Mobile Apps



Phase A: Static Information Extraction



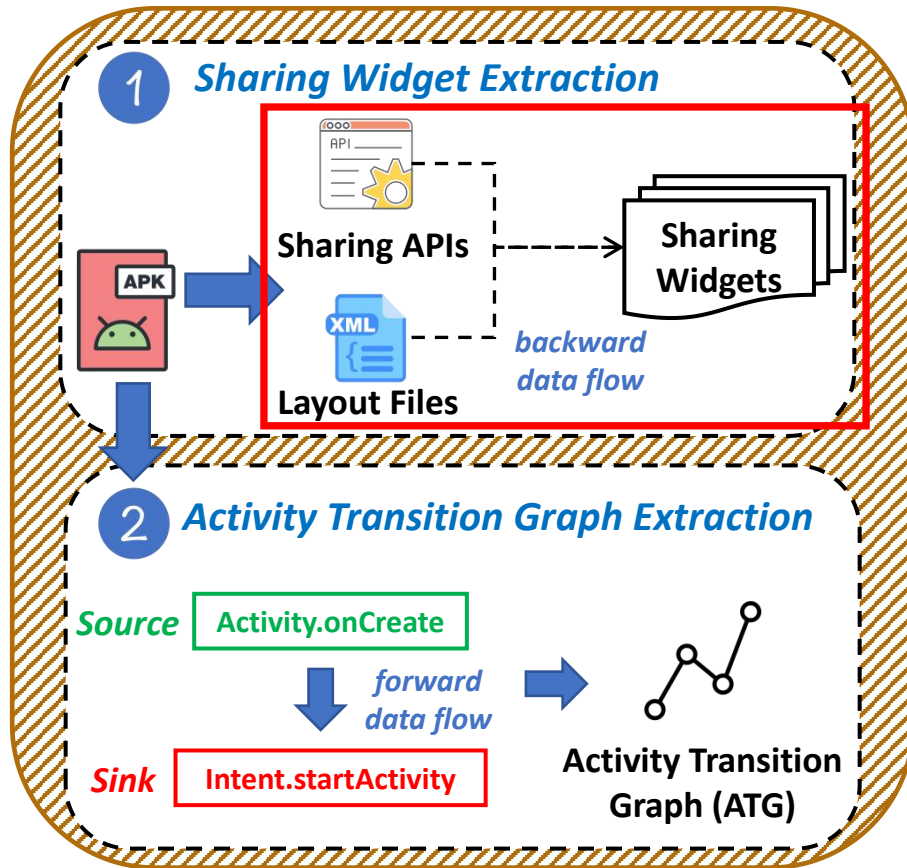
Phase B: Dynamic Leakage Confirmation



Analyzing CRACS Data Practices in Mobile Apps



Phase A: Static Information Extraction



Sharing API : provided by target app, used for content sharing

- `com.facebook.share.ShareApi: void share(ShareContent)`

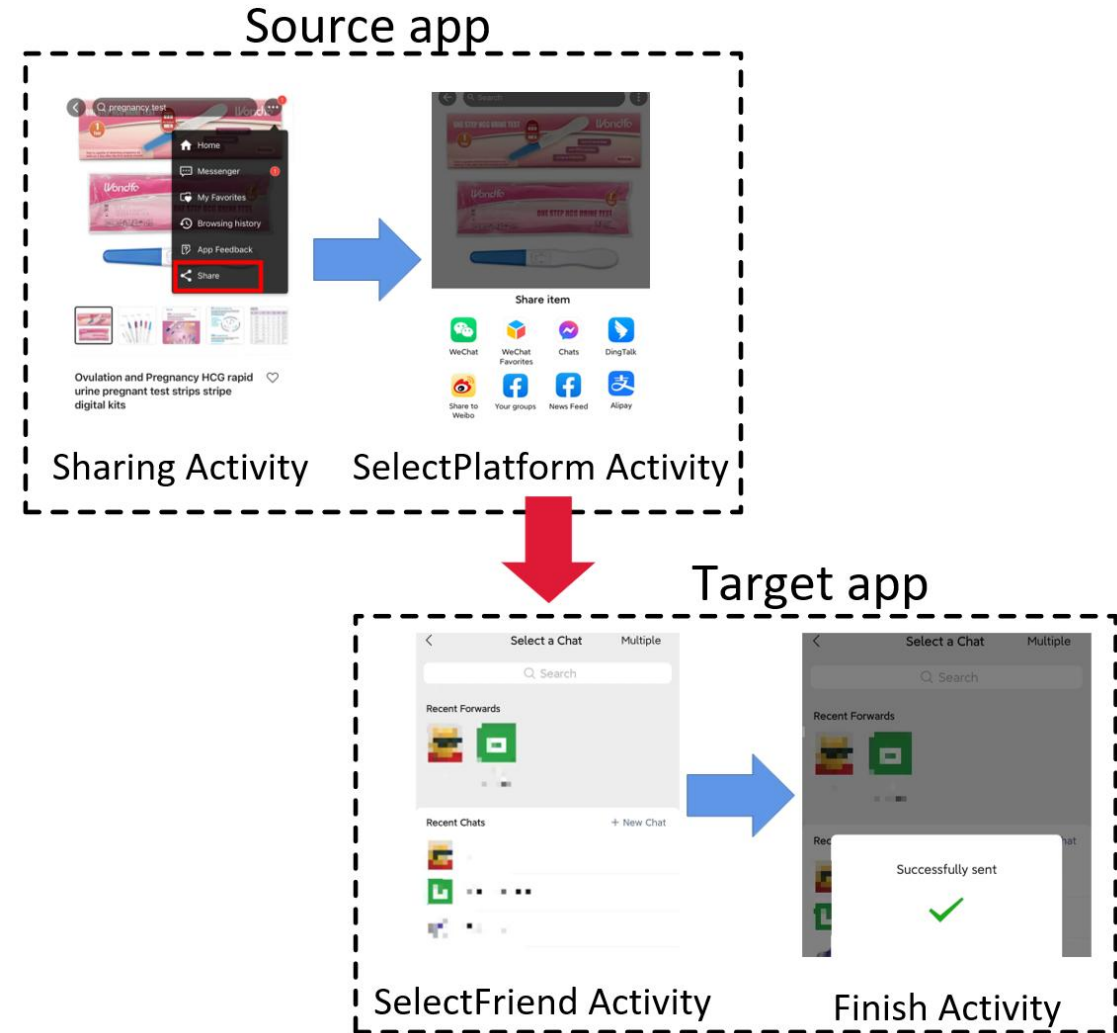
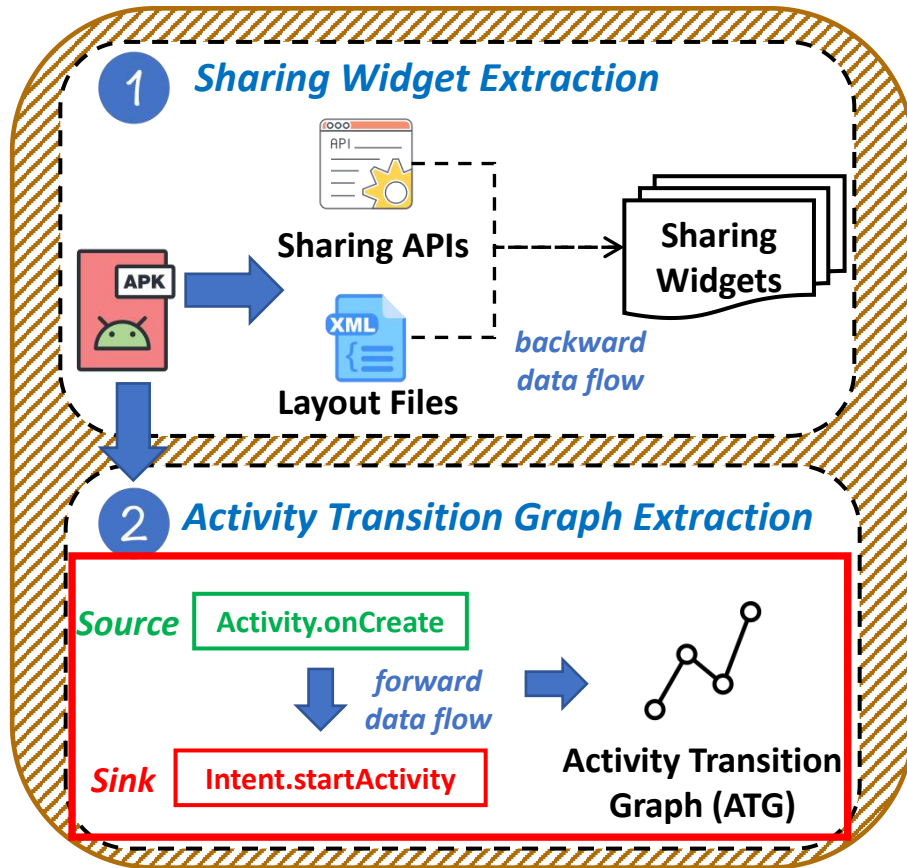
Sharing Widgets : used for trigger the sharing activity once the sharer clicks it



Analyzing CRACS Data Practices in Mobile Apps



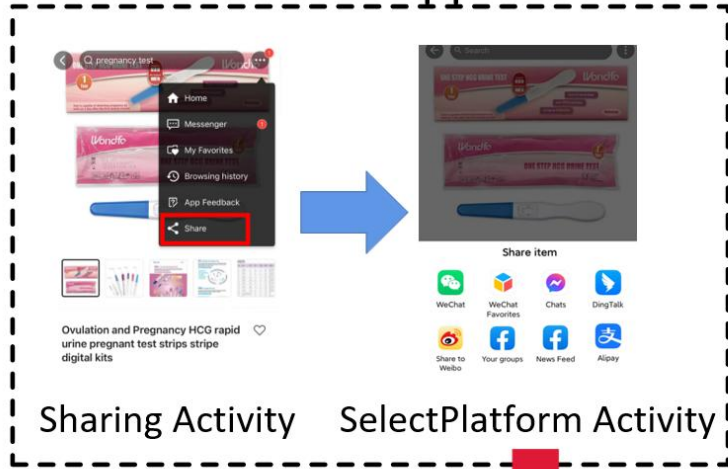
Phase A: Static Information Extraction



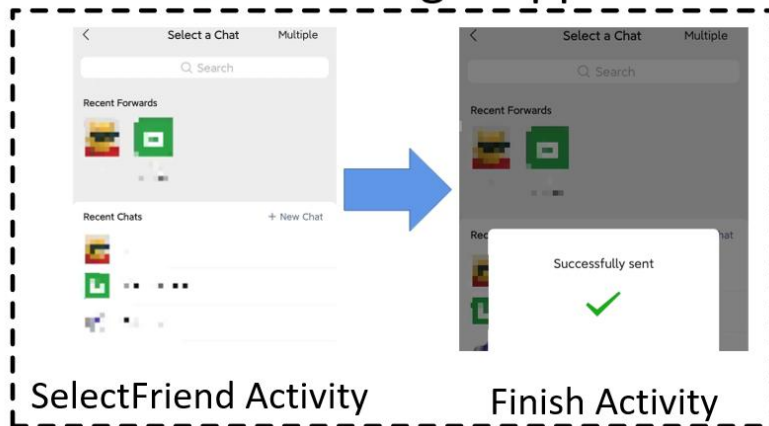
Analyzing CRACS Data Practices in Mobile Apps



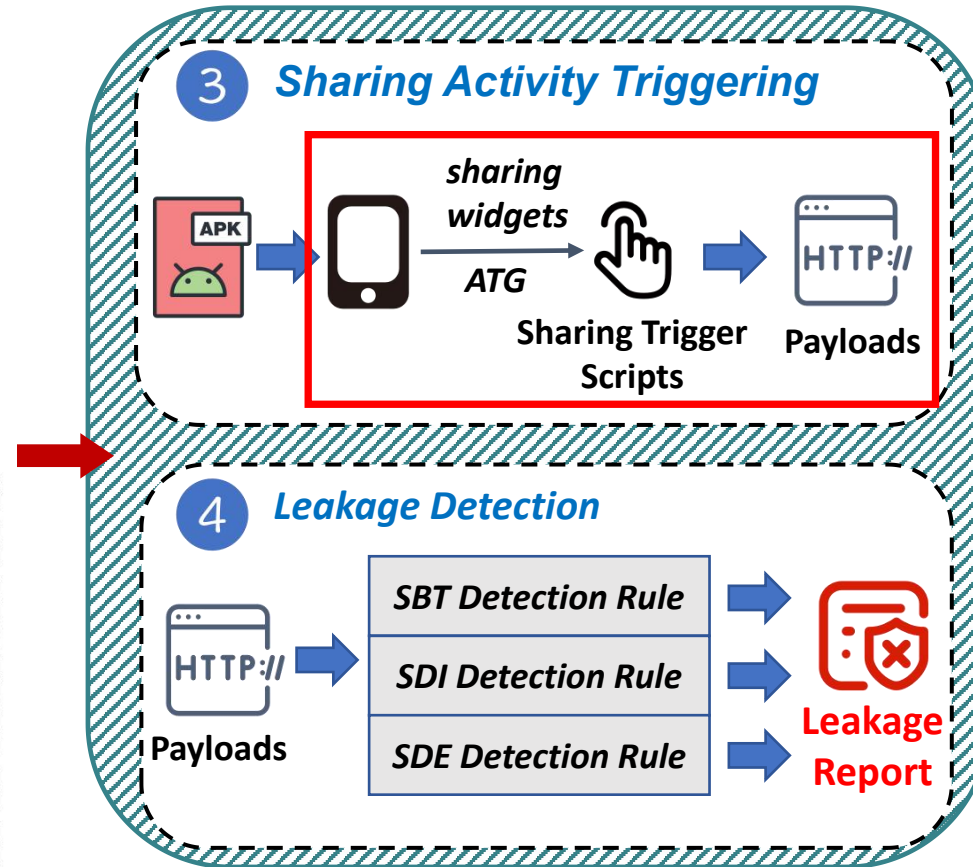
Source app



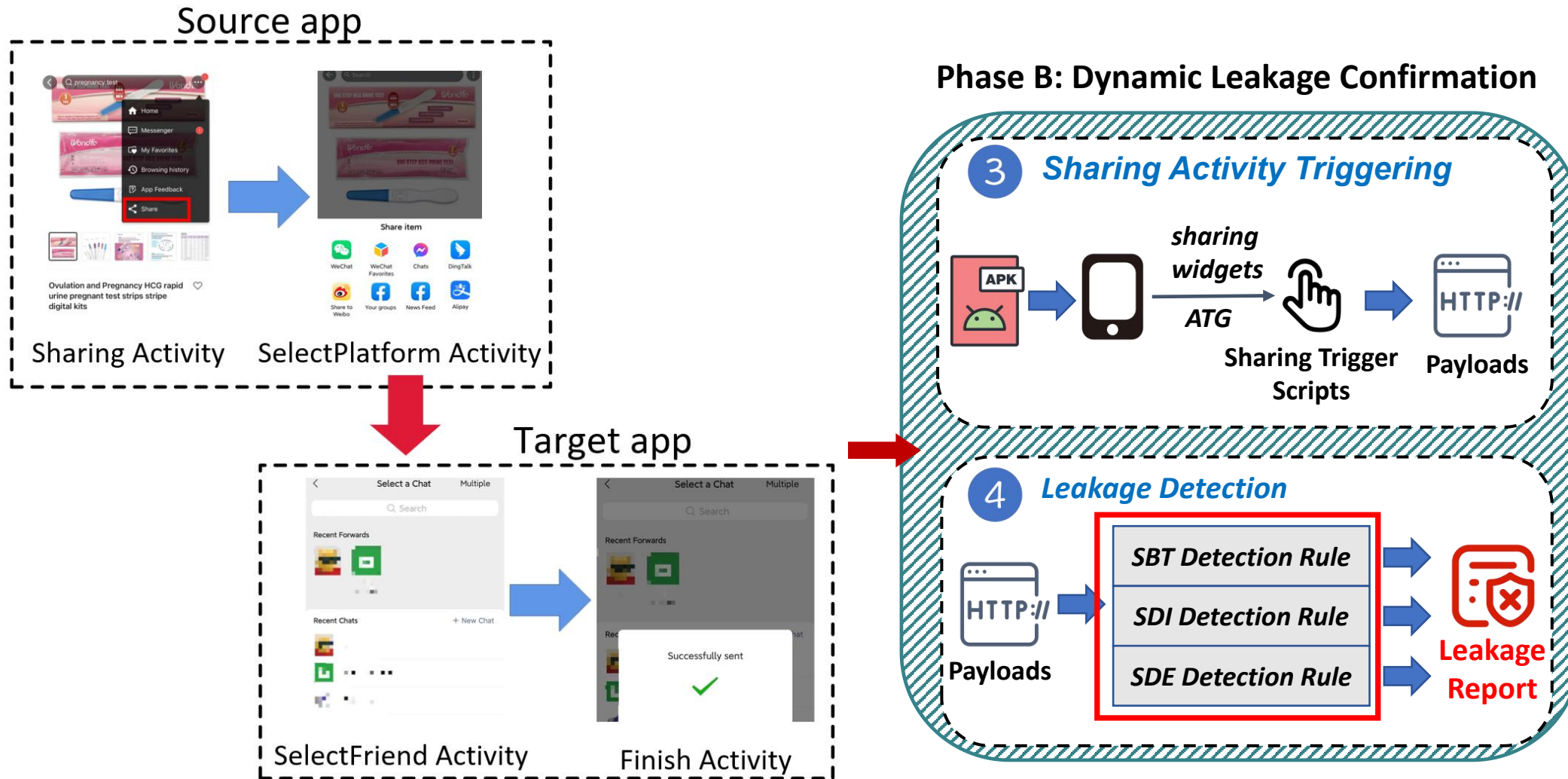
Target app



Phase B: Dynamic Leakage Confirmation



Analyzing CRACS Data Practices in Mobile Apps



Please check our paper for more details 😊

Sharing Leaks in the Wild



Datasets

- Top 300 download apps in two region
 - Top 150 download apps from China (Xiaomi store)
 - Top 150 download apps from US (Google play)

Sharing Leaks in the Wild



Datasets

- Top 300 download apps in two region
 - Top 150 download apps from China (Xiaomi store)
 - Top 150 download apps from US (Google play)

Overall result

- 186/300 apps (62%) have provided **CRACS** activity for users

Sharing Leaks in the Wild



Datasets

- Top 300 download apps in two region
 - Top 150 download apps from China (Xiaomi store)
 - Top 150 download apps from US (Google play)

Overall result

- 186/300 apps (62%) have provided **CRACS** activity for users
- **39.78% (74/186)** apps have at least one privacy threat pattern during **CRACS**

Sharing Leaks in the Wild



Overall result in China and U.S.

Region	Type	# Apps with share function	# Confirmed pattern	Percentage
China	SBT	120	52	43.33%
	SDI		19	15.83%
	SDE		26	21.67%
	Total	120	67	55.83%
U.S.	SBT	66	5	7.57%
	SDI		3	4.54%
	SDE		1	1.50%
	Total	66	7	10.60%

- Compared to the apps from U.S., there are more Chinese apps that have privacy leakage risk (**55.83% vs. 10.60%**).

Sharing Leaks in the Wild



Top 15 download apps of *SBT*

App Name	Package Name	Version	Downloads	Category
App-CN-1	c**.s*.a*****.u**.a****	25.9.0	13.4B+	Short video
App-CN-2	c**.x*****.p*****	6.64.0	11.6B+	Shopping
App-CN-3	c**.s****.g*****	11.5.20.31491	7.6B+	Short video
App-CN-4	c**.t*****.t*****	10.25.10	6.3B+	Shopping
App-CN-5	c**.s***.w****	13.6.1	5.4B+	Social Contact
App-CN-6	c**.s*****.m*****	12.10.406	4.4B+	Life Style
App-CN-7	t*.d*****.b***	7.35.0	3.6B+	Video social
App-CN-8	c**.s*.a*****.a*****.v* ***	7.6.4	3.2B+	Video social
App-CN-11	c**.t*****.n***	7.1.60	2.8B+	News
App-CN-12	c**.x*****.x**	7.91.0	2.5B+	Social Contact

- Significant and broad user impact (**Billions of downloads**)

Sharing Leaks in the Wild



Multiple types of trackers

Type	# Total	Example
UserID	28	<i>uuid</i> =d5c***aad
IMEI/DeviceID	3	<i>imei</i> =ad***0639 <i>device_id</i> =199***454
Other Identifiers	31	<i>uni</i> =119***407 <i>lch</i> =71****94b

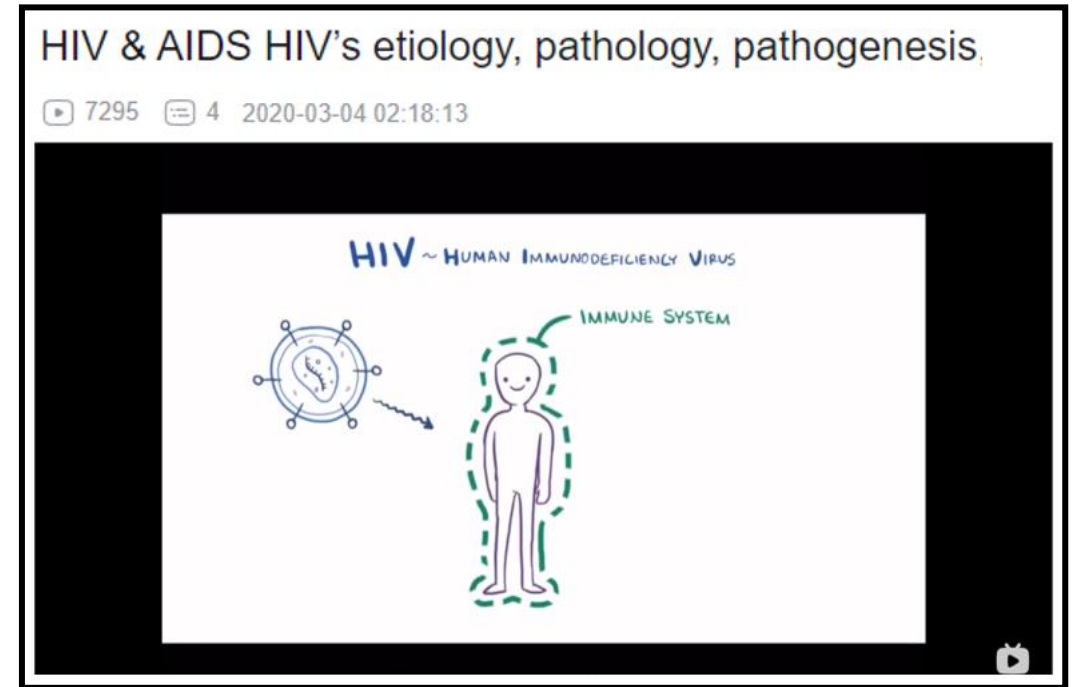
Sharing Leaks in the Wild



Multiple types of trackers

Type	# Total	Example
UserID	28	<i>uuid</i> =d5c***aad
IMEI/DeviceID	3	<i>imei</i> =ad***0639 <i>device_id</i> =199***454
Other Identifiers	31	<i>uni</i> =119***407 <i>lch</i> =71****94b

Example: Popular video app



https://www.b*****.com/video/BV1HE411A7Gb/?buvid=Z74F747F2****&mid=5ieLSWv3PT****×tamp=1688023207

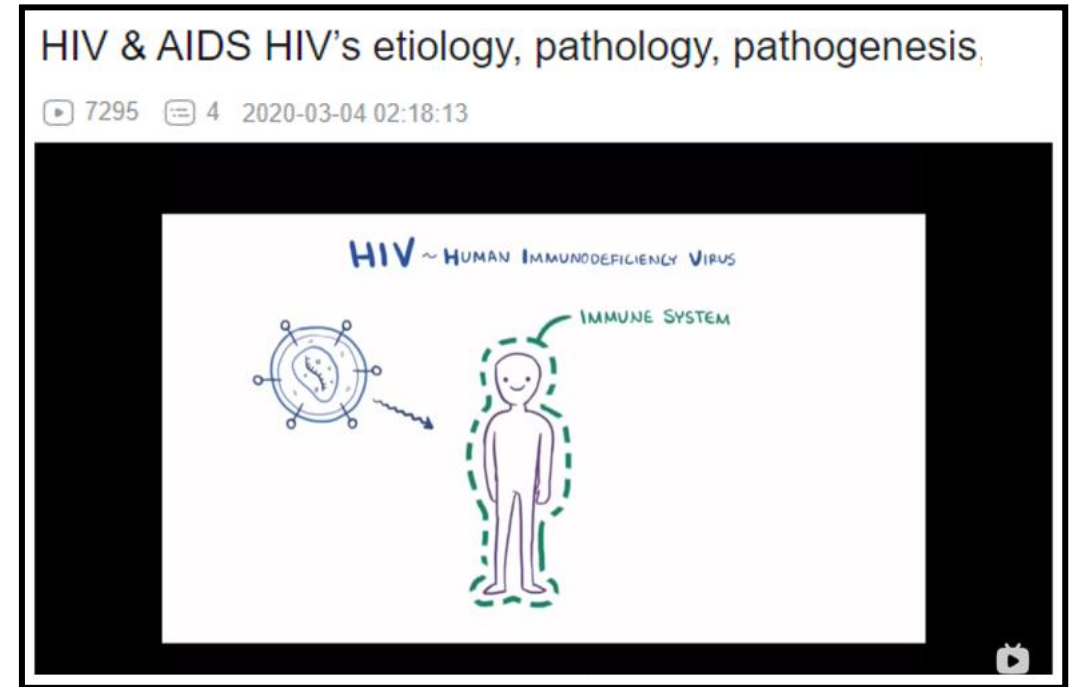
Sharing Leaks in the Wild



Example: Popular video app

Multiple types of trackers

Type	# Total	Example
UserID	28	<i>uuid</i> =d5c***aad
IMEI/DeviceID	3	<i>imei</i> =ad***0639 <i>device_id</i> =199***454
Other Identifiers	31	<i>uni</i> =119***407 <i>lch</i> =71****94b



- Infer social relationships through trackers (**buvid, mid**)
- Infer potential groups of HIV patients (sensitive attributes in video content)



https://www.b*****.com/video/BV1HE411A7Gb/?buvid=Z74F747F2****&mid=5ieLSWv3PT****×tamp=1688023207

Sharing Leaks in the Wild



Third-party SDK that collect the shared content

Package Name	Version	Downloads	Category	Third-party Sharing SDK
c**.m***.m*** ****	9.0200.02	710M+	Weather	SDK-1
c**.d*****.c** **_s*	5.4.3.1	310M+	Education	SDK-1
c**.h***.s***** *	6.79.0	150M+	Shopping	SDK-1
c**.k***.v***** *****	5.47.0.547002	140M+	VideoPlayer	SDK-2
c**.v*****	6.1.10.211025	88M+	VideoPlayer	SDK-2

Sharing Leaks in the Wild



Third-party SDK that collect the shared content

Package Name	Version	Downloads	Category	Third-party Sharing SDK
c**.m***.m*** ****	9.0200.02	710M+	Weather	SDK-1
c**.d*****.c** **_s*	5.4.3.1	310M+	Education	SDK-1
c**.h***.s**** *	6.79.0	150M+	Shopping	SDK-1
c**.k***.v**** *****	5.47.0.547002	140M+	VideoPlayer	SDK-2
c**.v*****	6.1.10.211025	88M+	VideoPlayer	SDK-2

Example: Popular third-party SDK

```
{
  "imgs": [
    "https://****.com/suo/image/Cw.webp?urlModule=templateCover"
  ],
  "text": "share a fun template for you, come to experience!",
  "attach": {
    "musicFileUrl": "https://****.com/share/template/index.html?id=8****1&trace_id=D*****73090",
    "image": [
      "https://****.com/suo/image/Cw.webp?urlModule=templateCover"
    ],
    "title": "[template]",
    "url": "https://****.com/share/template/index.html?id=8****1&trace_id=D*****73090",
    "content": "share a fun template for you, come to experience!"
  },
  "url": [
    "https://****.com/share/template/index.html?id=8****1&trace_id=D*****73090"
  ]
}
```

- Unnecessary collects the shared content during **CRACS**
- Integrated by apps with more than 2.2 billion downloads in our dataset

Summary



- New understandings of cross-app privacy leakage
 1. Sharing Behavior Tracking (**SBT**)
 2. Sharing Data Interception (**SDI**)
 3. Sharer Data Exposure (**SDE**)

- New analysis pipeline to detect various privacy exposure venues in **CRACS**

- Systematical analyzed 300 top downloaded apps to reveal the pervasiveness of the privacy threats in **CRACS** in the real world



Thanks

Jiangrong Wu
Sun Yat-sen University
wujr28@mail2.sysu.edu.cn



中山大學
SUN YAT-SEN UNIVERSITY



INDIANA
UNIVERSITY

Alibaba Group
阿里巴巴集团



復旦大學
FUDAN UNIVERSITY