



# Unpacking the Threats of All-in-One Mobile Super Apps

Zhiqiang Lin

Distinguished Professor of Engineering

[zlin@cse.ohio-state.edu](mailto:zlin@cse.ohio-state.edu)

May 8<sup>th</sup>, 2024



# Acknowledgement



Yue Zhang



Bayan Turkistani



Chaoshun Zuo



Yuqing Yang



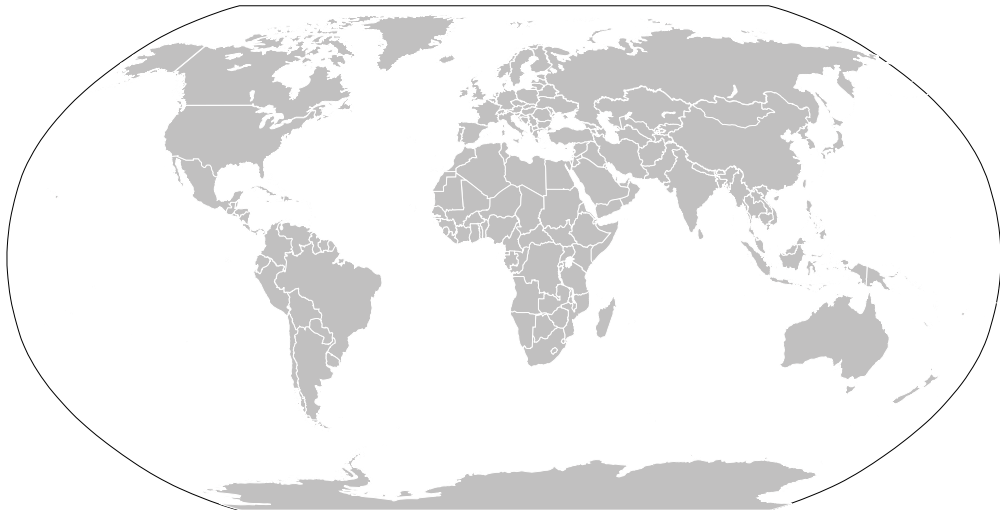
Chao Wang



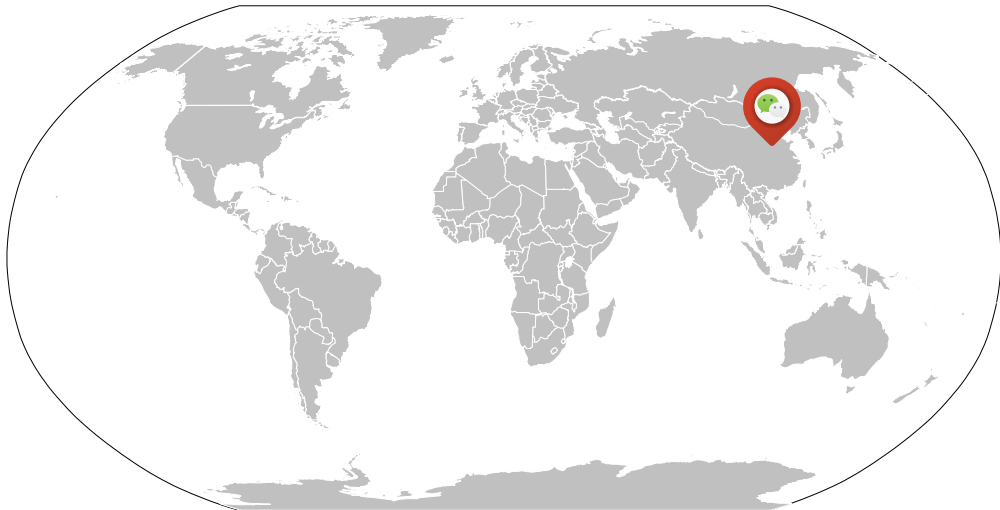
Ronny Ko

- 1 A Measurement Study of Wechat Mini-Apps. In [SIGMETRICS 2021](#) [ZTY<sup>+</sup>21]
- 2 Cross Miniapp Request Forgery: Root Causes, Attacks, and Vulnerability Detection. In [CCS 2022](#) [YZL22]
- 3 TAINTMINI: Detecting Flow of Sensitive Data in Mini-Programs with Static Taint Analysis. In [ICSE 2023](#) [WKZ<sup>+</sup>]
- 4 One Size Does Not Fit All: Uncovering And Exploiting Cross Platform Discrepant APIs in Wechat. In [USENIX Security 2023](#) [WZL23a]
- 5 Don't Leak Your Keys: Understanding, Measuring, and Exploiting the AppSecret Leaks in Mini-Programs. In [CCS 2023](#) [ZYL23]
- 6 Uncovering and Exploiting Hidden APIs in Mobile Super Apps. In [CCS 2023](#) [WZL23b]
- 7 Root Free Attacks: Exploiting Mobile Platform's Super Apps From Desktop. In [ASIACCS 2024](#) [WZL24]

# The World of Mobile Super Apps (“One App with Multiple Services”)

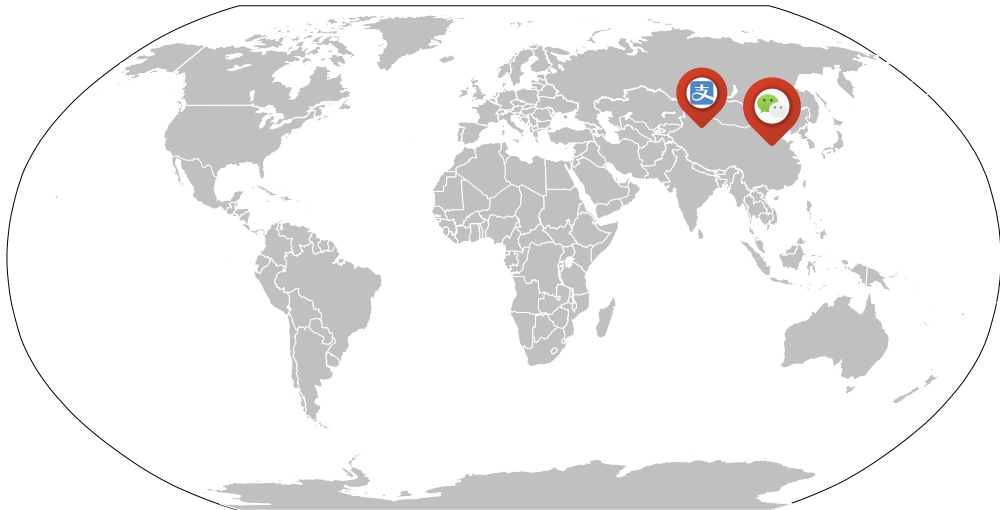


# The World of Mobile Super Apps (“One App with Multiple Services”)

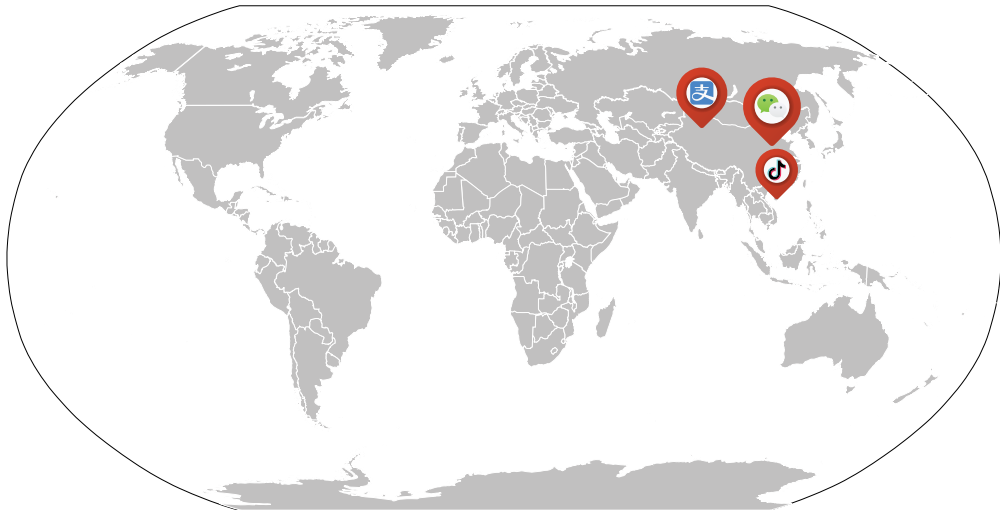




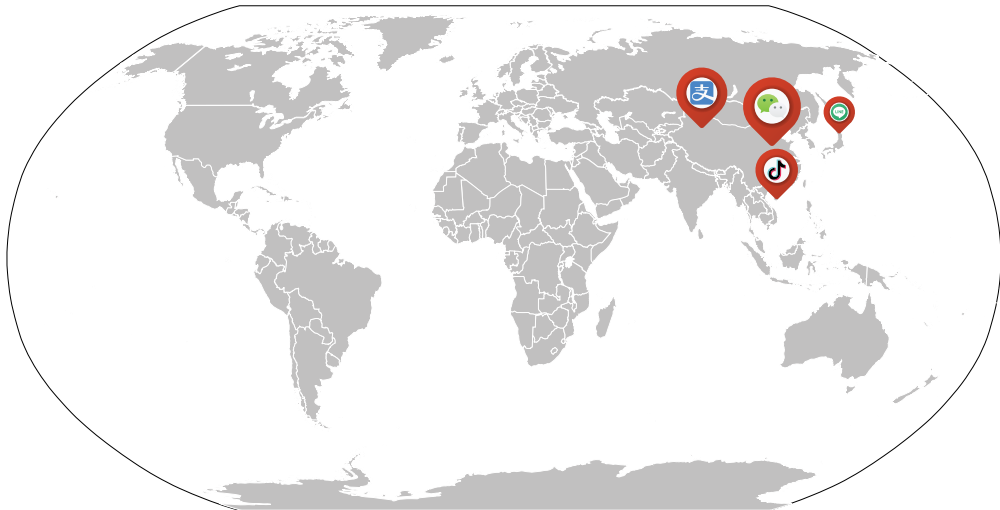
# The World of Mobile Super Apps (“One App with Multiple Services”)



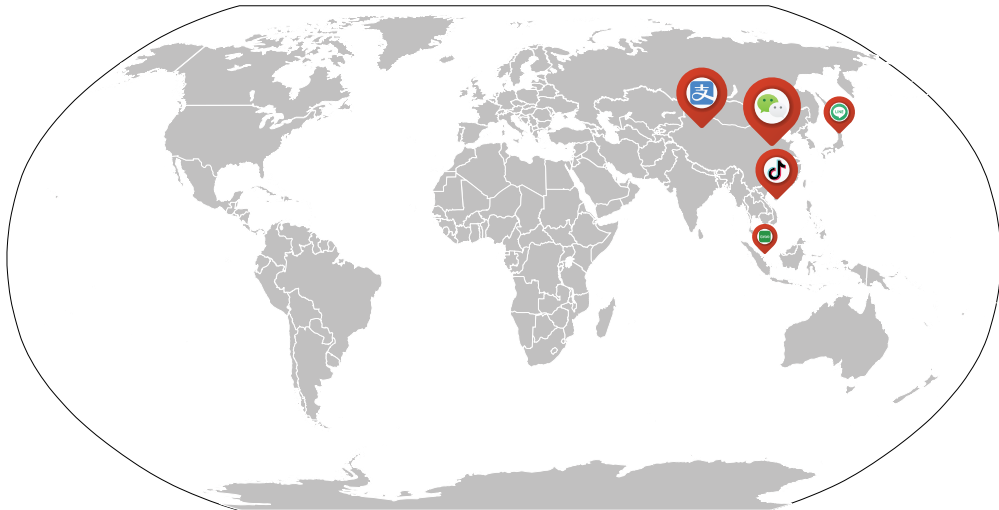
# The World of Mobile Super Apps (“One App with Multiple Services”)



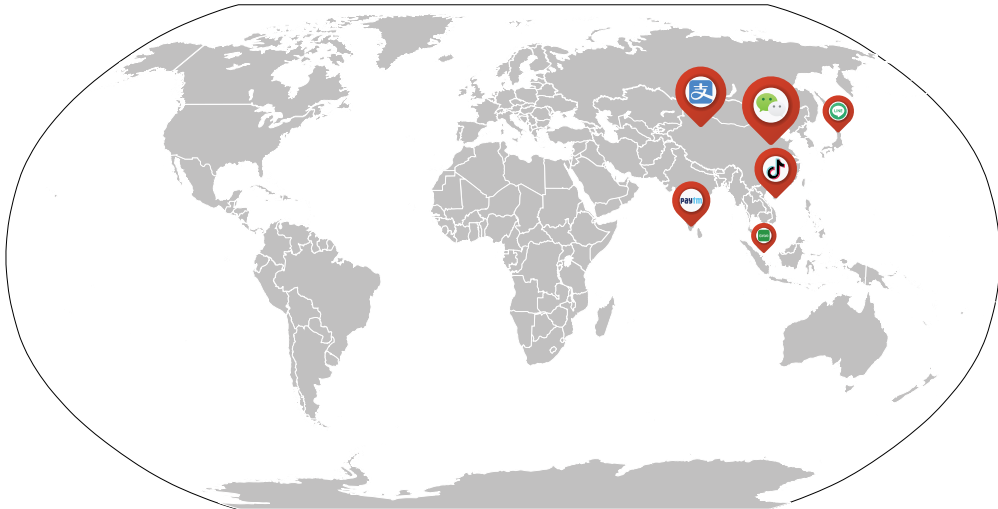
# The World of Mobile Super Apps (“One App with Multiple Services”)



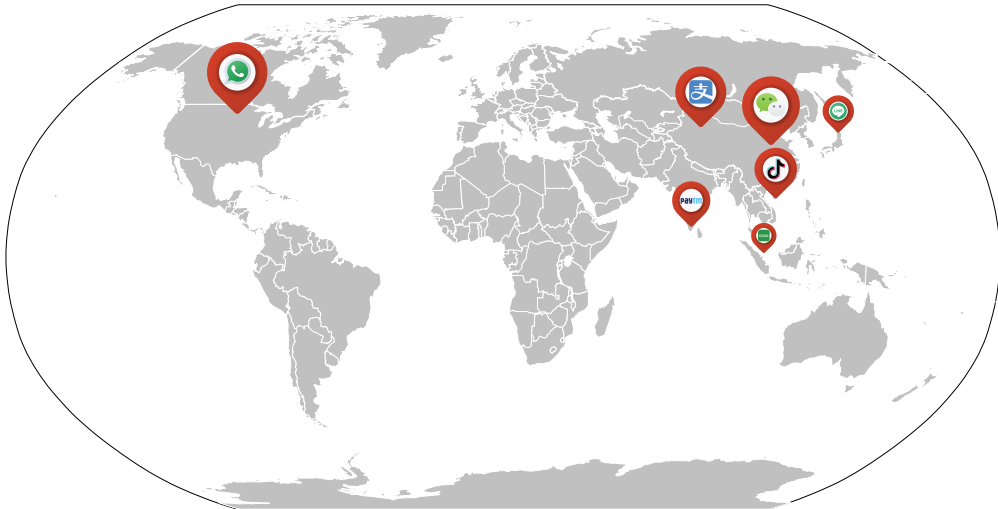
# The World of Mobile Super Apps (“One App with Multiple Services”)



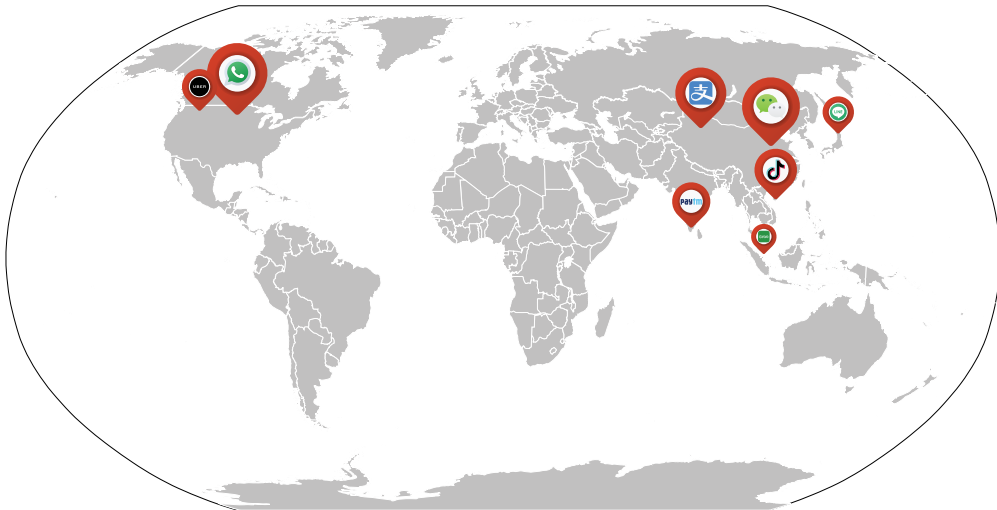
# The World of Mobile Super Apps (“One App with Multiple Services”)



# The World of Mobile Super Apps (“One App with Multiple Services”)



# The World of Mobile Super Apps (“One App with Multiple Services”)



# The World of Mobile Super Apps (“One App with Multiple Services”)





# The World of Mobile Super Apps (“One App with Multiple Services”)

Super App	Category	Monthly Users	Country	Business	Education	Communication	Finance	Food Delivery	Games	Lifestyle	Ride-hailing	Shopping	Social	Android	iOS	Windows	Android	iOS	Windows	
				Services										Platform			Miniapp			
WeChat	Social	1,200 million +	China	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tiktok	Social	1,000 million +	China	✗	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗
Alipay	Finance	730 million +	China	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
Snapchat	Social	347 million +	U.S.	✗	✗	✓	✗	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
WeCom	Business	180 million +	China	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Paytm	Finance	150 million +	India	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗
Go-Jek	Finance	100 million +	Indonesia	✓	✗	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗
Zalo	Social	52 million +	Vietnam	✓	✗	✓	✗	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗
Kakao	Social	45 million +	South Korea	✗	✗	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗
Grab	Delivery	25 million +	Singapore	✗	✗	✗	✓	✓	✗	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗

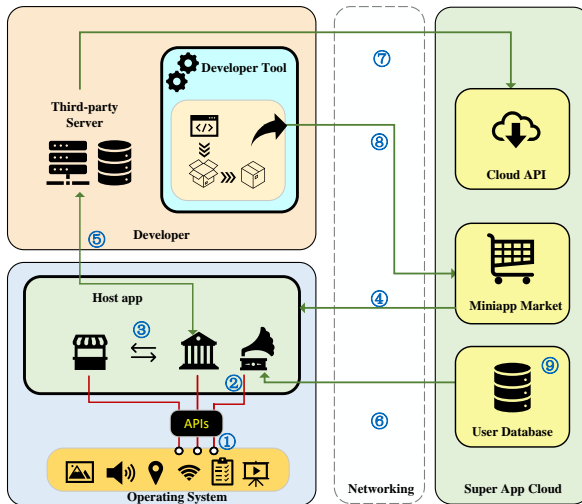
# What is WeChat?

"It's sort of like Twitter, plus PayPal, plus a whole bunch of things all rolled into one, with a great interface."

— Elon Musk



# Mobile Superapps in a Nutshell

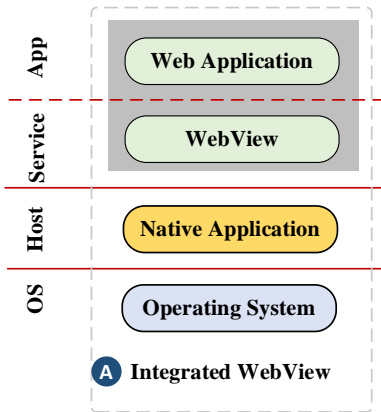


# The Benefits a Superapp Can Offer

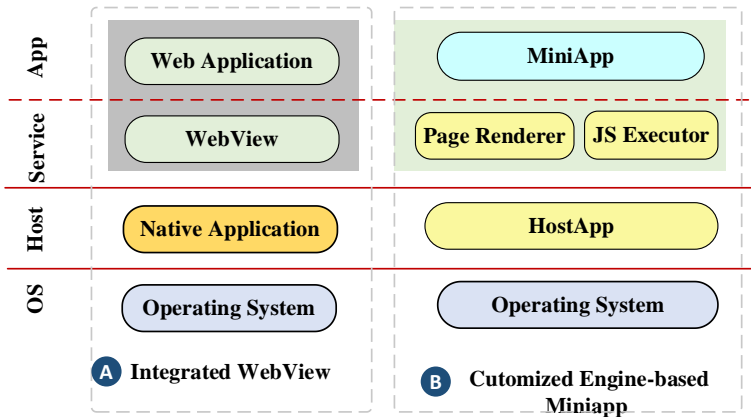
Hosts	Mobile OS (Native Apps)	Web Browsers (Web Apps)	Super Apps (Miniapps)
Example Platform	Android	Chrome	WeChat
System Resources?	●	⦿	●
Super-app Services?	○	⦿	●
User Data/States? Account?	⦿	●	●
App Packages?	●	○	●
Cloud Services?	⦿	●	●
API Support?	Rich	Poor	Rich
Compatible with Platforms?	○	●	●
Backend?	⦿	●	⦿
Centralized Vetting?	●	○	●
Install-free?	○	●	●
Market?	●	○	●
Storage Consumption?	High	Low	Low
Update?	Client-based	Client-based	Server-based
Performance?	High	Browser-specific	Super-app-specific
Offline Loading?	High	Low	Median
Register and Login?	●	●	○

“●” represents full support; “⦿” represents partial support; “○” represents no support.

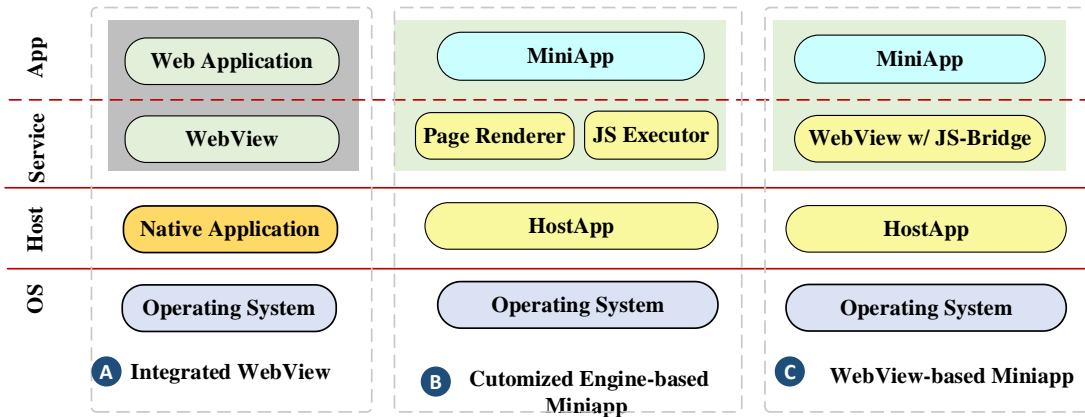
# The Taxonomy of Super Apps



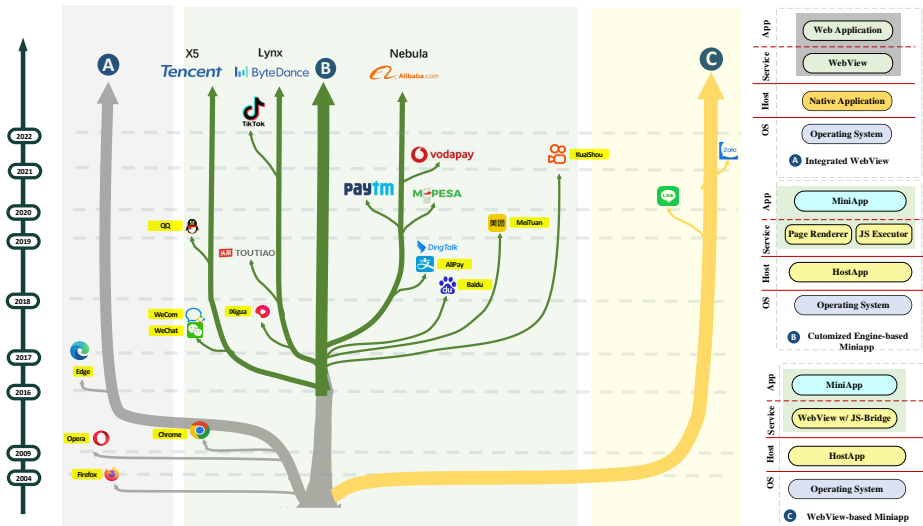
# The Taxonomy of Super Apps



# The Taxonomy of Super Apps



# Evolution of the Superapps





# Security Threats

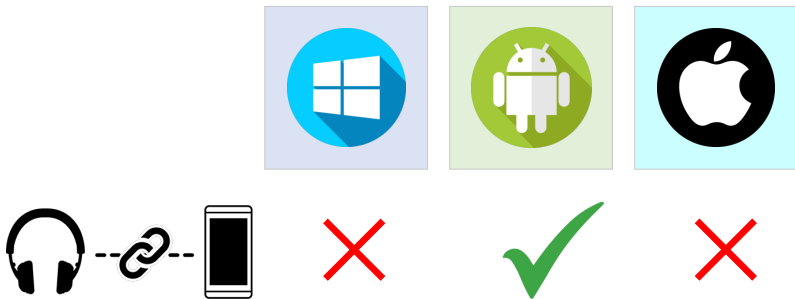
## Threats from Vulnerability Exploitation

- ① Vulnerabilities in Host Apps
  - (T1) Platform Discrepancies [WZL23a]
  - (T2) Privileged APIs [WZL23b]
  - (T3) Identity Confusion [ZZL<sup>+</sup>22]
- ② Vulnerabilities in Miniapps
  - (T4) Cross Miniapp Request Forgery [YZL22]
  - (T5) AppSecret Key Leakage [ZYL23]
  - (T6) Missing Signature Verification [ZZW23]

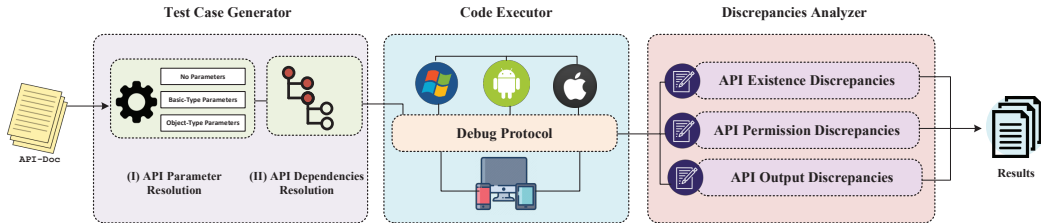
## Threats from Malware Attacks

- ① API Misuse/Abuse (Payload)
  - (T7) Collecting User Privacy
  - (T8) Service Abusing
  - (T9) Grayware
- ② Bypassing Vetting
  - (T10) Code Vetting Bypassing
  - (T11) Content Vetting Bypassing
  - (T12) Reporting Bypassing

# (T1) Exploiting Cross-platform Discrepancies [WZL23a]



# (T1) Exploiting Cross-platform Discrepancies [WZL23a]



# (T1) Exploiting Cross-platform Discrepancies [WZL23a]

APIs	Permission Scope	Mobile				PC	
		Android		iOS		Windows	
		A	P	A	P	A	P
getLocation	userLocation	✓	✓	✓	✓	✓	✗
chooseLocation		✓	✓	✓	✓	✓	✗
startLocationUpdate		✓	✓	✓	✓	✓	✗
SLUBackground*	userLocationBackground	✓	✓	✓	✓	✗	-
startRecord	record	✓	✓	✓	✓	✓	✗
joinVoIPChat		✓	✓	✓	✓	✗	-
RecorderManager.start		✓	✓	✓	✓	✓	✗
createCameraContext	camera	✓	✓	✓	✓	✓	✗
createVKSession		✓	✓	✓	✓	✗	-
openBluetoothAdapter	bluetooth	✗	-	✓	✓	✗	-
BLEPeripheralServer		✓	✓	✓	✓	✗	-
saveImageToPhotosAlbum	writePhotosAlbum	✓	✓	✓	✓	✓	✗
saveVideoToPhotosAlbum		✓	✓	✓	✓	✓	✗
addPhoneContact	addPhoneContact	✓	✓	✓	✓	✗	-
addPhoneRepeatCalendar	addPhoneCalendar	✓	✓	✓	✓	✗	-
addPhoneCalendar		✓	✓	✓	✓	✗	-
getWeRunData	werun	✓	✓	✓	✓	✗	-

# (T1) Exploiting Cross-platform Discrepancies [WZL23a]

APIs				Mobile						Desktop		
				Android			iOS			Windows		
Name	Category	Type	Precision	A	S	U	A	S	U	A	S	U
createAudioContext	Media	➔	X	✓	X	✓	✓	X	✓	✓	X	✓
createBufferURL	Storage	➔	X	✓	X	✓	✓	X	✓	✓	X	✓
createCameraContext	Media	➔	X	✓	X	✓	✓	X	✓	✓	X	✓
createCanvasContext	Canvas	➔	X	✓	X	✓	✓	X	✓	✓	X	✓
createIntersectionObserver	WXML	➔	X	✓	X	✓	✓	X	✓	✓	X	✓
createLivePusherContext	Media	➔	X	✓	X	✓	✓	X	✓	✓	X	✓
createOffscreenCanvas	Canvas	➔	X	✓	X	✓	✓	X	✓	✓	X	✓
createSelectorQuery	WXML	➔	X	✓	X	✓	✓	X	✓	✓	X	✓
createWebAudioContext	Media	➔	X	✓	X	✓	✓	X	✓	✓	X	✓
getAccountInfoSync	OpenAPI	➔	X	✓	✓	X	✓	✓	✓	✓	✓	X
getAppAuthorizeSetting	Base	➔	X	✓	✓	✓	✓	✓	✓	✓	✓	X
getAppBaseInfo	Base	➔	X	✓	✓	✓	✓	✓	✓	✓	✓	✓
getDeviceInfo	Base	➔	X	✓	✓	✓	✓	✓	✓	✓	✓	✓
getLocalIPAddress	Device	➔	X	✓	✓	✓	✓	✓	X	✓	✓	X
getMenuButtonBoundingClientRect	UI	➔	X	✓	✓	X	✓	✓	✓	✓	✓	X
getPerformance	Base	➔	X	✓	✓	✓	✓	✓	X	✓	✓	X
getScreenBrightness	Device	➔	✓	✓	✓	✓	✓	✓	X	✓	✓	✓
getSystemInfo	Base	➔	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
getSystemInfoAsync	Base	➔	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
getSystemInfoSync	Base	➔	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
getSystemSetting	Base	➔	X	✓	✓	X	✓	✓	✓	✓	✓	X
getWindowInfo	Base	➔	X	✓	✓	X	✓	✓	✓	✓	✓	✓

# (T2) Exploiting Hidden/Privileged APIs [WZL23b]

## Attacks Caused by Hidden APIs

- 1 Arbitrary Web Page Access
- 2 Malware Download and Installation
- 3 Screenshot-based Information Theft
- 4 Phone Number Theft
- 5 Contact Information Theft

```
1 // Documented API Implementation of Baidu
2 package com.baidu.swan.apps.scheme.actions.f;
3 public class a extends aa {
4     public a (e context) {
5         super(context, "/swanAPI/getLocation");
6     }
7
8     @Override
9     public boolean a (Context c, Scheme s, CallbackHandler cb, SwanApp a){
10         // some other logic
11     }
12 }
13
14 // Unocuemented API Implementation of Baidu
15 package com.baidu.swan.apps.impl.account.a;
16 public class f extends aa {
17     public f (e context) {
18         super(context, "/swanAPI/getBDUSS");
19     }
20
21     @Override
22     public boolean a (Context c, Scheme s, CallbackHandler cb, SwanApp a){
23         // some other logic
24     }
25 }
```

# (T2) Exploiting Hidden/Privileged APIs [WZL23b]

```

1 WeixinJSBridge = function(global) {
2   var NativeGlobal = global.NativeGlobal;
3   var globalCount = 0;
4
5   function invokeMethod(apiName, params, callbackHandler) {
6     params = WeixinNativeBuffer.pack(params);
7     var filteredParams = paramFilter(params || {}),
8         callbackId = ++globalCount;
9     callbackQueue[callbackId] = callbackHandler,
10    a(apiName, params, callbackId) {
11      callbackId = NativeGlobal.invokeHandler(apiName, params,
12        callbackId);
13      invokeCallbackHandler(callbackId, callbackHandler)
14    }(apiName, filteredParams, callbackId)
15  }
16  return this;
17 }(global);

```

JavaScript Framework Layer

```

1 // Implementation of invoke handler in Java framework
2 package com.tencent.magicbrush;
3 public abstract class MBRRuntime {
4   protected String nativeInvokeHandler(String apiName, String apiParam, int id) {
5     if (this.nativeHandler != null) {
6       try {
7         return this.nativeHandler.invoke(apiName, apiParam, id);
8       } catch (Throwable e) {
9         Logger.printStackTrace("MBRRuntime", e, "crash when invoke jsapi!");
10        throw e;
11      }
12    }
13    Logger.error("MBRRuntime", "no native invoke handler");
14    return "";
15  }
16 }

```

Service Abstraction Layer

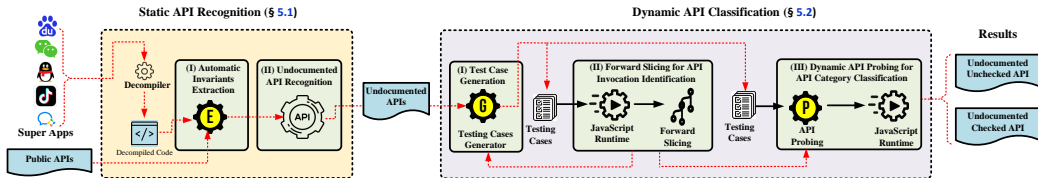
```

1 // Implementation of invokeHandler in NativeGlobal JavaScript Object (C++)
2 int magicbrush::BindingNativeGlobal::BindTo(v8::Object *a1, v8::Isolate *a2) {
3   /* Code Omitted */
4
5   v13 = 0;
6   v7 = (v8::Value *)mm::JSGet<v8::Local<v8::Value>>(a1, v6, "NativeGlobal", &v12);
7   if ( !v7 || (v9 = (int)v7, !v8::Value::IsObject(v7)) )
8     v9 = v8::Object::New(a1, v8);
9   v13 = v9;
10
11   /* Code Omitted */
12
13   mm::JSSetWithData((int)a1,
14     v13,
15     (int)"invokeHandler",
16     (int)magicbrush::nativeglobal::invokeHandler,
17     a2);
18   mm::JSSet<v8::Local<v8::Object>>(a1, *a3, "NativeGlobal", v13);
19   return v13;
20 }
21
22 int magicbrush::nativeglobal::invokeHandler(v8::Isolate *a1, DWORD *a2) {
23   /* Code Omitted */
24
25   mm::JSConvert<std::string, void>::fromV8(api_name, a1, v6);
26   mm::JSConvert<char16_t const*, void>::fromV8(api_param, a1, v6);
27   mm::JSConvert<int, void>::fromV8(callback_id, a1, v6);
28   Java_com_tencent_magicbrush_MBRuntime_nativeInvokeHandler(
29     api_name,
30     api_param,
31     callback_id
32   )
33
34   /* Code Omitted */
35 }

```

Customized V8 Layer

# (T2) Exploiting Hidden/Privileged APIs [WZL23b]

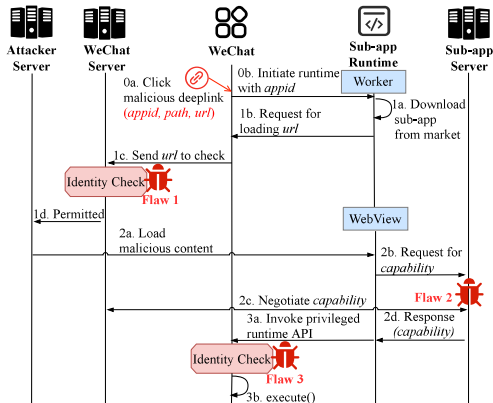




## (T2) Exploiting Hidden/Privileged APIs [WZL23b]

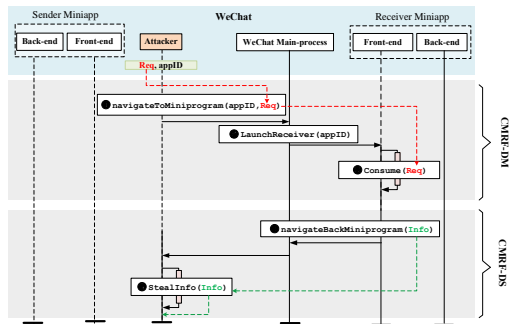
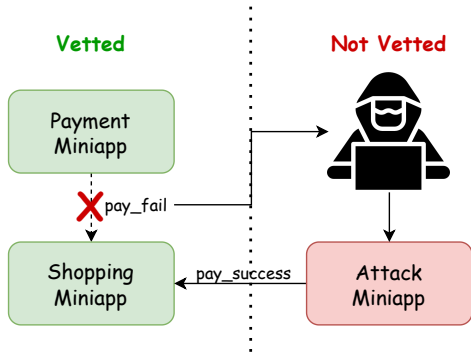
Available APIs	WeChat				WeCom				Baidu				TikTok				QQ														
	D	% UU	% UC	%	D	% UU	% UC	%	D	% UU	% UC	%	D	% UU	% UC	%	D	% UU	% UC	%											
Basic	5	71.4	2	28.6	0.0	6	66.7	3	33.3	0.0	8	72.7	2	18.2	1	9.1	7	63.6	4	36.4	0.0	3	100.0	-	0.0	-	0.0				
App	13	39.4	14	42.4	6	18.2	13	37.1	16	45.7	6	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	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	0.0	10	52.6	9	47.4	0.0	9	100.0	-	0.0	-	0.0				
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	0.0	9	81.8	2	18.2	0.0	6	40.0	9	60.0	-	0.0	-	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	0.0	5	100.0	-	0.0	0.0	4	33.3	8	66.7	-	0.0	-	0.0		
UI	Animation	32	100.0	-	0.0	32	100.0	-	0.0	0.0	21	95.5	1	4.5	0.0	0.0	1	100.0	-	0.0	0.0	31	100.0	-	0.0	-	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	0.0	14	73.7	5	26.3	0.0	18	42.9	24	57.1	-	0.0	-	0.0		
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	0.0	6	60.0	4	40.0	0.0	4	66.7	2	33.3	-	0.0	-	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	4	100.0	-	0.0	6	60.0	4	40.0	-	0.0	-	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	4	100.0	-	0.0	6	75.0	2	25.0	-	0.0	-	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	0.0	7	77.8	2	22.2	0.0	13	86.7	2	13.3	-	0.0	-	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	-	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	0.0	10	90.9	1	9.1	0.0	10	83.3	2	16.7	-	0.0	-	0.0		
Map	8	14.3	48	85.7	0.0	8	14.3	48	85.7	0.0	7	100.0	-	0.0	0.0	0.0	6	100.0	-	0.0	0.0	9	36.0	16	64.0	-	0.0	-	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	0.0	5	83.3	1	16.7	0.0	6	60.0	4	40.0	-	0.0	-	0.0		
Video	14	35.0	26	65.0	0.0	14	31.8	30	68.2	0.0	10	95.0	1	5.0	0.0	0.0	8	80.0	2	20.0	0.0	14	63.6	8	36.4	-	0.0	-	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	-	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	0.0	19	100.0	-	0.0	0.0	23	57.5	17	42.5	-	0.0	-	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	0.0	11	91.7	1	8.3	0.0	15	88.2	2	11.8	-	0.0	-	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	-	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	6	100.0	-	0.0	-	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	0.0	3	100.0	-	0.0	0.0	3	100.0	-	0.0	-	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	-	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	0.0	49	98.0	1	2.0	0.0	48	92.3	4	7.7	-	0.0	-	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	0.0	34	97.1	1	2.9	0.0	37	97.4	1	2.6	-	0.0	-	0.0		
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	-	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	2	50.0	1	25.0	1	25.0	-	0.0		
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		
Open API	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	-	0.0	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	1	100.0	-	0.0	3	100.0	-	0.0	-	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	-	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		
Wi-Fi	9	100.0	-	0.0	0.0	9	100.0	-	0.0	0.0	10	100.0	-	0.0	0.0	0.0	4	100.0	-	0.0	0.0	9	100.0	-	0.0	-	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	18	100.0	-	0.0	-	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	1	25.0	2	50.0	1	25.0	-	0.0		
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	-	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	4	100.0	-	0.0	-	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	-	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	-	0.0	
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	-	0.0	-	0.0		
Misc	-	0.0	-	0.0	-	0.0	1	100.0	-	0.0	11	100.0	-	0.0	0.0	0.0	7	100.0	-	0.0	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	-	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	66.0	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									

# (T3) Exploiting Identity Confusion Vulnerability [ZZL+22]



Source: <https://www.usenix.org/system/files/sec22-zhang-lei.pdf>

# (T4) Cross Miniapp Request Forgery (CMRF) [YZL22]



# (T4) Cross Miniapp Request Forgery (CMRF)

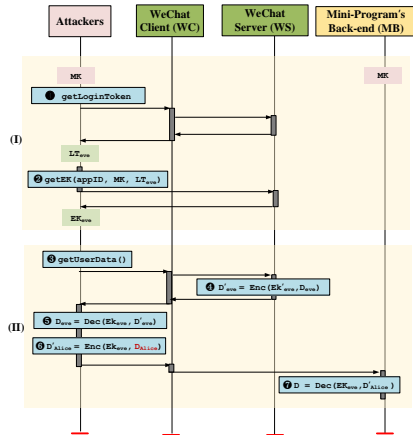
Category	WECHAT					
	No Use		Checked		Vulnerable	
	# app	%total	# app	%	# app	%
Business	131,078	5.1	81	8.07	923	91.93
E-learning	10,271	0.4	4	5.19	73	94.81
Education	240,077	9.34	184	3.72	4,756	96.28
Entertainment	29,442	1.14	140	33.02	284	66.98
Finance	3,509	0.14	6	6.67	84	93.33
Food	114,675	4.46	332	8.07	3,780	91.93
Games	88,056	3.42	10	2.09	469	97.91
Government	31,432	1.22	33	9.02	333	90.98
Health	27,716	1.08	37	5.44	643	94.56
Job	21,773	0.85	16	7.02	212	92.98
Lifestyle	394,493	15.34	269	4.23	6,092	95.77
Photo	9,039	0.35	3	4.41	65	95.59
Shopping	989,498	38.48	743	2.56	28,304	97.44
Social	20,671	0.8	6	2.99	195	97.01
Sports	15,980	0.62	69	22.48	238	77.52
Tool	261,467	10.17	122	3.72	3,161	96.28
Traffic	35,412	1.38	53	9.28	518	90.72
Travelling	10,524	0.41	5	3.62	133	96.38
Uncategorized	83,983	3.27	0	0.0	18	100.0
<b>Total</b>	<b>2,519,096</b>	<b>97.96</b>	<b>2,113</b>	<b>4.03</b>	<b>50,281</b>	<b>95.97</b>

Category	BAIDU					
	No Use		Checked		Vulnerable	
	# app	%total	# app	%	# app	%
Automobile	356	0.24	0	0.0	2	100.0
Business	5,201	3.5	0	0.0	113	100.0
Charity	2	0.0	0	0	0	0
E-commerce	96	0.06	0	0	0	0
Education	1,378	0.93	0	0.0	3	100.0
Efficiency	10,852	7.31	0	0.0	1	100.0
Entertainment	195	0.13	1	11.11	8	88.89
Finance	45	0.03	0	0.0	2	100.0
Food	123	0.08	0	0	0	0
Government	282	0.19	0	0.0	5	100.0
Health	2	0.0	0	0	0	0
Information	1,736	1.17	0	0.0	6	100.0
IT tech	113	0.08	0	0	0	0
Lifestyle	1,818	1.22	0	0	0	0
Medical	97	0.07	0	0	0	0
News	4	0.0	0	0	0	0
Post service	163	0.11	0	0	0	0
Real estate	1,510	1.02	0	0	0	0
Shopping	116,093	78.17	0	0.0	327	100.0
Social	205	0.14	0	0	0	0
Sports	145	0.1	0	0	0	0
Tool	46	0.03	0	0	0	0
Traffic	226	0.15	0	0.0	1	100.0
Travelling	1,473	0.99	0	0	0	0
Uncategorized	5,857	3.94	0	0.0	25	100.0
<b>Total</b>	<b>148,018</b>	<b>99.67</b>	<b>1</b>	<b>0.2</b>	<b>493</b>	<b>99.8</b>

# (T5) Exploiting Key Leakage from Miniapps [ZYL23]

## Attack Procedure

- ▶ (I) Obtaining Attacker's Encryption Key (EK)
  - ▶ Obtain leaked Master Key (MK)
  - ▶ Query for EK with the MK
- ▶ (II) Sensitive Data Retrieval and/or Manipulation
  - ▶ Capture encrypted data
  - ▶ Decrypt with MK
  - ▶ Data manipulation
  - ▶ Re-encrypt and send to back-end

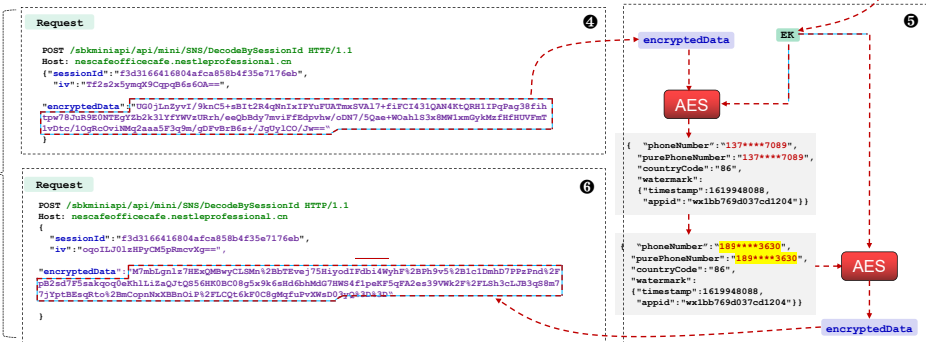


# (T5) Key Leakage from Miniapps [ZYL23]

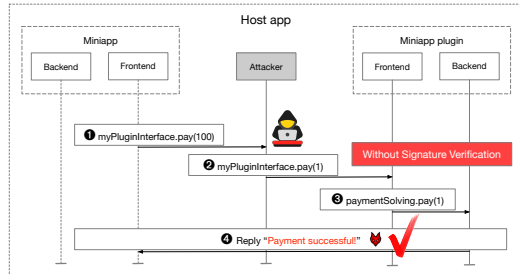
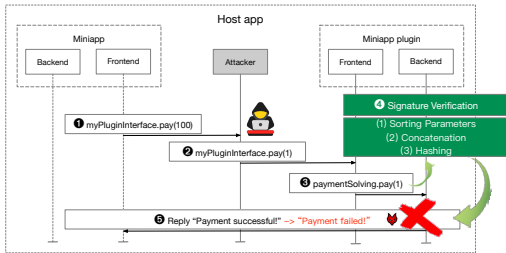
(I) Obtaining Attacker's  
Encryption Key (EK)













(II) User Phone Number  
Retrieval and Manipulation



# (T6) Missing Signature Verification [ZYL23]



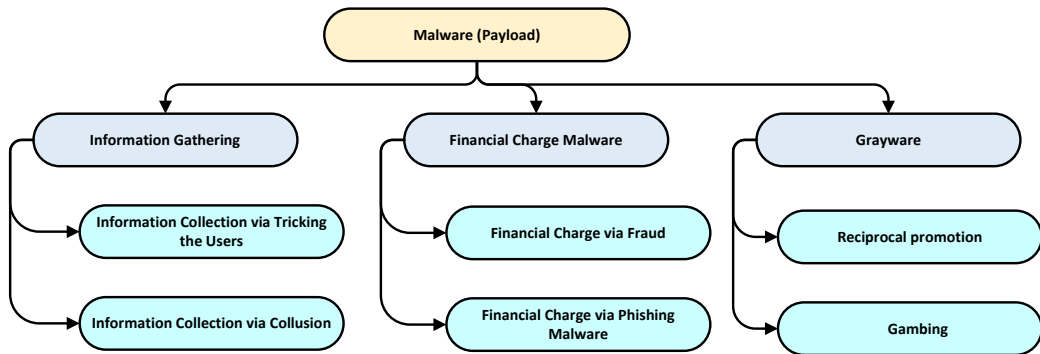
# Tencent's Security Hall of Fame

Rank	Nickname	Link	Reputation	Credits
 1	 djurado		Experienced ...	113
 2	 Sergey Bobrov	<a href="https://twitter.com/Black2Fan">https://twitter.com/Black2Fan</a>	Proficient	46
 3	 OSU SecLab	<a href="https://seclab.engineering.osu.edu/">https://seclab.engineering.osu.edu/</a>	Proficient	46
4	 kazan71p		Proficient	43
5	 xCHCQg		Proficient	36
6	 sh1yo	<a href="https://sh1yo.art">https://sh1yo.art</a>	Proficient	32
7	 NamHB		Proficient	31

<https://en.security.tencent.com/index.php/thanks>



# Malware Taxonomy Based on Payloads



# T7: Information Gathering

## Information Gathering via Tricking the Users [opr]

Date of Brith

手机卜易居 > 生辰八字算命

### 八字算命

以下八字程序仅支持阳历(公历)生日, 只知道阴历(农历), 请点击『阴阳历互换』进行查询。欲知详尽运程, 请点击『五行八字运程』。

姓氏:  名字:

性别:  血型:

公历: 1980 年 1 月 1 日

点  分

◇ 八字算命简介

什么是八字算命? 八字算命, 即生辰八字算

Phone Number

● 手机号测富贵: v1.3.5

● 注册码: 39266745

在线使用说明 [www.appluopan.cn](http://www.appluopan.cn)

已注册版本, 可以使用

在此输入你要测的手机号码

● 01 霸延年星(平顺、魄力、责任)  
02 霸五鬼星(凶煞、偏架、歪斜)  
02 霸伏位星(普通、不好不坏)  
02 霸六煞星(情绪不稳、桃花煞)  
03 霸天福星(文昌、财富、智慧)

13683661345:  
分数: 50

Blood types

血型配对

不同的血型不同的性格, 聚在一起, 必然会产生不同的化学反应, 你与他(她)的爱情配对会如何? 会是只羡鸳鸯不羡仙, 是欢喜冤家, 还是如何的一对组合呢? 《血型配对》为您揭开答案!

男方血型:  
 A型  B型  AB型  O型

女方血型:  
 A型  B型  AB型  O型

# T7: Information Gathering

## Information Gathering via Collusion [opr]

你好, 是需要寻人定位还是什么呢?

寻人定位

你好, 是需要寻人定位吗?

建议你使用寻亲平台的红包定位功能

这目前是全网独创的新技术, 保证你和你朋友都没见过!

请点击下面蓝色字链接, 注册后才可以体验红包定位功能哦

注意: 如果你是丢失了手机, 我们是帮不了您的, 只能建议您报警处理~

### 手机定位帮手

帐号 请输入帐号(手机号)

密码 请输入帐号密码

登录

注册账号 帮助教程

官方客服电话: \_\_\_\_\_

### 3、发送分享定位链接

添加定位链接

点击刚才新建的图标定位

老公1  
创建时间: 2018-01-31 21:23:06

添加定位地址, 开始定位跟踪

注意:

- 1.如果只有手机号, 也可以定位, 具体教程请往下看
- 2.如果推荐用微信发送, 成功率高一点

返回 定位链接

当前定位链接地址是:

如果只有手机号, 也可以定位, 教程请继续往下看

微信发送 QQ发送

发送连接帮助教程

注意:

建议用微信发送, 成功率高一点

52%

操作说明

转发本页微信定位人或者复制本链接给定位人, 待被定位人同意分享位置, 返回查看实时位置

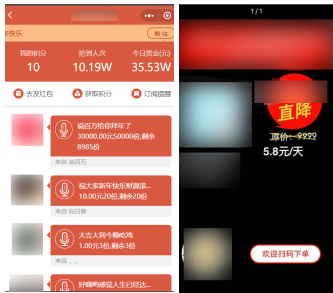
操作帮助

返回

# T8: Financial Charge Malware

## Financial Charge via Fraud [opr]

### Fake Red Packet

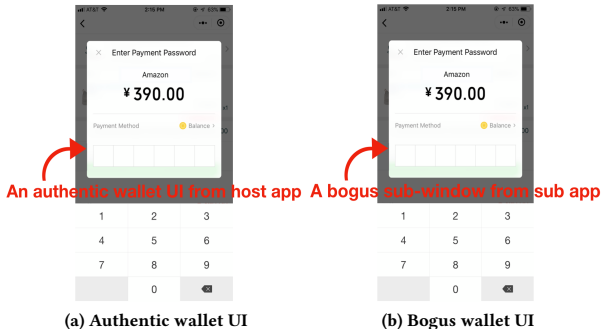


### Online Earning



# T8: Financial Charge Malware

## Financial Charge via Phishing Malware



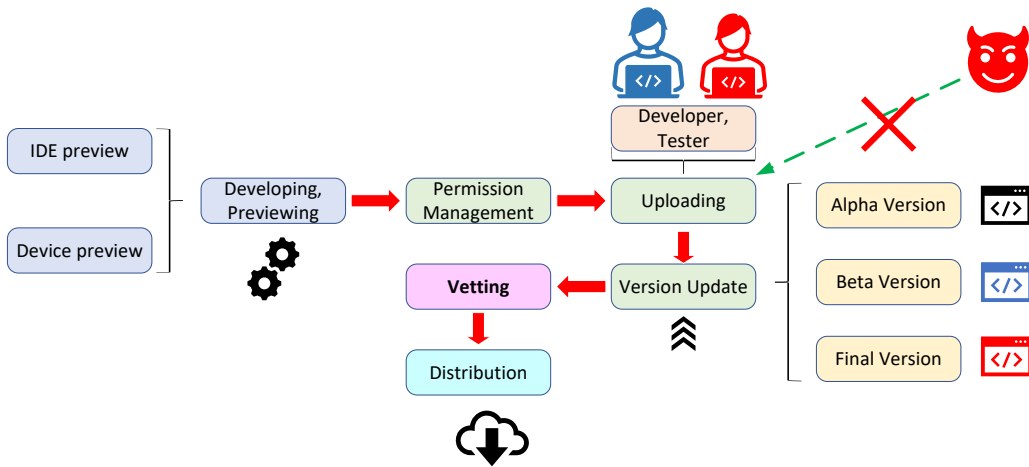
Mobile wallet UI confusion [LXX+20]

## T9: Grayware

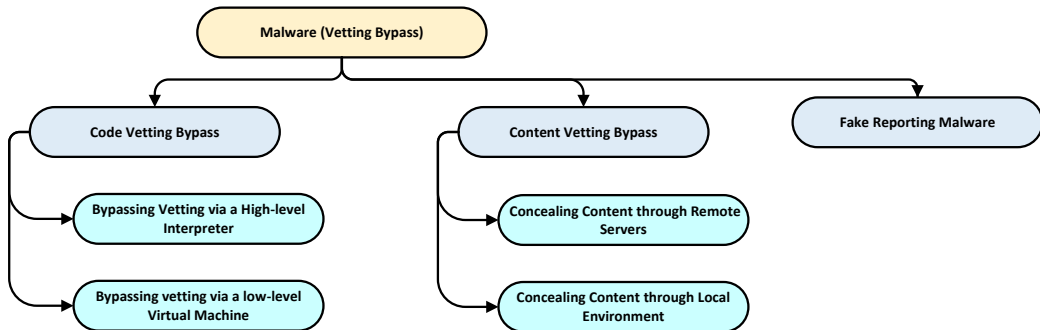
## Gambling [opr]



# Code Vetting



# Vetting Bypassing Malware





# T10: Code Vetting Bypassing Malware

## Bypassing Vetting via Interpreter [CN]

☰ README.md

### mini-hot [🔗](#)

⚠️ 注意: 该方案使用的开源库已被[微信官方禁用](#), 谨慎使用!

`npm v0.2.4`

[Demo 工程](#)

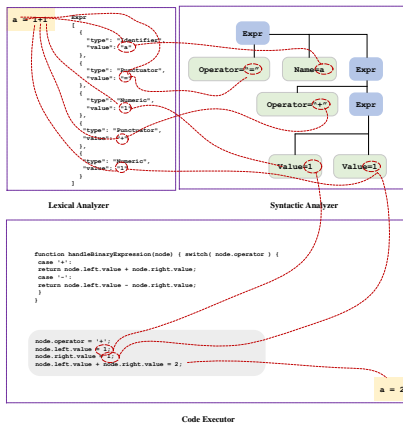
### API [🔗](#)

`createRemotePage` - 单个页面远程加载 [🔗](#)

```
// SomePage.ts
import { createRemotePage } from '@mini-hot/taro'
export default createRemotePage(() => import('./SomePage'))
```

`createRemoteApp` - 小程序 SPA 化后远程加载 [🔗](#)

```
// SPA.ts
import { createRemoteApp } from '@mini-hot/taro'
```



# T11: Content Vetting Bypassing Malware [Sin]



```
<!-- pages/add/add.wxml -->
<view wx:if="{{isChecked}}" class="p">
  添加功能尚在完善中
  <view class="in">
    这是一个英语句子随机小程序，给英语爱好者提供丰富的英语美剧供欣赏或摘抄。
  </view>
</view>
<!-- 给审核看的页面 -->

<view wx:else class="box">...
</view>
<!-- 给用户看的页面 -->
```



Controlled By Time

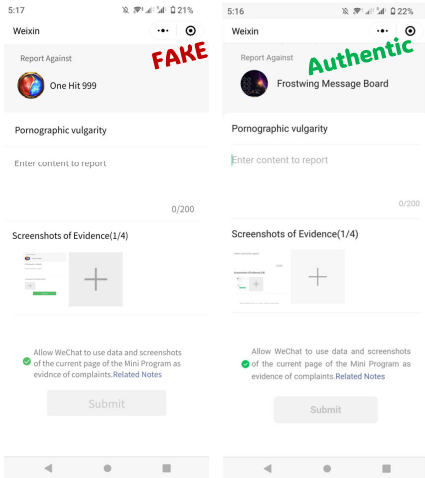
```
var time='2021-03-24 21:17:15';//是三天后的时间
var t= util.fulltime(new Date());//返回现在的时间
this.setData({
  isChecked: t<time?true:false,
  //现在的时间大于三天后的时间是false，表示没有在审核，正常显示页面
});
```



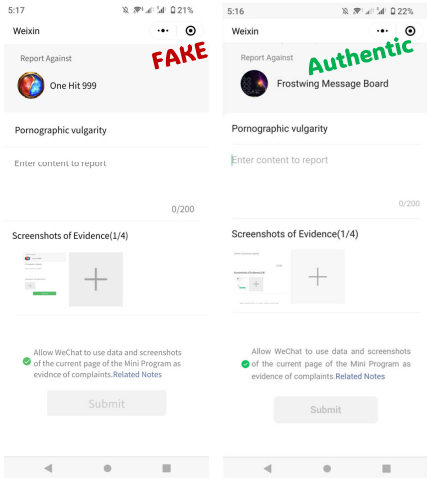
Controlled By Remote Server

```
1 onLaunch (options) {
2   const accountInfo = wx.getAccountInfoSync();
3   if(accountInfo.miniProgram.envVersion === 'develop'){
4     // 跳转预留好的页面
5     wx.navigateTo() // 开发时，可以注释本行，方便自己预览
6   }
7 }
```

# T12: Reporting Bypassing Malware



# T12: Reporting Bypassing Malware



	Web App	Mobile App	Miniapp
Environment	Browser	Mobile Operating System	Suer App
Authority	Decentralized	Seperate App Store	Super App
Vetting	Decentralized	By Certain App Store	By Super App
Reporting	Decentralized	Write email to App Store	Via built-in Inter.

Table: Comparison of the authorities

# The World of Mobile Super Apps (“One App with Multiple Services”)



# Security Threats

## Threats from Vulnerability Exploitation

- ① Vulnerabilities in Host Apps
  - (T1) Platform Discrepancies [WZL23a]
  - (T2) Privileged APIs [WZL23b]
  - (T3) Identity Confusion [ZZL+22]
- ② Vulnerabilities in Miniapps
  - (T4) Cross Miniapp Request Forgery [YZL22]
  - (T5) AppSecret Key Leakage [ZYL23]
  - (T6) Missing Signature Verification [ZZW23]

## Threats from Malware Attacks

- ① API Misuse/Abuse (Payload)
  - (T7) Collecting User Privacy
  - (T8) Service Abusing
  - (T9) Grayware
- ② Bypassing Vetting
  - (T10) Code Vetting Bypassing
  - (T11) Content Vetting Bypassing
  - (T12) Reporting Bypassing

## Other Open Problems

### Vulnerability Identification

- ▶ Memory vulnerabilities (e.g., JavaScript engines, native layers)
- ▶ Logic vulnerabilities in both host apps (e.g., permission mgmt) and miniapps

### Malware Analysis

- ▶ Semantic-aware miniapp vetting
- ▶ Developing static, dynamic, or symbolic analysis tools for miniapp malware analysis

### Security/Privacy Compliance Analysis

- ▶ Various regulations/laws in privacy-rich platform
- ▶ Tools for compliance checks, and even supply chain analysis

### Security Mechanism Standardization

- ▶ Super app implementation variations can cause security risks.
- ▶ Standardizing the interface/APIs for these platforms.

Thank You

# Unpacking the Threats of All-in-One Mobile Super Apps

Zhiqiang Lin

Distinguished Professor of Engineering

[zlin@cse.ohio-state.edu](mailto:zlin@cse.ohio-state.edu)





May 8<sup>th</sup>, 2024



# References |

-  Wu Changming and Super Nos, *mini-hot*, <https://github.com/mini-hot/mini-hot>.
-  Haoran Lu, Luyi Xing, Yue Xiao, Yifan Zhang, Xiaojing Liao, XiaoFeng Wang, and Xueqiang Wang, *Demystifying resource management risks in emerging mobile app-in-app ecosystems*, Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020, pp. 569–585.
-  *Weixin mini program platform operation rules*, <https://developers.weixin.qq.com/miniprogram/en/product/>.
-  SinkingPeople, *How to bypass vetting?*, [https://blog.csdn.net/weixin\\_43614065/article/details/125778486](https://blog.csdn.net/weixin_43614065/article/details/125778486).
-  Chao Wang, Ronny Ko, Yue Zhang, Yuqing Yang, and Zhiqiang Lin, *Taintmini: Detecting flow of sensitive data in mini-programs with static taint analysis*, ICSE.
-  Chao Wang, Yue Zhang, and Zhiqiang Lin, *One size does not fit all: Uncovering and exploiting cross platform discrepant apis in wechat*, 31st USENIX Security Symposium (USENIX Security 23), 2023.
-  \_\_\_\_\_, *Uncovering and exploiting hidden apis in mobile super apps*, Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, 2023.
-  Chao Wang, Yue Zhang, , and Zhiqiang Lin, *Characterizing and detecting bugs in wechat mini-programs*, Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, 2024.
-  Yuqing Yang, Yue Zhang, and Zhiqiang Lin, *Cross miniapp request forgery: Root causes, attacks, and vulnerability detection*, Proceedings of the 29th ACM Conference on Computer and Communications Security, 2022.

# References II

-  Yue Zhang, Bayan Turkistani, Allen Yuqing Yang, Chaoshun Zuo, and Zhiqiang Lin, *A measurement study of wechat mini-apps*, Proceedings of the ACM on Measurement and Analysis of Computing Systems 5 (2021), no. 2, 1–25.
-  Yue Zhang, Yuqing Yang, and Zhiqiang Lin, *Don't leak your keys: Understanding, measuring, and exploiting the appsecret leaks in mini-programs.*, Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, 2023.
-  Lei Zhang, Zhibo Zhang, Ancong Liu, Yinzhi Cao, Xiaohan Zhang, Yanjun Chen, Yuan Zhang, Guangliang Yang, and Min Yang, *Identity confusion in webview-based mobile app-in-app ecosystems*, 31st USENIX Security Symposium (USENIX Security'22), 2022.
-  Yanjie Zhao, Yue Zhang, and Haoyu Wang, *Potential risks arising from the absence of signature verification in miniapp plugins*, ACM Workshop on Secure and Trustworthy Superapps (SaTS), 2023.