July week4

Progress

2020019252 김나현

Reading Paper

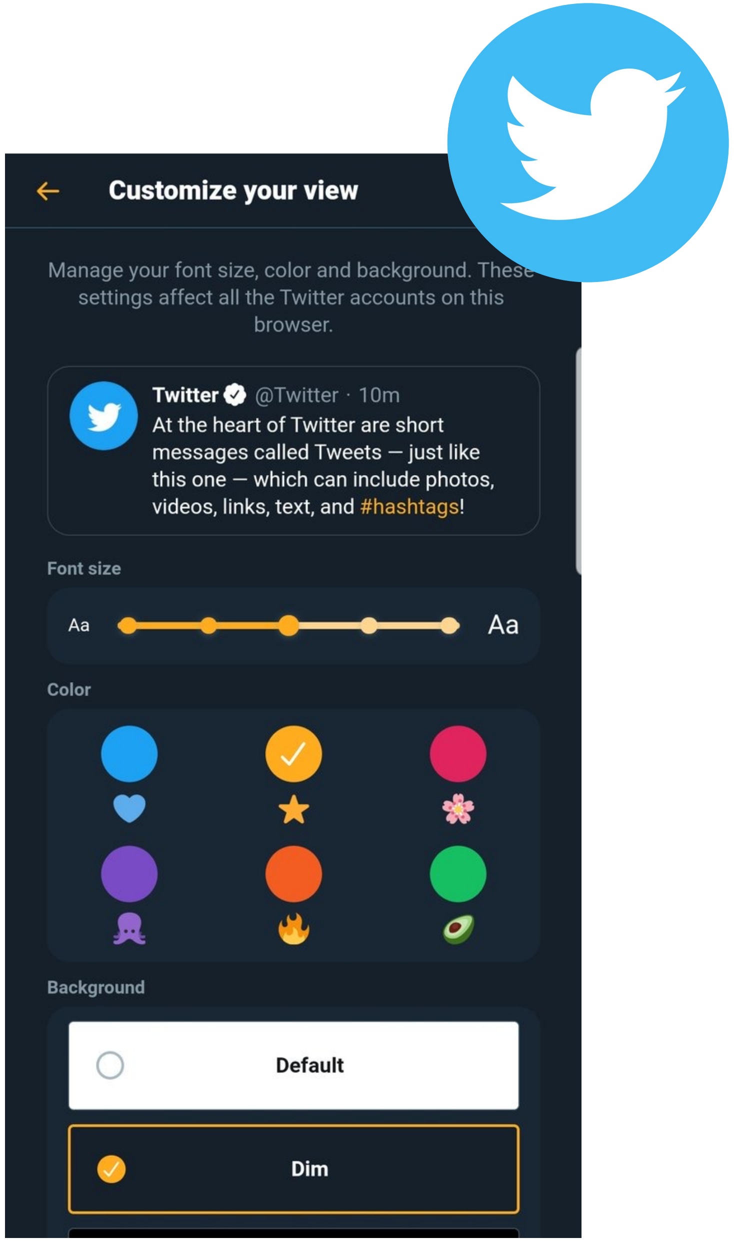
App in the Middle:
Demystify **Application Virtualization** in Android
and **its Security Threats**

Proceedings of the ACM on Measurement and Analysis of Computing Systems, 2019

Demand of customizing

Android users tend to…

Multiple Account
Whatsapp
Whatsapp+



Customize your view

Manage your font size, color and background. These settings affect all the Twitter accounts on this browser.

Twitter @Twitter · 10m
At the heart of Twitter are short messages called Tweets — just like this one — which can include photos, videos, links, text, and #hashtags!

Font size

Aa ——●—— Aa

Color

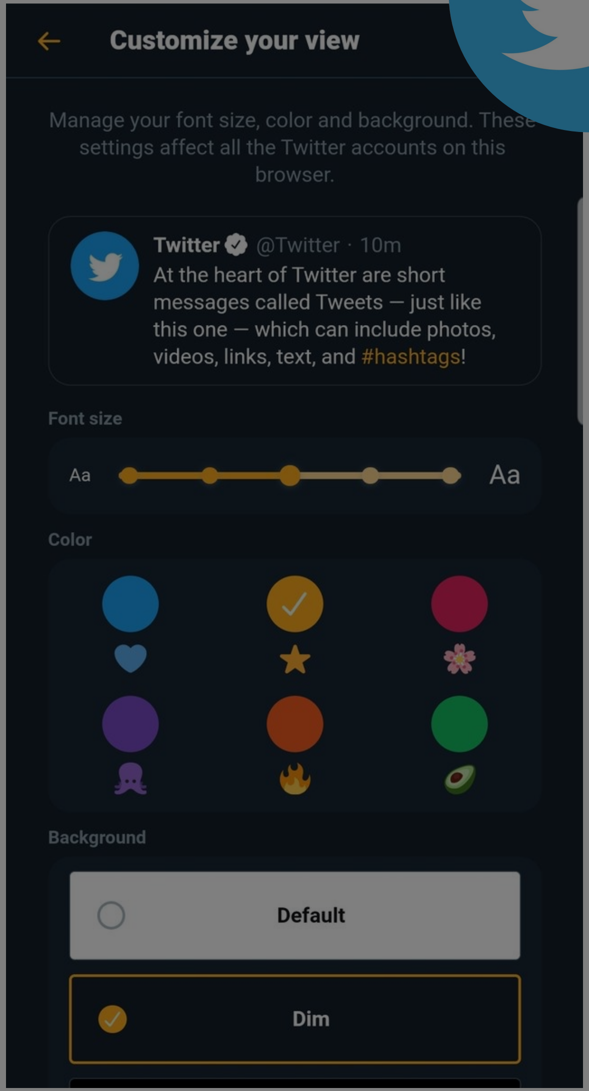
Background

○ Default

● Dim

Demand of customizing

Android user



Customize your view

Manage your font size, color and background. These settings affect all the Twitter accounts on this browser.

Twitter @Twitter · 10m
At the heart of Twitter are short messages called Tweets — just like this one — which can include photos, videos, links, text, and #hashtags!

Font size

Aa Aa

Color

Background

○ Default

● Dim

Solution:

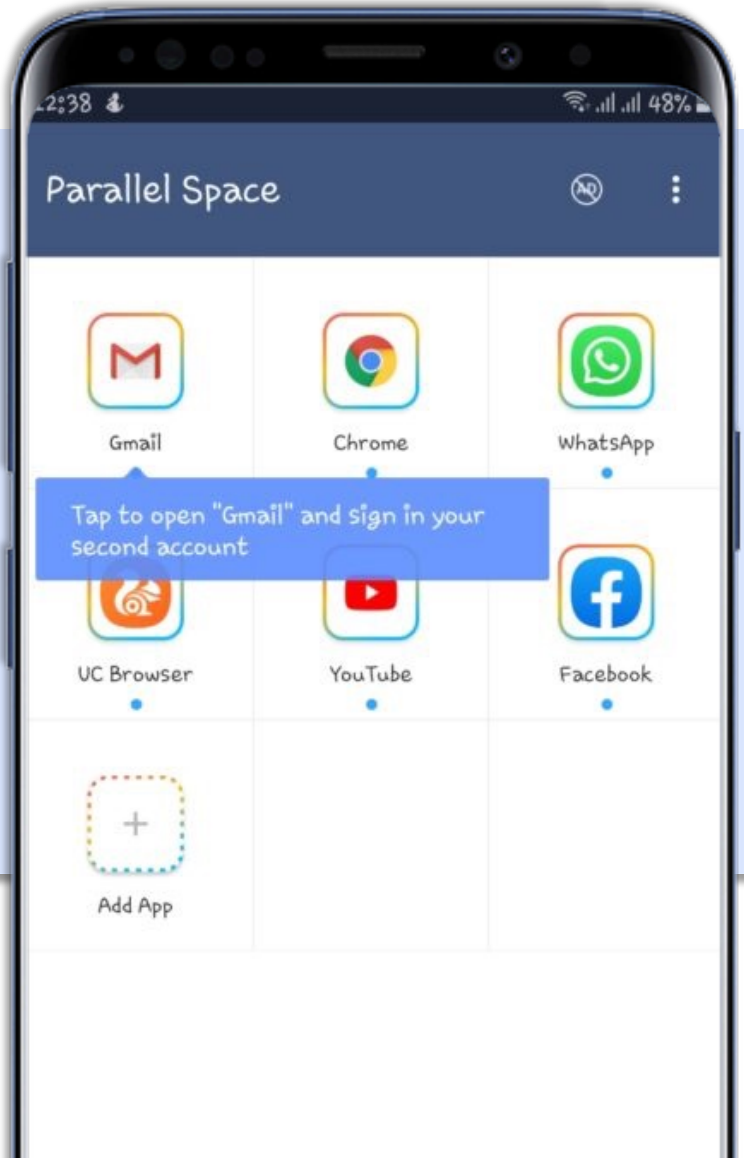
App virtualization !

Do you know parallel space?

Parallel Space

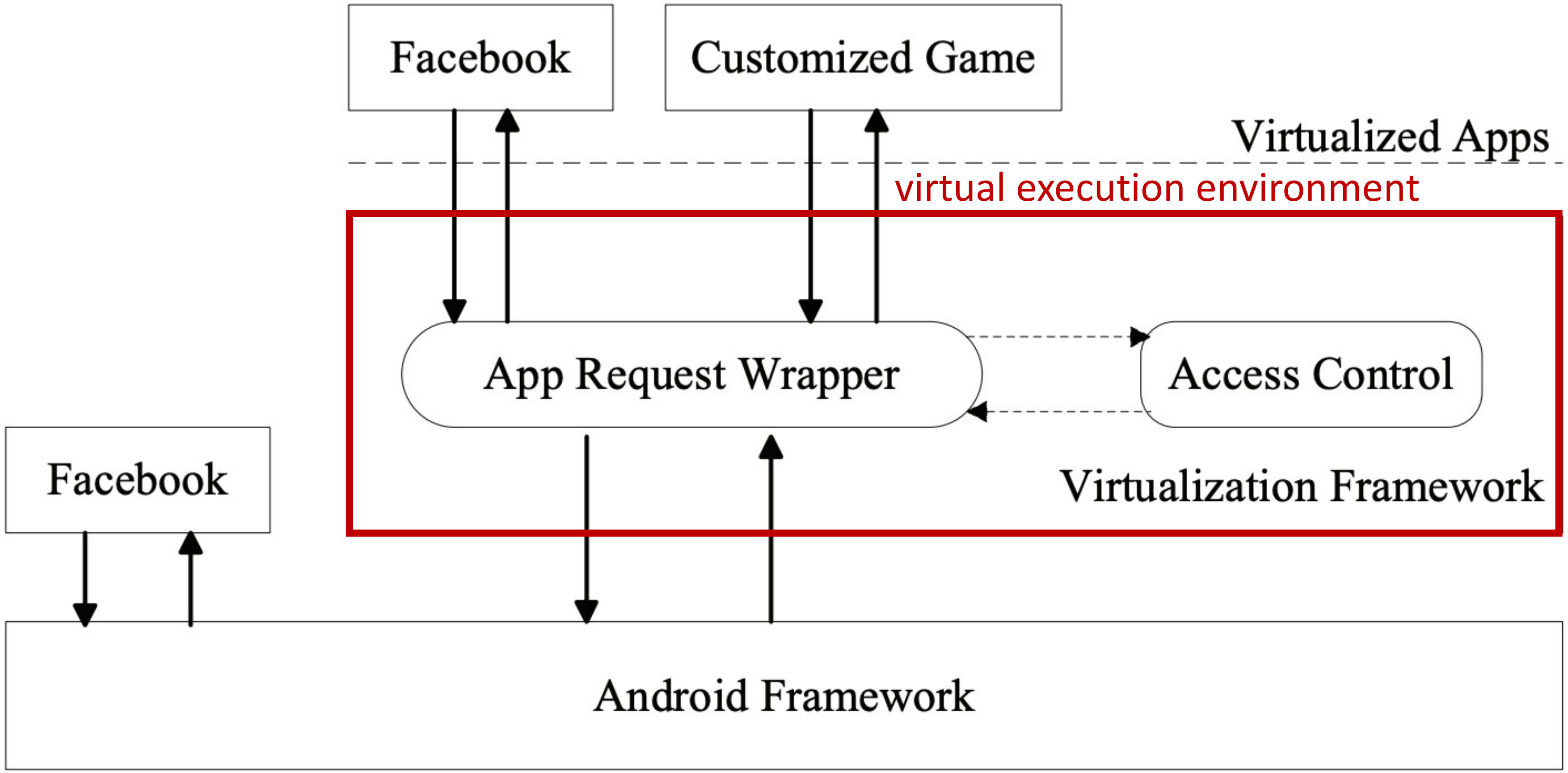
Multi accounts, online simultaneously

- Sign in two different social accounts on just one device
- Play two game accounts, switch with just one tap
- Install apps only in Parallel Space through Incognito Installation

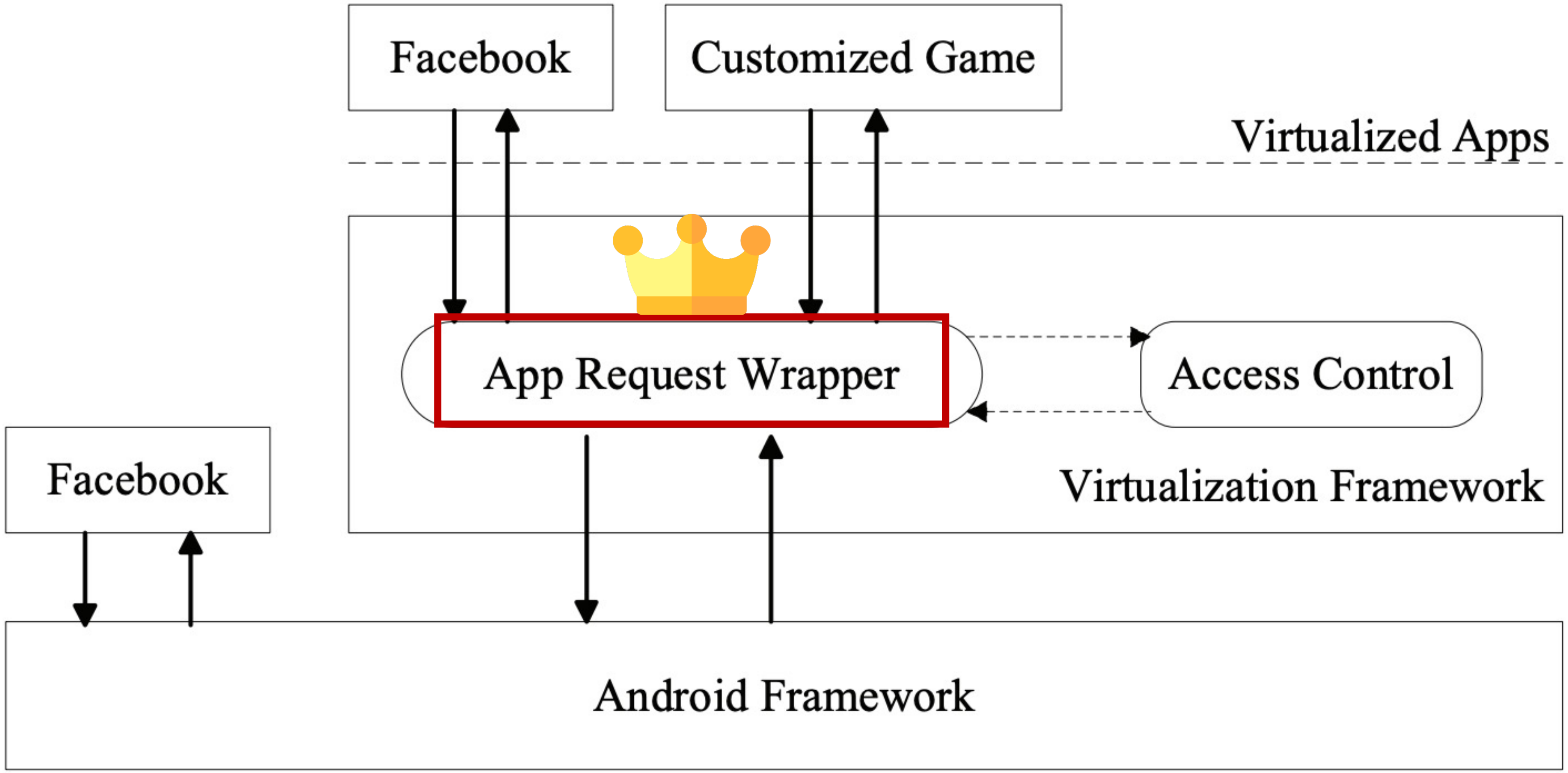


Tap to open "Gmail" and sign in your second account

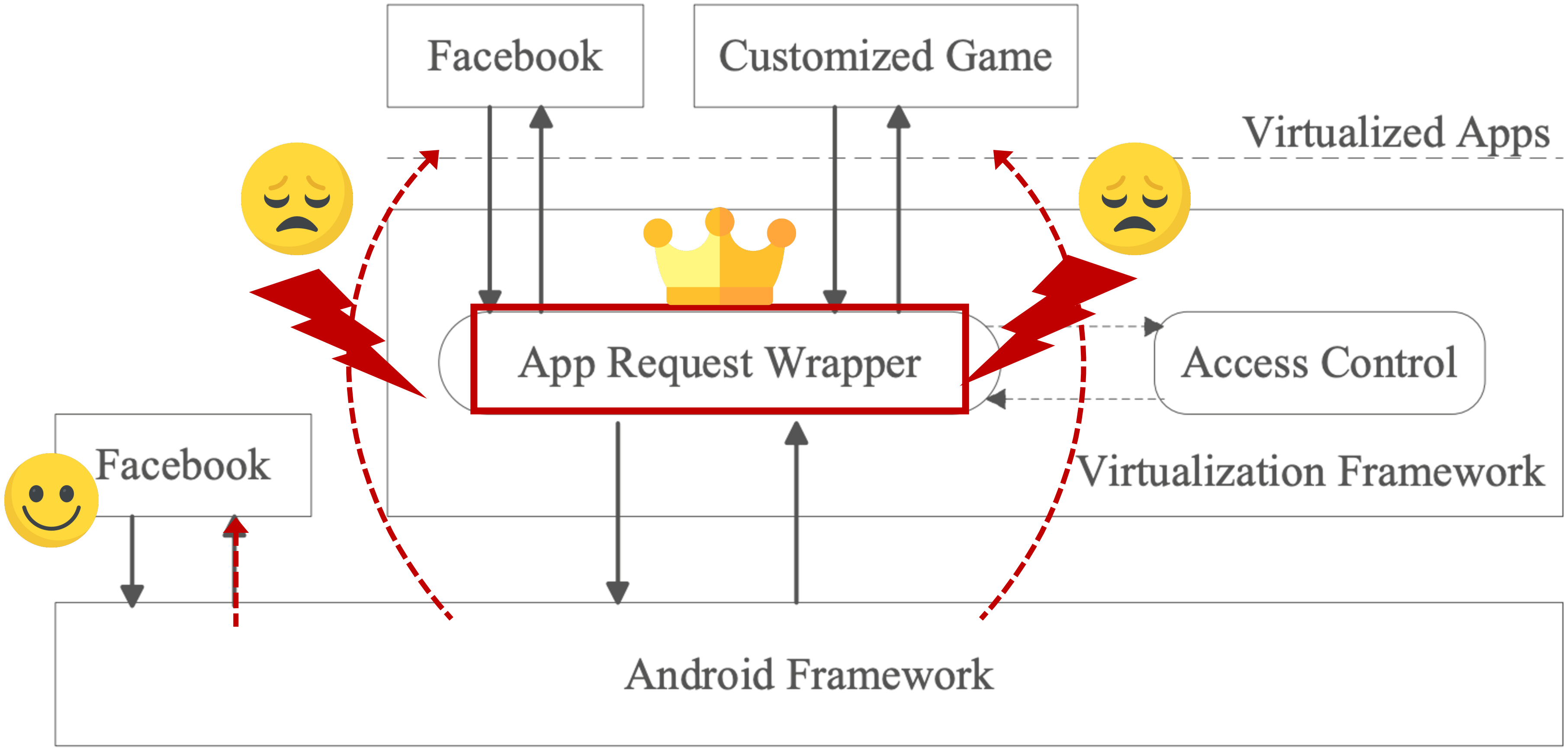
App virtualization framework



App virtualization framework

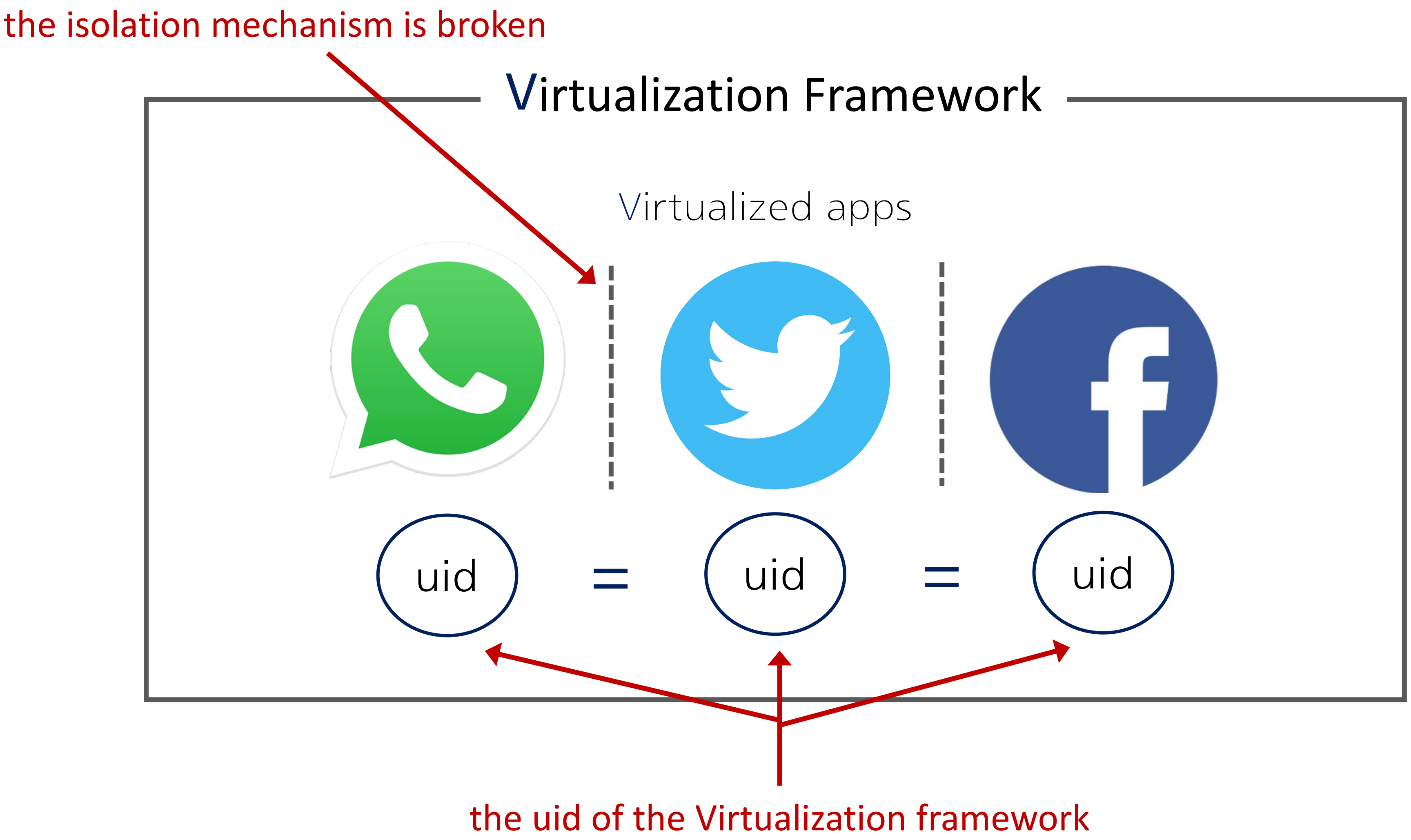


Invalid Android access control policies



No direct communication

Invalid Android access control policies



the isolation mechanism is broken

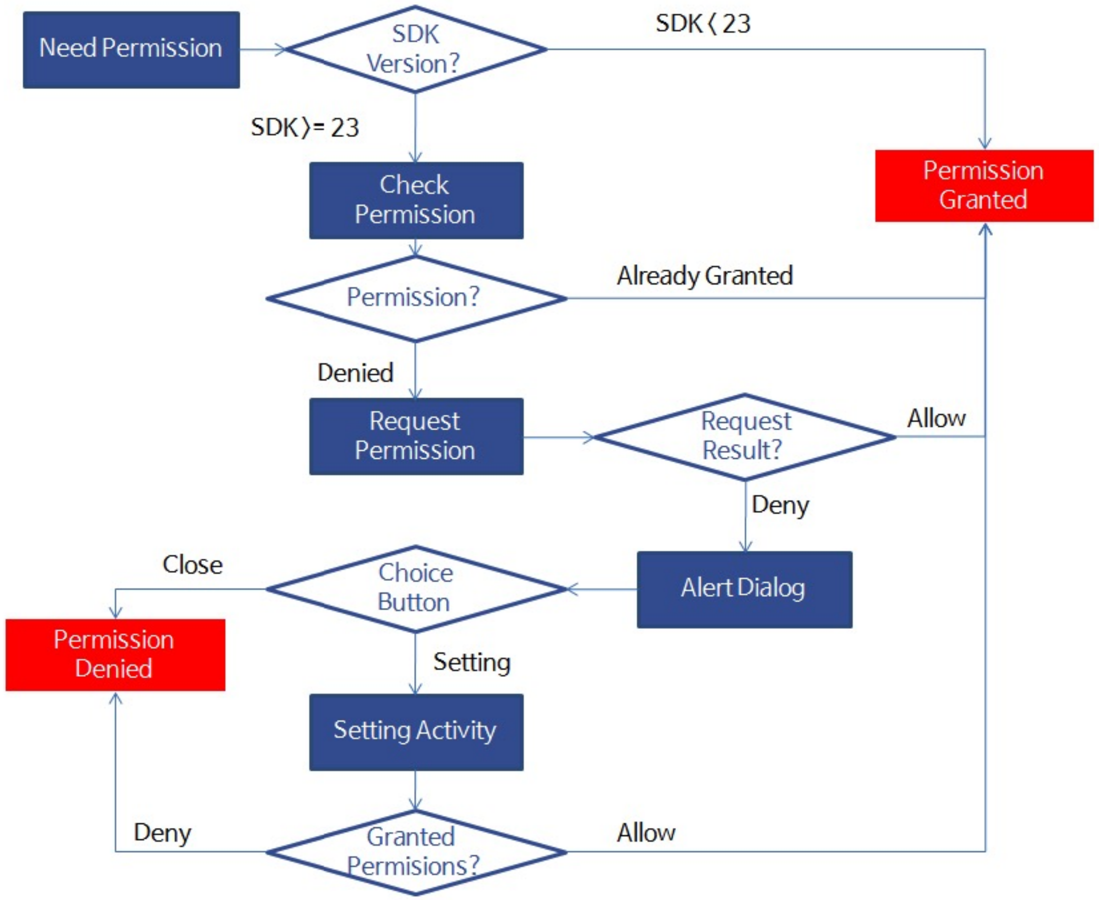
Virtualization Framework

Virtualized apps

the uid of the Virtualization framework

Android access control policies

1. Permissions



Need Permission

SDK Version?

SDK < 23

SDK >= 23

Check Permission

Permission Granted

Permission?

Already Granted

Denied

Request Permission

Request Result?

Allow

Deny

Alert Dialog

Close

Choice Button

Permission Denied

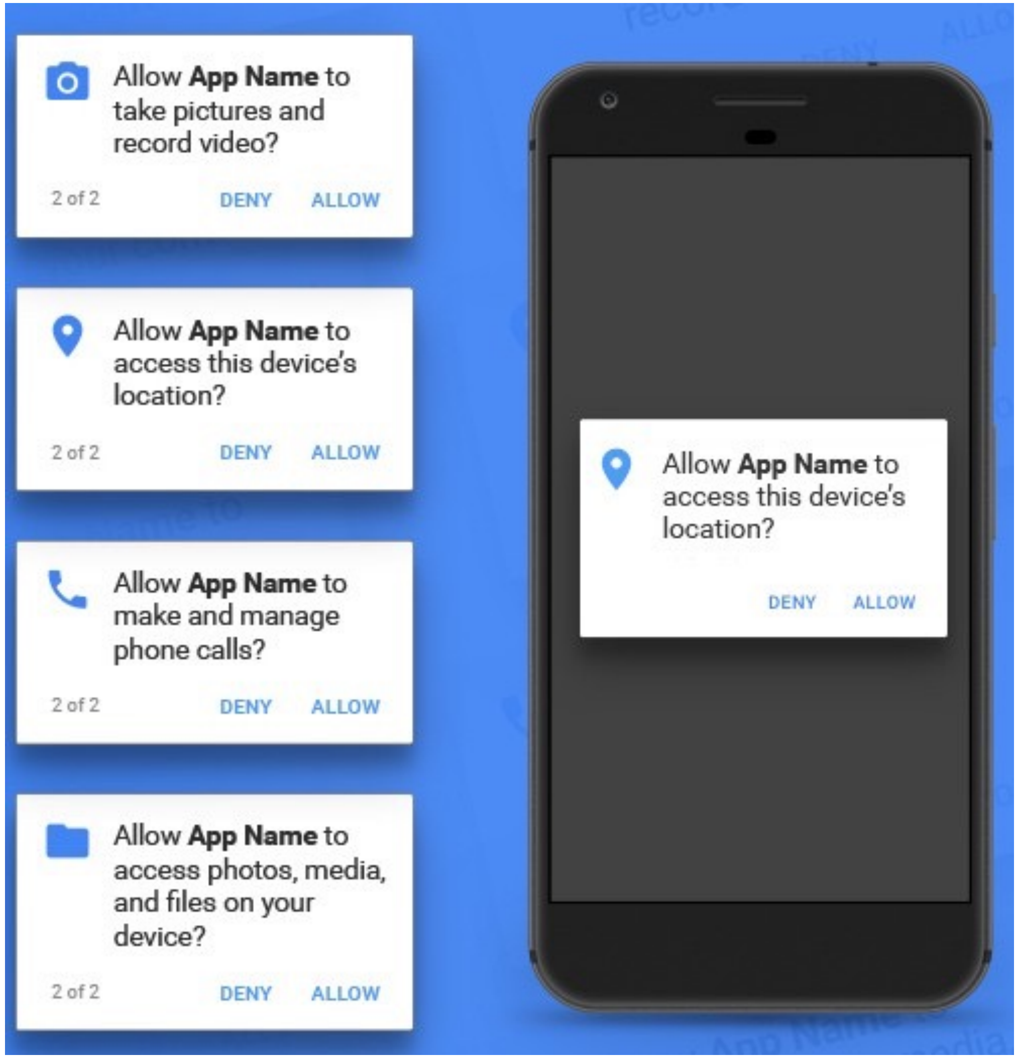
Setting

Setting Activity

Deny

Granted Permisions?

Allow



Allow **App Name** to take pictures and record video?

2 of 2 DENY ALLOW

Allow **App Name** to access this device's location?

2 of 2 DENY ALLOW

Allow **App Name** to make and manage phone calls?

2 of 2 DENY ALLOW

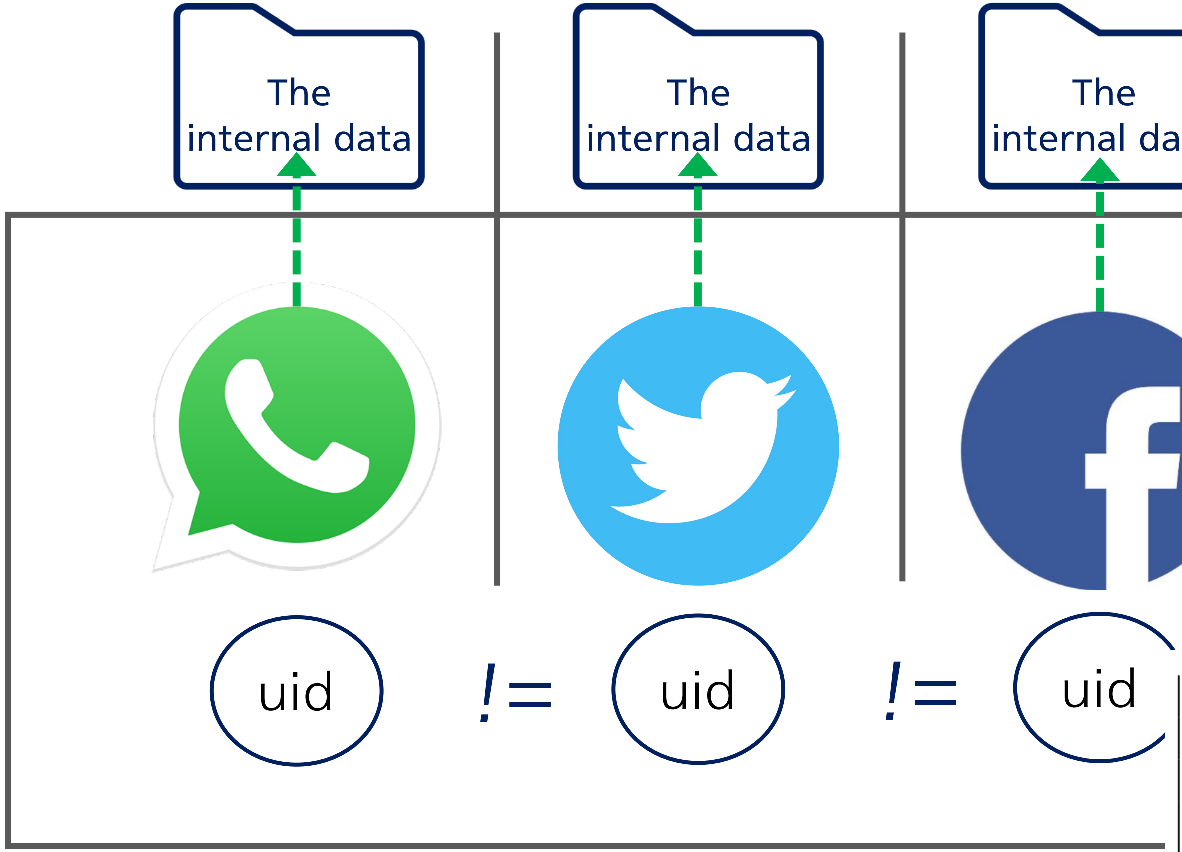
Allow **App Name** to access photos, media, and files on your device?

2 of 2 DENY ALLOW

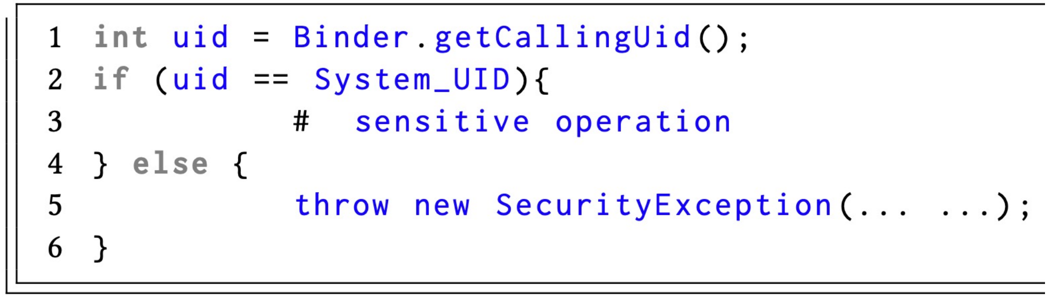
Allow **App Name** to access this device's location?

DENY ALLOW

2. App-level Isolations



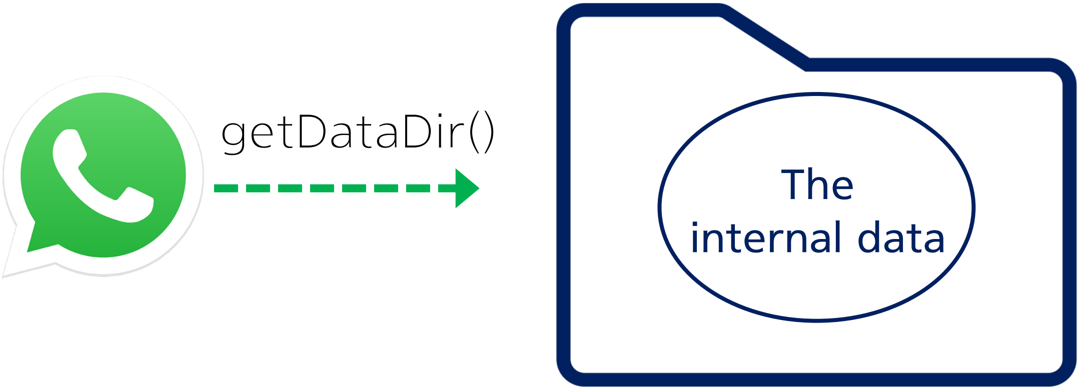
checking its uid



```
int uid = Binder.getCallingUid();
if (uid == System_UID){
            #  sensitive operation
} else {
            throw new SecurityException(... ...);
}
```

Vulneravilities
# of virtualization frameworks

A motivating example

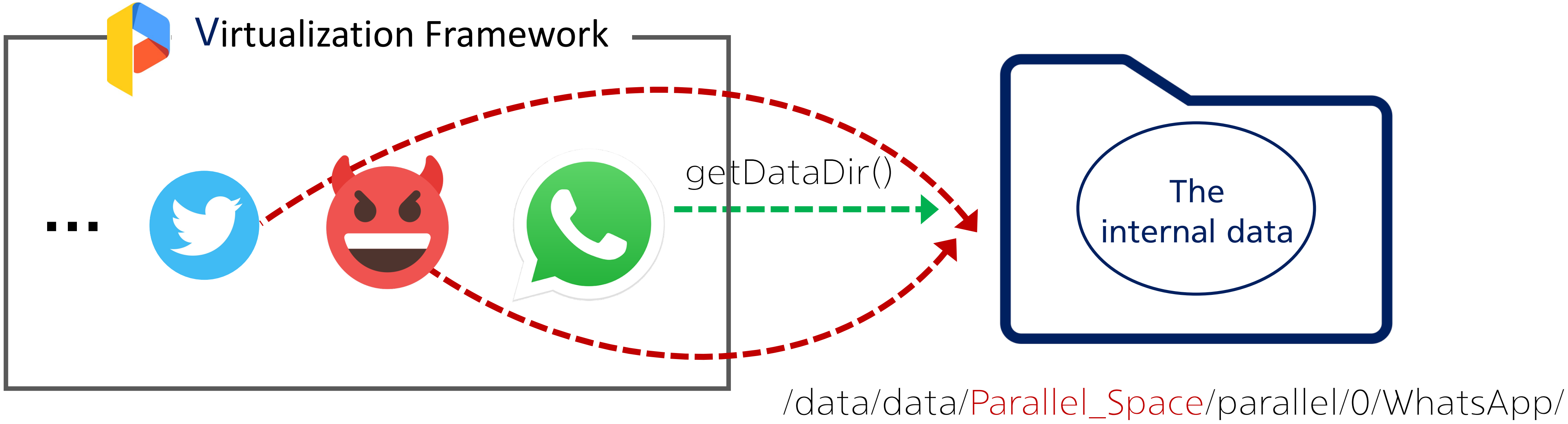


getDataDir()

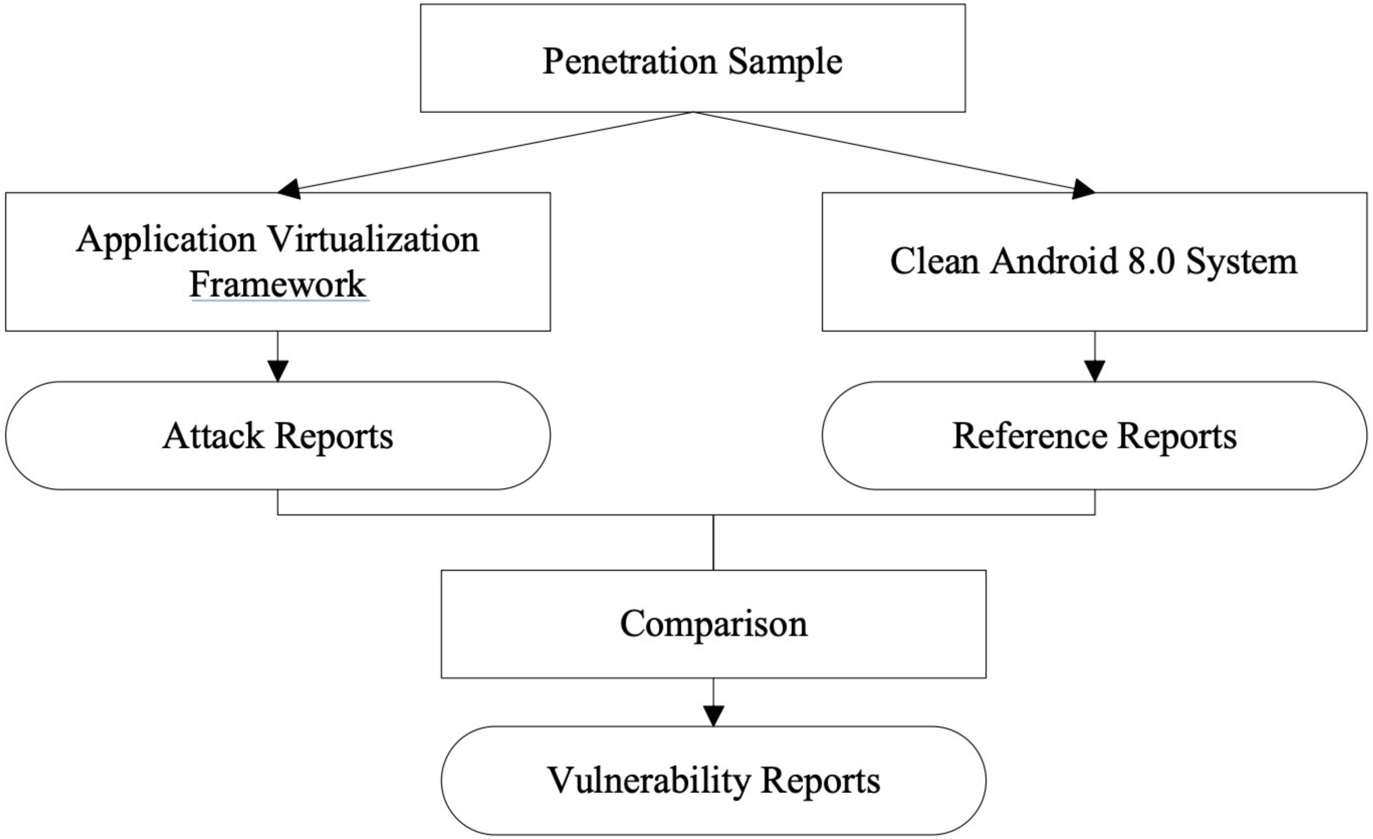
The internal data

/data/data/ WhatsApp/

A motivating example



Architecture of methodology



Penetration Sample

Application Virtualization Framework

Clean Android 8.0 System

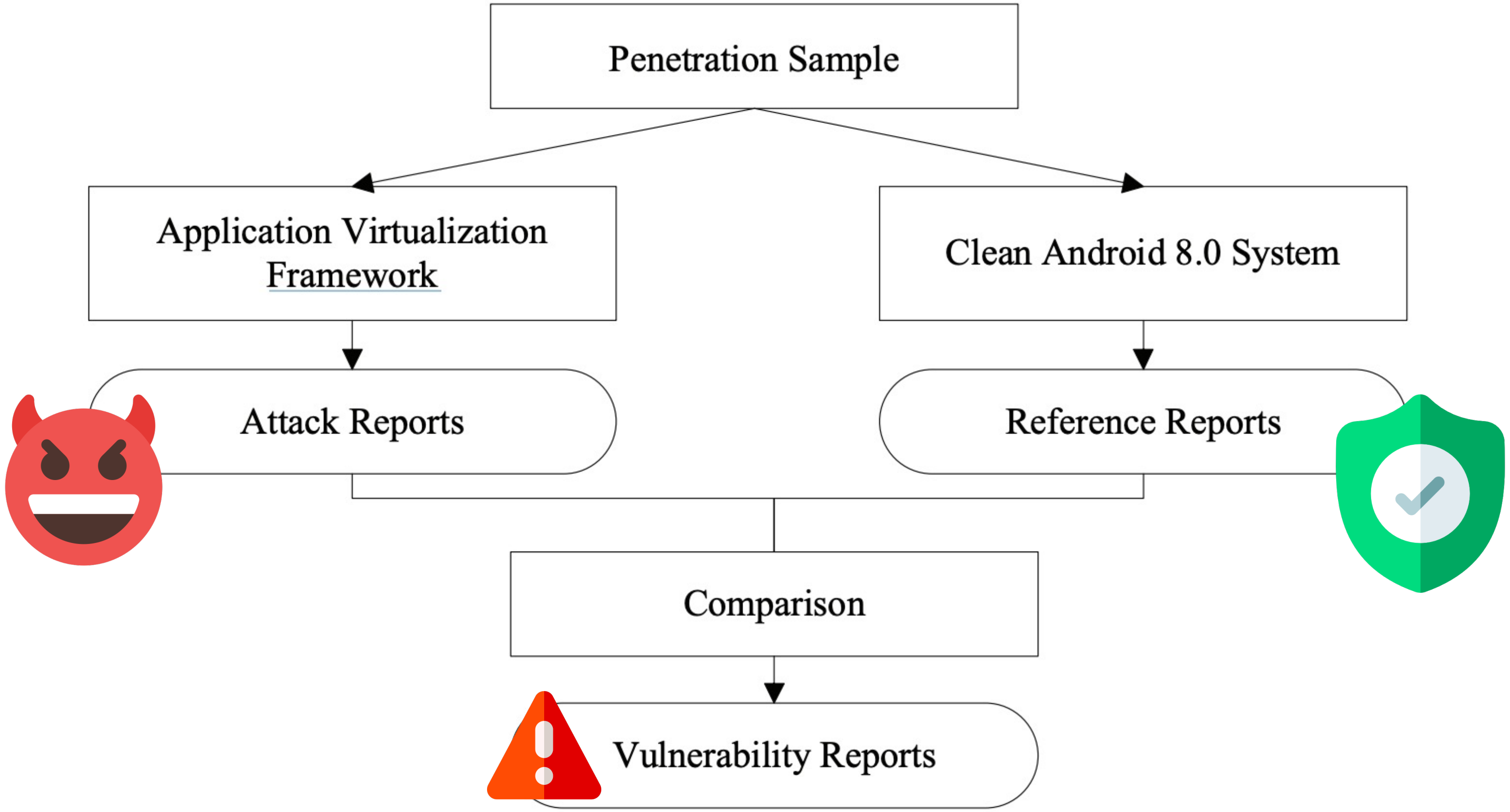
Attack Reports

Reference Reports

Comparison

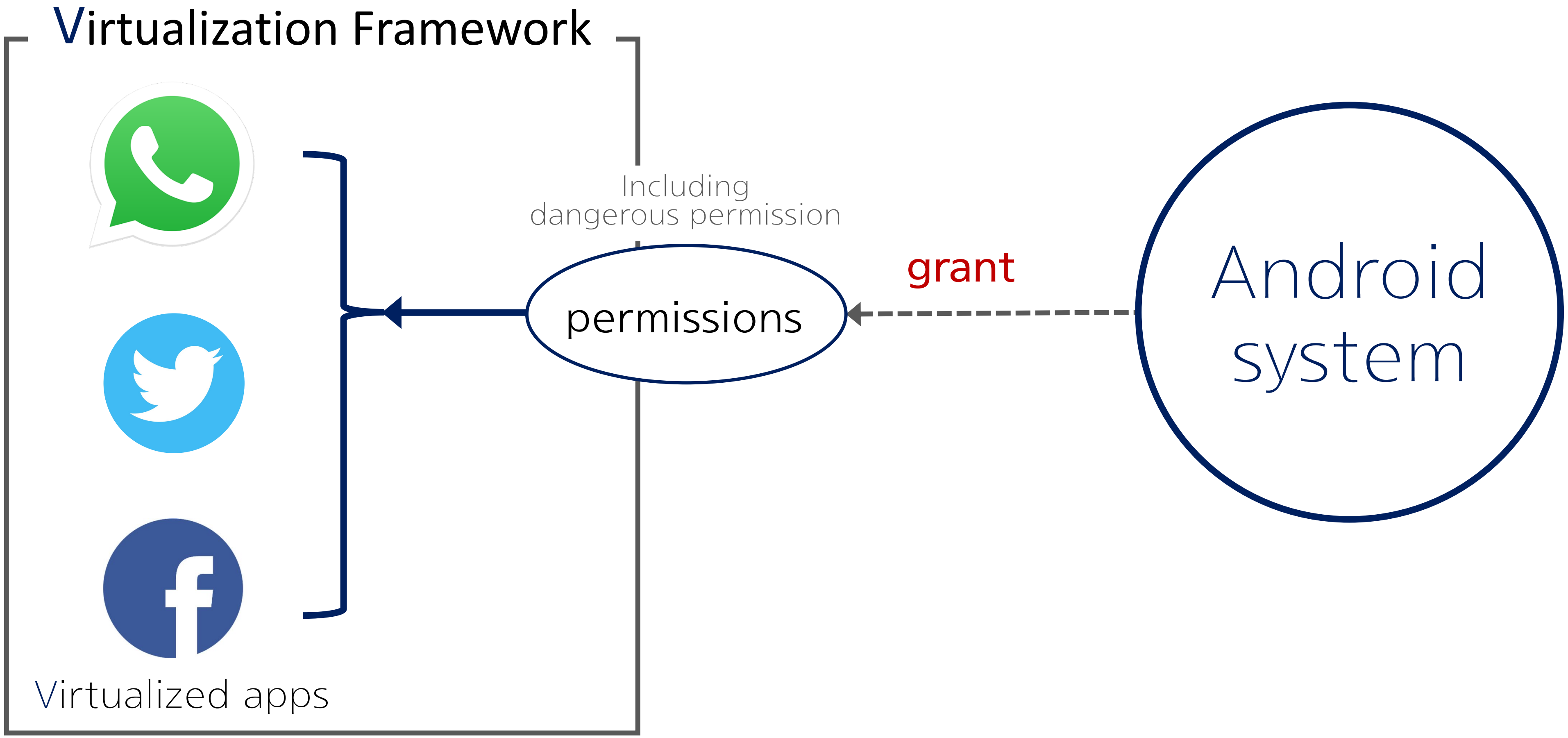
Vulnerability Reports

Architecture of methodology

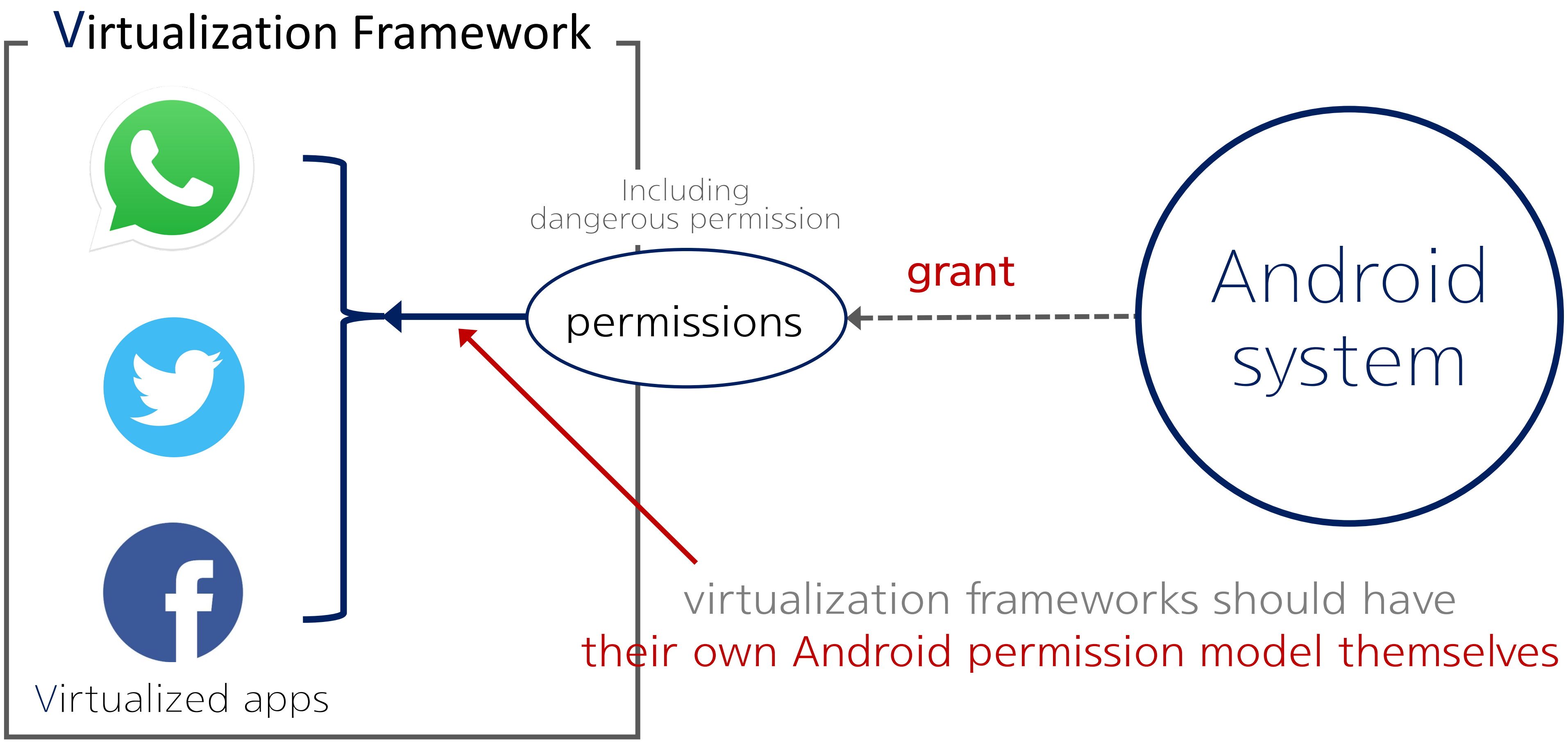


Penetration test configuration

Permissions



Permissions



Virtualization Framework

Virtualized apps

Including dangerous permission

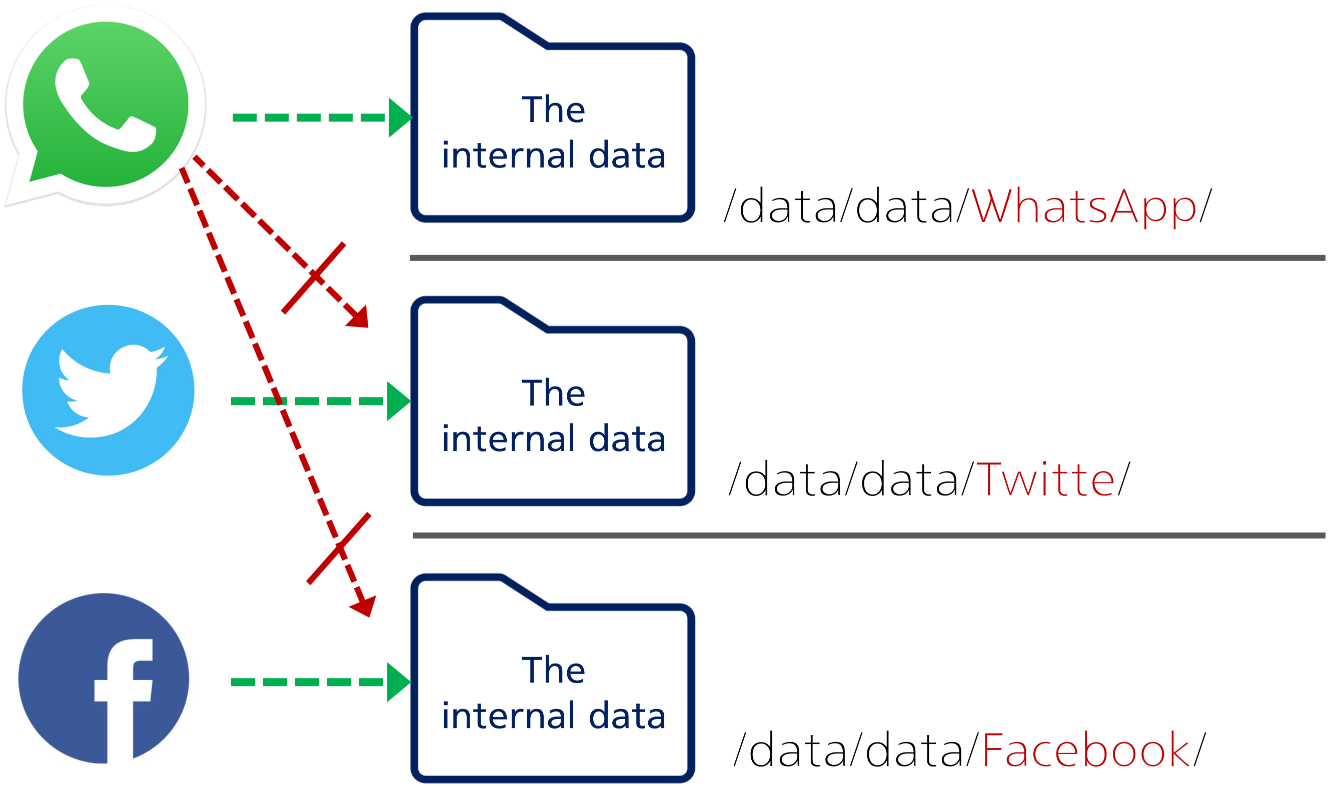
permissions

grant

Android system

virtualization frameworks should have
their own Android permission model themselves

Internal storage



The internal data

/data/data/WhatsApp/

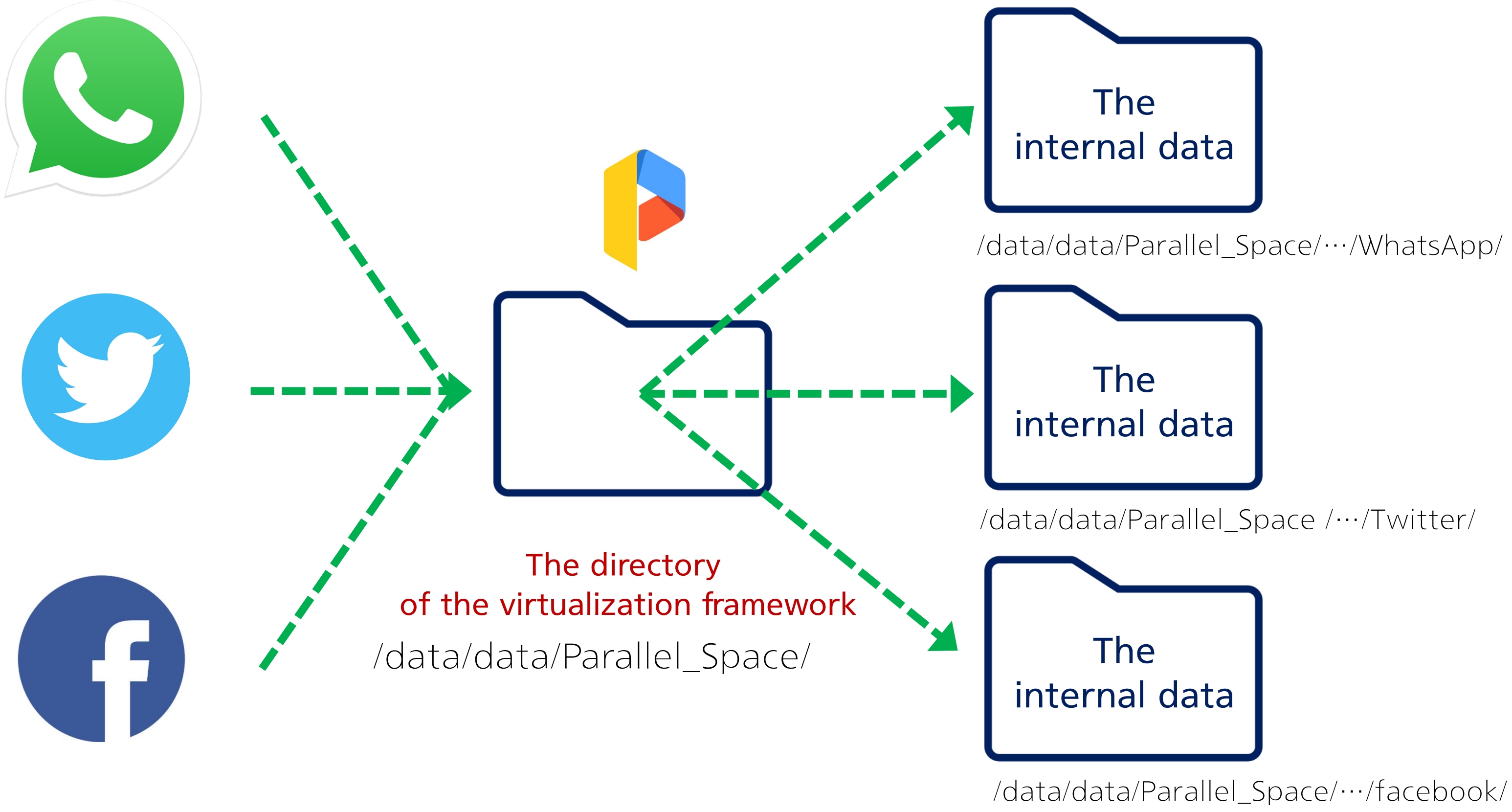
The internal data

/data/data/Twitte/

The internal data

/data/data/Facebook/

Internal storage



The internal data

/data/data/Parallel_Space/…/WhatsApp/

The internal data

/data/data/Parallel_Space /…/Twitter/

The internal data

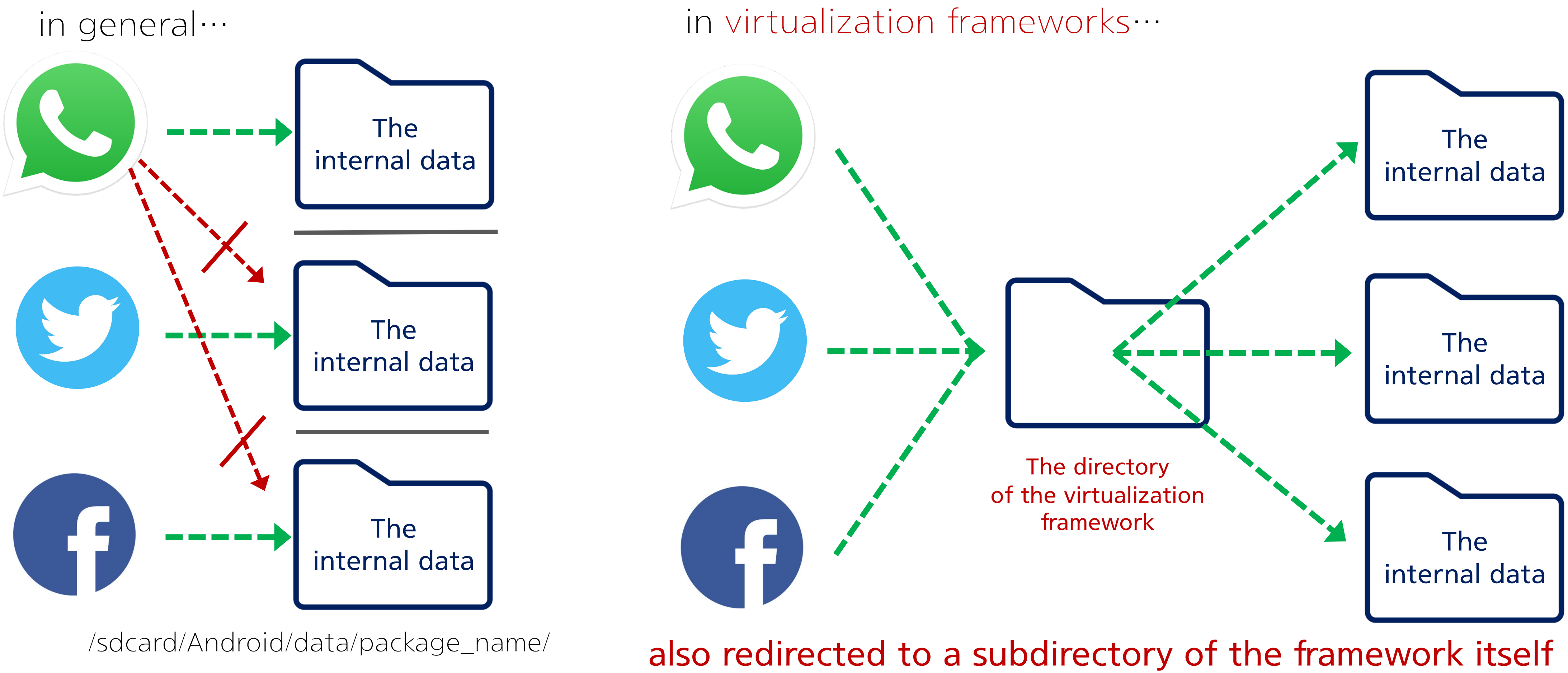
/data/data/Parallel_Space/…/facebook/

The directory
of the virtualization framework

/data/data/Parallel_Space/

Protected external storage

(Similar to internal storage)



also redirected to a subdirectory of the framework itself

Android App Programming

Almost finished reading

Plan

Android App Reverse Engineering 101

Finish tutorial quickly