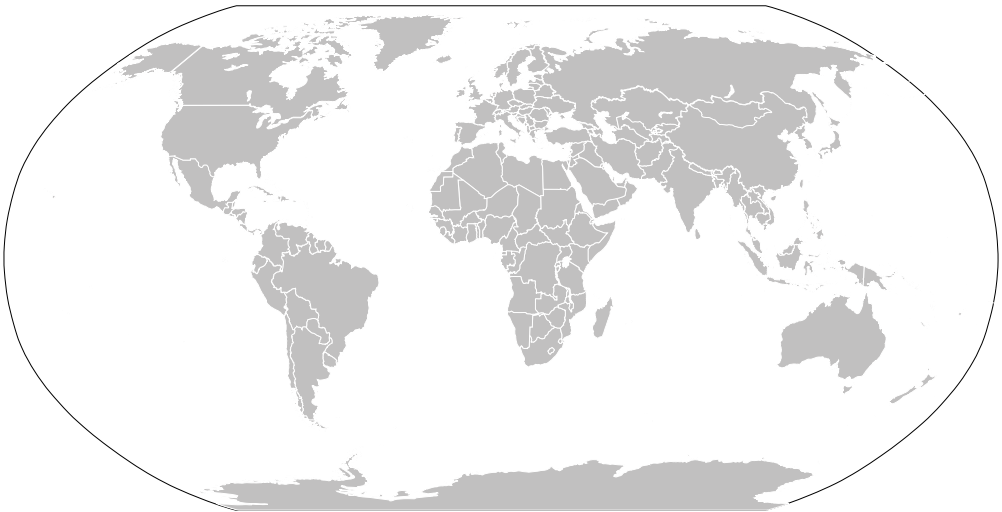
Uncovering and Exploiting Hidden APIs in Mobile Super Apps

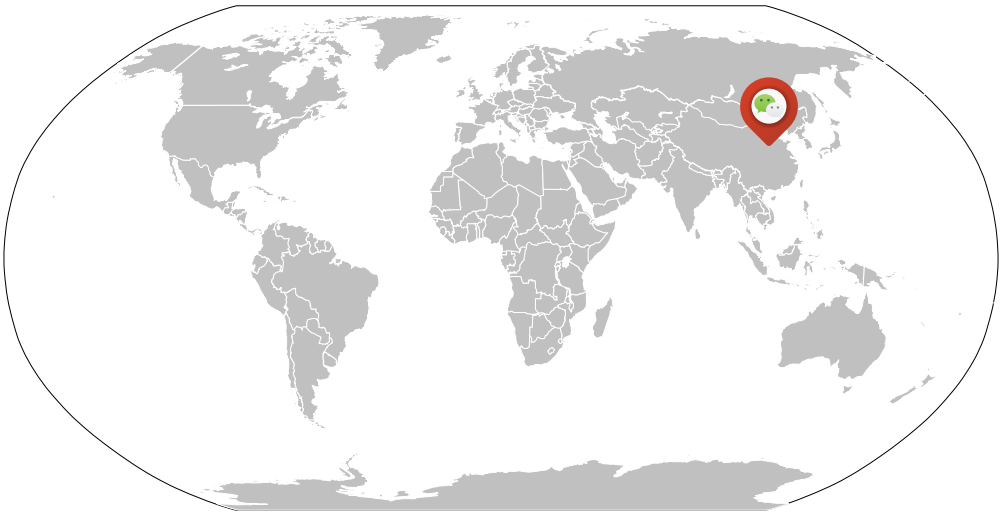
Chao Wang, Yue Zhang, and **Zhiqiang Lin**

ACM CCS 2023

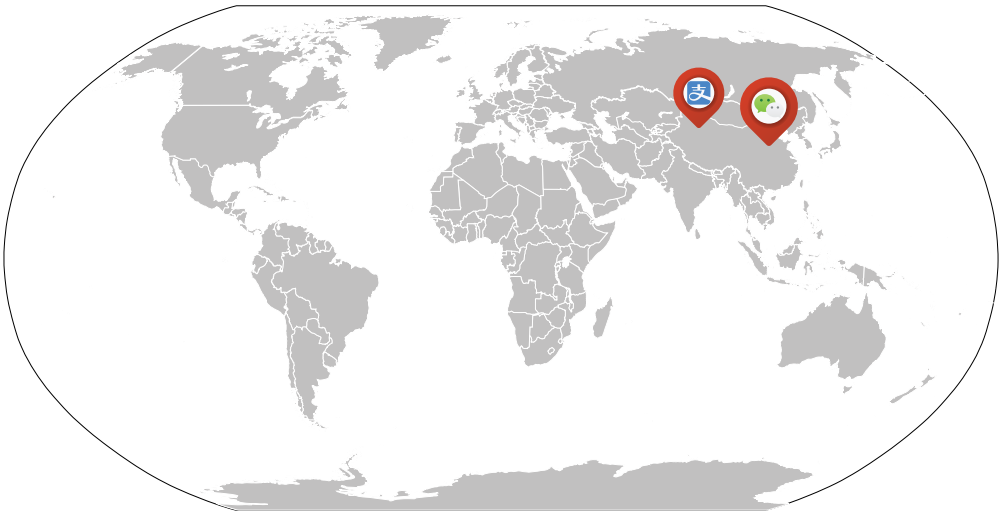
The World of SuperApps



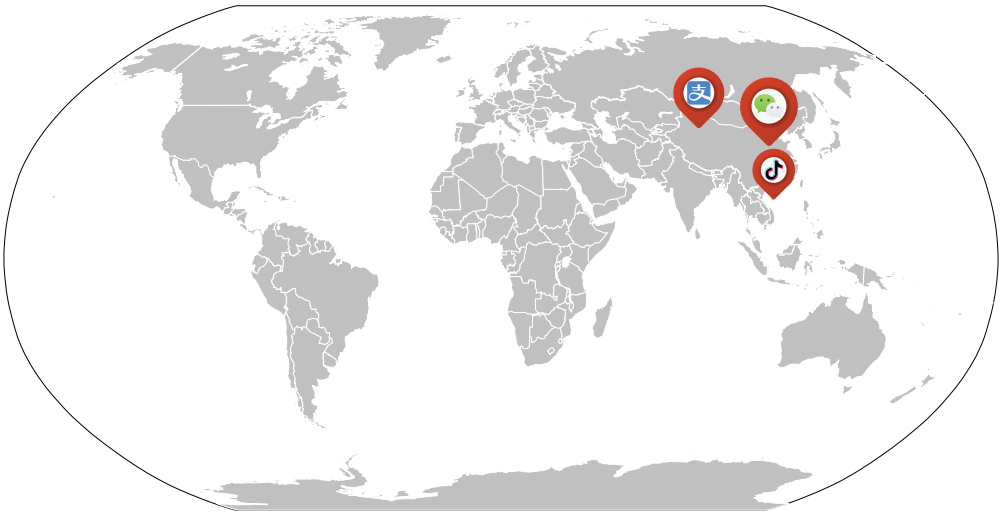
The World of SuperApps



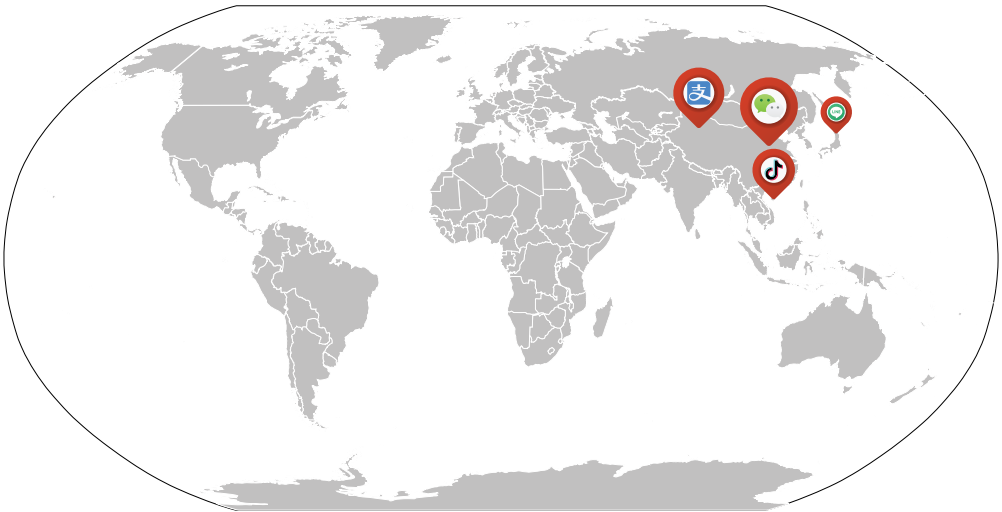
The World of SuperApps



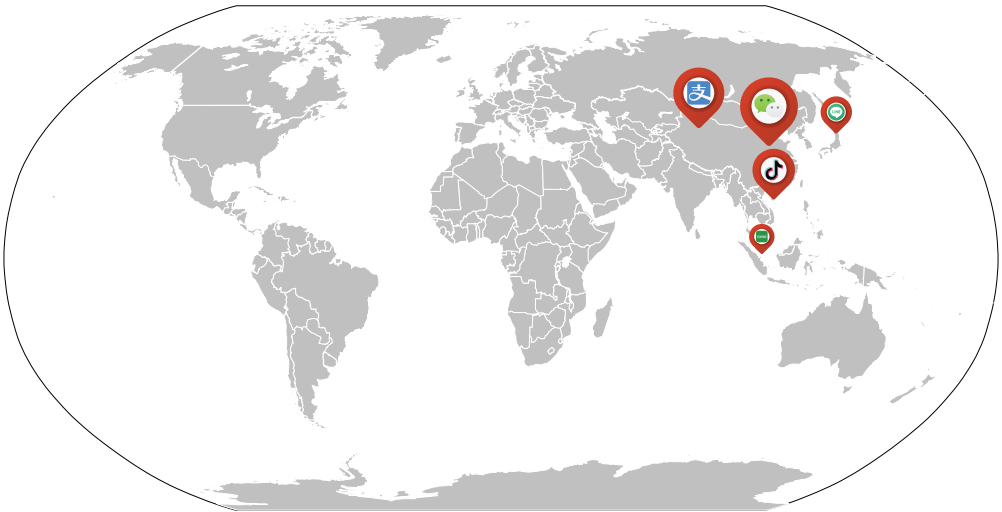
The World of SuperApps



The World of SuperApps



The World of SuperApps



The World of SuperApps

The World of SuperApps

The World of SuperApps

The World of SuperApps

The World of SuperApps

The New York Times | https://www.nytimes.com/2023/07/23/business/elon-musk-twitter-logo.html

Elon Musk Changes Twitter Logo to an X

The tech billionaire replaced the company's blue bird silhouette with "X," a term for what he has described as an "everything app."


By Noam Scheiber and Ryan Mac

Published July 23, 2023 Updated July 24, 2023, 6:11 a.m. ET

Elon Musk has made one of the most visible changes to Twitter since he took control of the social media company last fall: replacing its widely recognized bird logo.

...

"X" is a term for what Mr. Musk has described as an "everything app" that could combine social media, instant messaging and payment services, akin to the popular Chinese app WeChat.

Mr. Musk has said that buying Twitter is "an accelerant to creating X," and the corporate entity he created to purchase and control Twitter is called X Holdings.

…

The World of SuperApps

The New York Times | https://www.nytimes.com/2023/07/23/business/elon-musk-twitter-logo.html

Elon Musk Changes Twitter Logo to an X

The tech billionaire replaced the company's blue bird silhouette with "X," a term for what he has described as an "everything app."

By Noam Scheiber and Ryan Mac

Published July 23, 2023 Updated July 24, 2023, 6:11 a.m. ET

Elon Musk has made one of the most visible changes to Twitter since he took control of the social media company last fall: replacing its widely recognized bird logo.

...

"X" is a term for what Mr. Musk has described as an "everything app" that could combine social media, instant messaging and payment services, akin to the popular Chinese app WeChat.

Mr. Musk has said that buying Twitter is "an accelerant to creating X," and the corporate entity he created to purchase and control Twitter is called X Holdings.

…

Superapps Provide Multiple Services

From daily life essentials to governmental services






Superapps Provide Multiple Services

But how do those superapps accomplish that?






Superapps Provide Multiple Services

Miniapps

Superapps Provide Multiple Services

Miniapps ... how?

Miniapps are Built on Top of APIs

The power of APIs

Miniapps are Built on Top of APIs

Some APIs can be more powerful!

Miniapps are Built on Top of APIs

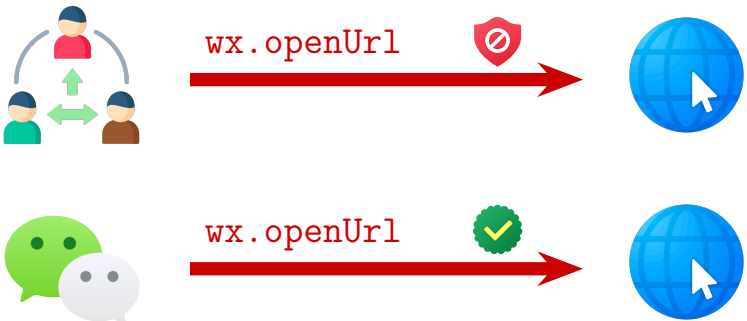
Third-party miniapps use documented APIs that are vetted

Miniapps are Built on Top of APIs

First-party miniapps can use privileged APIs

Miniapps are Built on Top of APIs

But third-party Miniapps cannot access privileged APIs



Miniapps are Built on Top of APIs

Moreover, not all APIs are equally mentioned in official documents

Chinese Document **975 APIs**

Miniapps are Built on Top of APIs

Moreover, not all APIs are equally mentioned in official documents

Chinese Document **975 APIs**

English Document **570 APIs**

Miniapps are Built on Top of APIs

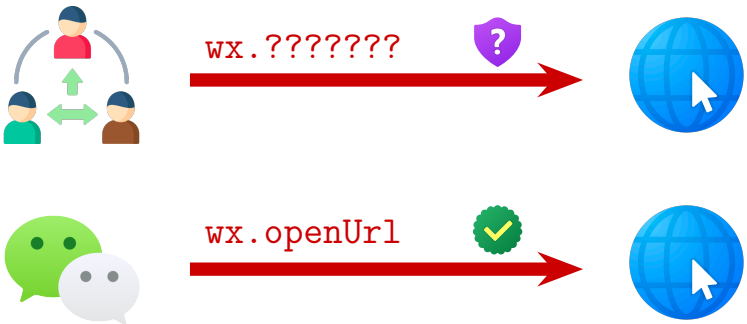
They are not 100% transparent ...

Chinese Document **975 APIs**

English Document **570 APIs**

Hidden APIs

Will there be any hidden APIs that can do the same thing?



Hidden APIs

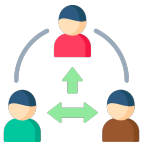
Yes! via `wx.private_openUrl` for example

`wx.private_openUrl`

`wx.openUrl`

Hidden APIs

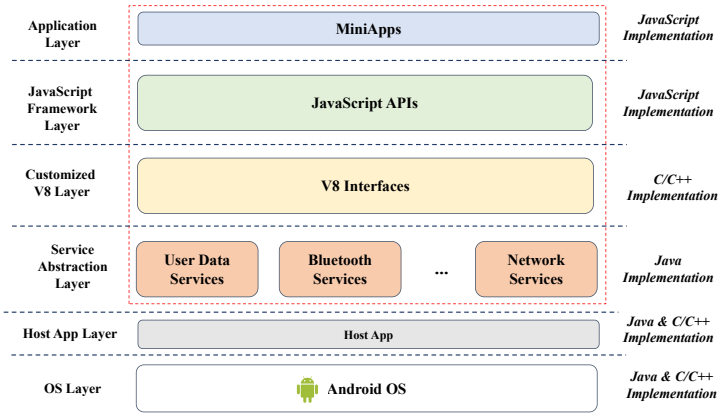
So, we must systematically find those hidden APIs?



`wx.private_openUrl`

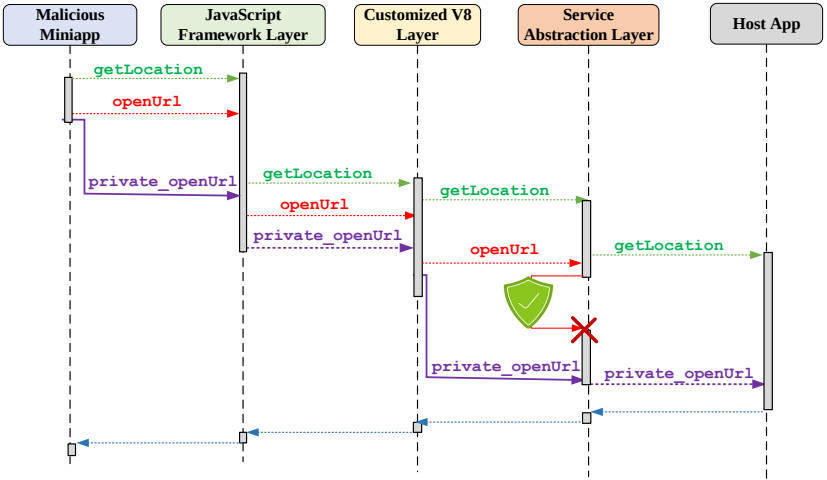
`wx.openUrl`

The Superapp Runtime



Architecture of Superapp Runtime in Android.

The Workflow of API Invocations



It is Challenging to Uncover Hidden APIs...

Challenges

1. How to identify undocumented APIs in different superapps
2. How to classify undocumented APIs into different categories (privileged vs unprivileged)
3. How to determine undocumented APIs whether are invocable

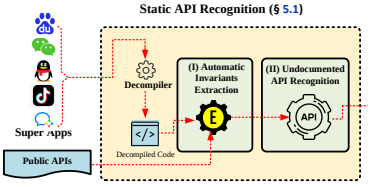
Our Solution

Solutions

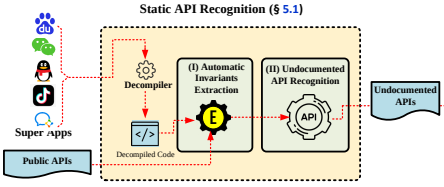
1. How to identify undocumented APIs in different superapps
   Automatic invariants extraction
2. How to classify undocumented APIs into different categories (privileged vs unprivileged)
   Dynamic API probing for API category classification
3. How to determine undocumented APIs whether are invocable
   Forward slicing for API invocation identification

APIScope

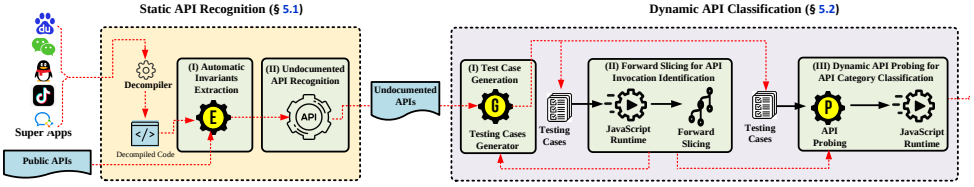
APIScope


Static API Recognition (§ 5.1)
Super Apps
Public APIs
Decompiler
Decompiled Code
(I) Automatic Invariants Extraction
(II) Undocumented API Recognition
API

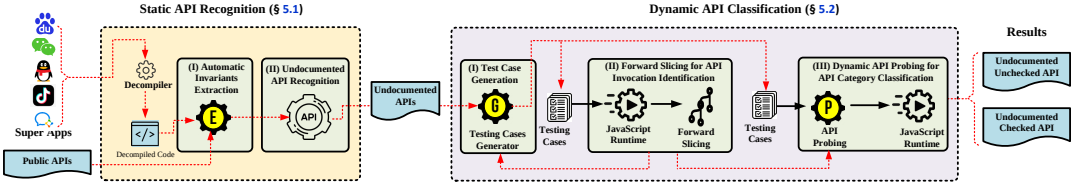
APIScope


Static API Recognition (§ 5.1)
Super Apps
Public APIs
Decompiler
Decompiled Code
(I) Automatic Invariants Extraction
(II) Undocumented API Recognition
API
Undocumented APIs

APIScope


Static API Recognition (§ 5.1)
Dynamic API Classification (§ 5.2)
Super Apps
Public APIs
Decompiler
Decompiled Code
(I) Automatic Invariants Extraction
(II) Undocumented API Recognition
Undocumented APIs
(I) Test Case Generation
Testing Cases Generator
Testing Cases
(II) Forward Slicing for API Invocation Identification
JavaScript Runtime
Forward Slicing
Testing Cases
(III) Dynamic API Probing for API Category Classification
API Probing
JavaScript Runtime

APIScope


Static API Recognition (§ 5.1)
Dynamic API Classification (§ 5.2)
Results
Super Apps
Public APIs
Decompiler
Decompiled Code
(I) Automatic Invariants Extraction
(II) Undocumented API Recognition
API
Undocumented APIs
(I) Test Case Generation
Testing Cases Generator
Testing Cases
(II) Forward Slicing for API Invocation Identification
JavaScript Runtime
Forward Slicing
Testing Cases
(III) Dynamic API Probing for API Category Classification
API Probing
JavaScript Runtime
Undocumented Unchecked API
Undocumented Checked API

Experiment Setup

APIScope

- 5,000+ LoC, based on Soot (static) & FRIDA (dynamic)
- Tested on Baidu, QQ, Tiktok, WeChat and WeCom
- Measured the usage of undocumented APIs in 1st-party and 3rd-party miniapps

Categories of Documented and Undocumented APIs

Available APIs		WeChat					WeCom					Baidu					TikTok					QQ				
		D	% UU		% UC	%	D	% UU		% UC	%	D	% UU		% UC	%	D	% UU		% UC	%	D	% UU		% UC	%
Base	Basic	5	71.4	2	28.6	- 0.0	6	66.7	3	33.3	- 0.0	8	72.7	2	18.2	1 9.1	7	63.6	4	36.4	- 0.0	3	100.0	-	0.0	- 0.0
	App	13	39.4	14	42.4	6 18.2	13	37.1	16	45.7	6 17.1	8	42.1	10	52.6	1 5.3	6	50.0	6	50.0	- 0.0	9	34.6	17	65.4	- 0.0
	Debug	15	88.2	2	11.8	- 0.0	15	88.2	2	11.8	- 0.0	1	3.3	28	93.3	1 3.3	-	0.0	-	0.0	- 0.0	20	100.0	-	0.0	- 0.0
	Misc	10	58.8	7	41.2	- 0.0	10	55.6	8	44.4	- 0.0	9	100.0	-	0.0	- 0.0	10	52.6	9	47.4	- 0.0	9	100.0	-	0.0	- 0.0
UI	Interaction	6	46.2	7	53.8	- 0.0	6	46.2	7	53.8	- 0.0	7	41.2	10	58.8	- 0.0	9	81.8	2	18.2	- 0.0	6	40.0	9	60.0	- 0.0
	Navigation	4	44.4	5	55.6	- 0.0	4	40.0	6	60.0	- 0.0	4	100.0	-	0.0	- 0.0	5	100.0	-	0.0	- 0.0	4	33.3	8	66.7	- 0.0
	Animation	32	100.0	-	0.0	- 0.0	32	100.0	-	0.0	- 0.0	21	95.5	1	4.5	- 0.0	1	100.0	-	0.0	- 0.0	31	100.0	-	0.0	- 0.0
	WebView	-	0.0	22	95.7	1 4.3	-	0.0	24	96.0	1 4.0	-	0.0	3	75.0	1 25.0	-	0.0	3	100.0	- 0.0	-	0.0	16	100.0	- 0.0
	Misc	20	27.0	54	73.0	- 0.0	20	25.6	58	74.4	- 0.0	37	77.1	11	22.9	- 0.0	14	73.7	5	26.3	- 0.0	18	42.9	24	57.1	- 0.0
Network	Request	5	55.6	4	44.4	- 0.0	5	55.6	4	44.4	- 0.0	2	66.7	1	33.3	- 0.0	6	60.0	4	40.0	- 0.0	4	66.7	2	33.3	- 0.0
	Download	7	24.1	21	72.4	1 3.4	7	23.3	22	73.3	1 3.3	11	100.0	-	0.0	- 0.0	-	0.0	4	100.0	- 0.0	6	60.0	4	40.0	- 0.0
	Upload	7	50.0	5	35.7	2 14.3	7	46.7	6	40.0	2 13.3	6	100.0	-	0.0	- 0.0	-	0.0	4	100.0	- 0.0	6	75.0	2	25.0	- 0.0
	Websocket	14	93.3	1	6.7	- 0.0	14	93.3	1	6.7	- 0.0	13	100.0	-	0.0	- 0.0	7	77.8	2	22.2	- 0.0	13	86.7	2	13.3	- 0.0
	Misc	23	88.5	3	11.5	- 0.0	23	85.2	4	14.8	- 0.0	-	0.0	-	0.0	- 0.0	-	0.0	-	0.0	- 0.0	10	55.6	8	44.4	- 0.0
Storage		10	66.7	5	33.3	- 0.0	10	66.7	5	33.3	- 0.0	10	100.0	-	0.0	- 0.0	10	90.9	1	9.1	- 0.0	10	83.3	2	16.7	- 0.0
Media	Map	8	14.3	48	85.7	- 0.0	8	14.3	48	85.7	- 0.0	7	100.0	-	0.0	- 0.0	6	100.0	-	0.0	- 0.0	9	36.0	16	64.0	- 0.0
	Image	6	60.0	4	40.0	- 0.0	6	60.0	4	40.0	- 0.0	6	85.7	1	14.3	- 0.0	5	83.3	1	16.7	- 0.0	6	60.0	4	40.0	- 0.0
	Video	14	35.0	26	65.0	- 0.0	14	31.8	30	68.2	- 0.0	19	95.0	1	5.0	- 0.0	8	80.0	2	20.0	- 0.0	14	63.6	8	36.4	- 0.0
	Audio	64	84.2	9	11.8	3 3.9	64	79.0	14	17.3	3 3.7	44	100.0	-	0.0	- 0.0	44	81.5	10	18.5	- 0.0	61	85.9	10	14.1	- 0.0
	Live	26	46.4	30	53.6	- 0.0	26	39.4	40	60.6	- 0.0	8	100.0	-	0.0	- 0.0	19	100.0	-	0.0	- 0.0	23	57.5	17	42.5	- 0.0
	Recorder	16	84.2	3	15.8	- 0.0	16	84.2	3	15.8	- 0.0	12	100.0	-	0.0	- 0.0	11	91.7	1	8.3	- 0.0	15	88.2	2	11.8	- 0.0
	Camera	9	60.0	6	40.0	- 0.0	9	52.9	8	47.1	- 0.0	9	50.0	9	50.0	- 0.0	20	95.2	1	4.8	- 0.0	4	36.4	7	63.6	- 0.0
	Misc	12	75.0	3	18.8	1 6.3	12	75.0	3	18.8	1 6.3	18	100.0	-	0.0	- 0.0	-	0.0	-	0.0	- 0.0	6	100.0	-	0.0	- 0.0
Location		3	42.9	4	57.1	- 0.0	3	42.9	4	57.1	- 0.0	7	100.0	-	0.0	- 0.0	3	100.0	-	0.0	- 0.0	3	100.0	-	0.0	- 0.0
Share		4	33.3	7	58.3	1 8.3	4	16.7	19	79.2	1 4.2	3	100.0	-	0.0	- 0.0	5	71.4	2	28.6	- 0.0	5	35.7	9	64.3	- 0.0
Canvas		60	74.1	21	25.9	- 0.0	60	74.1	21	25.9	- 0.0	46	92.0	4	8.0	- 0.0	49	98.0	1	2.0	- 0.0	48	92.3	4	7.7	- 0.0
File		39	97.5	1	2.5	- 0.0	39	92.9	3	7.1	- 0.0	35	100.0	-	0.0	- 0.0	34	97.1	1	2.9	- 0.0	37	97.4	1	2.6	- 0.0
Open API	Login	2	100.0	-	0.0	- 0.0	5	83.3	1	16.7	- 0.0	3	42.9	1	14.3	3 42.9	2	100.0	-	0.0	- 0.0	2	100.0	-	0.0	- 0.0
	Navigate	2	33.3	2	33.3	2 33.3	2	22.2	5	55.6	2 22.2	3	100.0	-	0.0	- 0.0	7	100.0	-	0.0	- 0.0	2	50.0	1	25.0	1 25.0
	User Info	2	16.7	7	58.3	3 25.0	5	23.8	13	61.9	3 14.3	1	10.0	6	60.0	3 30.0	2	13.3	13	86.7	- 0.0	2	28.6	4	57.1	1 14.3
	Payment	1	3.4	13	44.8	15 51.7	1	3.2	15	48.4	15 48.4	1	50.0	-	0.0	1 50.0	1	33.3	1	33.3	1 33.3	2	22.2	7	77.8	- 0.0
	Bio-Auth	3	27.3	3	27.3	5 45.5	3	21.4	6	42.9	5 35.7	-	0.0	-	0.0	- 0.0	-	0.0	1	100.0	- 0.0	3	100.0	-	0.0	- 0.0
	Enterprise	-	0.0	1	100.0	- 0.0	5	17.9	6	21.4	17 60.7	-	0.0	-	0.0	- 0.0	-	0.0	-	0.0	- 0.0	-	0.0	-	0.0	- 0.0
	Misc	14	19.4	42	58.3	16 22.2	14	16.7	54	64.3	16 19.0	16	57.1	2	7.1	10 35.7	25	55.6	20	44.4	- 0.0	12	13.0	78	84.8	2 2.2
Device	Wi-Fi	9	100.0	-	0.0	- 0.0	9	100.0	-	0.0	- 0.0	10	100.0	-	0.0	- 0.0	4	100.0	-	0.0	- 0.0	9	100.0	-	0.0	- 0.0
	Bluetooth	18	60.0	11	36.7	1 3.3	18	58.1	12	38.7	1 3.2	-	0.0	-	0.0	- 0.0	-	0.0	-	0.0	- 0.0	18	100.0	-	0.0	- 0.0
	Contact	1	10.0	5	50.0	4 40.0	1	9.1	6	54.5	4 36.4	1	33.3	2	66.7	- 0.0	-	0.0	-	0.0	- 0.0	1	25.0	2	50.0	1 25.0
	NFC	5	26.3	14	73.7	- 0.0	9	39.1	14	60.9	- 0.0	-	0.0	-	0.0	- 0.0	-	0.0	-	0.0	- 0.0	5	100.0	-	0.0	- 0.0
	Screen	4	36.4	6	54.5	1 9.1	4	36.4	6	54.5	1 9.1	3	100.0	-	0.0	- 0.0	9	100.0	-	0.0	- 0.0	4	100.0	-	0.0	- 0.0
	Phone	1	4.3	21	91.3	1 4.3	1	4.3	21	91.3	1 4.3	1	100.0	-	0.0	- 0.0	1	100.0	-	0.0	- 0.0	1	50.0	1	50.0	- 0.0
	Misc	28	63.6	15	34.1	1 2.3	28	59.6	18	38.3	1 2.1	21	80.8	5	19.2	- 0.0	16	69.6	7	30.4	- 0.0	28	82.4	6	17.6	- 0.0
AI	CV	19	100.0	-	0.0	- 0.0	19	100.0	-	0.0	- 0.0	18	90.0	2	10.0	- 0.0	-	0.0	-	0.0	- 0.0	-	0.0	-	0.0	- 0.0
	Misc	-	0.0	-	0.0	- 0.0	-	0.0	1	100.0	- 0.0	11	100.0	-	0.0	- 0.0	7	100.0	-	0.0	- 0.0	-	0.0	-	0.0	- 0.0
AD		19	95.0	1	5.0	- 0.0	19	95.0	1	5.0	- 0.0	9	64.3	4	28.6	1 7.1	13	61.9	8	38.1	- 0.0	3	25.0	9	75.0	- 0.0
Uncategorized		30	38.5	47	60.3	1 1.3	30	36.6	51	62.2	1 1.2	15	53.6	10	35.7	3 10.7	17	68.0	7	28.0	1 4.0	34	68.0	15	30.0	1 2.0
All		590	51.0	502	43.4	65 5.6	606	47.3	593	46.3	82 6.4	464	77.1	113	18.8	25 4.2	383	75.8	120	23.8	2 0.4	506	62.7	295	36.6	6 0.7

Usage of Undocumented APIs in 1st-party Miniapps

Category	WeChat			WeCom			Baidu			QQ		
	$\#App_{UAPI}$	$\#App_{Total}$	%	$\#App_{UAPI}$	$\#App_{Total}$	%	$\#App_{UAPI}$	$\#App_{Total}$	%	$\#App_{UAPI}$	$\#App_{Total}$	%
Business	14	49	28.6	16	49	32.7	21	38	55.3	1	3	33.3
Education	6	26	23.1	7	26	26.9	5	16	31.3	-	3	0.0
E-learning	5	9	55.6	5	9	55.6	12	33	36.4	-	1	0.0
Entertainment	9	17	52.9	9	17	52.9	29	75	38.7	2	2	100.0
Finance	1	1	100.0	1	1	100.0	21	23	91.3	-	-	0.0
Food	-	-	0.0	-	-	0.0	-	5	0.0	-	-	0.0
Games	18	36	50.0	18	36	50.0	-	-	0.0	-	-	0.0
Government	2	7	28.6	2	7	28.6	3	8	37.5	1	1	100.0
Health	2	7	28.6	2	7	28.6	1	5	20.0	-	1	0.0
Job	-	1	0.0	-	1	0.0	-	-	0.0	-	-	0.0
Lifestyle	2	5	40.0	2	5	40.0	3	15	20.0	-	1	0.0
Photo	3	7	42.9	3	7	42.9	-	-	0.0	-	-	0.0
Shopping	1	1	100.0	1	1	100.0	-	2	0.0	-	-	0.0
Social	4	8	50.0	4	8	50.0	1	4	25.0	-	1	0.0
Sports	-	-	0.0	-	-	0.0	-	1	0.0	-	-	0.0
Tool	15	55	27.3	15	55	27.3	16	47	34.0	4	8	50.0
Traffic	3	5	60.0	3	5	60.0	4	10	40.0	-	1	0.0
Travelling	2	2	100.0	2	2	100.0	1	56	1.8	1	2	50.0
Uncategorized	-	-	0.0	-	-	0.0	1	2	50.0	-	-	0.0
Total	**87**	**236**	**36.9**	**90**	**236**	**38.1**	**118**	**340**	**34.7**	**9**	**24**	**37.5**

Usage of Undocumented APIs in 3rd-party Miniapps

API Name	Category	# App	% *App	w/ Check
wx.requestFacetoFacePayment	Payment	40,091	14.98	✓
wx.operateWXData	Misc	21,834	8.16	✗
wx.setPageOrientation	UI	18,499	6.91	✗
wx.enterContact	Contact	17,421	6.51	✓
wx.openUrl	Misc	17,140	6.41	✓
wx.preloadWebview	WebView	15,335	5.73	✓
wx.navigateBackNative	Navigate	13,407	5.01	✓
wx.editTextWithPopForm	Misc	13,390	5.00	✗
wx.openAddressWithLightMode	Address	13,390	5.00	✗
wx.requestPersonalPay	Payment	10,263	3.84	✗
wx.previewMedia	Media	6,635	2.48	✗
wx.drawCanvas	Canvas	6,055	2.26	✗
wx.openBusinessView	Misc	3,800	1.42	✗
wx.onDeviceOrientationChange	Device	1,626	0.61	✗
wx.startFacialRecognitionVerify	Bio-Auth	1,239	0.46	✓
wx.checkIsSupportFacialRecognition	Bio-Auth	669	0.25	✓
wx.notifyBLECharacteristicValueChanged	Bluetooth	603	0.23	✗
wx.getBackgroundFetchData	Misc	498	0.19	✗
wx.setBackgroundFetchToken	Misc	485	0.18	✗
wx.startFacialRecognitionVerifyAndUploadVideo	Bio-Auth	464	0.17	✓
wx.updateApp	Update	448	0.17	✗
wx.openOfflinePayView	UI	324	0.12	✓
wx.sendBizRedPacket	Payment	212	0.08	✓
wx.getVideoInfo	Video	193	0.07	✗
wx.compressVideo	Video	148	0.06	✗
wx.setBLEMTU	Bluetooth	127	0.05	✗
wx.getPhoneNumber	User Info	122	0.05	✗
wx.openVideoEditor	Video	118	0.04	✗
wx.chooseContact	Contact	100	0.04	✗
wx.openChannelsLive	Misc	97	0.04	✗
wx.openAddress	Address	96	0.04	✗
wx.setMenuStyle	Menu	74	0.03	✗

Undocumented Unchecked Sensitive (UUS) APIs Usage

Resource	WeChat		WeCom		Baidu		Tiktok		QQ	
	# UUS	%	# UUS	%	# UUS	%	# UUS	%	# UUS	%
Bluetooth	3	0.59	3	0.51	-	-	-	-	-	-
Camera	1	0.20	1	0.17	-	-	-	-	1	0.34
Location	-	-	-	-	-	-	-	-	1	0.34
Media	5	0.96	5	0.84	-	-	11	9.17	11	3.73
NFC	3	0.59	3	0.51	-	-	-	-	-	-
Network	16	3.19	16	2.70	7	6.19	20	16.67	24	8.14
Package	3	0.59	4	0.67	1	0.88	-	-	1	0.34
Storage	25	4.98	26	4.38	3	2.65	2	1.67	8	2.71
Telephony	-	-	-	-	-	-	1	0.83	-	-
Total	39	7.77	40	6.75	8	7.08	32	26.67	38	12.88

Real Attacks

Attacks	Targeted Resources	Exploited APIs	Vulnerable Super Apps

A1	Web Resources	`private_openUrl`
		`openUrl`
		`postMessage`
			WeChat,WeCom
			QQ, Baidu

A2	Web Resources	`installDownloadTask`
		`addDownloadTaskStraight`
		`startDownloadAppTask`
		`installApp`
			WeChat,WeCom
			QQ

A3	User information	`captureScreen`	WeChat, WeCom
A4	User phonenumber	`getLocalPhoneNumber`	Tiktok
A5	User contacts	`searchContacts`	WeChat

Real Attacks

Attacks	Targeted Resources	Exploited APIs	Vulnerable Super Apps

A1	Web Resources	`private_openUrl`
		`openUrl`
		`postMessage`
			WeChat,WeCom
			QQ, Baidu

A2	Web Resources	`installDownloadTask`
		`addDownloadTaskStraight`
		`startDownloadAppTask`
		`installApp`
			WeChat,WeCom
			QQ

A3	User information	`captureScreen`	WeChat, WeCom
A4	User phonenumber	`getLocalPhoneNumber`	Tiktok
A5	User contacts	`searchContacts`	WeChat

Real Attacks

Attacks	Targeted Resources	Exploited APIs	Vulnerable Super Apps

A1	Web Resources	`private_openUrl`
		`openUrl`
		`postMessage`
			WeChat,WeCom
			QQ, Baidu

A2	Web Resources	`installDownloadTask`
		`addDownloadTaskStraight`
		`startDownloadAppTask`
		`installApp`
			WeChat,WeCom
			QQ

A3	User information	`captureScreen`	WeChat, WeCom
A4	User phonenumber	`getLocalPhoneNumber`	Tiktok
A5	User contacts	`searchContacts`	WeChat

Real Attacks

Attacks	Targeted Resources	Exploited APIs	Vulnerable Super Apps

A1	Web Resources	`private_openUrl`
		`openUrl`
		`postMessage`
			WeChat,WeCom
			QQ, Baidu

A2	Web Resources	`installDownloadTask`
		`addDownloadTaskStraight`
		`startDownloadAppTask`
		`installApp`
			WeChat,WeCom
			QQ

A3	User information	`captureScreen`	WeChat, WeCom
A4	User phonenumber	`getLocalPhoneNumber`	Tiktok
A5	User contacts	`searchContacts`	WeChat

Real Attacks

Attacks	Targeted Resources	Exploited APIs	Vulnerable Super Apps

A1	Web Resources	`private_openUrl`
		`openUrl`
		`postMessage`
			WeChat,WeCom
			QQ, Baidu

A2	Web Resources	`installDownloadTask`
		`addDownloadTaskStraight`
		`startDownloadAppTask`
		`installApp`
			WeChat,WeCom
			QQ

A3	User information	`captureScreen`	WeChat, WeCom
A4	User phonenumber	`getLocalPhoneNumber`	Tiktok
A5	User contacts	`searchContacts`	WeChat

Conclusion

APIScope

- Undocumented APIs identification
- Undocumented APIs classification
- Undocumented APIs verification

Evaluated w/ 5 Superapps

- Uncovered **hidden** APIs in Superapps
- Quantified hidden APIs **usage**
- Demonstrated **real-world** attacks