App in App Resource Management Risks

APINA Resource Risks

Sean Zeng CS702 2021 S1
University of Auckland

APINA Resource Risks

Authors

Haoran Lu, Luyi Xing∗, Yue Xiao, Yifan Zhang,
Xiaojing Liao, XiaoFeng Wang, Xueqiang Wang

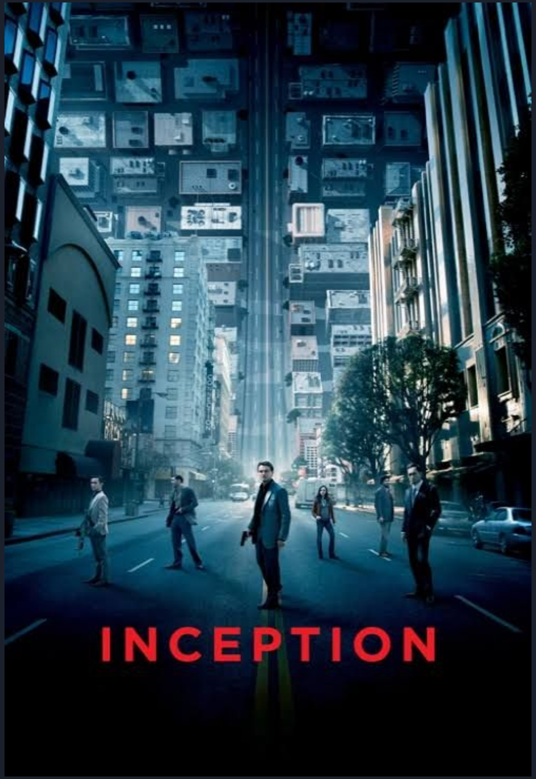
Indiana University Bloomington

Published

ACM SIGSAC Conference on Computer and
Communications October 2020

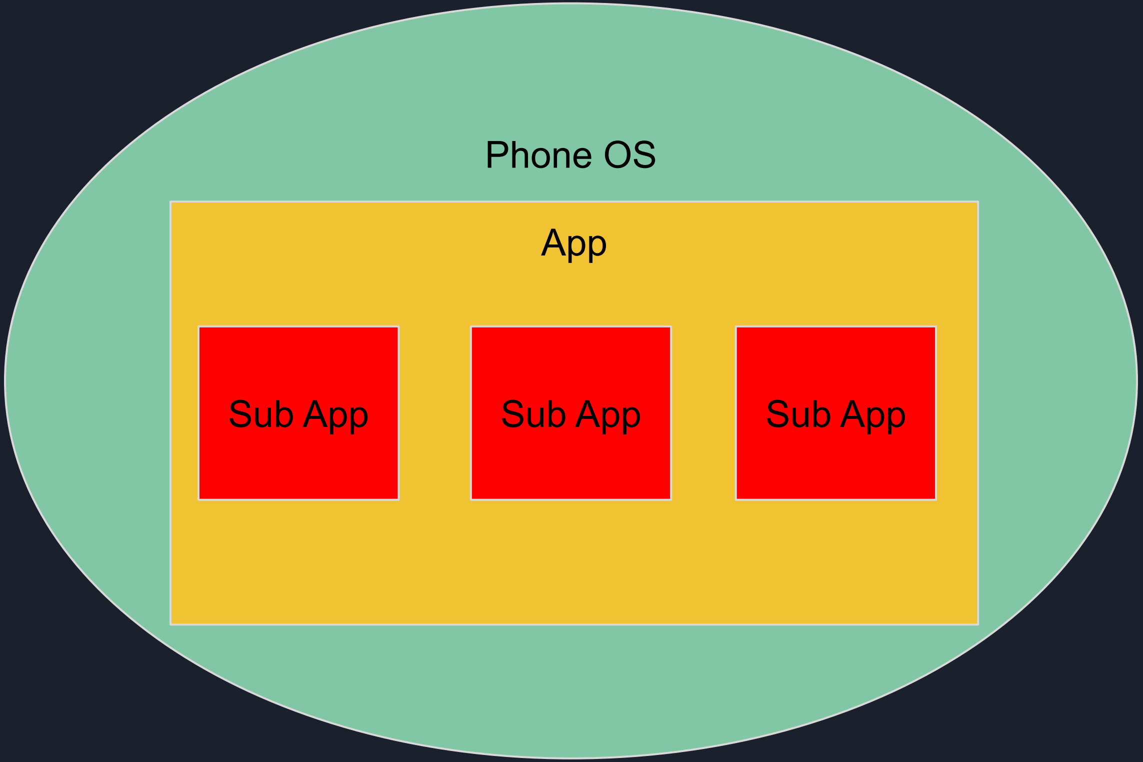
App in App Resource Management Risks

What is App in App?

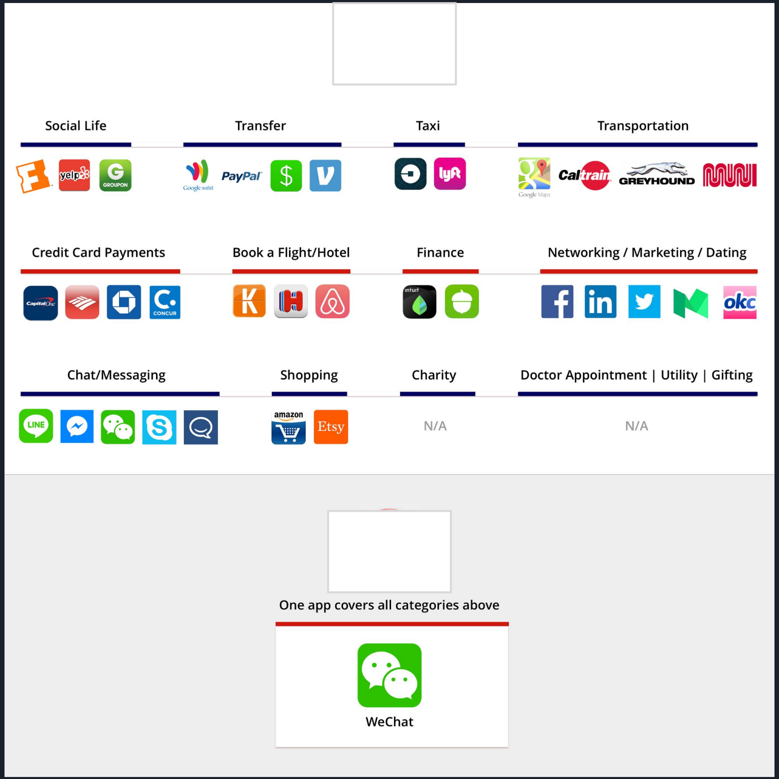


App in App Resource Management Risks

What is App in App?



What is App in App? - Super App Example



Social Life

Transfer

Taxi

Transportation

Credit Card Payments

Book a Flight/Hotel

Finance

Networking / Marketing / Dating

Chat/Messaging

Shopping

Charity

N/A

Doctor Appointment | Utility | Gifting

N/A

One app covers all categories above

WeChat

What is App in App? - Super App Example

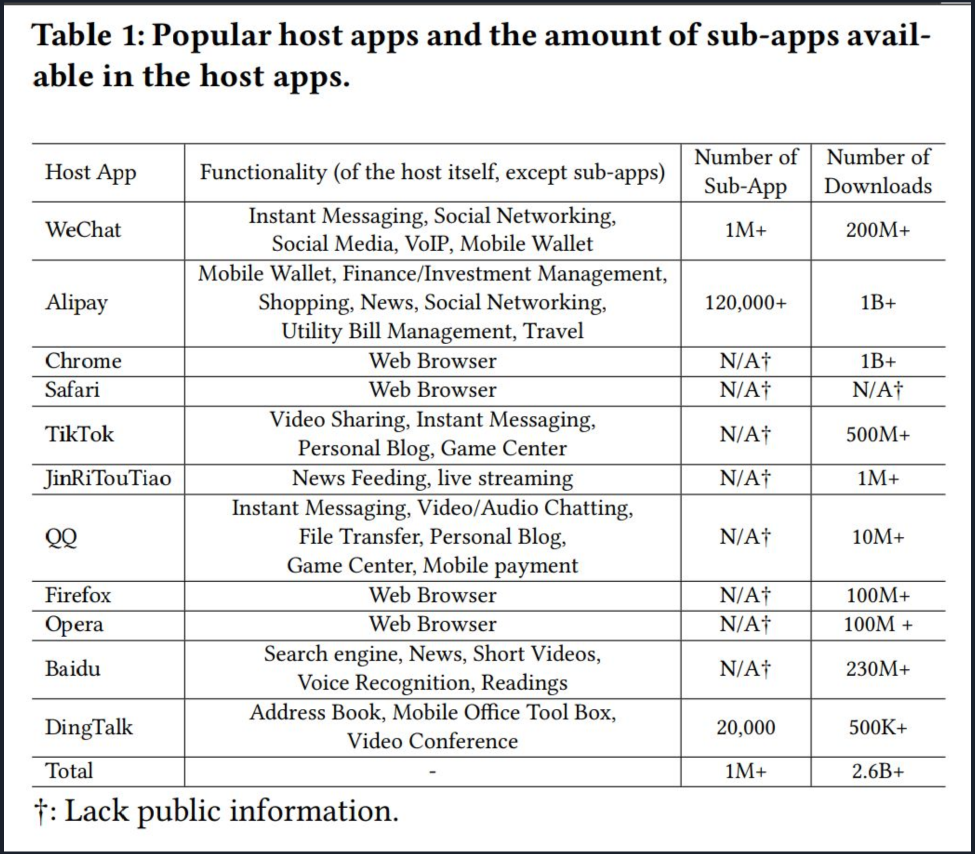
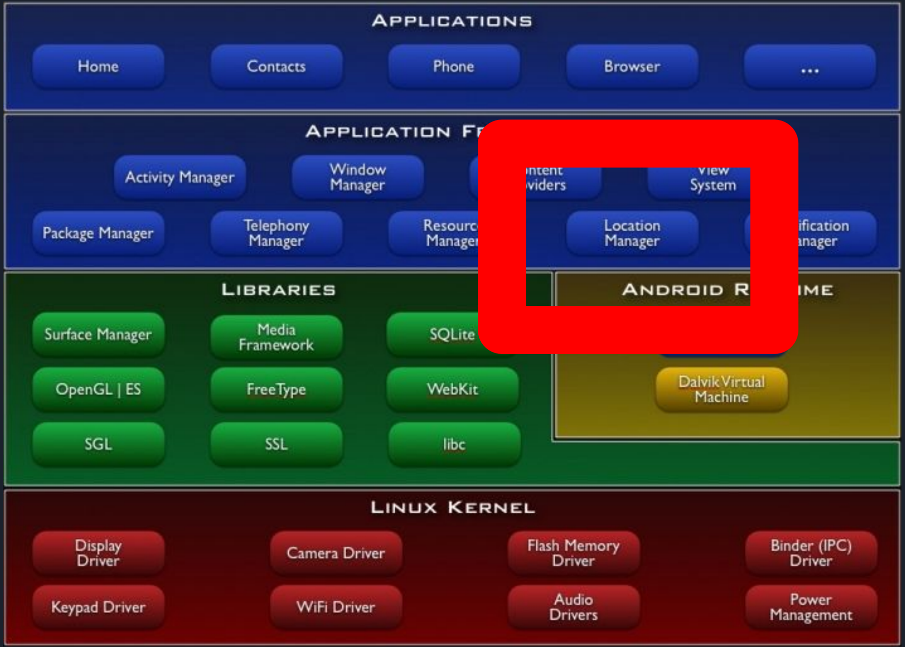


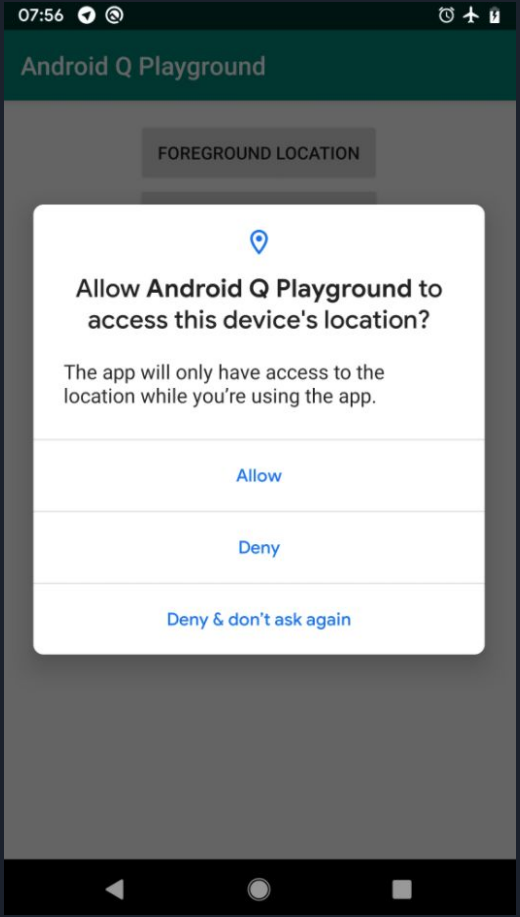
Table 1: Popular host apps and the amount of sub-apps available in the host apps.

Host App	Functionality (of the host itself, except sub-apps)	Number of Sub-App	Number of Downloads
WeChat	Instant Messaging, Social Networking, Social Media, VoIP, Mobile Wallet	1M+	200M+
Alipay	Mobile Wallet, Finance/Investment Management, Shopping, News, Social Networking, Utility Bill Management, Travel	120,000+	1B+
Chrome	Web Browser	N/A†	1B+
Safari	Web Browser	N/A†	N/A†
TikTok	Video Sharing, Instant Messaging, Personal Blog, Game Center	N/A†	500M+
JinRiTouTiao	News Feeding, live streaming	N/A†	1M+
QQ	Instant Messaging, Video/Audio Chatting, File Transfer, Personal Blog, Game Center, Mobile payment	N/A†	10M+
Firefox	Web Browser	N/A†	100M+
Opera	Web Browser	N/A†	100M +
Baidu	Search engine, News, Short Videos, Voice Recognition, Readings	N/A†	230M+
DingTalk	Address Book, Mobile Office Tool Box, Video Conference	20,000	500K+
Total	-	1M+	2.6B+

†: Lack public information.

Android Typical Architecture





Allow Android Q Playground to access this device's location?

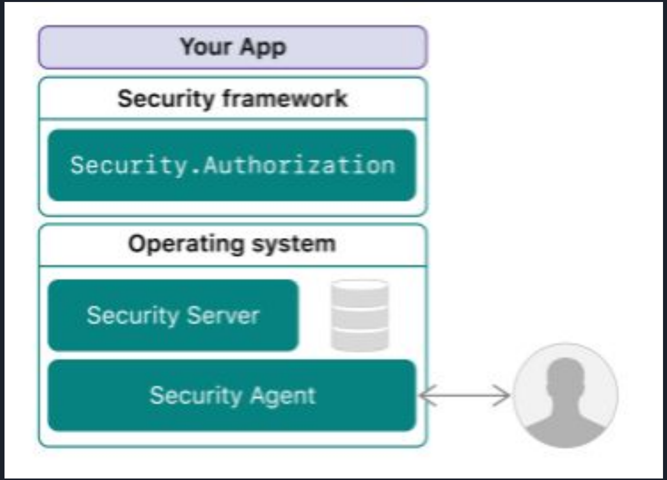
The app will only have access to the location while you're using the app.

Allow

Deny

Deny & don't ask again

IOS Typical Architecture



Your App

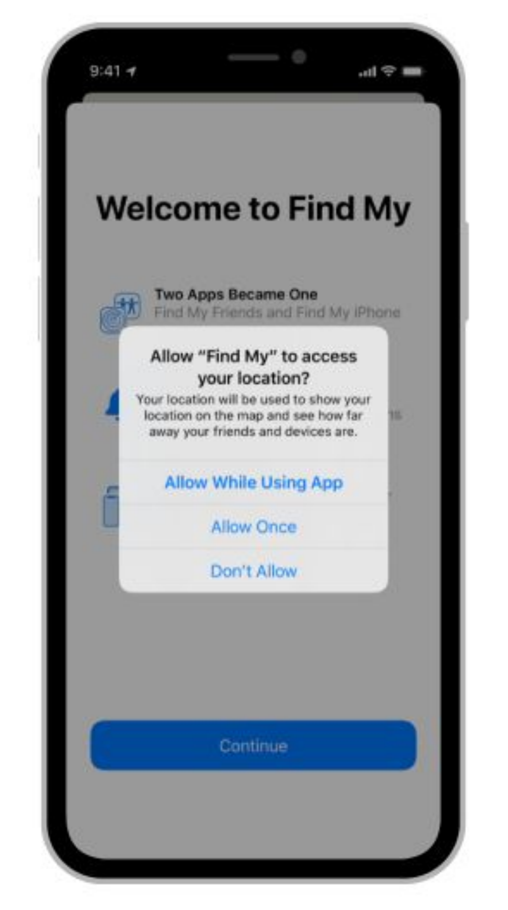
Security framework

Security.Authorization

Operating system

Security Server

Security Agent



9:41

Welcome to Find My

Two Apps Became One

Find My Friends and Find My iPhone

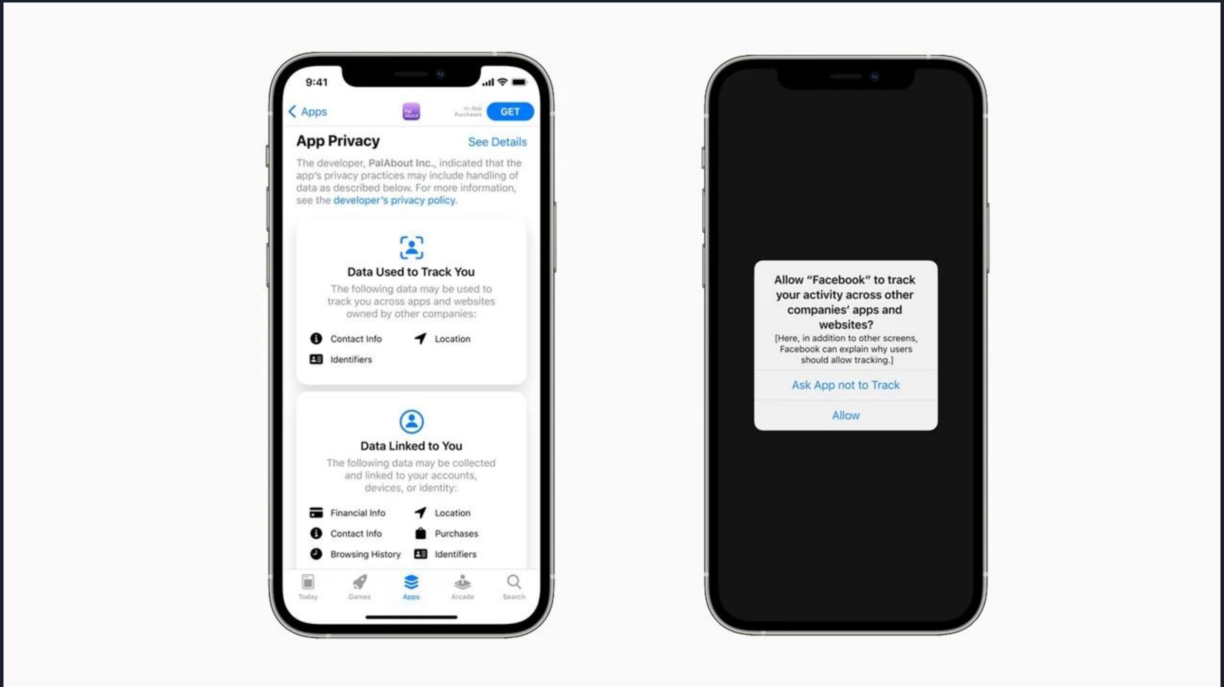
Allow “Find My” to access your location?

Your location will be used to show your location on the map and see how far away your friends and devices are.

Motivation - Protect Malicious Actors

Spyware, Ransomware, Advertisements, Etc, etc

Motivation - Protect Malicious Actors



App Privacy See Details

The developer, **PalAbout Inc.**, indicated that the app's privacy practices may include handling of data as described below. For more information, see the developer's privacy policy.

Data Used to Track You

The following data may be used to track you across apps and websites owned by other companies:

- Contact Info
- Location
- Identifiers

Data Linked to You

The following data may be collected and linked to your accounts, devices, or identity:

- Financial Info
- Location
- Contact Info
- Purchases
- Browsing History
- Identifiers

Allow "Facebook" to track your activity across other companies' apps and websites?

[Here, in addition to other screens, Facebook can explain why users should allow tracking.]

Phone data is Valuable!

APINA Typical Architecture

OS Permissions middleman!

Bypasses fine grain control for convenience

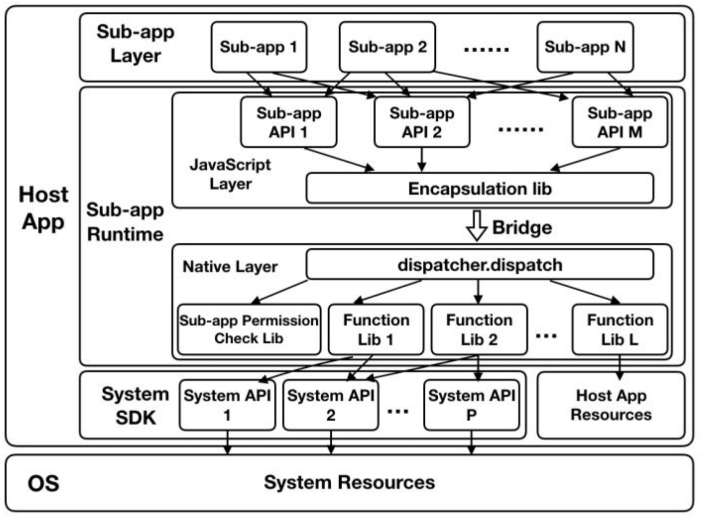
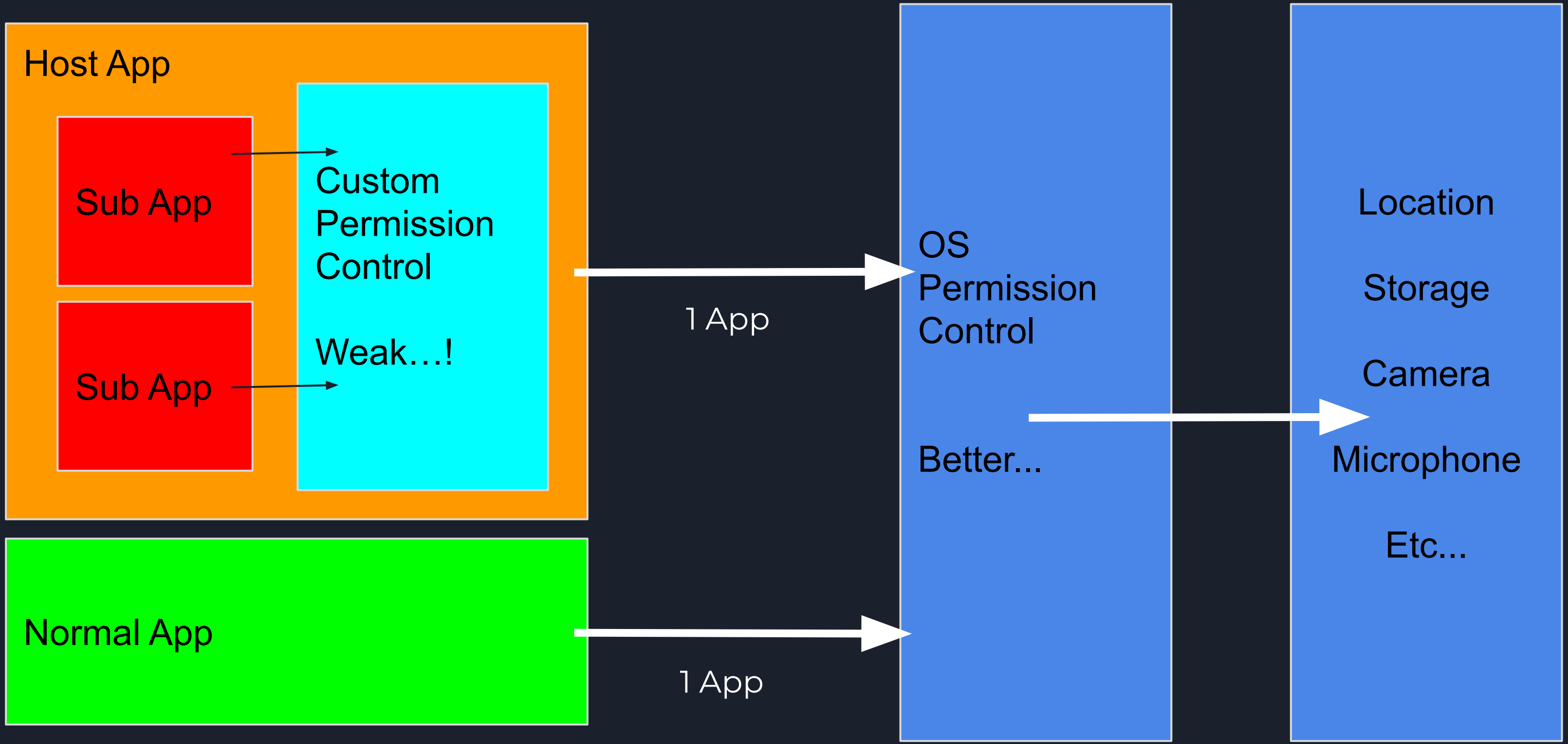


Figure 1: A typical app-in-app architecture

APINA Typical Architecture



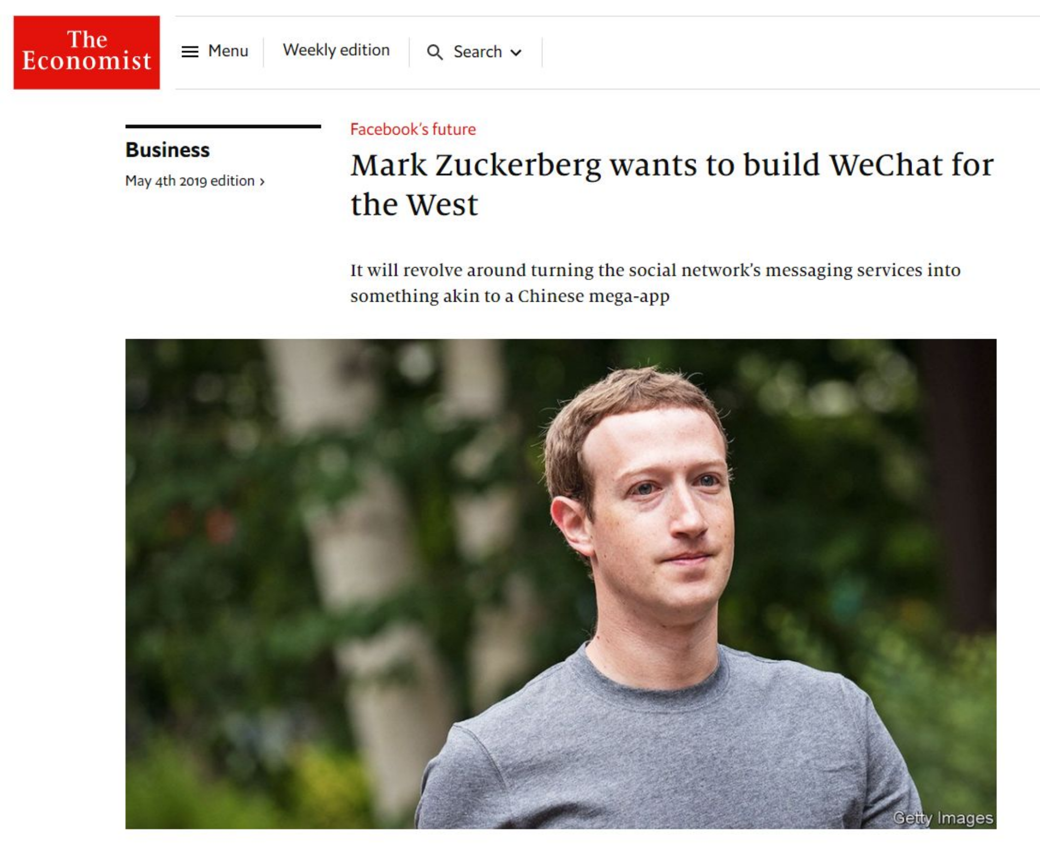
APINA Typical Architecture

Bypasses App store Vetting

Different Quality of Security

Is it relevant? - Yes!

facebook



Business

May 4th 2019 edition ›

Facebook's future

Mark Zuckerberg wants to build WeChat for the West

It will revolve around turning the social network's messaging services into something akin to a Chinese mega-app

Getty Images

Is it relevant? - Yes!

People want to protect their phones.

Phones are a data haven.

Location. Camera. Microphone. Photos, Data, Documents

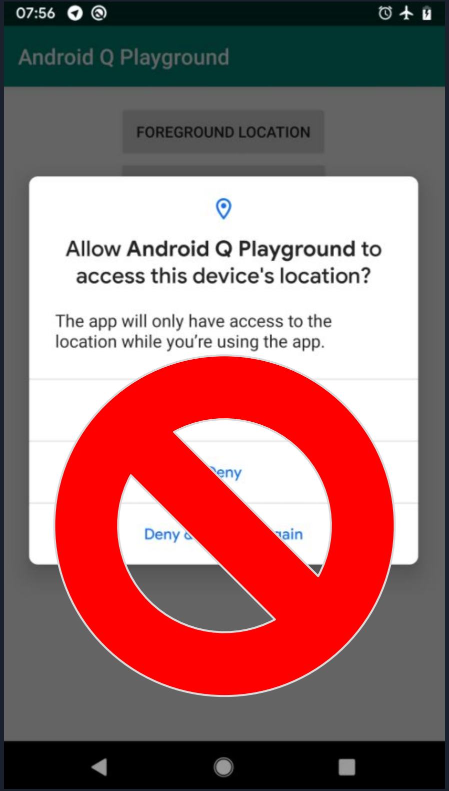
Impact #1 - Permission Exposure

Wechat v6.7.3 Location Leak!

wx.getWifiList

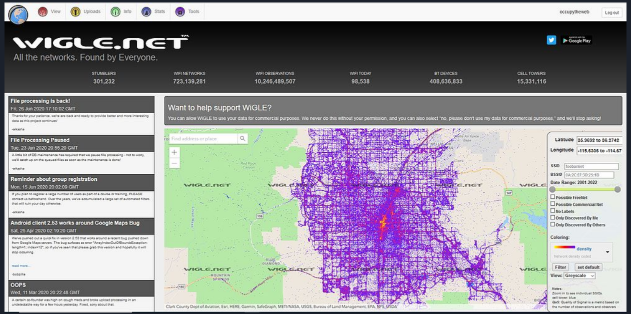
Android and iOS

Exposed sub-app API to perform Wi-Fi scan



Allow Android Q Playground to access this device's location?

The app will only have access to the location while you're using the app.



All the networks. Found by Everyone.

STUMBLERS	WIFI NETWORKS	WIFI OBSERVATIONS	WIFI TODAY	BT DEVICES	CELL TOWERS
301,232	723,139,281	10,246,489,507	98,538	408,636,833	15,331,116

File processing is back!
Fri, 26 Jun 2020 17:10:02 GMT

Thanks for your patience, we're are back and ready to provide better and more interesting data as this project continues!

-arkasha

File Processing Paused
Tue, 23 Jun 2020 20:55:20 GMT

A little bit of DB maintenance has required that we pause file processing - not to worry, we'll catch up on the queued files as soon as the maintenance is done!

-arkasha

Reminder about group registration
Mon, 15 Jun 2020 20:02:09 GMT

If you plan to register a large number of users as part of a course or training, PLEASE contact us beforehand. Over the years, we've accumulated a large set of automated filters that will ruin your day otherwise.

-arkasha

Android client 2.53 works around Google Maps Bug
Sat, 25 Apr 2020 02:19:20 GMT

We've pushed out a quick fix in version 2.53 that works around a recent bug pushed down from Google Maps servers. The bug surfaces as error "ArrayIndexOutOfBoundsException: length=1; index=12", so if you've seen that please grab this version and hopefully it will stop occurring.

read more...

-bobzilla

OOPS
Wed, 11 Mar 2020 20:22:48 GMT

A certain co-founder was high on cough meds and broke upload processing in an undetectable way for a few hours yesterday. Fixed, sorry about that.

Want to help support WiGLE?

You can allow WiGLE to use your data for commercial purposes. We never do this without your permission, and you can also select "no, please don't use my data for commercial purposes," and we'll stop asking!

Latitude: 35.9692 to 36.2742
Longitude: -115.6306 to -114.67
SSID: foobarnet
BSSID: 0A:2C:EF:3D:25:1B
Date Range: 2001-2022

□ Possible FreeNet
□ Possible Commercial Net
□ No Labels
□ Only Discovered By Me
□ Only Discovered By Others

Coloring: density
Network density coded

Filter | set default

View: Greyscale

Notes:
Zoom in to see individual SSIDs
cell tower: blue
QoS: Quality of Signal is a metric based on the number of observations and observers

Clark County Dept of Aviation, Esri, HERE, Garmin, SafeGraph, METI/NASA, USGS, Bureau of Land Management, EPA, NPS, USDA

WIFI LIST == Location

Bug Bounty Award!

- Wechat and Alipay

Impact #1 - Permission Exposure risk

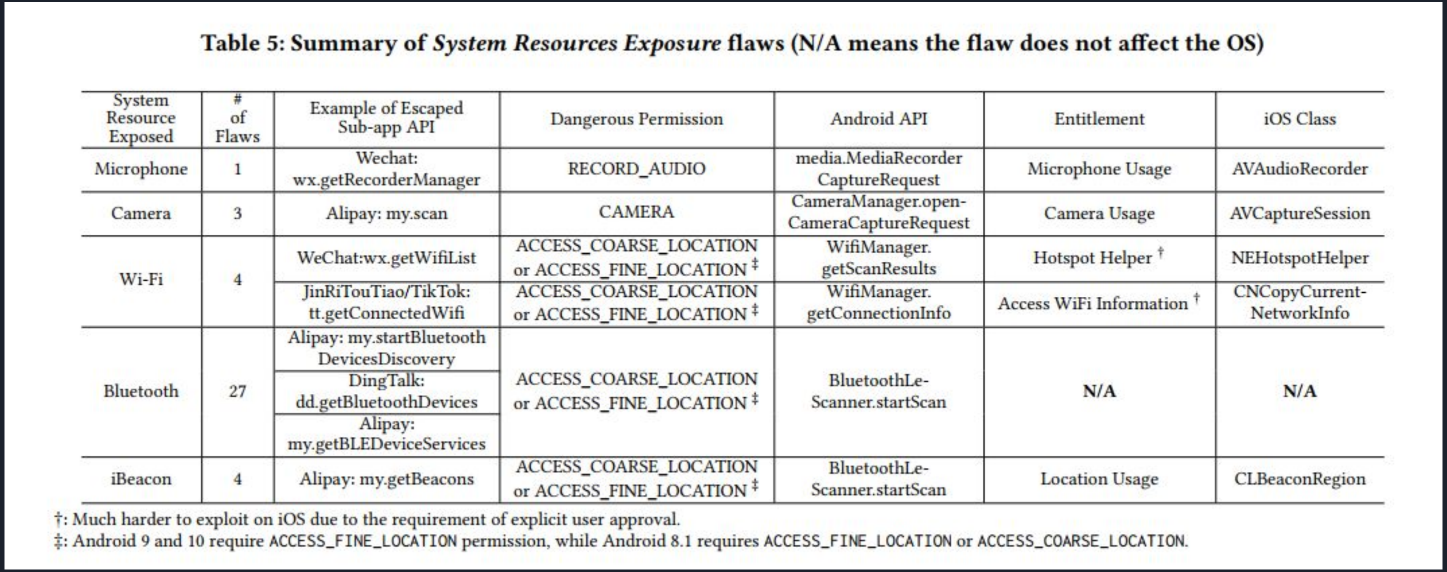


Table 5: Summary of *System Resources Exposure* flaws (N/A means the flaw does not affect the OS)

System Resource Exposed	# of Flaws	Example of Escaped Sub-app API	Dangerous Permission	Android API	Entitlement	iOS Class
Microphone	1	Wechat: wx.getRecorderManager	RECORD_AUDIO	media.MediaRecorder CaptureRequest	Microphone Usage	AVAudioRecorder
Camera	3	Alipay: my.scan	CAMERA	CameraManager.open-CameraCaptureRequest	Camera Usage	AVCaptureSession
Wi-Fi	4	WeChat:wx.getWifiList	ACCESS_COARSE_LOCATION or ACCESS_FINE_LOCATION ‡	WifiManager. getScanResults	Hotspot Helper †	NEHotspotHelper
		JinRiTouTiao/TikTok: tt.getConnectedWifi	ACCESS_COARSE_LOCATION or ACCESS_FINE_LOCATION ‡	WifiManager. getConnectionInfo	Access WiFi Information †	CNCopyCurrent-NetworkInfo
Bluetooth	27	Alipay: my.startBluetooth DevicesDiscovery	ACCESS_COARSE_LOCATION or ACCESS_FINE_LOCATION ‡	BluetoothLe-Scanner.startScan	**N/A**	**N/A**
		DingTalk: dd.getBluetoothDevices				
		Alipay: my.getBLEDeviceServices				
iBeacon	4	Alipay: my.getBeacons	ACCESS_COARSE_LOCATION or ACCESS_FINE_LOCATION ‡	BluetoothLe-Scanner.startScan	Location Usage	CLBeaconRegion

†: Much harder to exploit on iOS due to the requirement of explicit user approval.
‡: Android 9 and 10 require `ACCESS_FINE_LOCATION` permission, while Android 8.1 requires `ACCESS_FINE_LOCATION` or `ACCESS_COARSE_LOCATION`.

Impact #1 - Permission Exposure risk

“every single appin-app system we studied is vulnerable”

“and exploitable with serious consequences”...

Impact #1 - Permission Exposure risk

“every single appin-app system we studied is vulnerable”

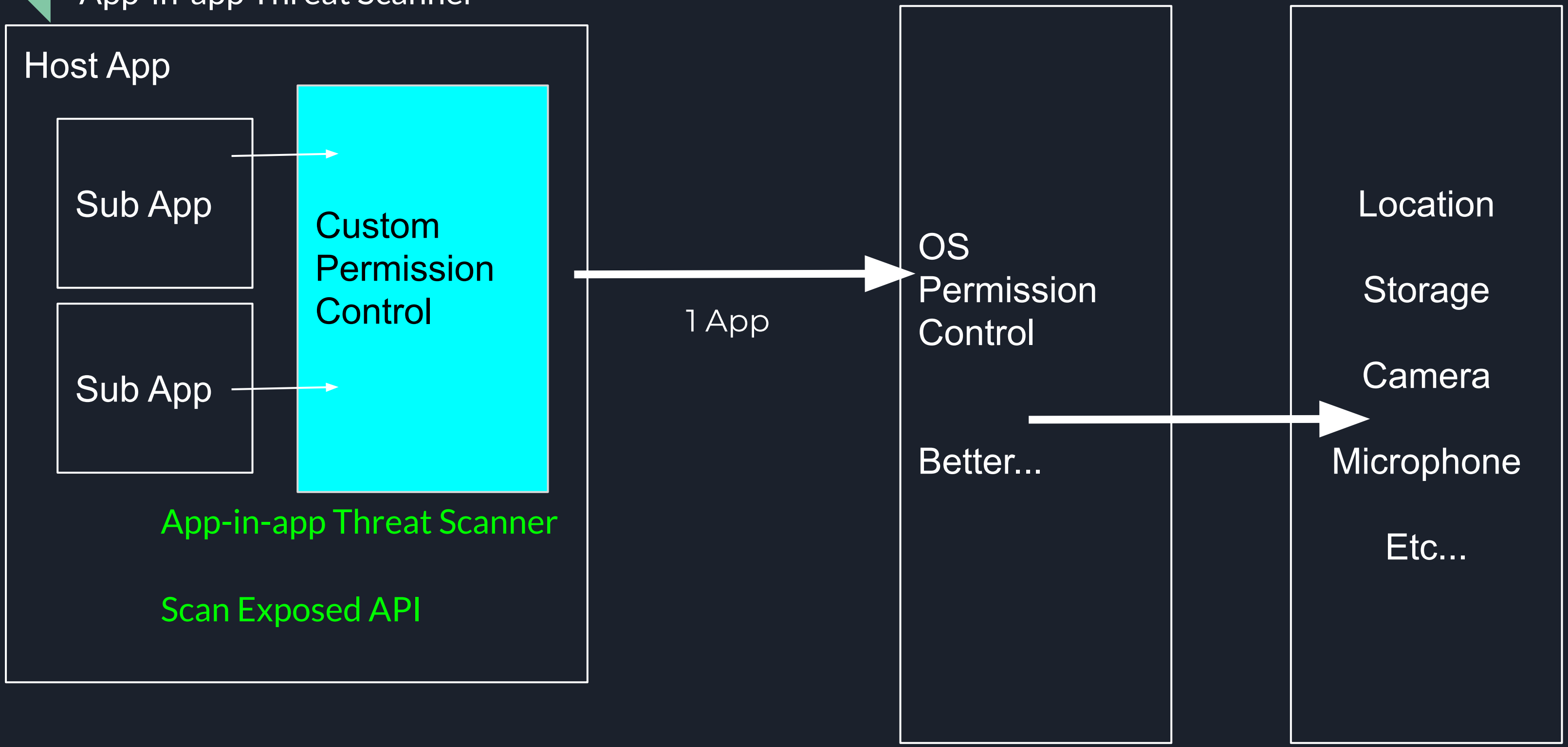
Impact #1 - Permission Exposure risk

“every single appin-app system we studied is vulnerable”

Super App = Knockoff App Store

Solution #1 - Apinat

App-in-app Threat Scanner



Host App

Sub App

Sub App

Custom Permission Control

App-in-app Threat Scanner

Scan Exposed API

1 App

OS Permission Control

Better...

Location

Storage

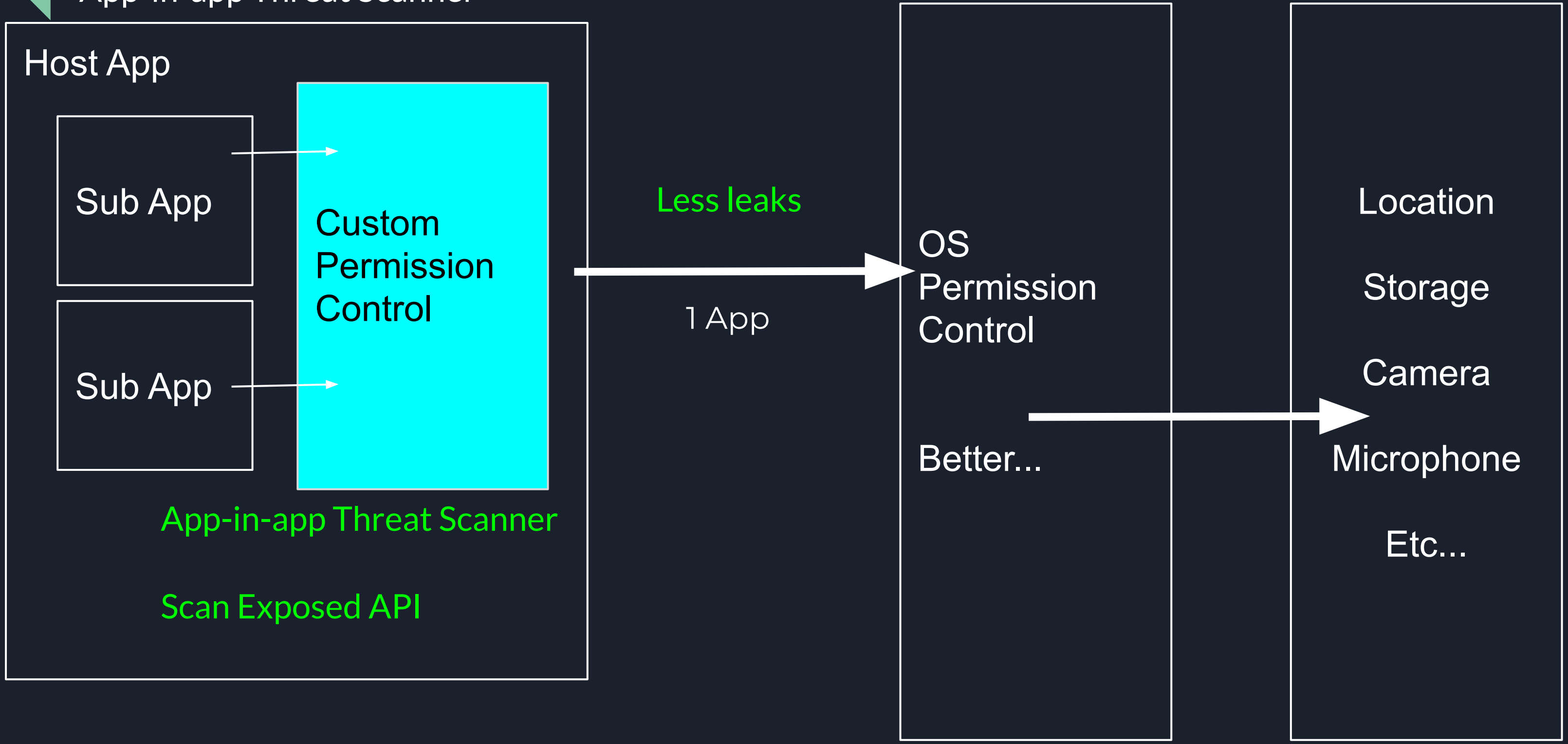
Camera

Microphone

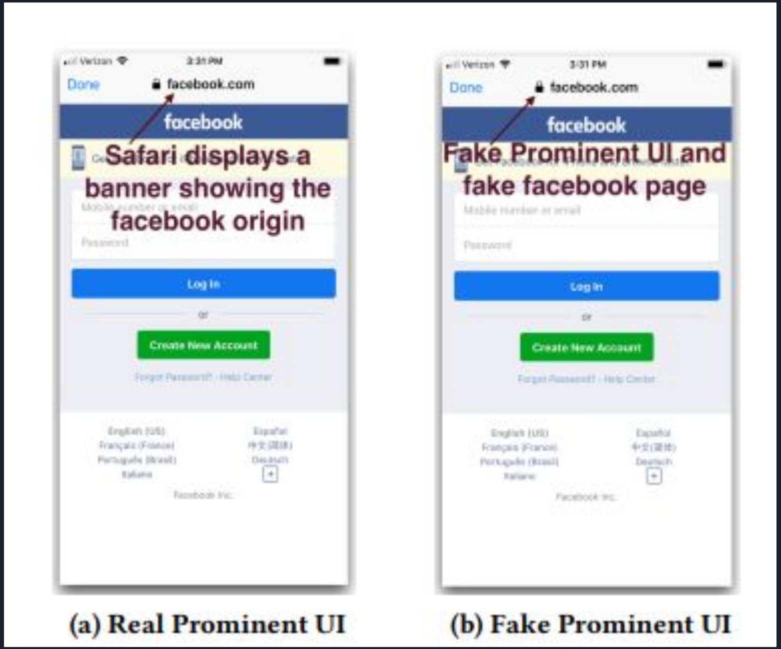
Etc...

Solution #1 - Apinat

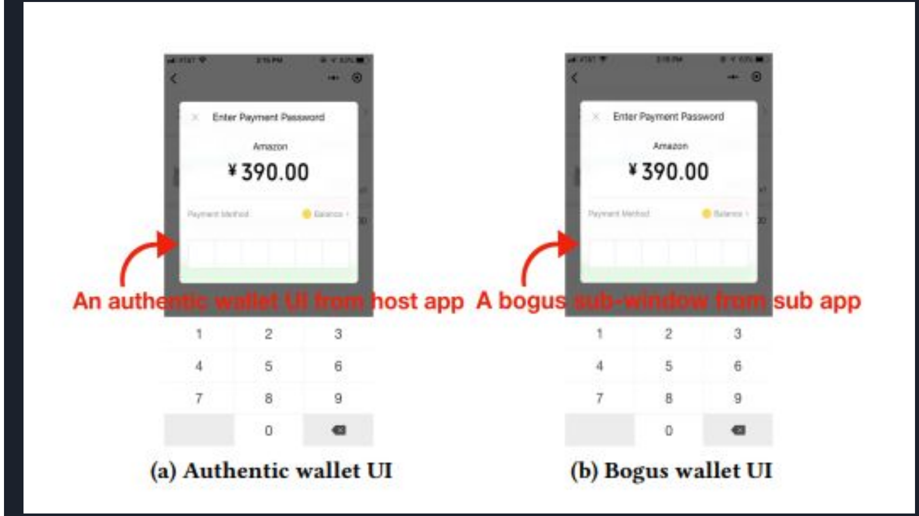
App-in-app Threat Scanner



Impact #2 - Sub window Deception


Done
facebook.com
facebook
Safari displays a banner showing the facebook origin
Log In
Create New Account
Fake Prominent UI and fake facebook page

(a) Real Prominent UI (b) Fake Prominent UI


Enter Payment Password
Amazon
¥390.00
An authentic wallet UI from host app
A bogus sub-window from sub app

(a) Authentic wallet UI (b) Bogus wallet UI

Trivial phishing attack vector

Impact #2 - Sub window Deception

Sub app UI is powerful, Full screen

Convenience vs Security Tradeoff

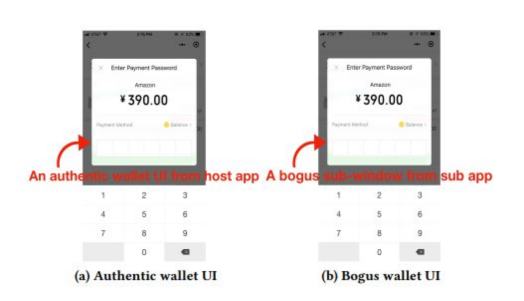
Solution #2 - Sub window Deception

Phones are more powerful now...

AI OBJECT DETECTION OF BAD WINDOWS

state-of-the-art object detection model

...battery drain...



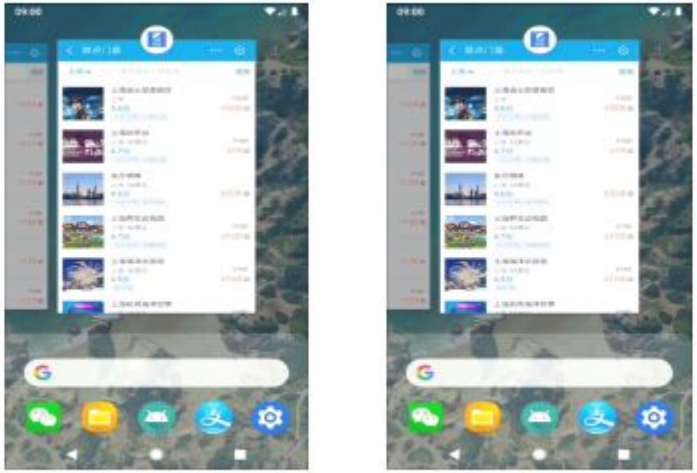
An authentic wallet UI from host app

A bogus sub-window from sub app

(a) Authentic wallet UI

(b) Bogus wallet UI

Impact #3 - Sub App Task Replacement



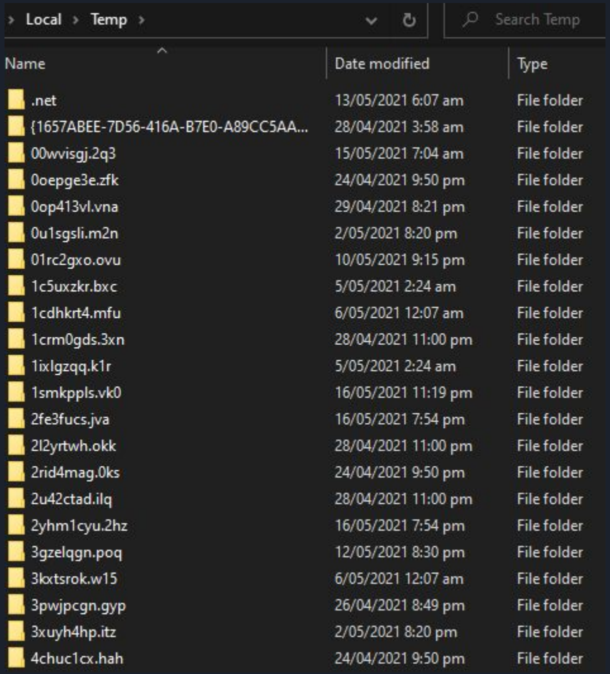
(a) Real sub-app task (b) Bogus sub-app task

Figure 5: Dedicated task for every sub-app in *Recents screen*

Requires malicious sub app to know what is open / not open

Impact #3 - Sub App Task Replacement

Snoops at temporary folder content



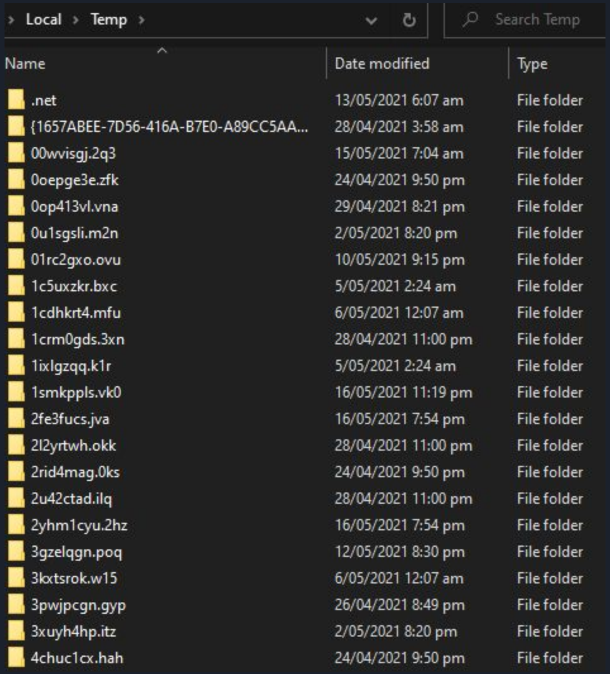
Name	Date modified	Type
.net	13/05/2021 6:07 am	File folder
{1657ABEE-7D56-416A-B7E0-A89CC5AA...	28/04/2021 3:58 am	File folder
00wvisgj.2q3	15/05/2021 7:04 am	File folder
0oepge3e.zfk	24/04/2021 9:50 pm	File folder
0op413vl.vna	29/04/2021 8:21 pm	File folder
0u1sgsli.m2n	2/05/2021 8:20 pm	File folder
01rc2gxo.ovu	10/05/2021 9:15 pm	File folder
1c5uxzkr.bxc	5/05/2021 2:24 am	File folder
1cdhkrt4.mfu	6/05/2021 12:07 am	File folder
1crm0gds.3xn	28/04/2021 11:00 pm	File folder
1ixlgzqq.k1r	5/05/2021 2:24 am	File folder
1smkppls.vk0	16/05/2021 11:19 pm	File folder
2fe3fucs.jva	16/05/2021 7:54 pm	File folder
2l2yrtwh.okk	28/04/2021 11:00 pm	File folder
2rid4mag.0ks	24/04/2021 9:50 pm	File folder
2u42ctad.ilq	28/04/2021 11:00 pm	File folder
2yhm1cyu.2hz	16/05/2021 7:54 pm	File folder
3gzelqgn.poq	12/05/2021 8:30 pm	File folder
3kxtsrok.w15	6/05/2021 12:07 am	File folder
3pwjpcgn.gyp	26/04/2021 8:49 pm	File folder
3xuyh4hp.itz	2/05/2021 8:20 pm	File folder
4chuc1cx.hah	24/04/2021 9:50 pm	File folder

Pseudo Task Manager

Requires sub app to know what is open / not open

Impact #3 - Sub App Task Replacement

When app Closes….
(Task limit)
(Auto battery manager)



Name	Date modified	Type
.net	13/05/2021 6:07 am	File folder
{1657ABEE-7D56-416A-B7E0-A89CC5AA...	28/04/2021 3:58 am	File folder
00wvisgj.2q3	15/05/2021 7:04 am	File folder
0oepge3e.zfk	24/04/2021 9:50 pm	File folder
0op413vl.vna	29/04/2021 8:21 pm	File folder
0u1sgsli.m2n	2/05/2021 8:20 pm	File folder
01rc2gxo.ovu	10/05/2021 9:15 pm	File folder
1c5uxzkr.bxc	5/05/2021 2:24 am	File folder
1cdhkrt4.mfu	6/05/2021 12:07 am	File folder
1crm0gds.3xn	28/04/2021 11:00 pm	File folder
1ixlgzqq.k1r	5/05/2021 2:24 am	File folder
1smkppls.vk0	16/05/2021 11:19 pm	File folder
2fe3fucs.jva	16/05/2021 7:54 pm	File folder
2l2yrtwh.okk	28/04/2021 11:00 pm	File folder
2rid4mag.0ks	24/04/2021 9:50 pm	File folder
2u42ctad.ilq	28/04/2021 11:00 pm	File folder
2yhm1cyu.2hz	16/05/2021 7:54 pm	File folder
3gzelqgn.poq	12/05/2021 8:30 pm	File folder
3kxtsrok.w15	6/05/2021 12:07 am	File folder
3pwjpcgn.gyp	26/04/2021 8:49 pm	File folder
3xuyh4hp.itz	2/05/2021 8:20 pm	File folder
4chuc1cx.hah	24/04/2021 9:50 pm	File folder

Replace!!!

Requires sub app to know what is open / not open

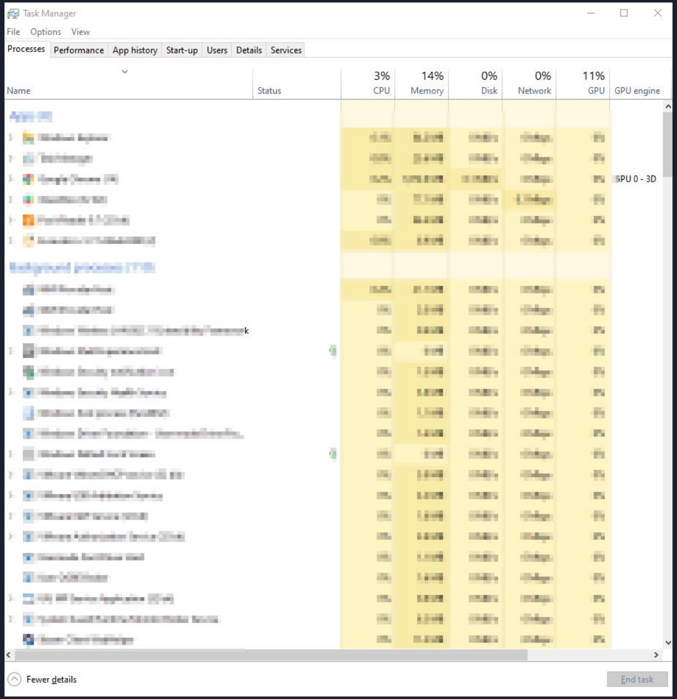
Impact #3 - Sub App Task Replacement

“Fingerprinting” to allow targeted attack

Solution #3 - Sub App Task Replacement

Hide task information == No attack timing

Hide via:
Sub App Data -> Protected phone storage



Conclusion

- Host app “middleman” permission manager

- Impact #1 - Expose of Protected API

- Impact #2 - Phishing Host App windows

- Impact #3 - Replacement of sibling sub apps

Conclusion - Future work

- Strengthen the quality of permission management
-
- Perhaps a fundamental architecture change e.g. App Virtual machine?

SAMSUNG Knox

Thank you!

App in app in app in app of an app in app that exposes an app in app of app permission - Future work