When Super Apps Become Operating Systems: The Good, The Bad, and The Ugly

Dr. Zhiqiang Lin
Distinguished Professor of Engineering
zlin@cse.ohio-state.edu

06/09/2023

Acknowledgement


Yue Zhang


Bayan Turkistani


Chaoshun Zuo


Yuqing Yang


Chao Wang


Ronny Ko

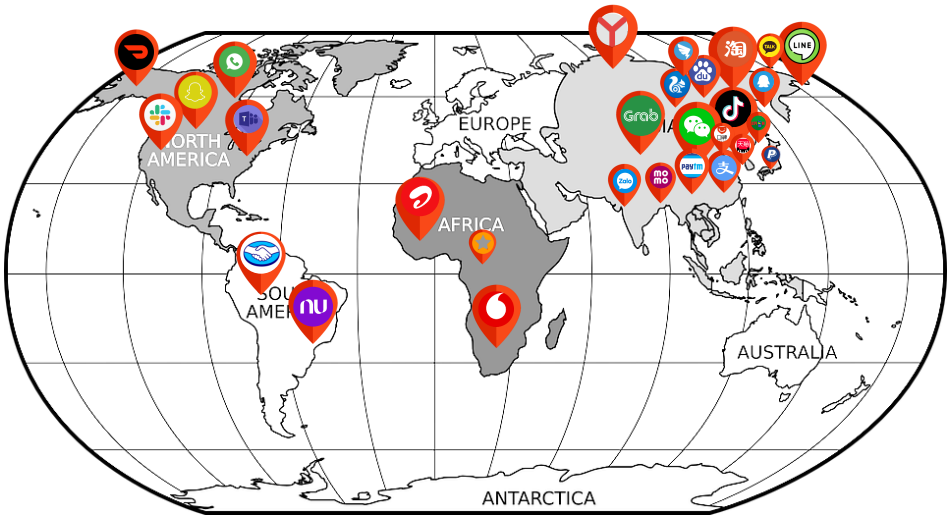
1. **One Size Does Not Fit All: Uncovering And Exploiting Cross Platform Discrepant APIs in Wechat.** In USENIX Security 2023 [WZL23a]
2. **Uncovering and Exploiting Hidden APIs in Mobile Super Apps.** In CCS 2023 [WZL23b]
3. **Don't Leak Your Keys: Understanding, Measuring, and Exploiting the AppSecret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

Mobile Super Apps are Becoming More and More Popular

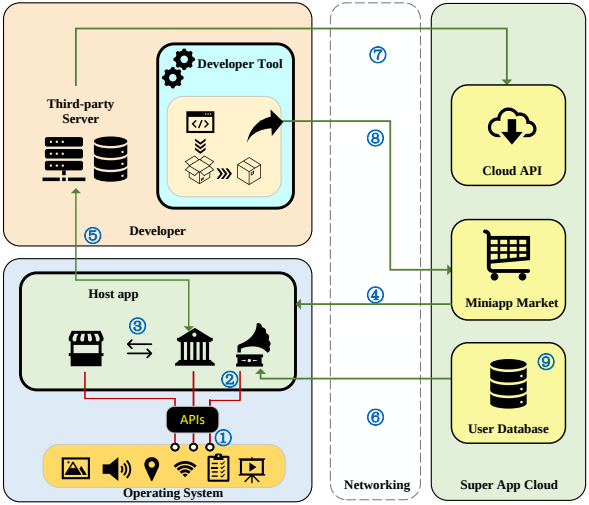
"It's sort of like Twitter, plus PayPal, plus a whole bunch of things all rolled into one, with a great interface."

— Elon Musk

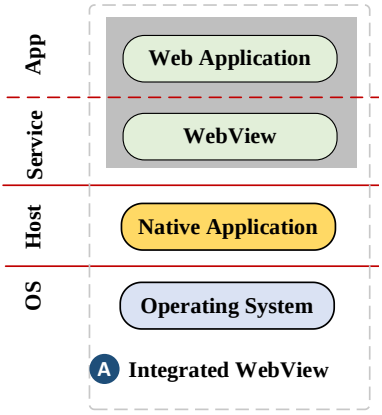
Mobile Super Apps are Becoming More and More Popular



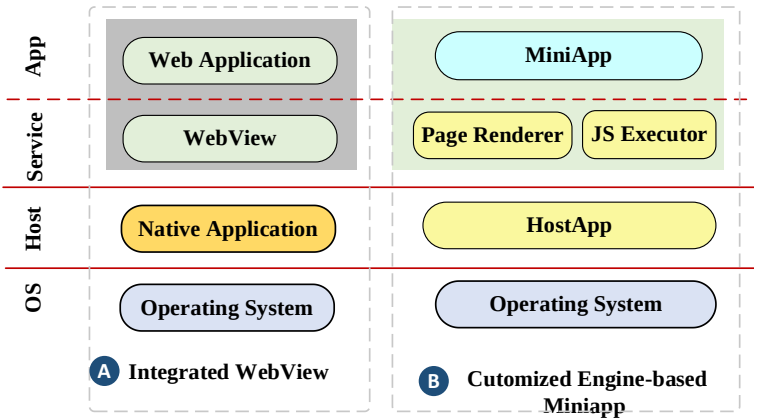
Mobile Superapps in a Nutshell



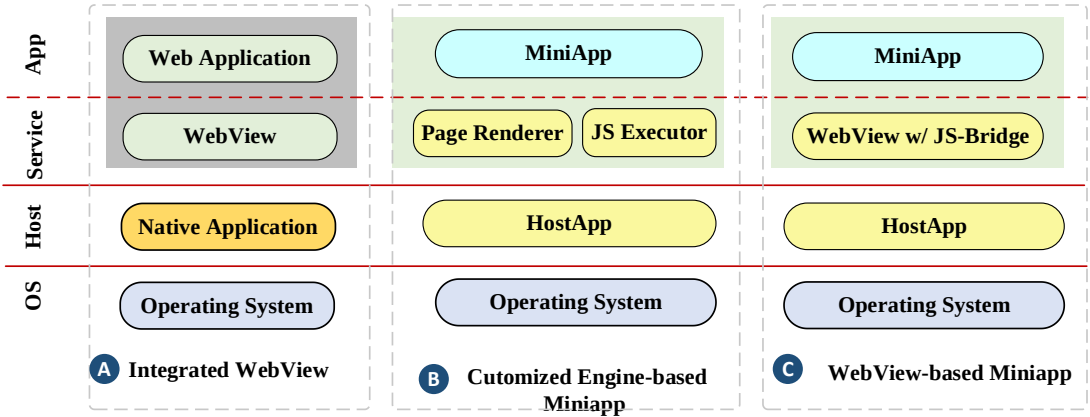
The Taxonomy of Super Apps



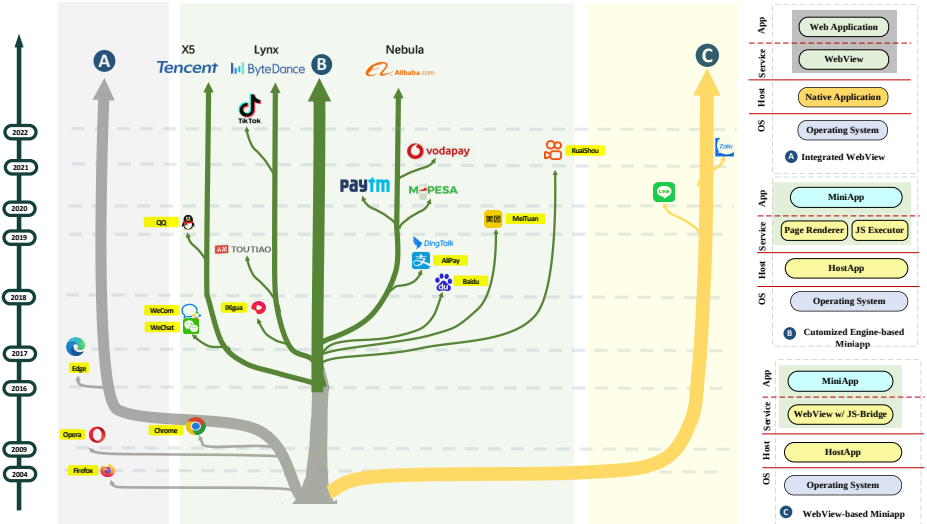
The Taxonomy of Super Apps



The Taxonomy of Super Apps



Evolution of the Superapps

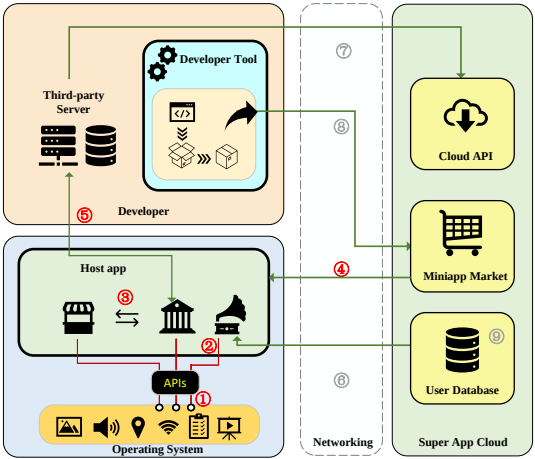


The Benefits a Superapp Can Offer

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.

Security Measures At Front-ends



- **(S1)** Permission Mechanism
- **(S2)** Sandboxing
- **(S3)** API Restriction
- **(S4)** Cross-miniapp Allowlisting
- **(S5)** Designated Distribution Channel

Protected Resources

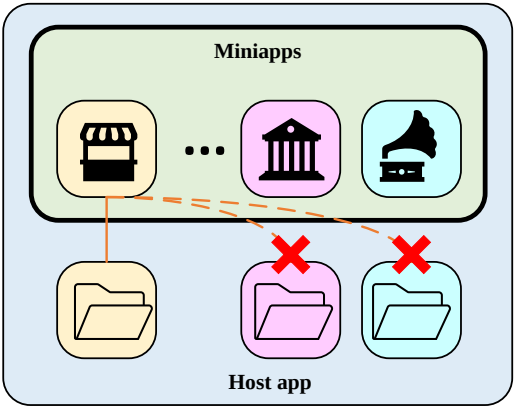
Contacts, Address, Location, Bluetooth, Audio, Camera, Photos, Files, JS Code Execution Environment

(S1) Permission Mechanism

Protected Resources

1. Contacts
2. Location
3. Address
4. Bluetooth
5. Audio
6. Video
7. Photo
8. ...

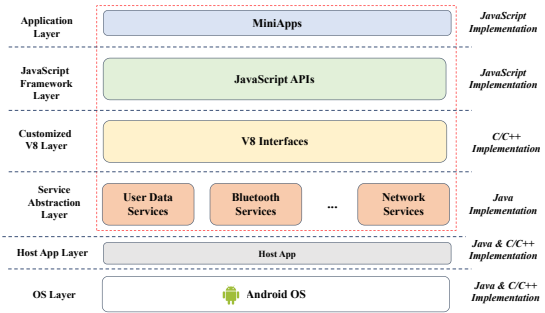
(S2) Sandboxing

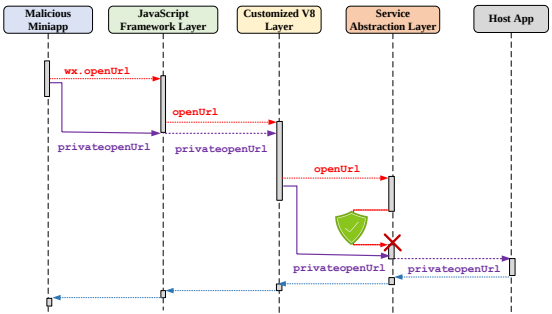


Protected Files

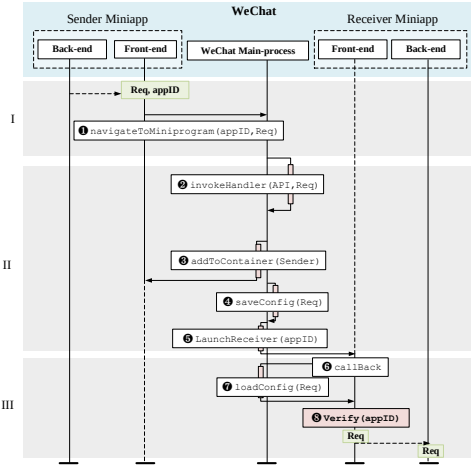
- **Code package file**
- **Other Local files**
  1. **Local temporary file** (The files automatically generated by mini-apps will be recycled by super-apps)
  2. **Local cached file** (e.g., the videos, audio, and images)
  3. **Local user file** (e.g., the user preferences and configurations)

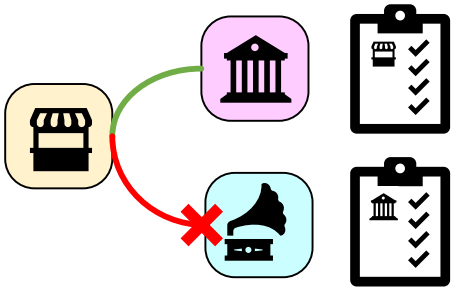
(S3) API Restriction



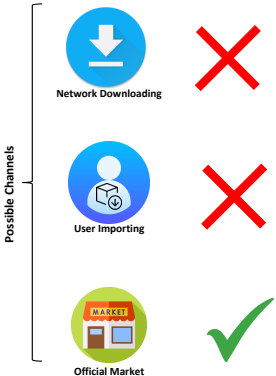


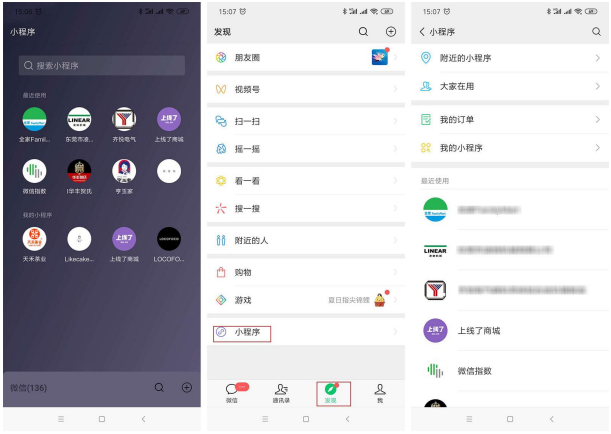
(S4) Cross-miniapp Allowlisting





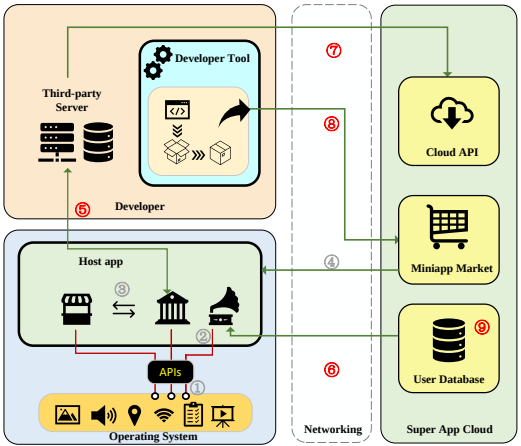
(S5) Designated Distribution Channel





WeChat Miniapp Market

Security Measures At Back-ends



- **(S6)** Domain Allowlisting
- **(S7)** Secure Communication
- **(S8)** Role-Based Access Control
- **(S9)** Data Encryption
- **(S10)** Token-based Services Access
- **(S11)** User Token Isolation
- **(S12)** Code Vetting
- **(S13)** Account Protection

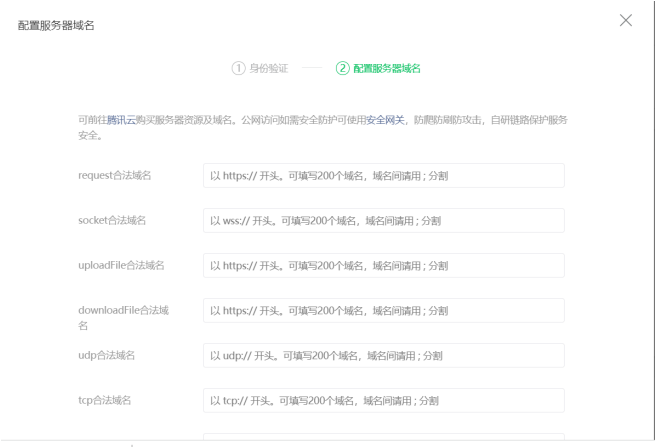
Protected Resources

External Web Domain, Internal Cloud, Database, Phone number, User Info, Werun data, Shareinfo, Miniapp Packages User Account

(S6) Domain Allowlisting & (S7) Secure Communication

Requirement for certificates

- Use a trusted certificate
- The domain name of the website where the SSL certificate is deployed must be the same as the domain name for which the certificate was issued.
- The certificate must not have been expired.
- The certificate's trust chain must be complete (server configuration is required).



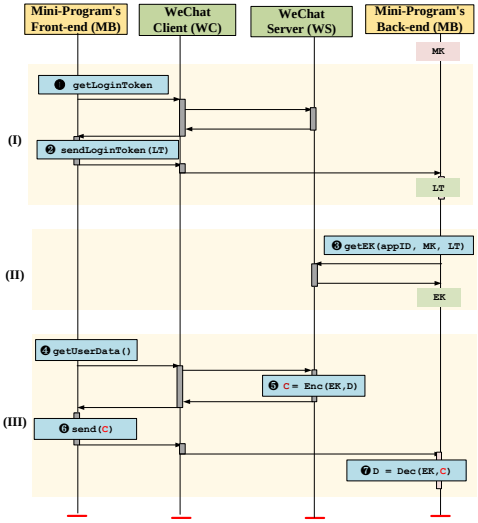
(S8) Role-Based Access Control

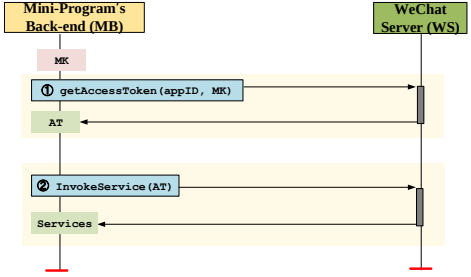
Access Control Rules

1. Only the creator can write the data (e.g., news article), but everyone can read it.
2. Only the creator can read and write the data (e.g., private photo album), other users cannot access it.
3. Only the admin can write the data (e.g., product info), but everyone can read it.
4. Only the admin can read and write the data (e.g., data in the backend that is not exposed).

	A miniapp read its own data	A miniapp write its own data	A miniapp read other miniapp's data	A miniapp write other miniapp's data	Admin read or write the data
Creator write only mode	✓	✓	✓	✗	✓
Creator read/write only mode	✓	✓	✗	✗	✓
Admin write only mode	✓	✗	✓	✗	✓
Admin read/write only mode	✗	✗	✗	✗	✓

(S9) Data Encryption & (S10-S11) Token-based Services Access

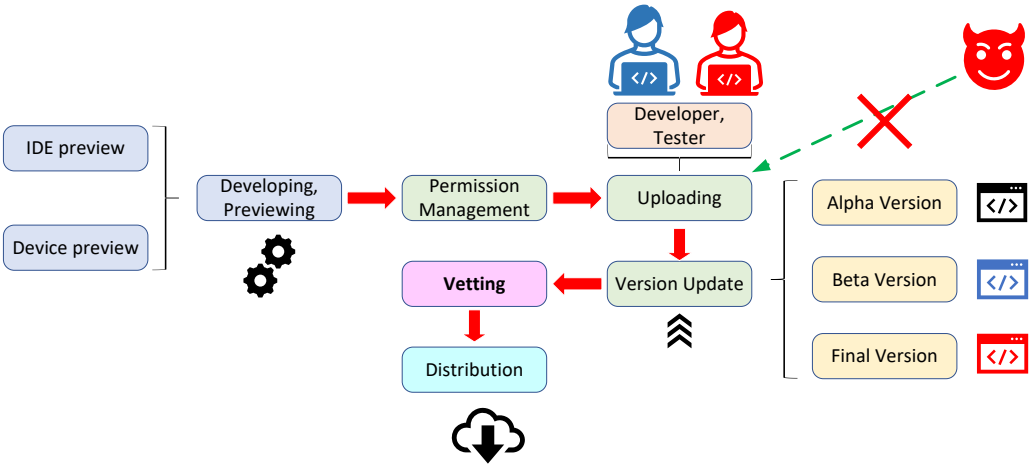




Masterkey (MK)

The Masterkey (MK) is a vital key for cryptographic access control in mini- programs, generated by WeChat upon authentication. WeChat offers two MK-based protocols for accessing resources: encryption- based for sensitive data (S9) and token-based for services (S10,S11).

(S12) Code Vetting & (S13) Account Protection



Security Threats

Threats in the front-ends

- **(T1)** **Threats against permission** [WKZ+]
- **(T2)** **Cross-platform vulnerability** [WZL23a]
- **(T3)** **Cross-miniapp Request Forgery (CMRF)** [YZL22]
- **(T4)** **Hidden API access** [WZL23b]
- **(T5)** Post-vetting hot update

Threats in the back-ends

- **(T6)** Identity confusion [ZZL+22]
- **(T7)** **Master key misuse** [ZYL23]
- **(T8)** Abused API token
- **(T9)** Weak token isolation
- **(T10)** Evasive malware

(T1) Colluding on Privileged Data [WKZ+, LXX+20]

Leaking phone number

- The sender Mini-Program collects users' phone numbers
- The sender Mini-Program transfers them to another mini-program

```
1
2    getPhoneNumber: function(e) {
3        ...
4        n.globalData.btnCanClick = !0, wx.hideLoading(); else {
5        var o = {
6        iv: e.detail.iv,
7        encryptedData: e.detail.encryptedData,
8        type: n.globalData.appType
9        };
10       var l = n.getUrl("info");
11       t.default.post(l, o).then(function(e) {
12       if (200 == e.data.status) {
13       wx.hideLoading();
14       var t = e.data.data.phoneNumber;
15       this.data.phone_number = e.data.data.phoneNumber,
         ↪ n.globalData.userInfo = {
16        phone_number: t }, console.log("Obtained Phone Number",
          ↪ n.globalData.userInfo.phone_number), a.loginProcess(t);
17        } else n.wx_toast(e.data.message);
18        }); } },
19   wx.navigateToMiniProgram({
20       appId: e.linkAppid,
21       path: t,
22       extraData: {
23       mallId: this.data.mallId || "",
24       mallInfo: this.data.mallInfo || "",
25       memberId: this.data.memberId || "",
26       phoneNumber: this.data.phone_number || "", token:
         ↪ this.data.token || "" })
```

(T1) Colluding on Privileged Data [WKZ+, LXX+20]

Leaking location data

- The receiver Mini-Program does not have permission to retrieve users' location
- The receiver Mini-Program receives location data from other Mini-Programs

```
1  var a = e.referrerInfo.extraData.location, n =
   ↪  e.referrerInfo.extraData.imp_data, o =
   ↪  e.referrerInfo.extraData.src_path;
2      void 0 != a && void 0 != n && null != a && null != n
3      "" == this.data.location ? (wx.showLoading({
4      title: "Loading ..."
5       }), this.locationApp(a, n, o)) : this.data.location = "");
6       } catch (e) {}
7        t.eventReady(function() {
8        t.beginTime();
9        });
10       ...
11     wx.request({
12           url: "https://********.***.***",
13     data: location
14 });
```

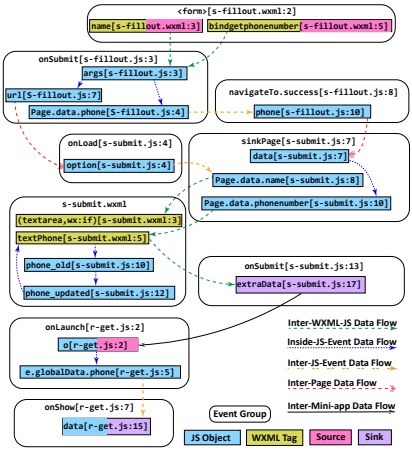
(T1) Colluding on Privileged Data [WKZ+, LXX+20]

TaintMini

- First **open source**, static taint analysis framework for Mini-Programs

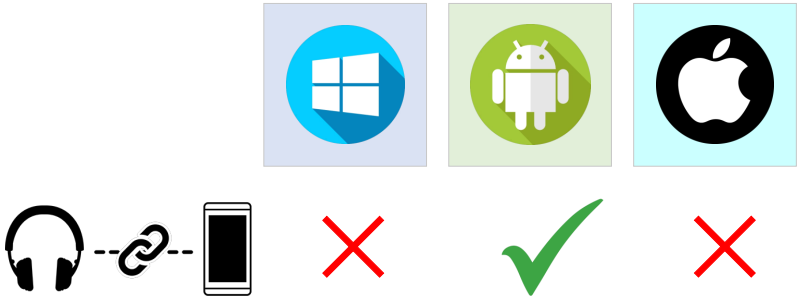
Evaluated w/ 238K Mini-Programs

- **Empirical Results.** Identified 27,184 (11.38%) Mini-Programs contain sensitive data flows
- **Security Application.** Identified 455 colluding apps

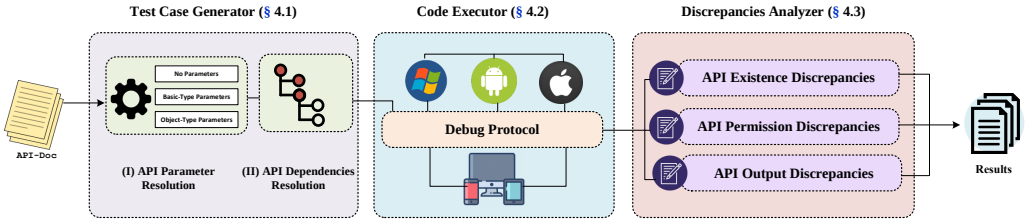


Source code of TaintMini has been made available at: github.com/OSUSecLab/TaintMini

(T2) Cross-platform Vulnerability [WZL23a]



(T2) Cross-platform Vulnerability [WZL23a]



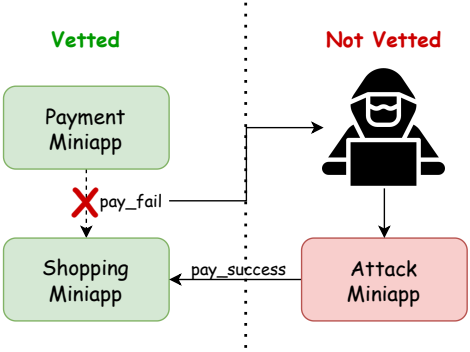
(T2) Cross-platform Vulnerability [WZL23a]

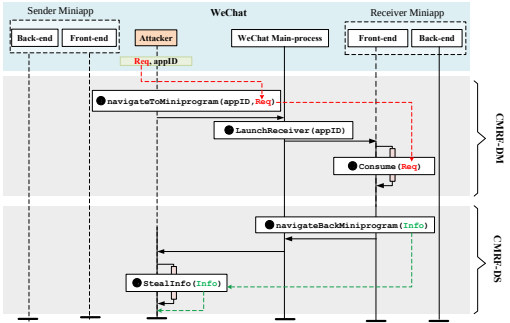
APIs	Permission Scope	Mobile				PC	
		A	P	A	P	A	P
getLocation		✓	✓	✓	✓	✓	✗
chooseLocation	userLocation	✓	✓	✓	✓	✓	✗
startLocationUpdate		✓	✓	✓	✓	✓	✗
SLUBackground*	userLocationBackground	✓	✓	✓	✓	✗	
startRecord		✓	✓	✓	✓	✓	✗
joinVoIPChat	record	✓	✓	✓	✓	✗	
RecorderManager.start		✓	✓	✓	✓	✓	✗
createCameraContext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

(T2) Cross-platform Vulnerability [WZL23a]

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

(T3) Cross Miniapp Request Forgery (CMRF) [YZL22]





(T3) Cross Miniapp Request Forgery (CMRF)

WECHAT

Category	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
Total	2,519,096	97.96	2,113	4.03	50,281	95.97

BAIDU

Category	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
Total	148,018	99.67	1	0.2	493	99.8

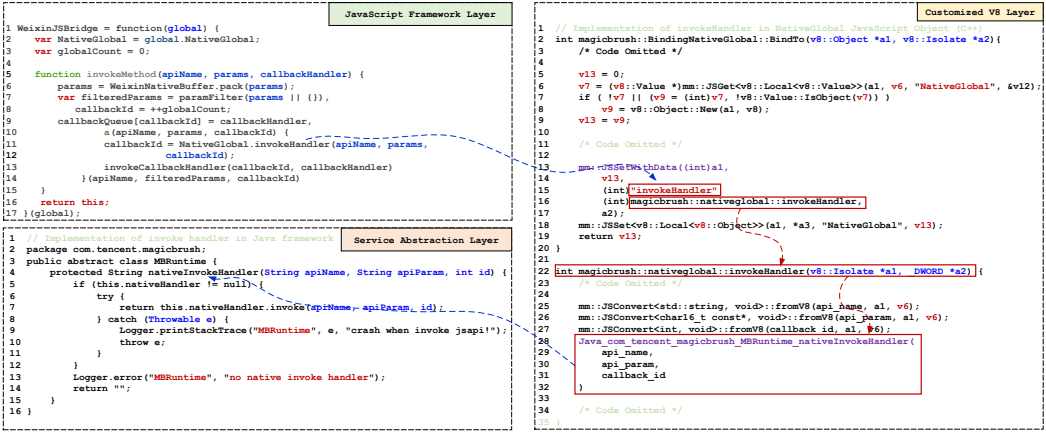
(T4) Hidden APIs [WZL23b]

Attacks Caused by Hidden APIs

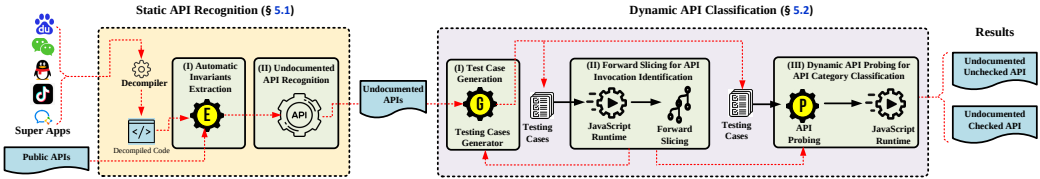
- Arbitrary Web Page Access
- Malware Download and Installation
- Screenshot-based Information Theft
- Phone Number Theft
- Contact Information Theft

```
1 // Documemented API Implemantation 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 Implemantation 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 }
```

(T4) Hidden APIs [WZL23b]



(T4) Hidden APIs [WZL23b]



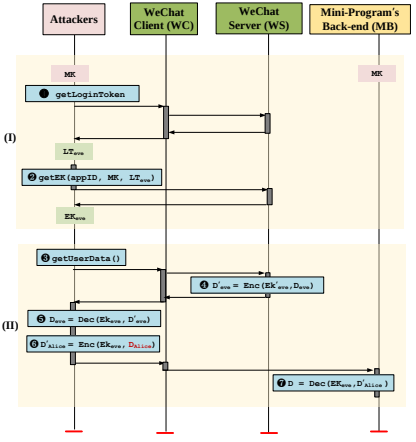
(T4) Hidden APIs [WZL23b]

Available APIs		WeChat				WeCom				Baidu				Tik Tok				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	10	100.0	-	0.0	-	0.0
Location		7	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	1	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	7	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	2	66.7	-	0.0	1	33.3	-	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

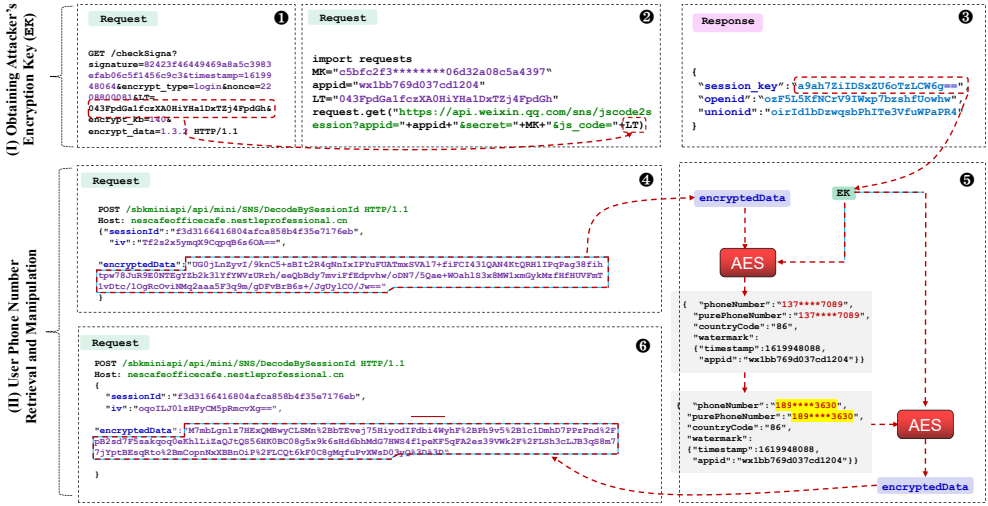
(T7) Key Leakage from Miniapps [ZYL23]

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



(T7) Key Leakage from Miniapps [ZYL23]



(T7) Key Leakage from Miniapps [ZYL23]

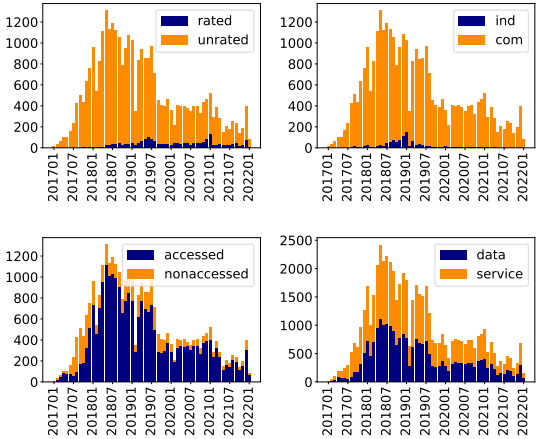


Figure: The trending of all vulnerable mini-programs w.r.t rating, developer, accessed resource type, and accessed data type.

Other Security Threats

Flawed permission [LXX+20]

Super app permission sets may be incomplete, enabling miniapps to access sensitive resources.

Identity confusion [ZZL+22]

Web domains are used to determine miniapp identities, allowing malware to obfuscate identities via fabricated domains.

Post-vetting hot update

Vetted miniapps may utilize dynamic code update to transfer into malware.

Weak token isolation

The tokens in some platforms are not strictly isolated between miniapps.

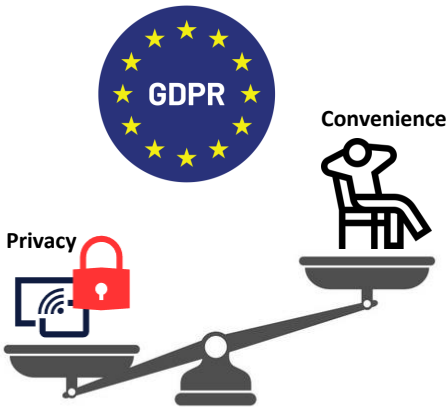
Evasive Malware

Super apps have attracted malware to exploit millions of user data stored in the platform. Specifically, Scam miniapps are emerging as a major concern as they are distributed via trusted social networks (e.g., among close friends)

Trade-off: Privacy and Convenience

Contradiction

- **Convenience:** Users enjoy convenience with miniapps, accessing personal info
- **Risks:** Privacy risk arises when data is shared with super apps.



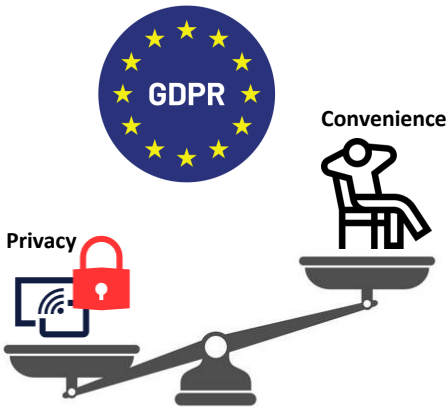
Trade-off: Privacy and Convenience

Contradiction

- **Convenience:** Users enjoy convenience with miniapps, accessing personal info
- **Risks:** Privacy risk arises when data is shared with super apps.

Trade-off

- The balance of convenience and privacy is critical when managing data for massive amount of users.



Trade-off: Security and Usability

Contradiction

- **Security:** Security is vital for the super app ecosystem to ensure user experience and data privacy.
- **Usability:** Prioritizing security measures may impact user experience negatively.

Trade-off: Security and Usability

Contradiction

- **Security:** Security is vital for the super app ecosystem to ensure user experience and data privacy.
- **Usability:** Prioritizing security measures may impact user experience negatively.

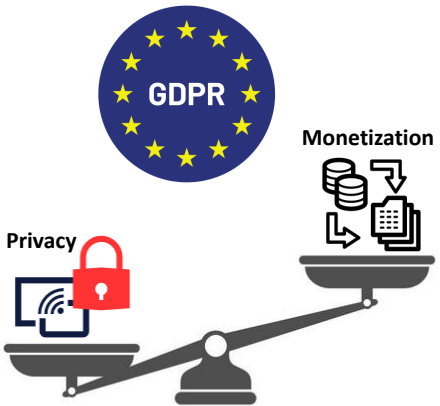
Trade-off

- Super apps need to seek the balance between security and user experiences

Trade-off: Privacy and Monetization

Contradiction

- **Attemption:** Super apps might monetize user data through third-party sharing.
- **Problem:** Privacy issues, with users potentially unaware of data usage control.



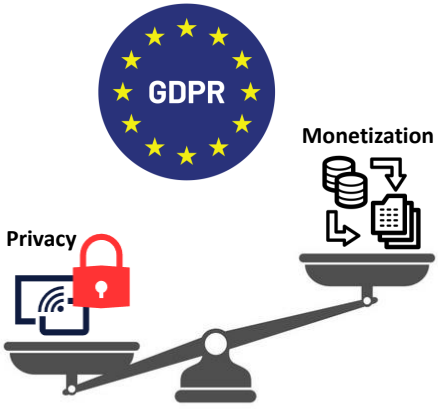
Trade-off: Privacy and Monetization

Contradiction

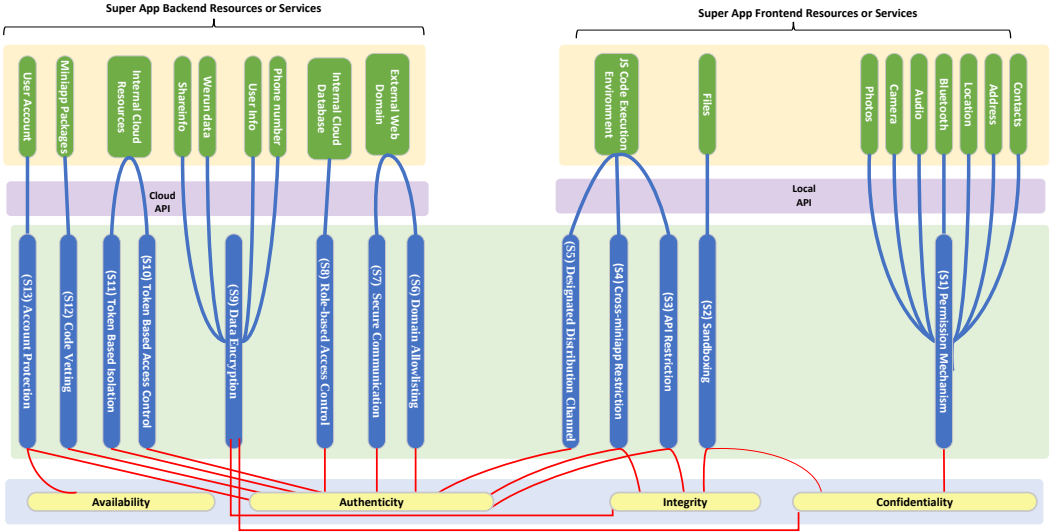
- **Attemption:** Super apps might monetize user data through third-party sharing.
- **Problem:** Privacy issues, with users potentially unaware of data usage control.

Trade-off

- Ensure transparent data practices
- Provide explicit privacy policies
- Use robust data protection
- Give users data control



Summary of Security Measures



Lessons Learned

Security Mechanism Analysis							Security Threat Analysis							Security Impact Analysis			
Security Mechanism		At		Assumption			Threat ID		Root Cause					Privileged Access	Vetting Bypass	Data Issue	
		#	F	B	A	I	V			Comp.	Impl.	Trust	Vetting			Injection	Leakage
S1	Permission mechanism	①	✓		✓			T1	Flawed Permission	Permission Management				Data			✓
S2	Sandboxing	①	✓		✓			T2	Cross-platform Vulnerability	Resource Management				Data			✓
S3	API Restriction	②	✓			✓		T3	Hidden API Access	Missing				Service			✓
S4	Cross-miniapp Allowlisting	③	✓				✓	T4	Cross-miniapp Injection	Miniapp				Miniapp		✓	
S5	Designated Distribution Channel	④	✓				✓	T5	Post-vetting Hot Update	Post-vetting				Service	✓		
S6	Domain Allowlisting	⑤		✓			✓	T6	Identity Confusion	Miniapp				Service	✓		
S7	Secure Communication	⑤		✓	✓				-	-				-		-	
S8	Role Based Access Control	⑥		✓	✓				-	-				-		-	
S9	Data Encryption	⑥		✓		✓		T7	Master Key Misuse	Developer				Data			✓
S10	Token-based Access Control	⑦		✓		✓		T8	Abused API Token	Developer				Data			✓
S11	User Token Isolation	⑦		✓		✓		T9	Weak Token Isolation	Weak				Data			✓
S12	Code Vetting	⑧		✓			✓	T10	Evasive Malware				Intra-vetting	Data	✓		
S13	Account Protection	⑨		✓			✓		-	-				-		-	

Adopted mechanisms

Adopted mechanisms need to be aware of the underlying implementation difference that potentially voids the security of super apps

Lessons Learned

Security Mechanism Analysis							Security Threat Analysis						Security Impact Analysis			
Security Mechanism		At		Assumption			Threat ID		Root Cause				Privileged Access	Vetting Bypass	Data Issue	
		#	F B	A	I	V			Comp.	Impl.	Trust	Vetting			Injection	Leakage
S1	Permission mechanism	①	✓	✓			T1	Flawed Permission	Permission Management				Data			✓
S2	Sandboxing	①	✓	✓			T2	Cross-platform Vulnerability	Resource Management				Data			✓
S3	API Restriction	②	✓		✓		T3	Hidden API Access		Missing			Service			✓
S4	Cross-miniapp Allowlisting	③	✓			✓	T4	Cross-miniapp Injection			Miniapp		Miniapp		✓	
S5	Designated Distribution Channel	④	✓			✓	T5	Post-vetting Hot Update				Post-vetting	Service	✓		
S6	Domain Allowlisting	⑤		✓		✓	T6	Identity Confusion			Miniapp		Service	✓		
S7	Secure Communication	⑤		✓	✓			-			-		-		-	
S8	Role Based Access Control	⑥		✓	✓			-			-		-		-	
S9	Data Encryption	⑥		✓		✓	T7	Master Key Misuse			Developer		Data			✓
S10	Token-based Access Control	⑦		✓		✓	T8	Abused API Token			Developer		Data			✓
S11	User Token Isolation	⑦		✓		✓	T9	Weak Token Isolation		Weak			Data			✓
S12	Code Vetting	⑧		✓		✓	T10	Evasive Malware				Intra-vetting	Data	✓		
S13	Account Protection	⑨		✓		✓		-			-		-		-	

Isolation mechanisms

Isolation mechanisms need to be prudently examined and adapted to the super apps to ensure comprehensive isolation, where developers should not be excessively trusted.

Lessons Learned

Security Mechanism Analysis							Security Threat Analysis							Security Impact Analysis			
Security Mechanism		At		Assumption			Threat ID		Root Cause					Privileged Access	Vetting Bypass	Data Issue	
		#	F	B	A	I	V			Comp.	Impl.	Trust	Vetting			Injection	Leakage
S1	Permission mechanism	①	✓		✓			T1	Flawed Permission	Permission Management				Data			✓
S2	Sandboxing	①	✓		✓			T2	Cross-platform Vulnerability	Resource Management				Data			✓
S3	API Restriction	②	✓			✓		T3	Hidden API Access		Missing			Service			✓
S4	Cross-miniapp Allowlisting	③	✓				✓	T4	Cross-miniapp Injection			Miniapp		Miniapp		✓	
S5	Designated Distribution Channel	④	✓				✓	T5	Post-vetting Hot Update				Post-vetting	Service	✓		
S6	Domain Allowlisting	⑤		✓			✓	T6	Identity Confusion			Miniapp		Service	✓		
S7	Secure Communication	⑤		✓	✓				-		-			-		-	
S8	Role Based Access Control	⑥		✓	✓				-		-			-		-	
S9	Data Encryption	⑥		✓		✓		T7	Master Key Misuse			Developer		Data			✓
S10	Token-based Access Control	⑦		✓		✓		T8	Abused API Token			Developer		Data			✓
S11	User Token Isolation	⑦		✓		✓		T9	Weak Token Isolation		Weak			Data			✓
S12	Code Vetting	⑧		✓			✓	T10	Evasive Malware				Intra-vetting	Data	✓		
S13	Account Protection	⑨		✓			✓		-		-			-		-	

Vetting mechanisms

Vetting mechanisms is not omnipotent. Evasive malware may circumvent vetting, and malware may be dynamically updated in post-vetting phases.

Other Open Problems

Security Compliance Analysis

- Protection mechanisms should meet or exceed security levels of underlying systems.
- **Future work**: Include systematic analysis tools for vulnerability detection.

Miniapp Developer Education

- Developers need training on proper security practices and Super apps should highlight security configuration.
- **Future work**: Include tools for automatic analysis and detection of data leaks.

Security Mechanism Standardization

- Super app implementation variations can cause security risks.
- **Future work**: Study viable security mechanisms for these platforms.

Semantic-aware Miniapp Vetting

- Current miniapp vetting mechanisms face challenges despite strict controls.
- **Future work**: Involve modeling super app-specific miniapp malware.

Thank You

When Super Apps Become Operating Systems: The Good, The Bad, and The Ugly

Dr. Zhiqiang Lin
Distinguished Professor of Engineering
zlin@cse.ohio-state.edu

06/09/2023

References I


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.


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.


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.


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.