

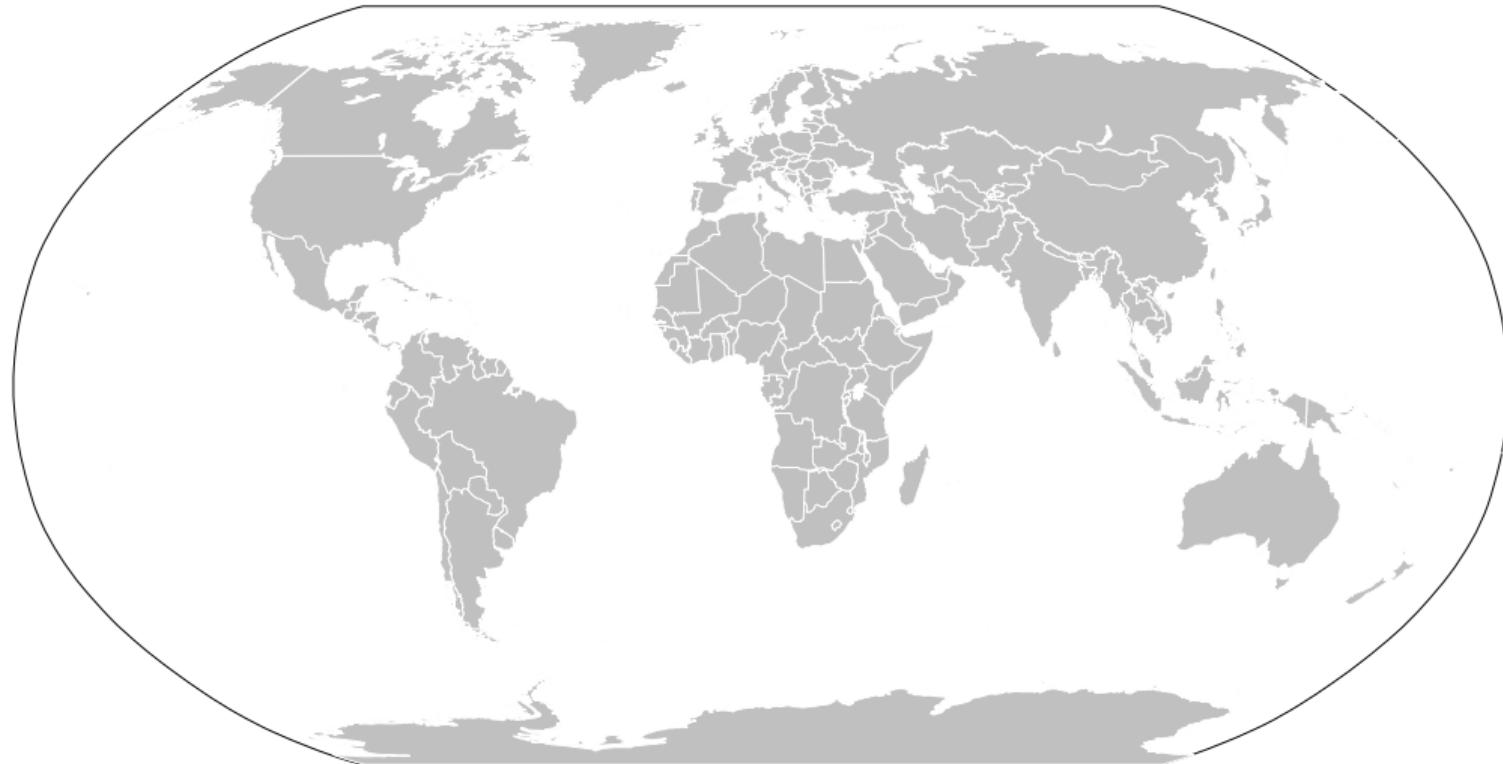


# One Size Does Not Fit All: Uncovering and Exploiting Cross Platform Discrepant APIs in WeChat

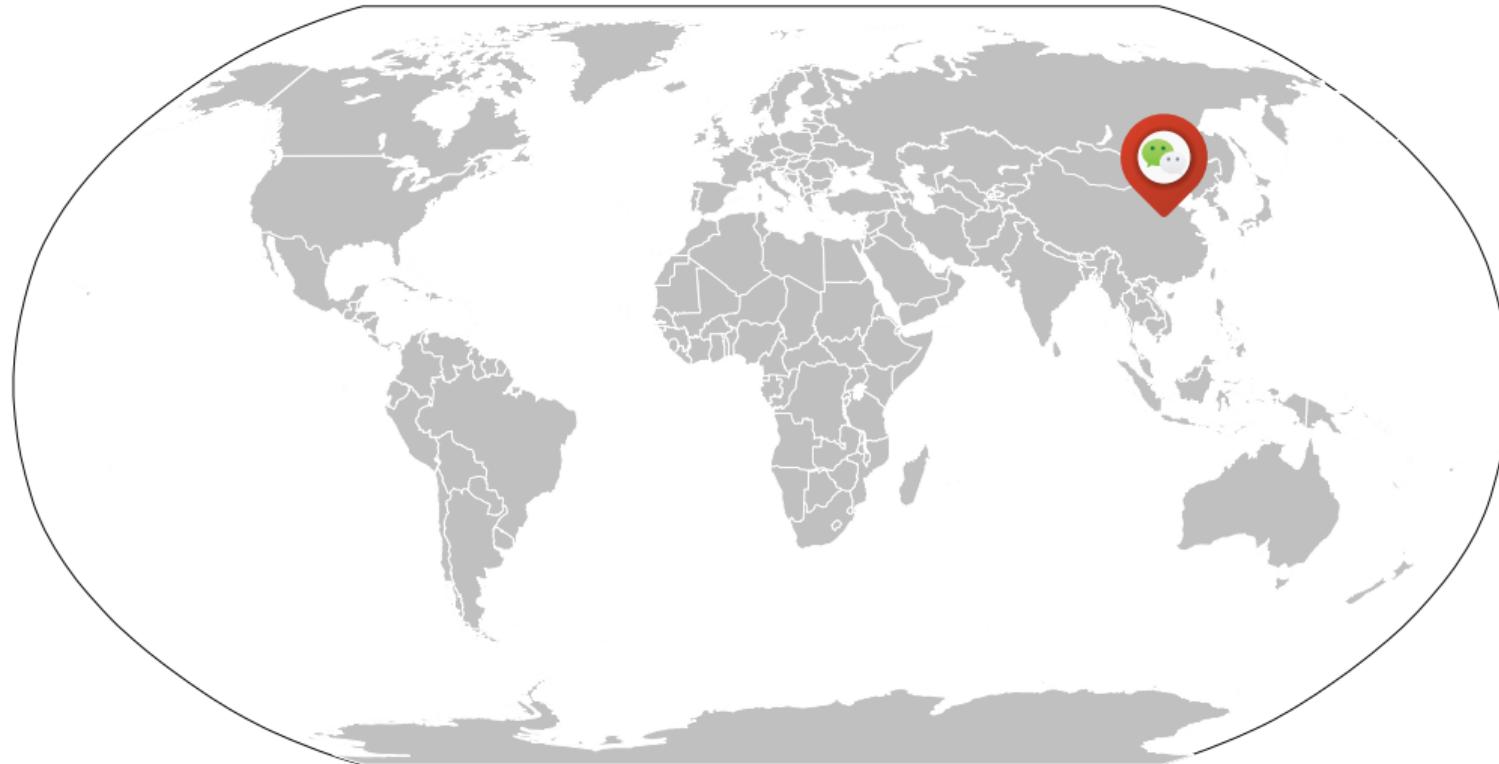
Chao Wang, Yue Zhang, and Zhiqiang Lin

USENIX Security 2023

# The world of SuperApps



# The world of SuperApps



# The world of SuperApps



# The world of SuperApps



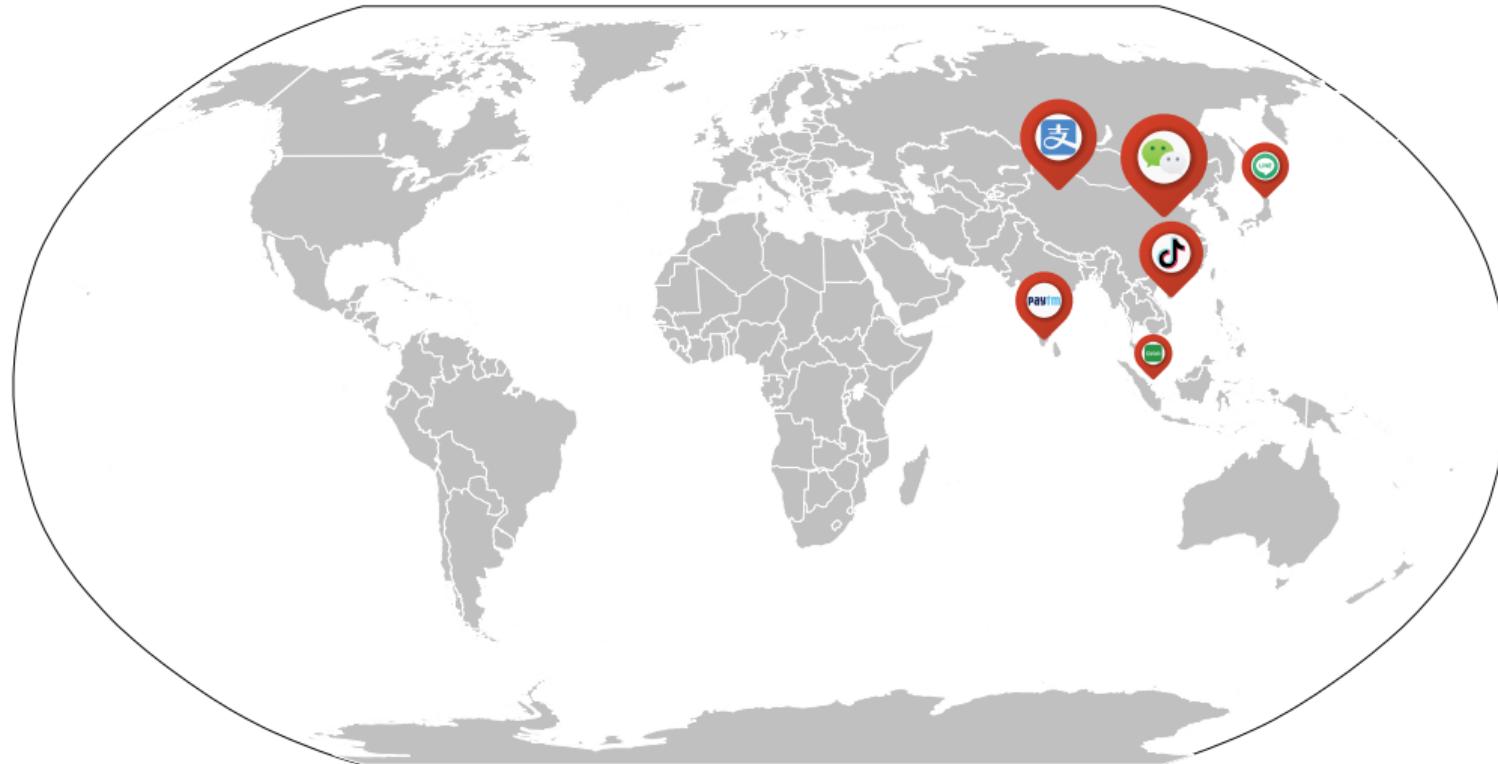
# The world of SuperApps



# 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.

...

# Our scope: WeChat

Super App	Category	Monthly Users	Country	Services									Platform		Miniapp				
				Business	Education	Communication	Finance	Food Delivery	Games	Lifestyle	Ride-hailing	Shopping	Social	Android	iOS	Windows	Android	iOS	Windows
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	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗

# Our scope: WeChat

Super App	Category	Monthly Users	Country	Services										Platform	Miniapp		
				Business	Education	Communication	Finance	Food Delivery	Games	Lifestyle	Ride-hailing	Shopping	Social				
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	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗

# SuperApps provide multiple services

From life essentials to government services



...

# SuperApps provide multiple services

But how do those SuperApps accomplish that?



• • •

# SuperApps provide multiple services

## MiniApps



# SuperApps provide multiple services

MiniApps ... why?



# Traditional application development



Android

# Traditional application development



Android



iOS

# Traditional application development



Android



iOS



Windows

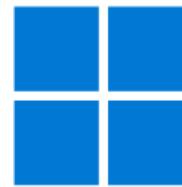
# Traditional application development



Java



Objective-C



C#

# Traditional application development



Java



Objective-C



C#

**Too costly!**

# One size fits all



Java



Objective-C



C#



JavaScript



# One size fits ... all?



Java



Objective-C



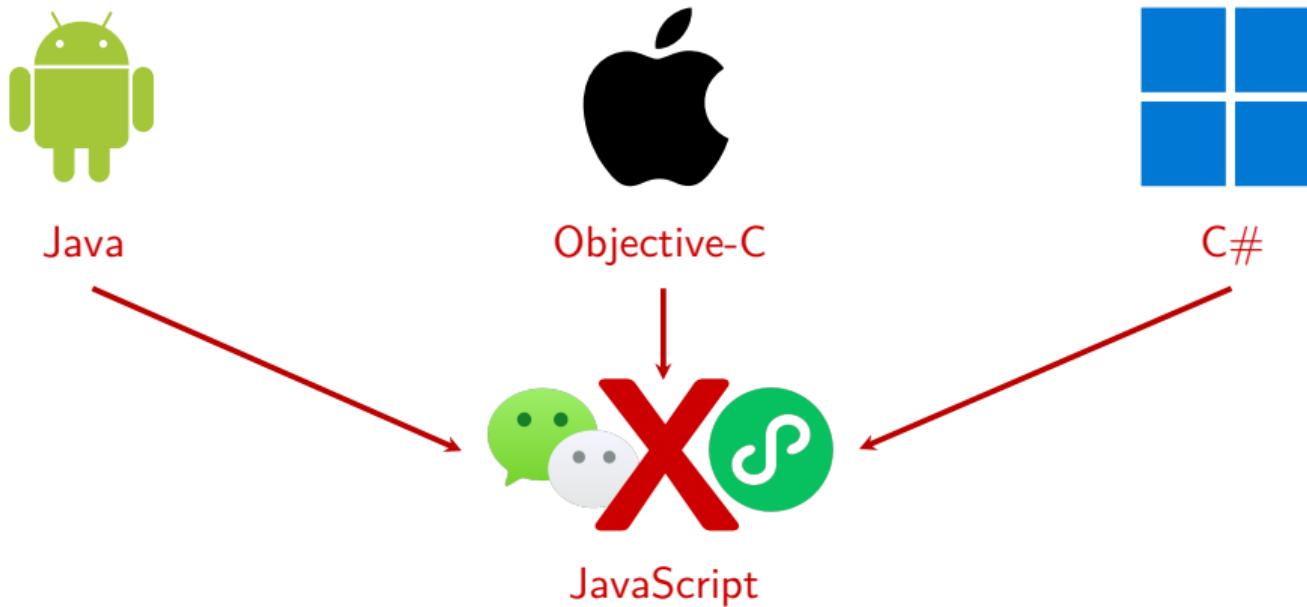
C#



JavaScript



# One size does not fit all!



## A running example

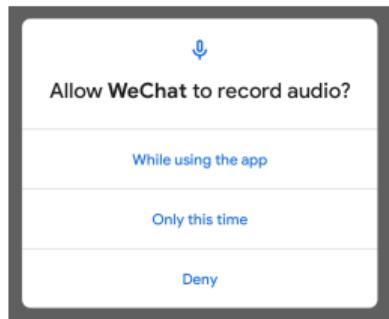
Mallory wants to record people's voice stealthily...



[Top secret chats]

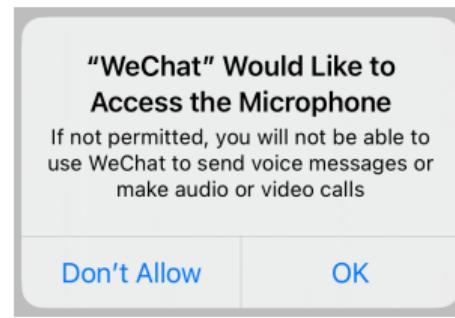
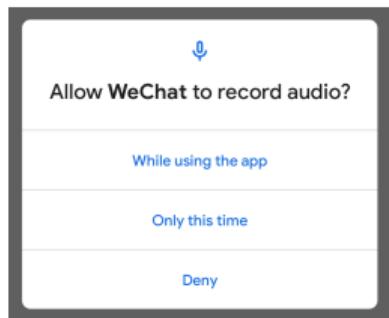
# A running example

Mallory wants to record people's voice stealthily...



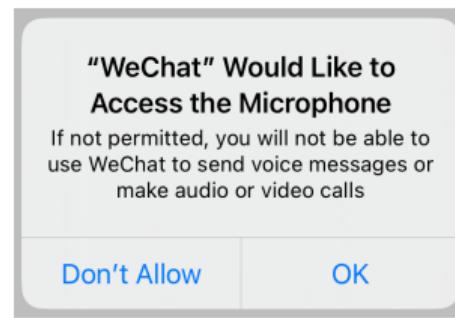
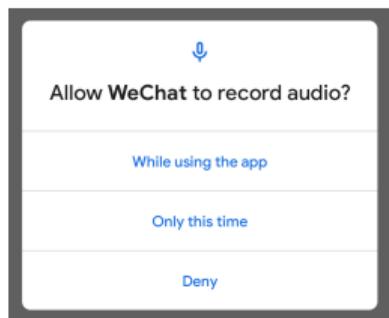
# A running example

Mallory wants to record people's voice stealthily...



# A running example

Mallory wants to record people's voice stealthily...

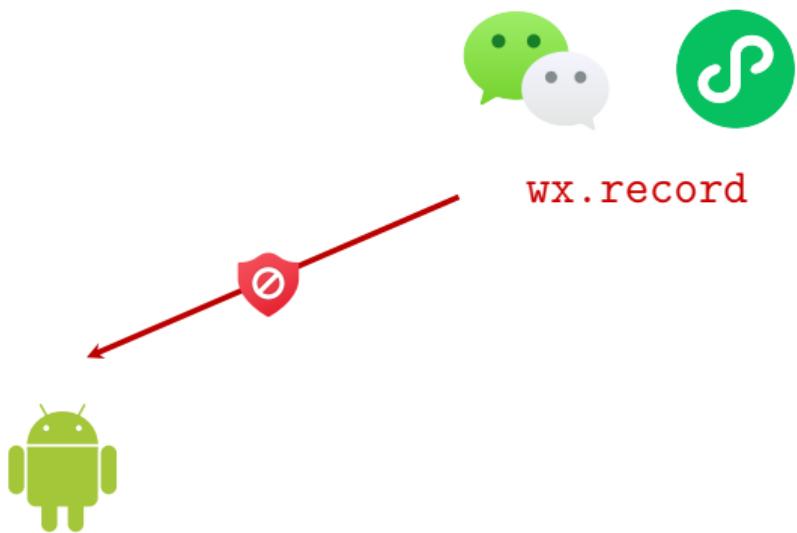


# When it comes to MiniApp



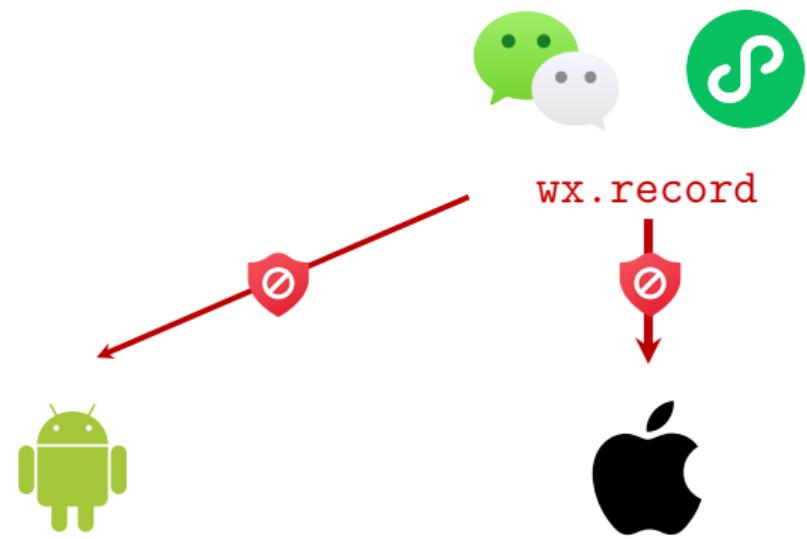
`wx.record`

# When it comes to MiniApp



AudioRecord

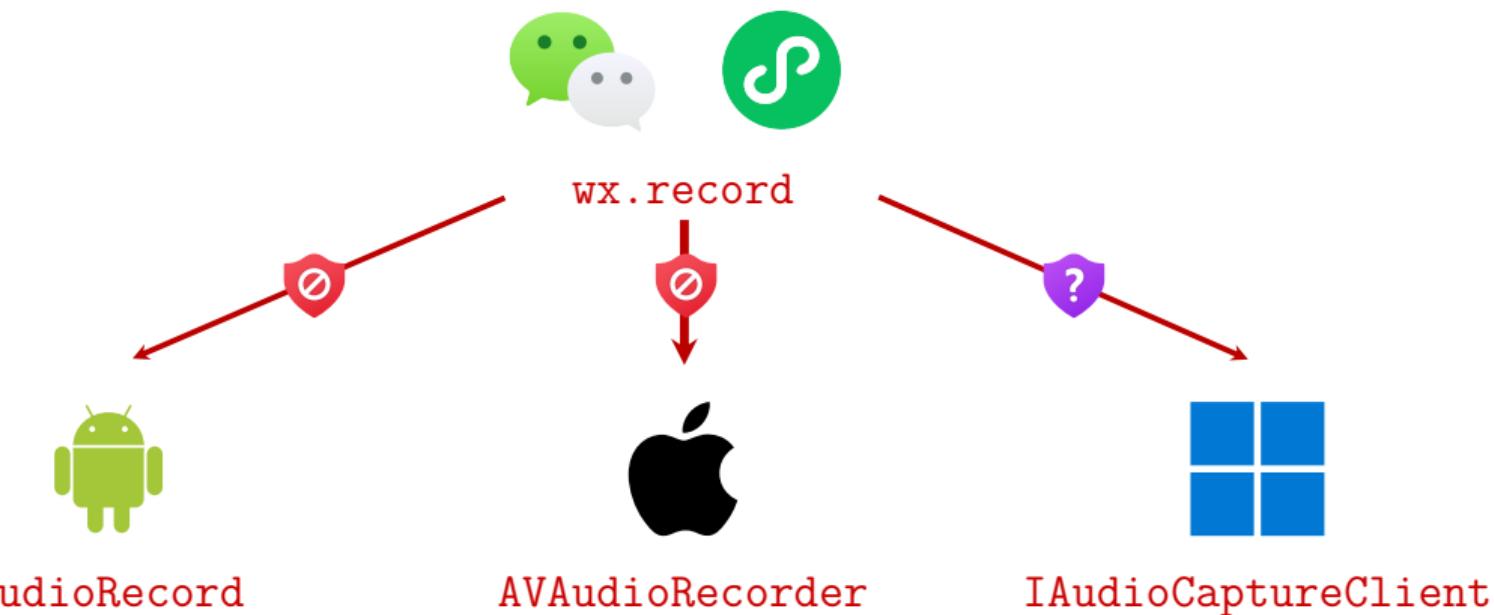
# When it comes to MiniApp



AudioRecord

AVAudioRecorder

# When it comes to MiniApp



# Permission control is not the only thing

The nature of cross-platform involves different host resources...



# Permission control is not the only thing

APIs accessing those resources may have discrepancies...



# Permission control is not the only thing

And WeChat must mitigate attacks from such discrepancies...?



# When it fails



## Three categories of discrepant APIs in WeChat

- ▶ **API existence discrepancies**
- ▶ **API permission discrepancies**
- ▶ **API output discrepancies**

# When it fails



Three categories of attacks due to API discrepancies in WeChat

- ▶ **API existence discrepancies** - **Man-in-the-Middle**
- ▶ **API permission discrepancies** - **Privacy breaches**
- ▶ **API output discrepancies** - **User fingerprinting**

# When it fails



Three categories of attacks due to API discrepancies in WeChat

- ▶ **API existence discrepancies** - **Man-in-the-Middle**
- ▶ **API permission discrepancies** - **Privacy breaches**
- ▶ **API output discrepancies** - **User fingerprinting**

Then how to systematically find such discrepant APIs?

# WeChat is powerful, but it's also challenging to test their APIs...

## Challenges

- ① How to generate valid test cases
- ② How to execute test cases on different platforms
- ③ How to identify the discrepant APIs

# Our solution

## Solutions

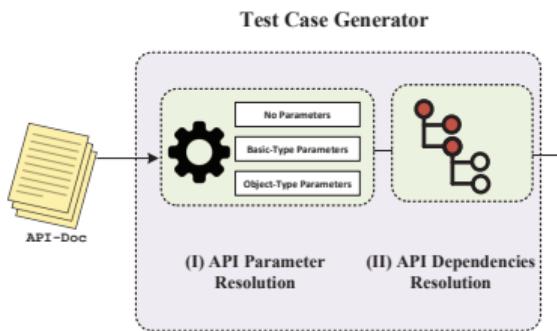
- ① How to generate valid test cases  
*Domain-guided brute-force approach*
- ② How to execute test cases on different platforms  
*Universal debug protocol*
- ③ How to identify the discrepant APIs  
*Specific detection policies*

# APIDiff

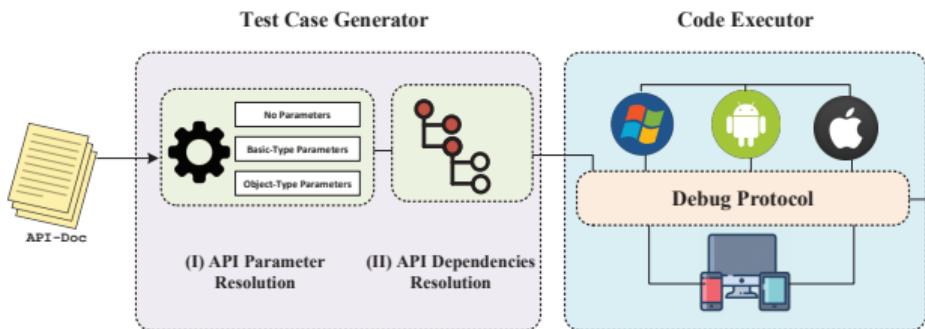


API-Doc

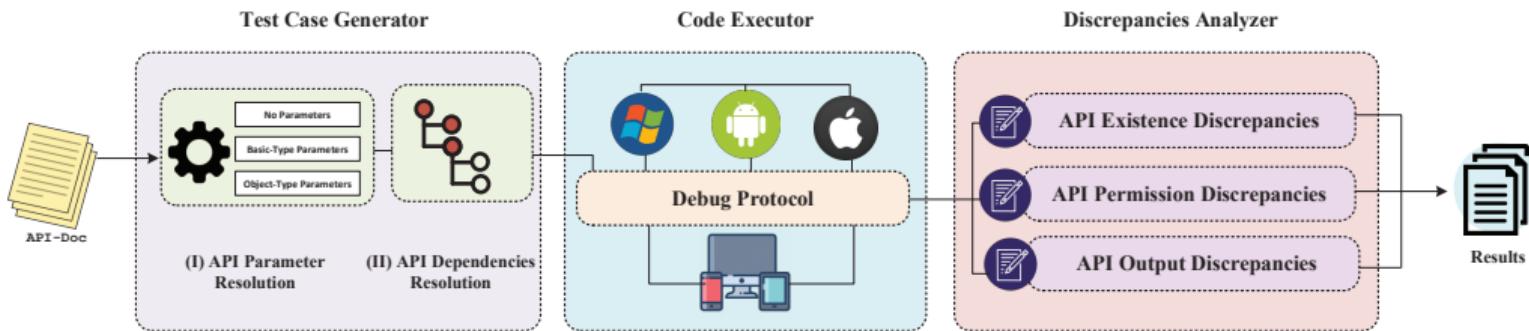
# APIDiff



# APIDiff



# APIDiff

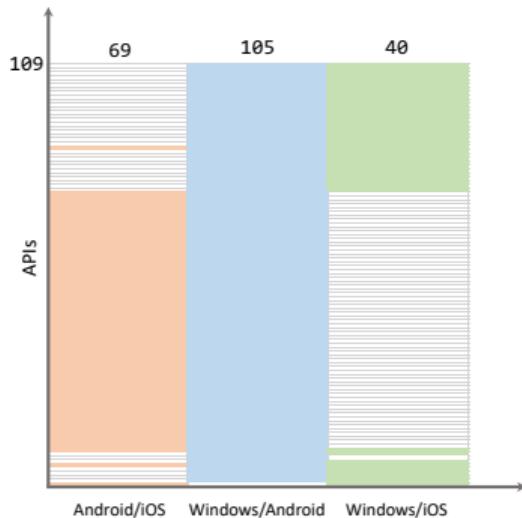


# Experiment setup

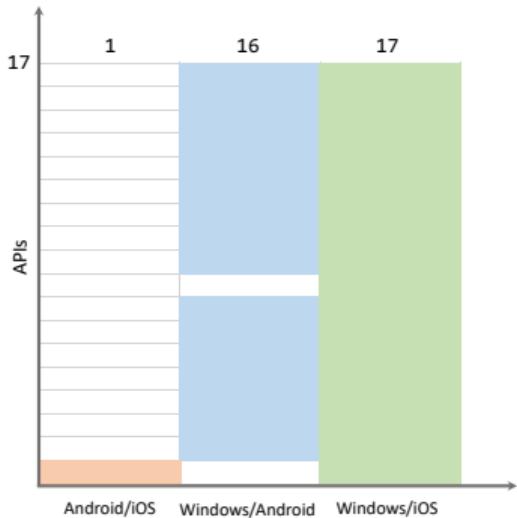
## APIDIFF

- ▶ 3,000+ LoC, pure TypeScript
- ▶ Server / Client model for scalability
- ▶ No root / jailbreak required for testing Android / iOS

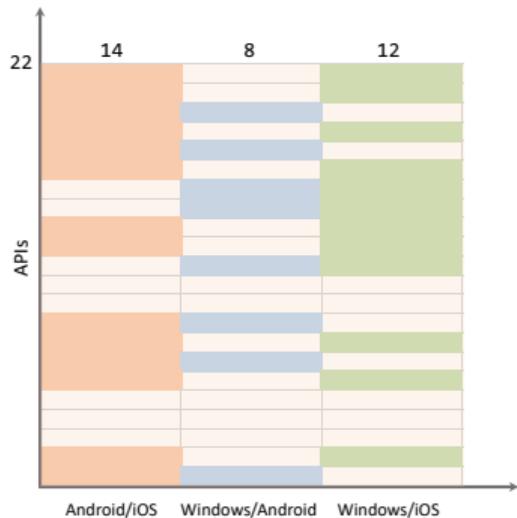
# Evaluation summary



**109**  
Existence Discrepancies



**17**  
Permission Discrepancies



**22**  
Output Discrepancies

# API existence discrepancies

- ▶ Hardware-specific (e.g., **NFC** on Windows)
- ▶ Platform's implementation discrepancies (e.g., accessibility services on Windows)
- ▶ WeChat's implementation discrepancies (e.g., crypto random number generation)

API Category	Total	Platforms							
		Android	Apple	%	Windows	Android	%	Windows	Apple
Devices	74	-	-	-	21	28.38	21	28.38	28.38
File	8	1	12.50	12.50	1	12.50	1	12.50	12.50
Location	12	-	-	-	2	16.67	2	16.67	16.67
Media	32	-	-	-	8	25.00	8	25.00	25.00
mDNS	10	-	-	-	1	10.00	1	10.00	10.00
<b>NFC</b>	<b>65</b>	<b>65</b>	<b>100.00</b>	<b>100.00</b>	<b>65</b>	<b>100.00</b>	<b>1</b>	<b>10.00</b>	<b>10.00</b>
OpenAPI	5	1	20.00	20.00	3	60.00	2	40.00	40.00
Storage	4	-	-	-	1	25.00	1	25.00	25.00
System	12	1	8.33	8.33	1	8.33	1	8.33	8.33
UI	9	1	11.11	11.11	2	22.22	3	33.33	33.33

# API permission discrepancies

- WeChat on Windows does not request any permissions from users to access privacy-sensitive resources, including **location**, **recording**, and **camera**

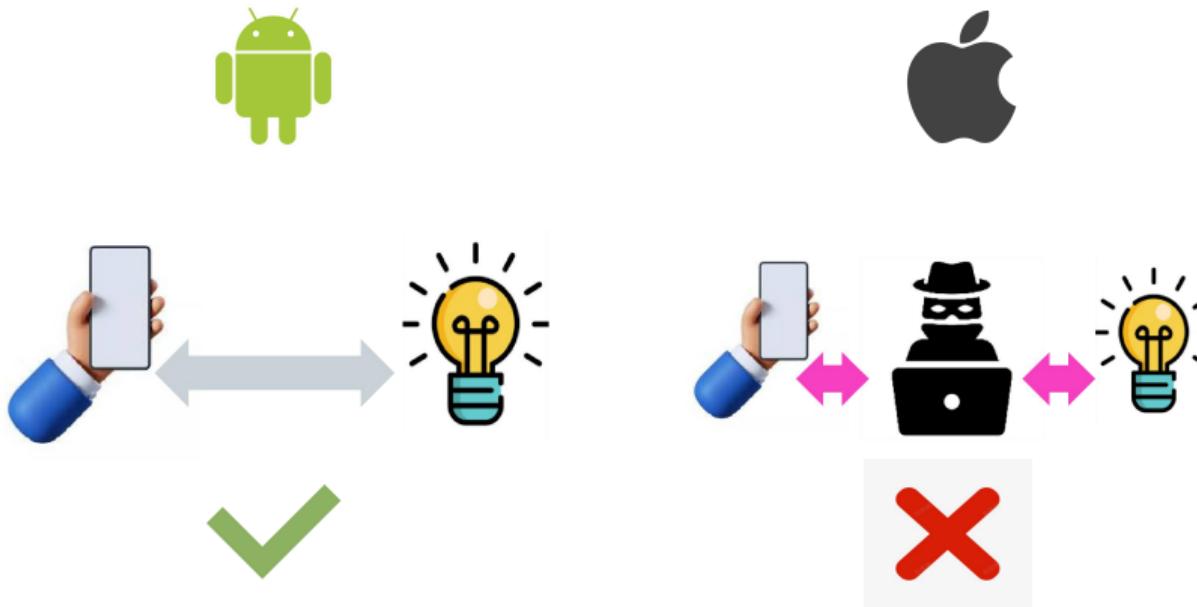
APIs	Permission Scope	Mobile				PC	
		Android		iOS		Windows	
		A	P	A	P	A	P
getLocation		✓	✓	✓	✓	✓	✗
chooseLocation	userLocation	✓	✓	✓	✓	✓	✗
startLocationUpdate		✓	✓	✓	✓	✓	✗
SLUBackground*	userLocationBackground	✓	✓	✓	✓	✗	-
startRecord		✓	✓	✓	✓	✓	✗
joinVoIPChat	record	✓	✓	✓	✓	✗	-
RecorderManager.start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

# API output discrepancies

- ▶ **22 APIs have unique output, 13 of them have stable output for fingerprinting**

Name	Category	Type	Precision	Mobile			Desktop			
				A     S     U			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			✓	✓		✓	✓		

# Man-in-the-Middle attack



# Information collection attack

The missing check in Windows WeChat...

① Location tracking attack

↪ via `wx.getLocation`



② Conversation eavesdropping attack

↪ via `wx.startRecord`



③ Stealthy photo and video capture

↪ via `CameraContext`



④ User information stealing

↪ via `wx.getUserInfo`



# Fingerprinting attack

Real-world attack via fingerprintable APIs

► Brand



► Model



► Screen



► Platform



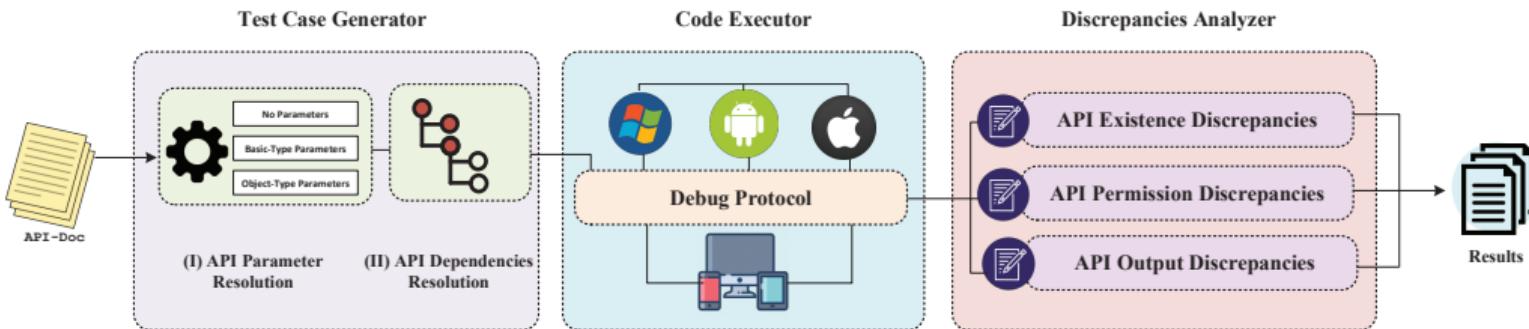
# Conclusion

## APIDIFF

- First **open source** tool for WeChat
  - API test case generation
  - API test case execution
  - API discrepancies identification

## Evaluated w/ 1,000+ APIs

- Uncovered **cross-platform** discrepant APIs
  - 109 existence discrepancies
  - 17 permission discrepancies
  - 22 output discrepancies



# Q&A

**APIDiff Source Code**

<https://github.com/OSUSecLab/APIDiff>

**SecLab @ OSU**

<https://go.osu.edu/seclab>