ILLINOIS
SECURITY LAB

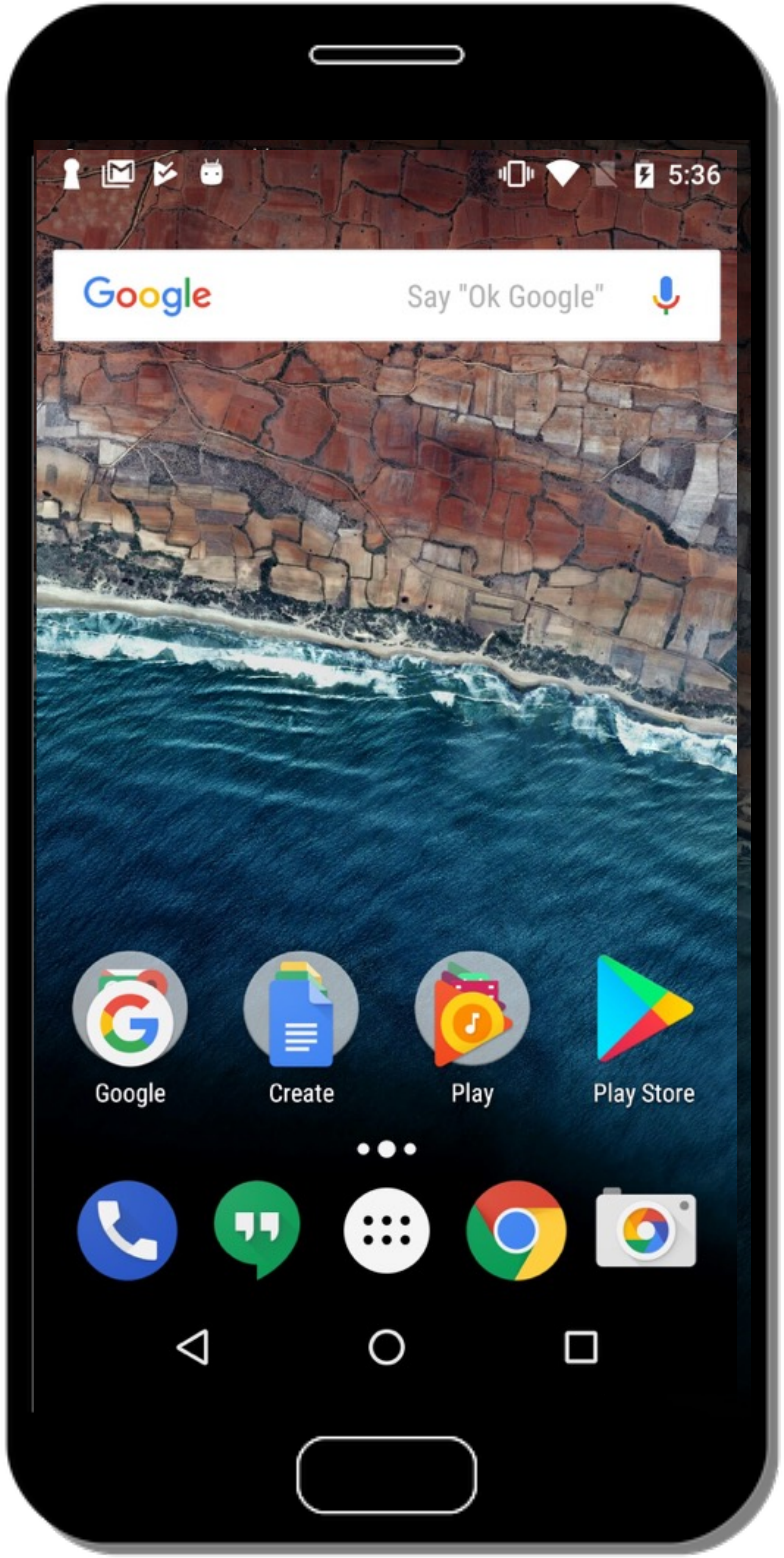
Resolving the Predicament of Android Custom Permissions

Güliz Seray Tuncay, **Soteris Demetriou**, Karan Ganju, Carl A. Gunter

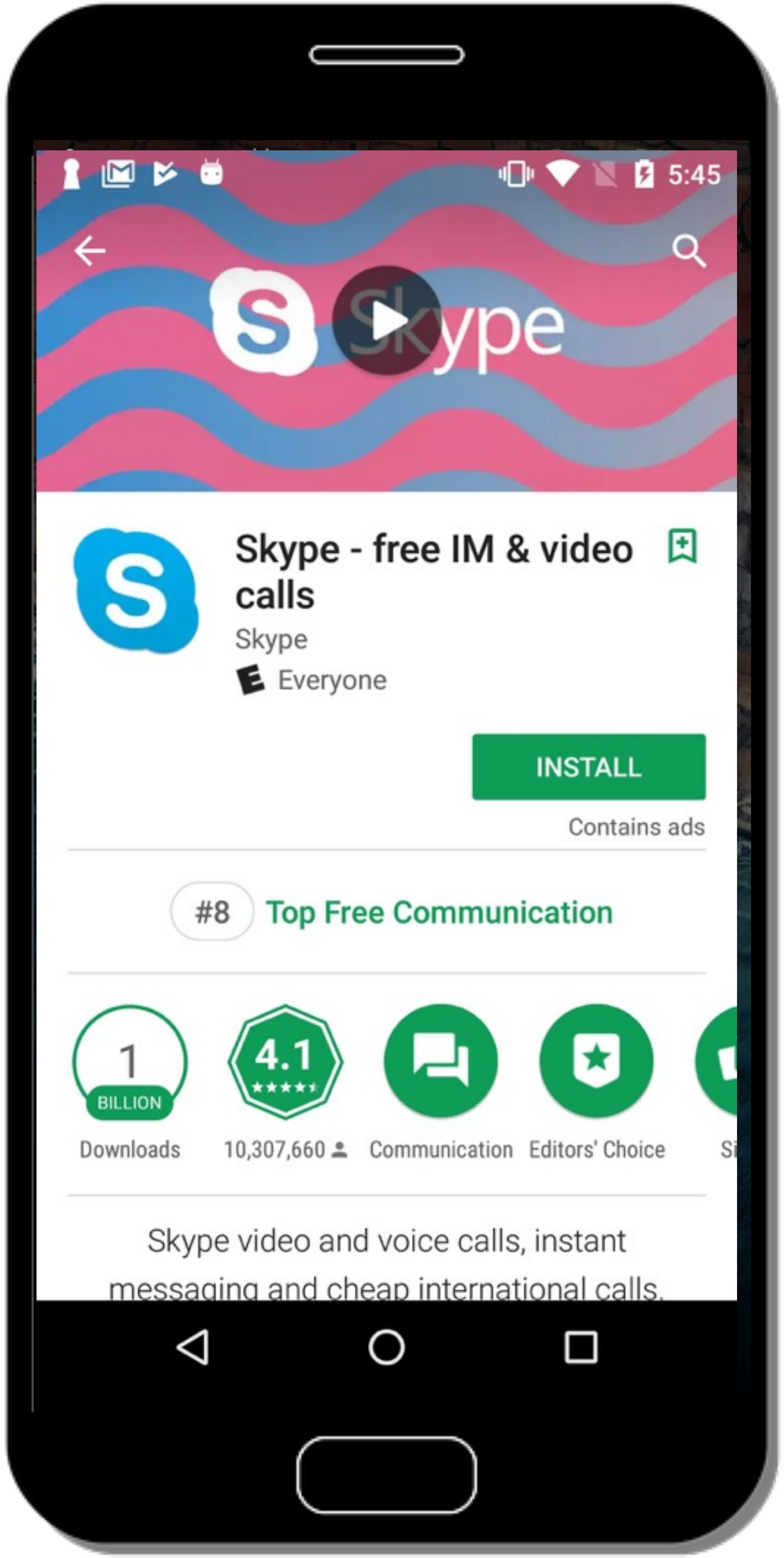
University of Illinois at Urbana - Champaign

#NDSS18

Install-time Permissions
< version 6

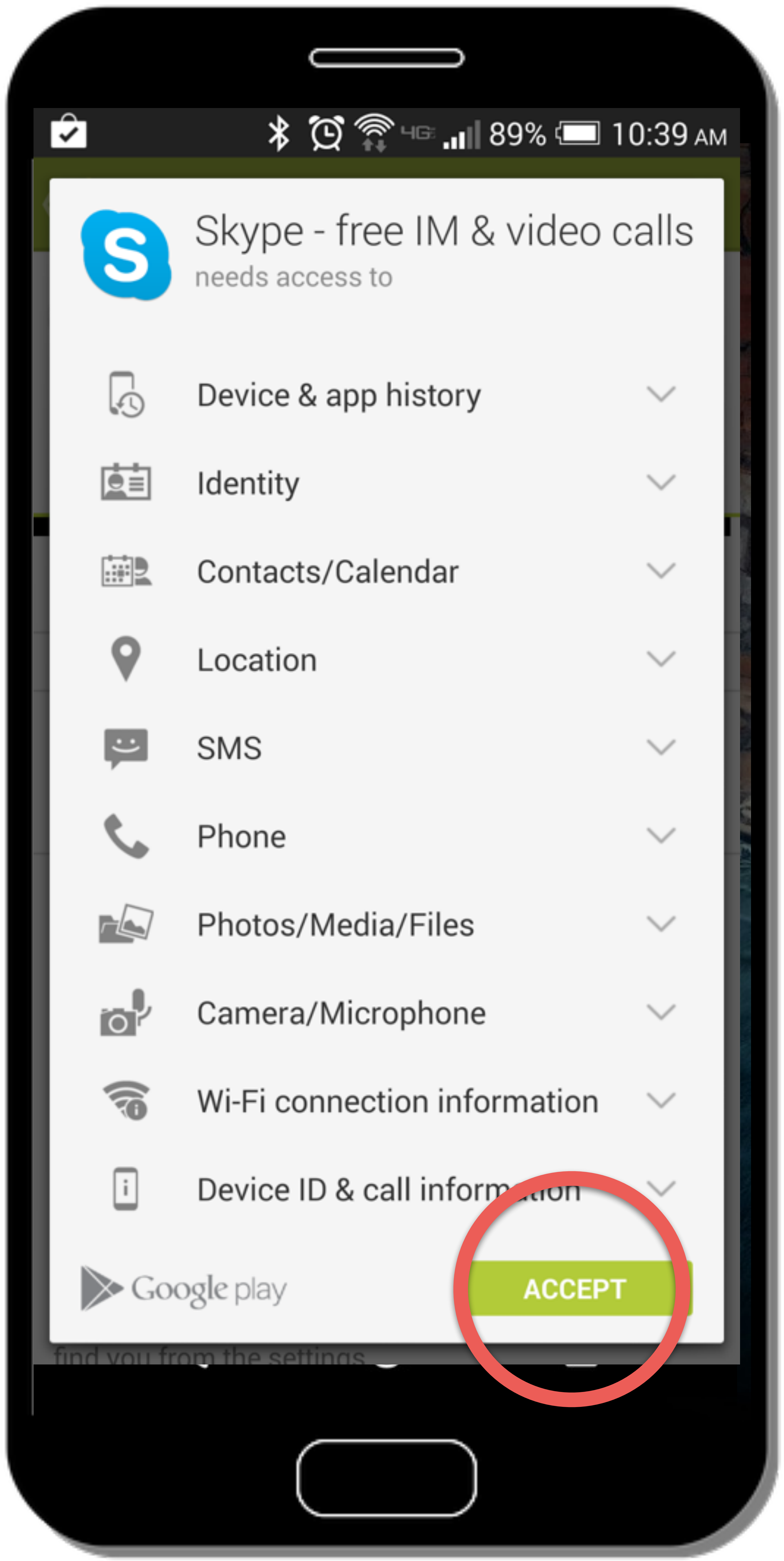


Install-time Permissions
< version 6



Skype video and voice calls, instant messaging and cheap international calls.

Install-time Permissions
< version 6



Skype - free IM & video calls
needs access to

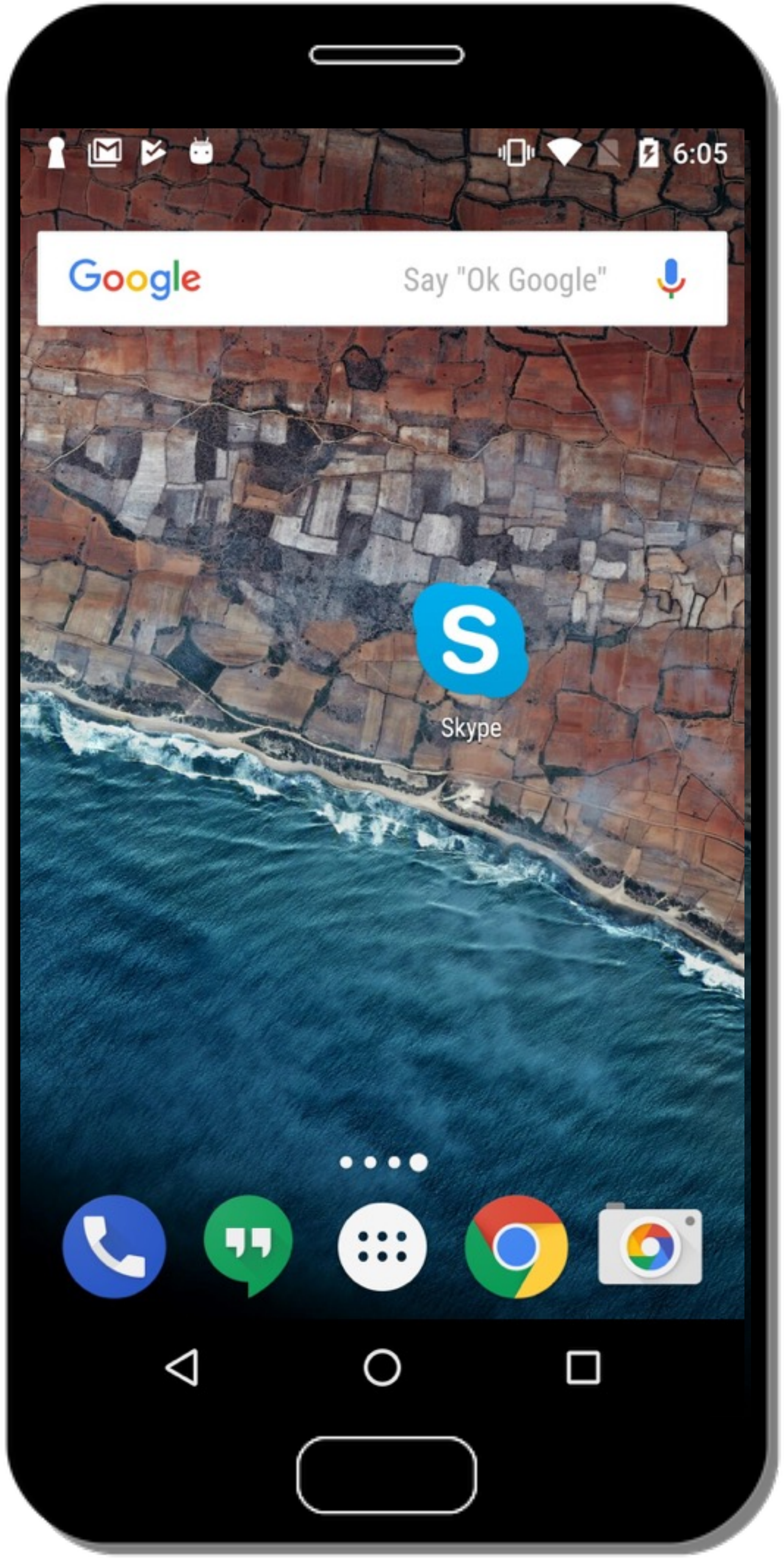
- Device & app history
- Identity
- Contacts/Calendar
- Location
- SMS
- Phone
- Photos/Media/Files
- Camera/Microphone
- Wi-Fi connection information
- Device ID & call information

find you from the settings

Permission Types

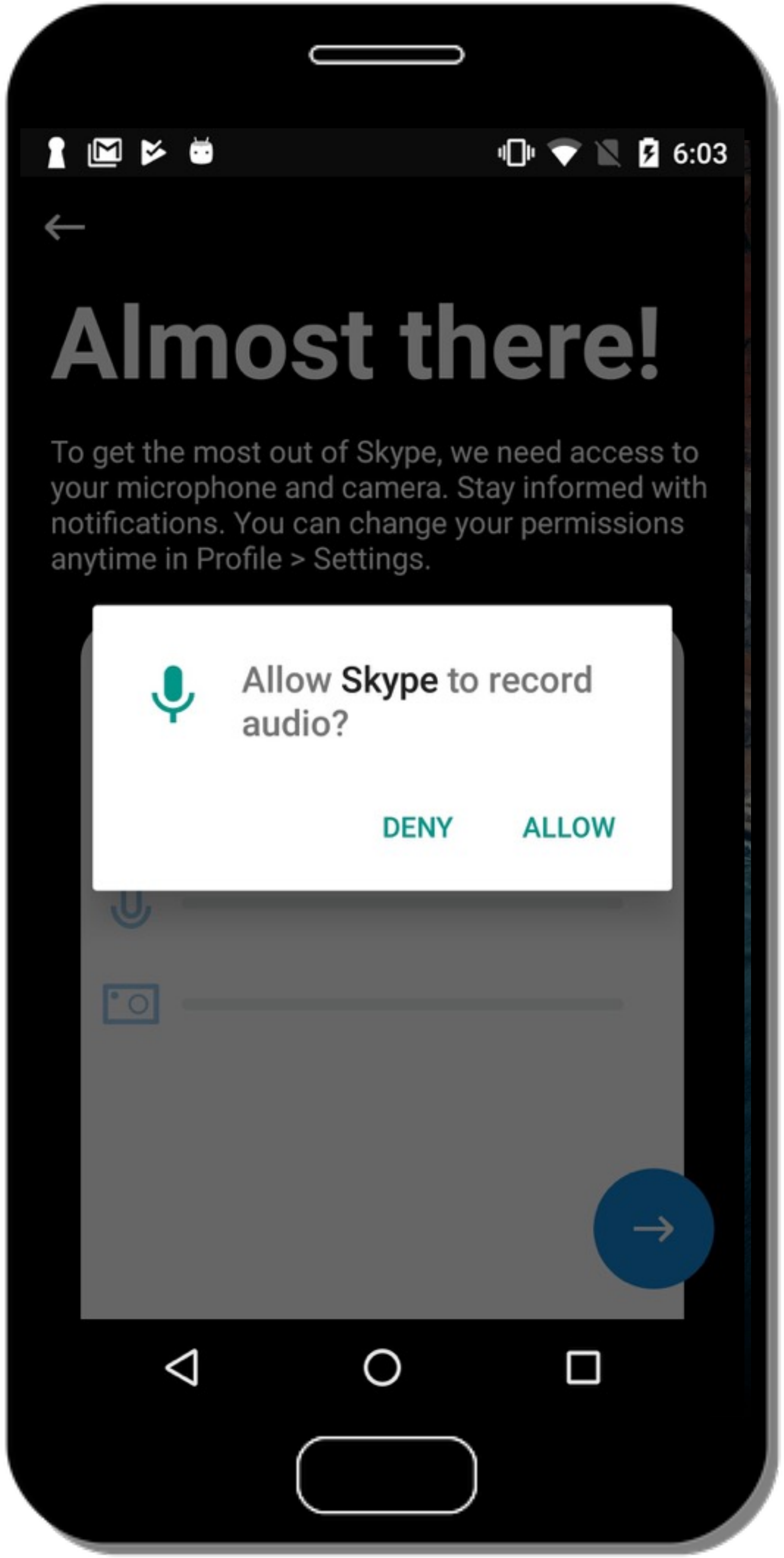
- ✓ Normal
- Signature
- Dangerous
- SignatureOr System

~~Install-time Permissions~~
~~< version 6~~



Runtime Permissions
>= version 6

Runtime Permissions
>= version 6



Almost there!

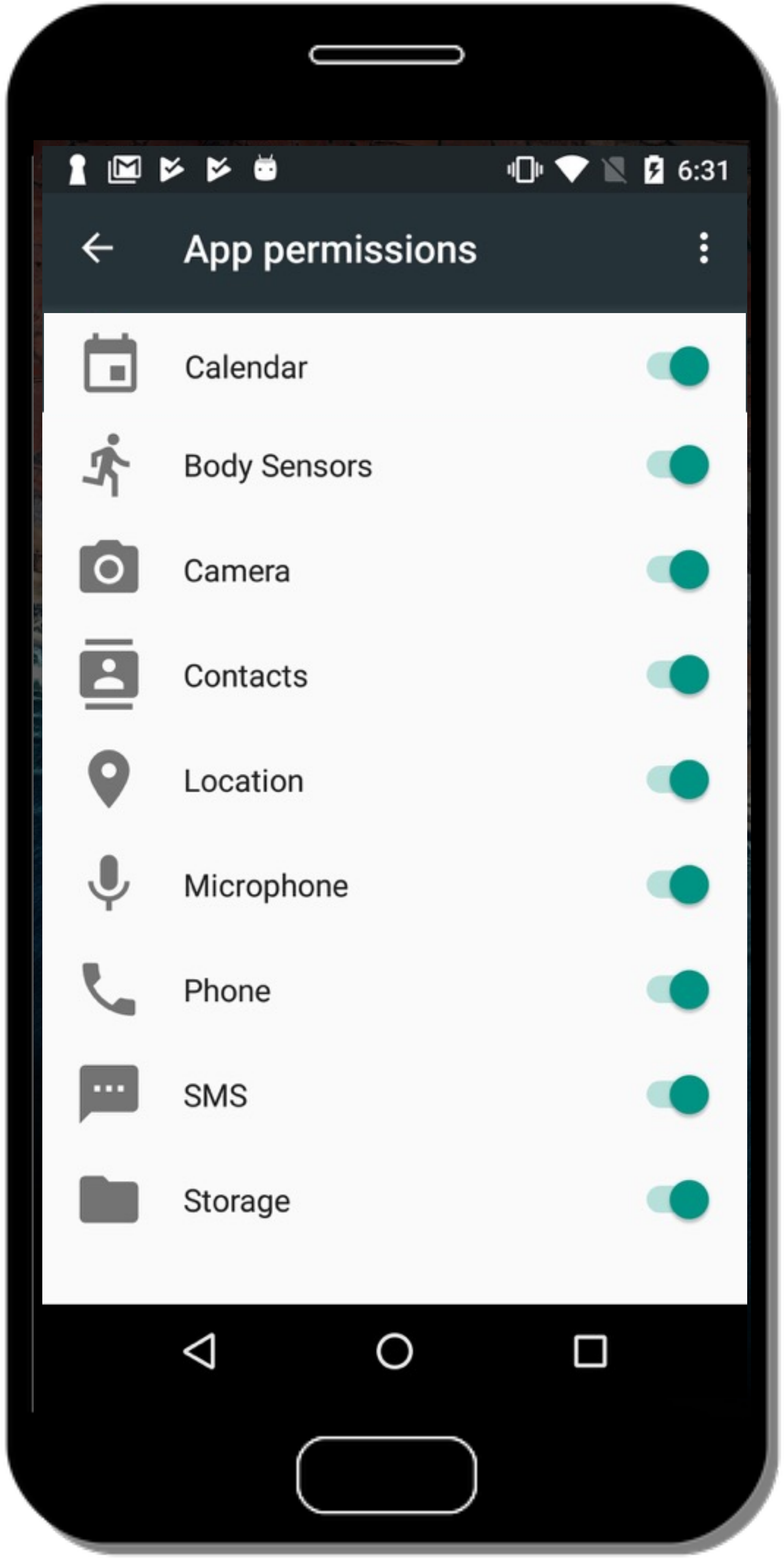
To get the most out of Skype, we need access to your microphone and camera. Stay informed with notifications. You can change your permissions anytime in Profile > Settings.

Allow **Skype** to record audio?

Permission Types

- ✓ Normal
- Signature
- Dangerous

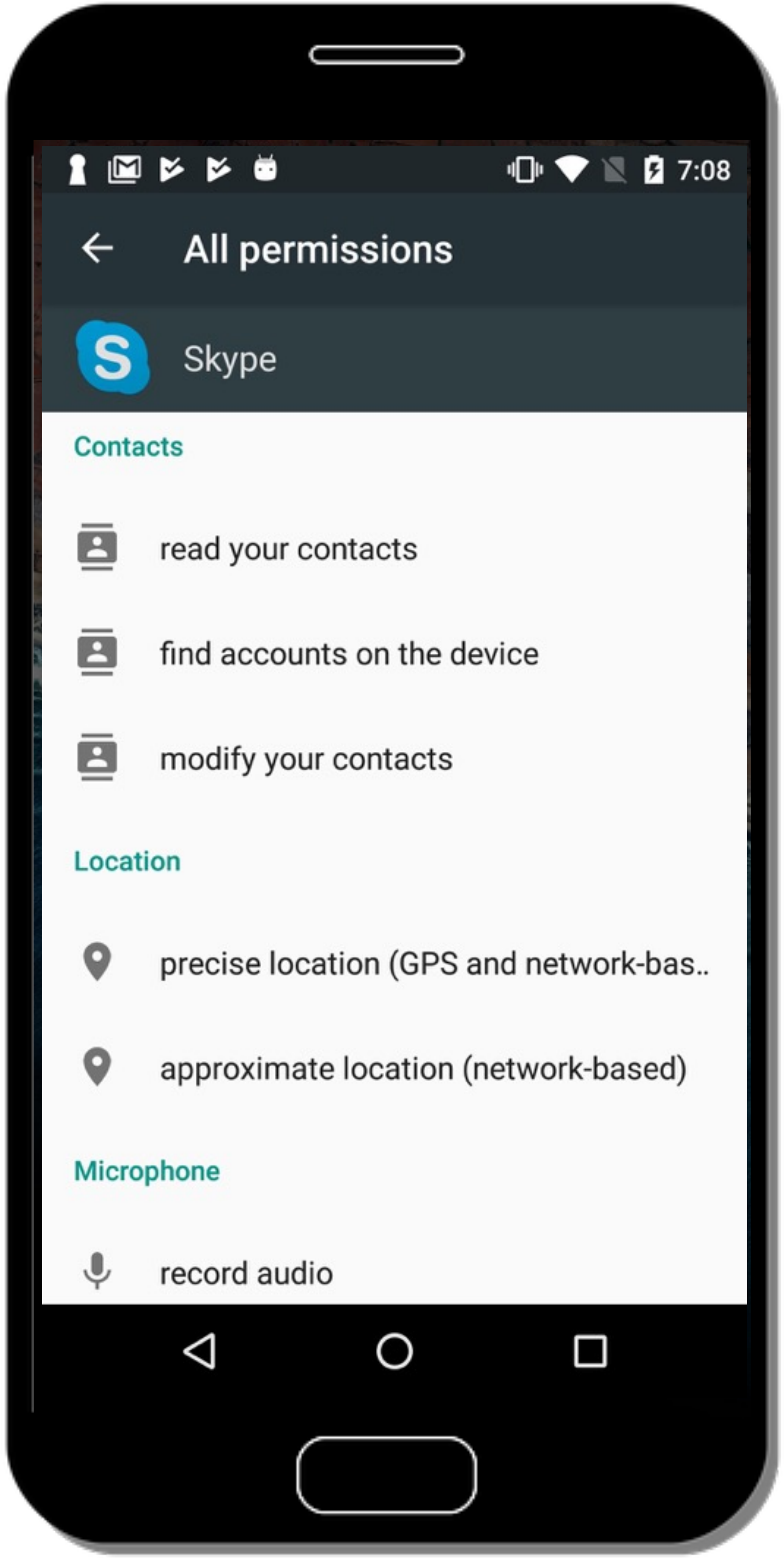
Permission Groups



App permissions

- Calendar ●
- Body Sensors ●
- Camera ●
- Contacts ●
- Location ●
- Microphone ●
- Phone ●
- SMS ●
- Storage ●

Permission Groups



7:08

All permissions

Skype

Contacts

- read your contacts
- find accounts on the device
- modify your contacts

Location

- precise location (GPS and network-bas..
- approximate location (network-based)

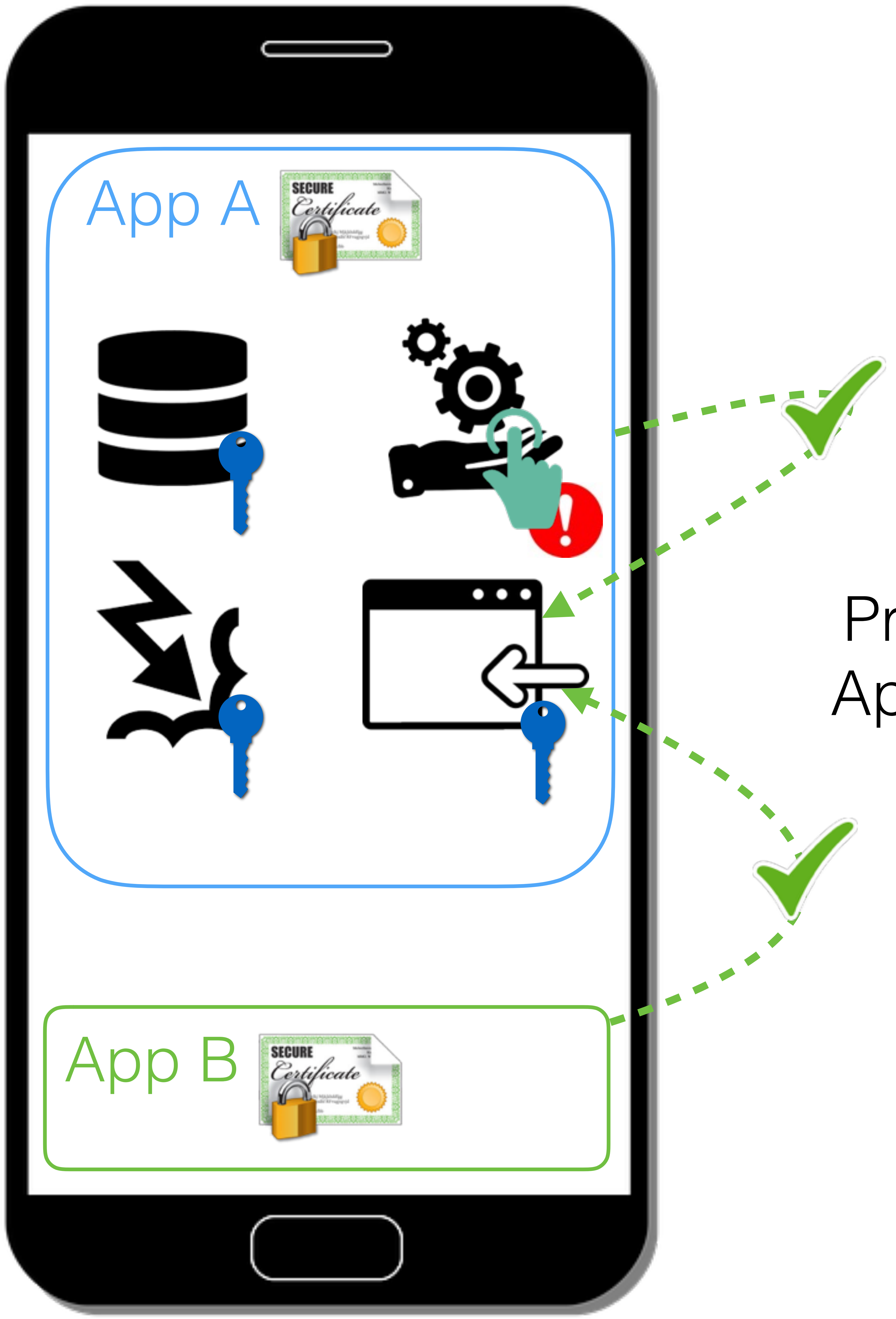
Microphone

- record audio

Custom Permissions

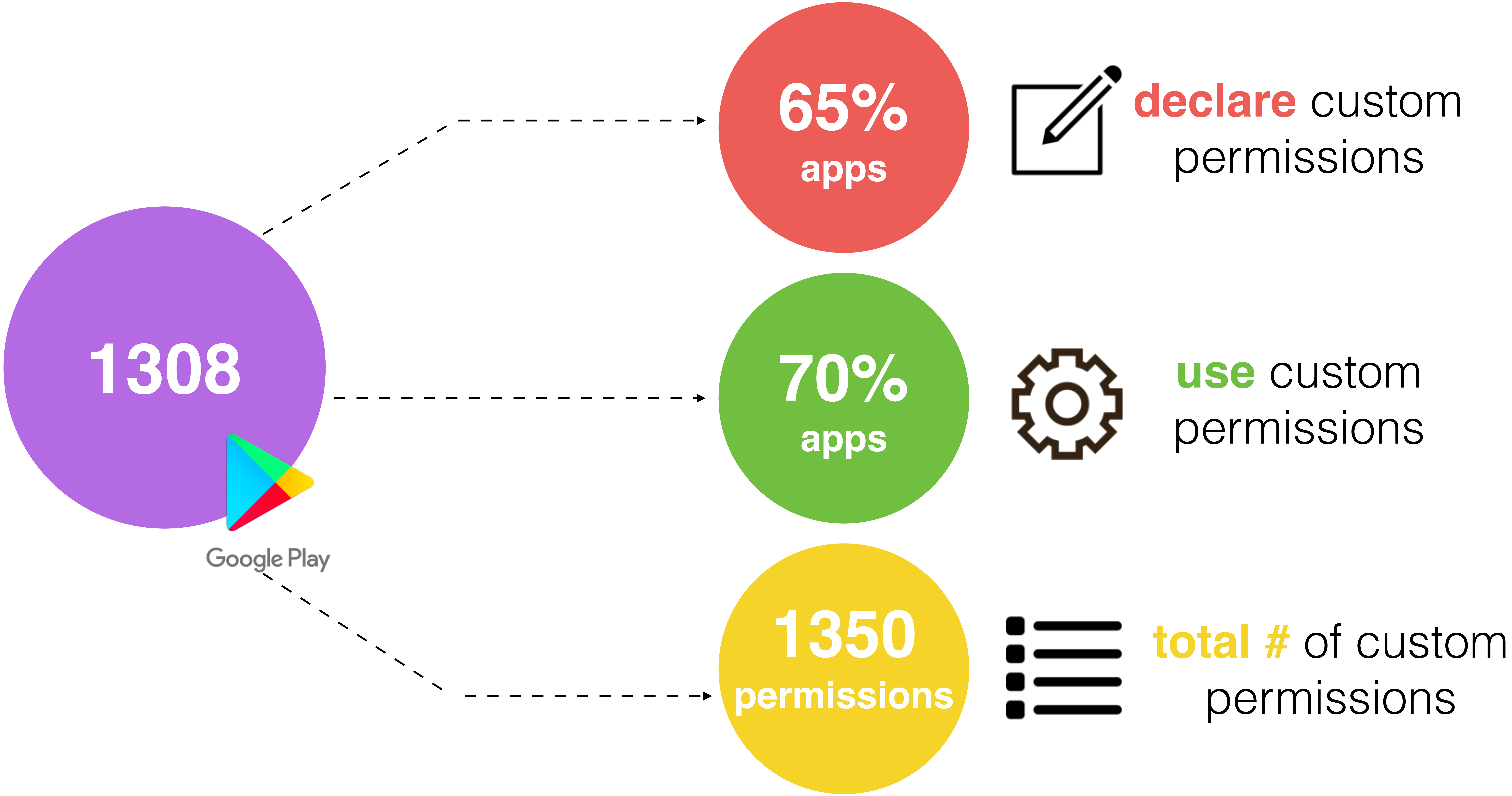
Permission Types

- ✓ Normal
- Signature
- Dangerous



Protect Exported App Components

Prevalence of custom permissions



1308

Google Play

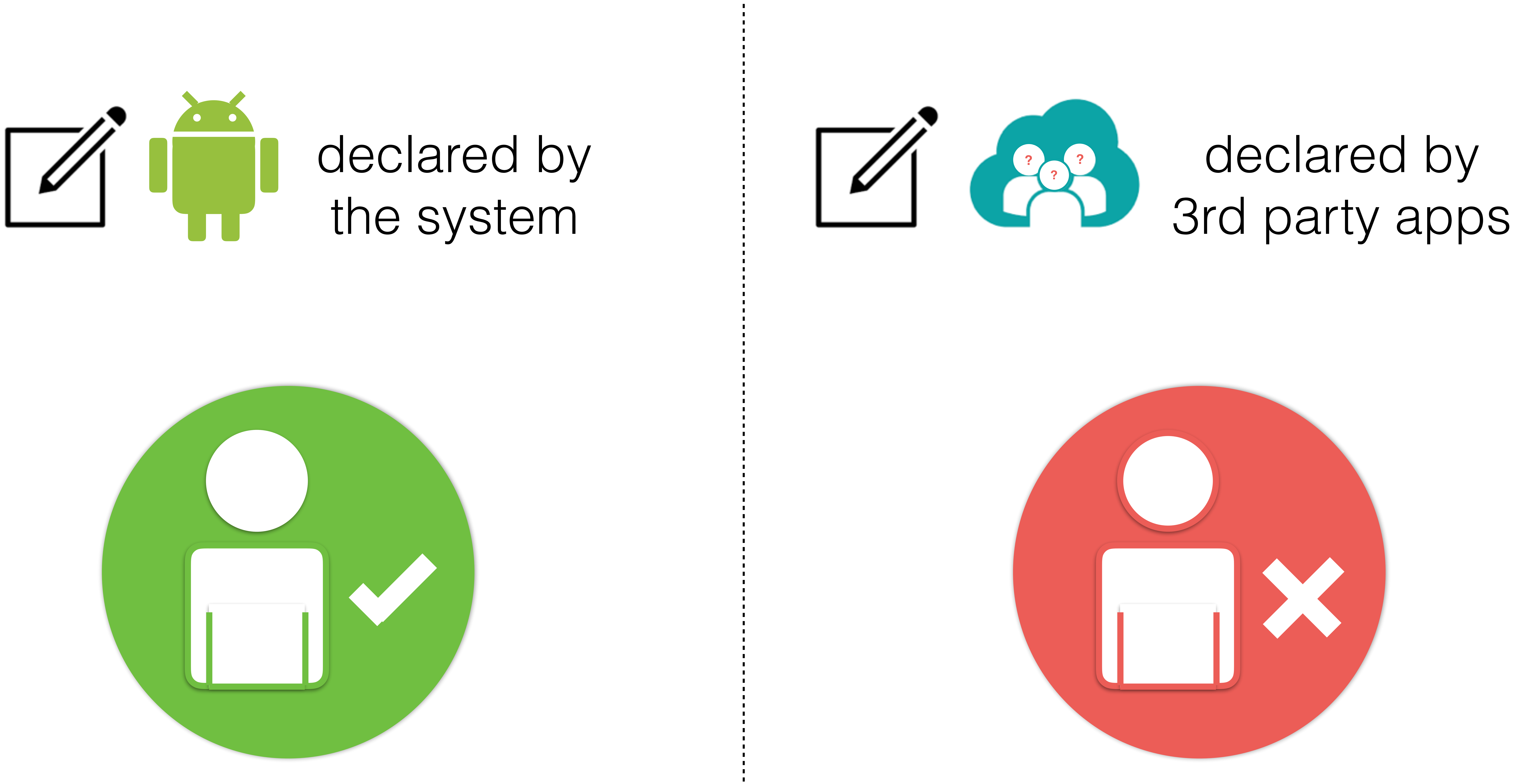
65% apps — declare custom permissions

70% apps — use custom permissions

1350 permissions — total # of custom permissions

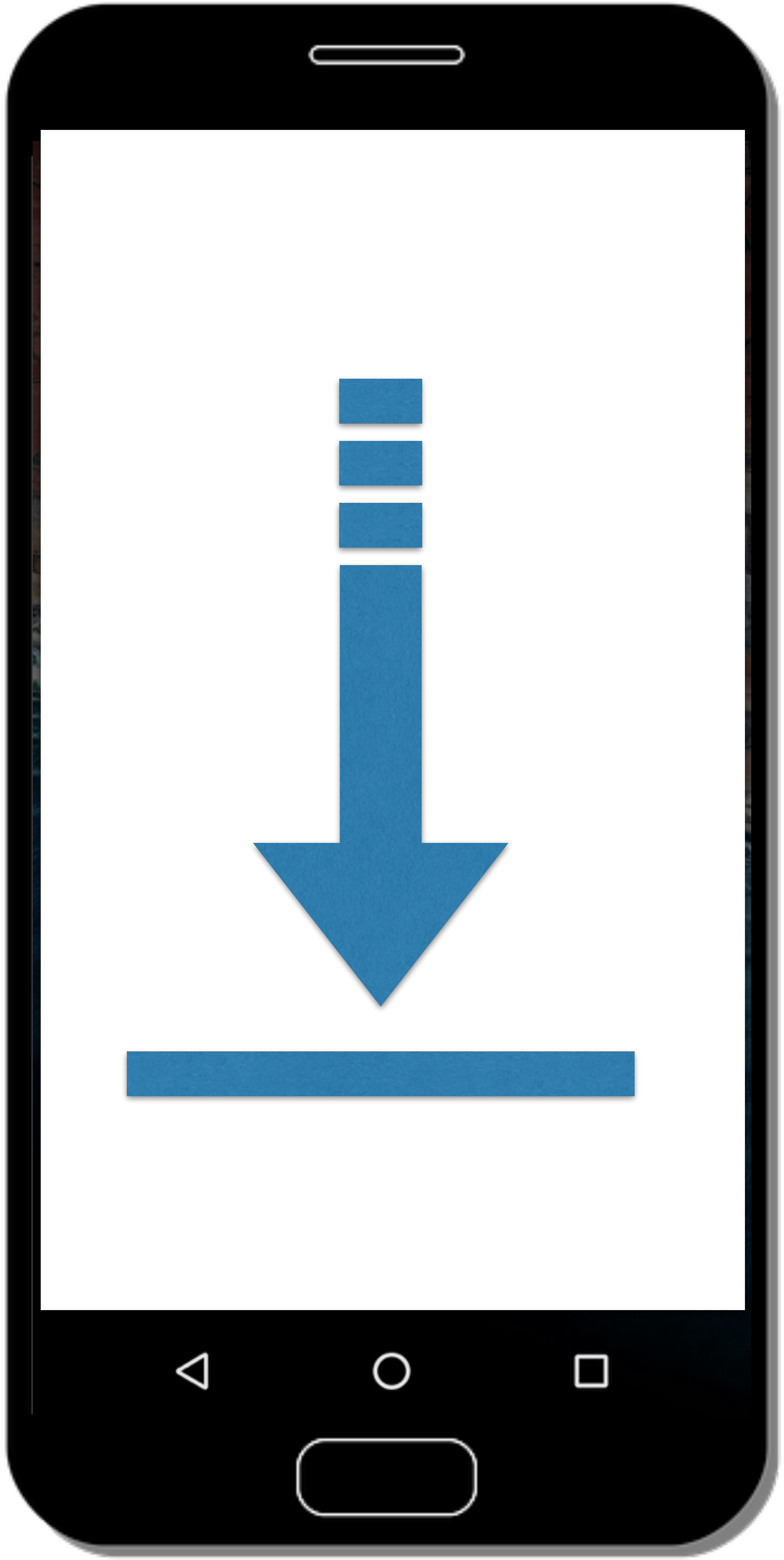
⚠ No clear distinction between
system permissions and custom permissions

No clear distinction between system permissions and custom permissions



declared by the system

declared by 3rd party apps



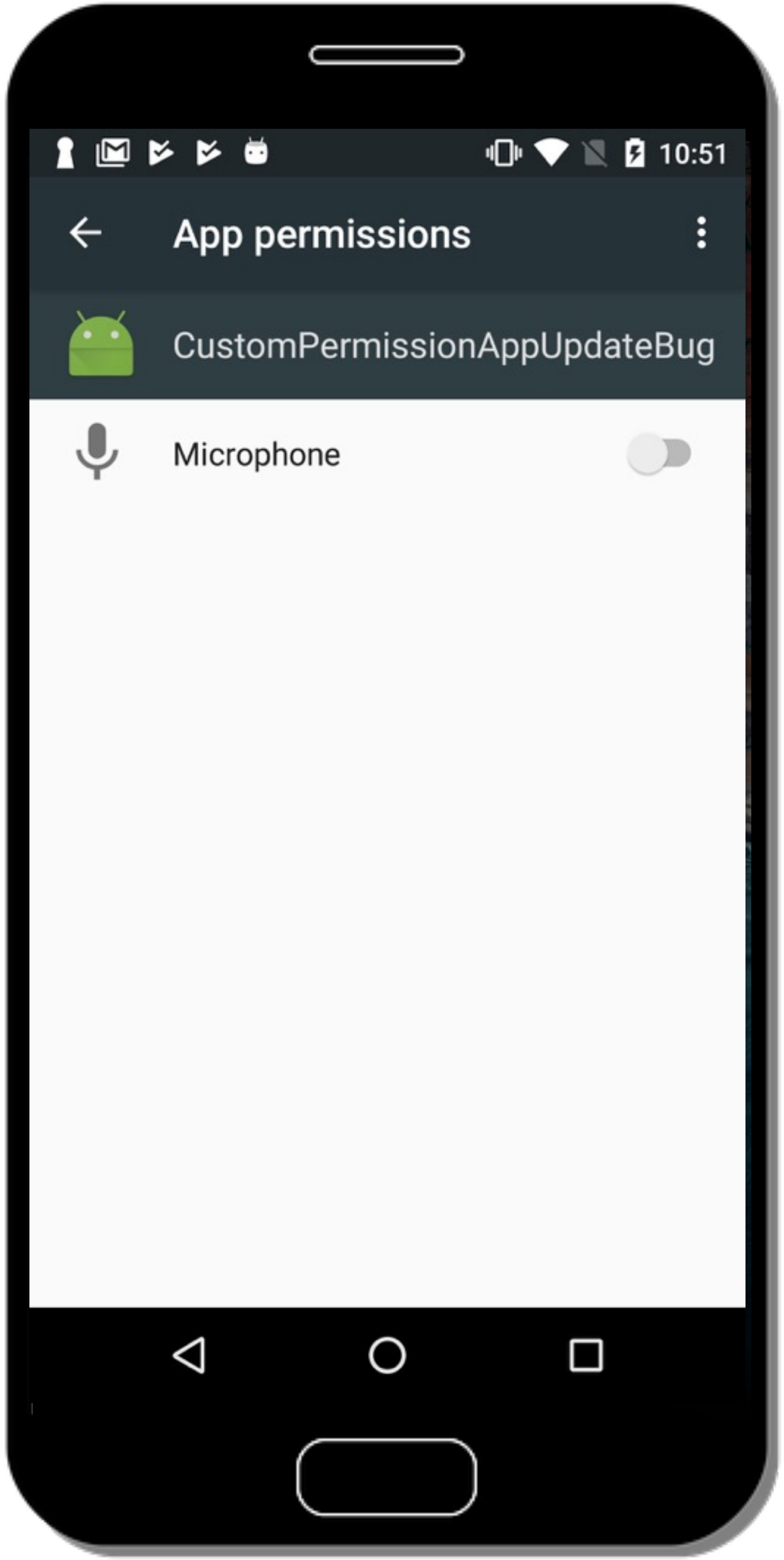
My_Permission

✓ normal

Microphone Group

My_Permission

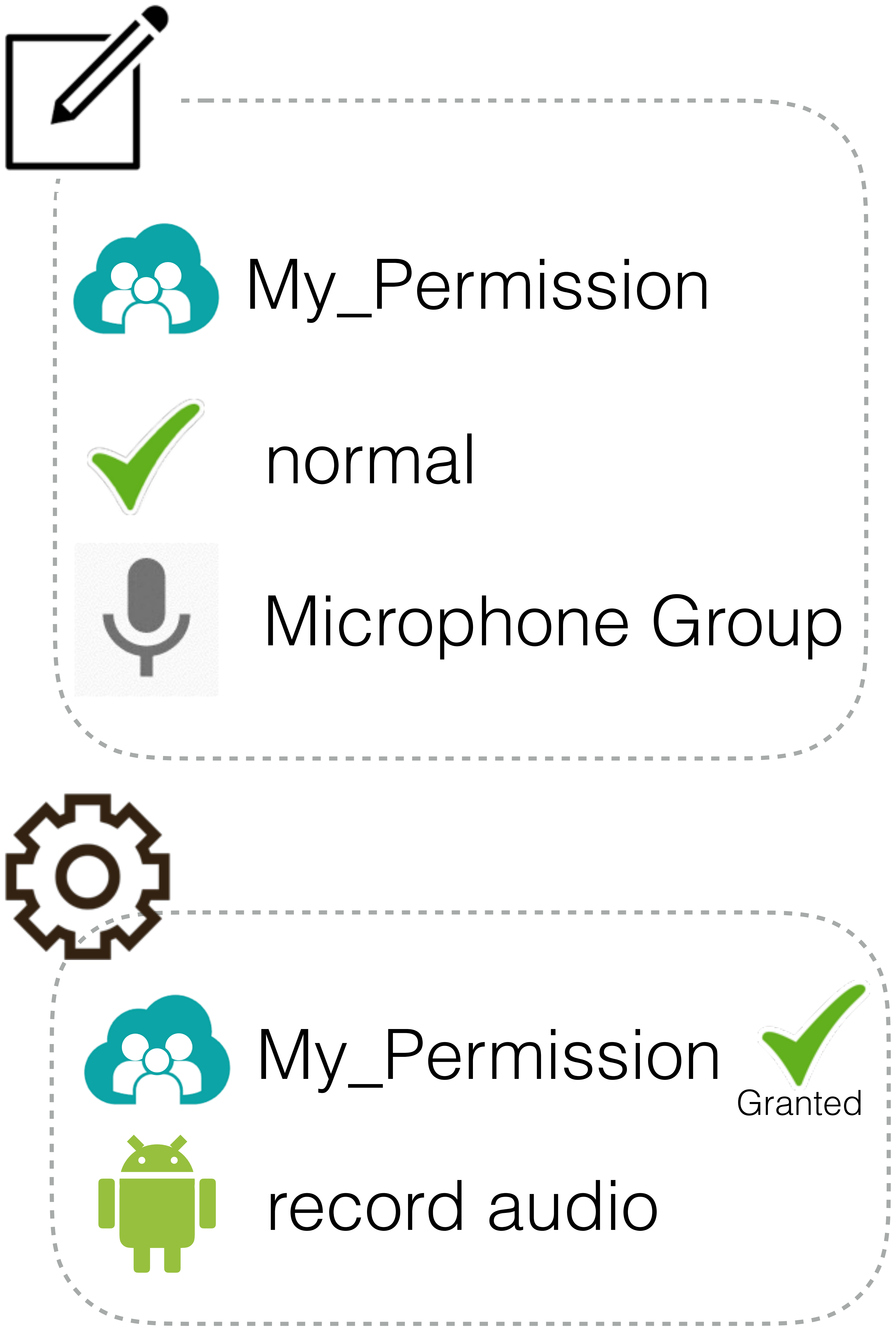
record audio



App permissions

CustomPermissionAppUpdateBug

Microphone



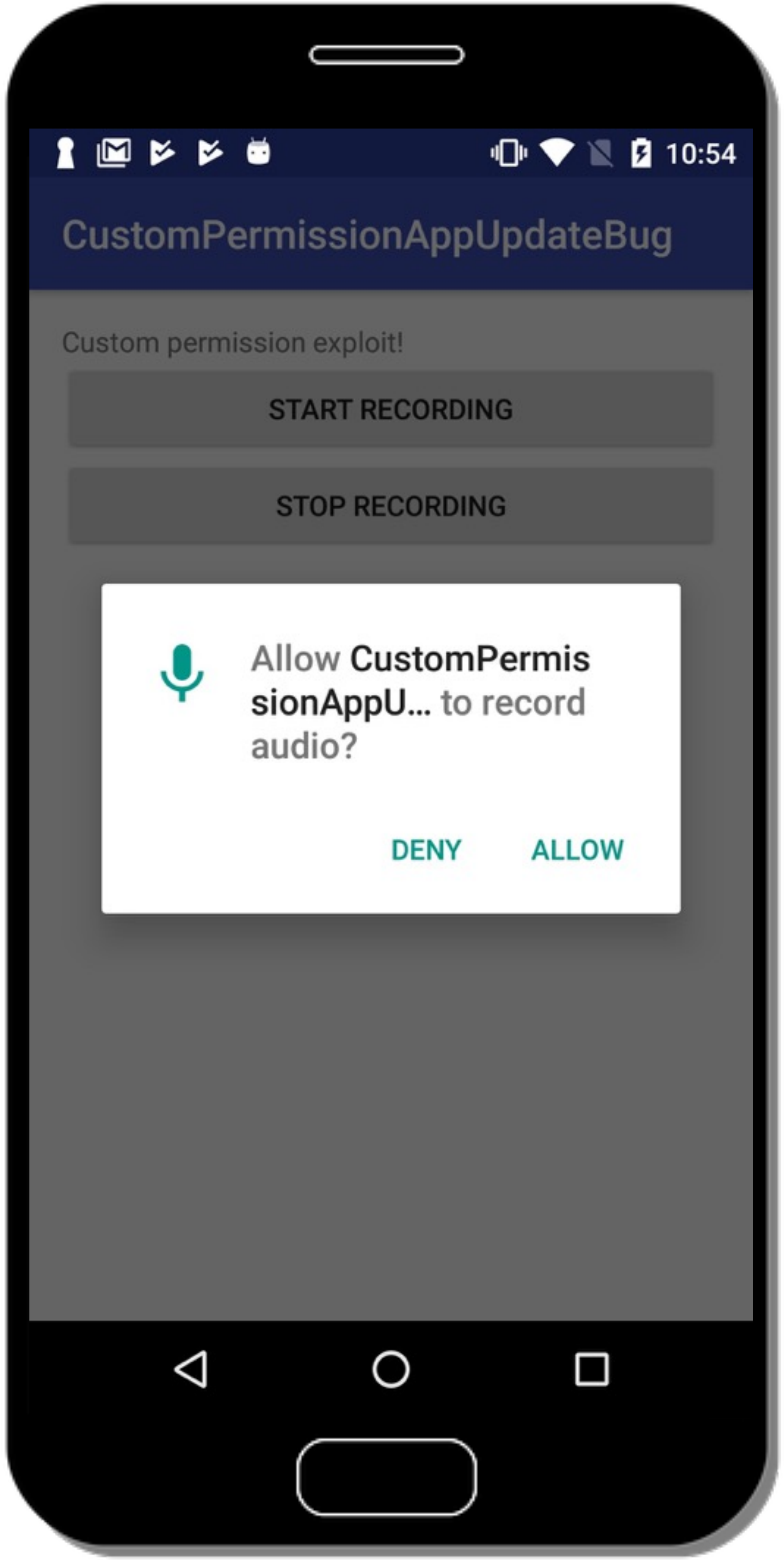
My_Permission

normal

Microphone Group

My_Permission ✓ Granted

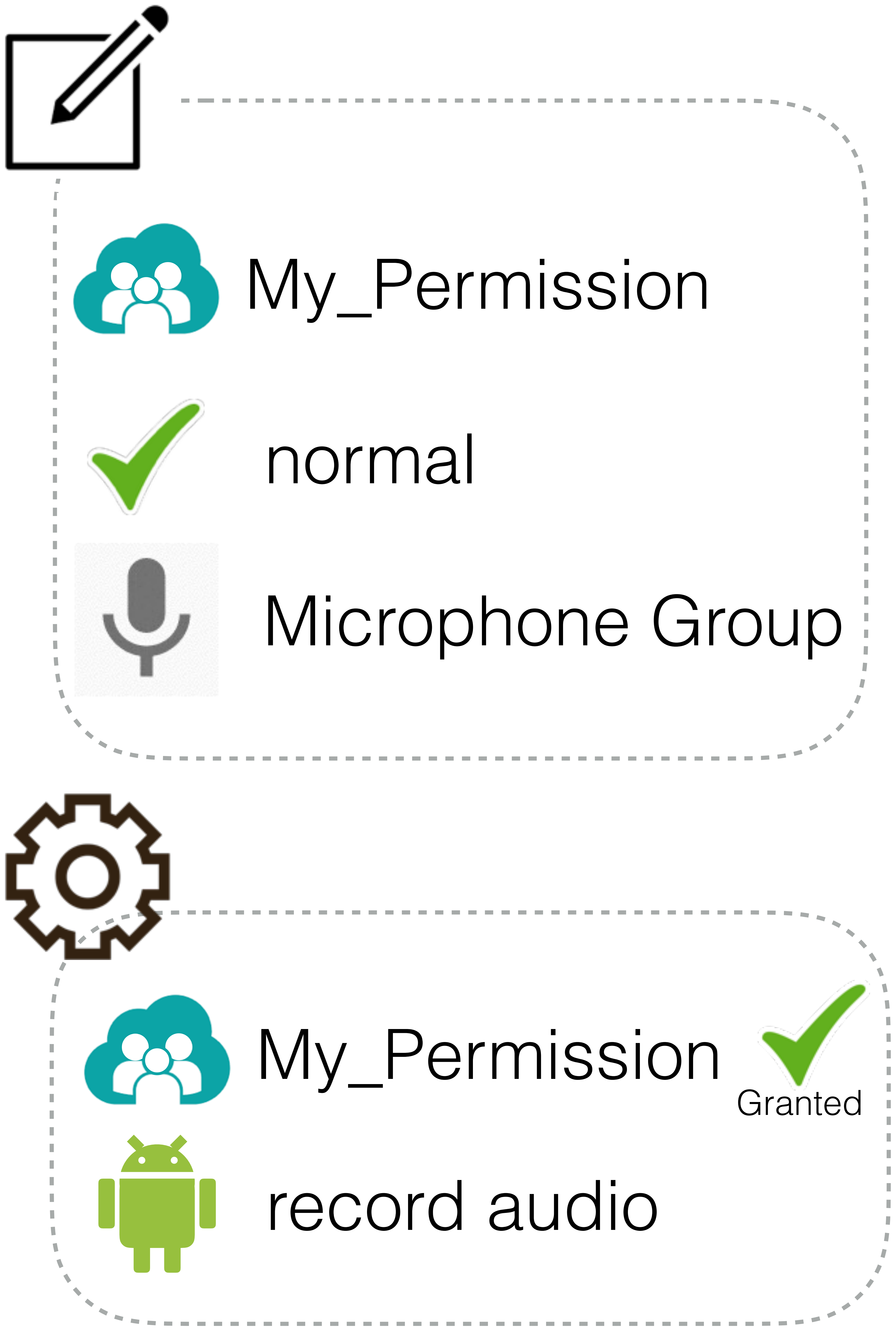
record audio



CustomPermissionAppUpdateBug

Custom permission exploit!

Allow CustomPermissionAppU... to record audio?



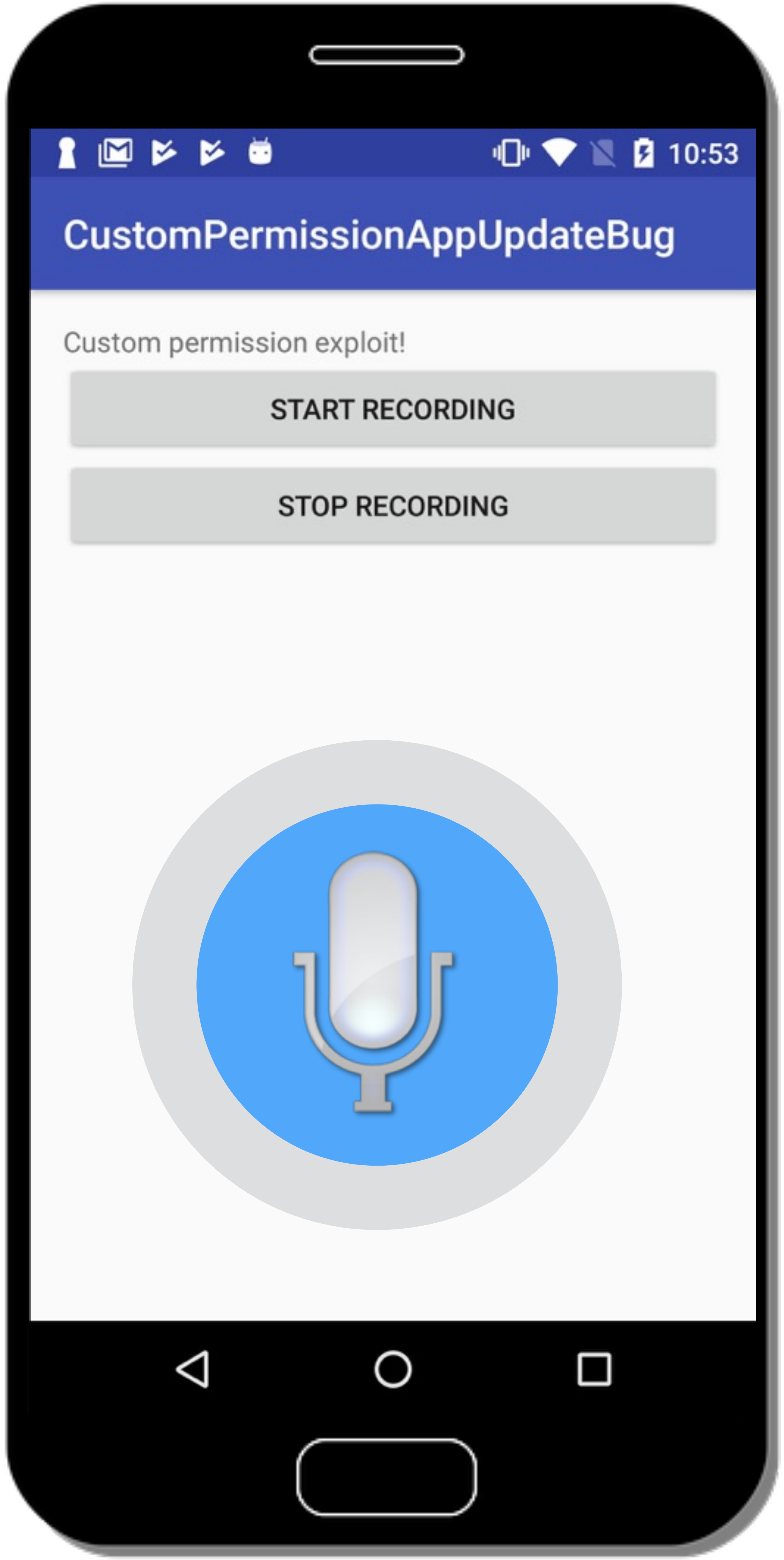
My_Permission

normal

Microphone Group

My_Permission ✓ Granted

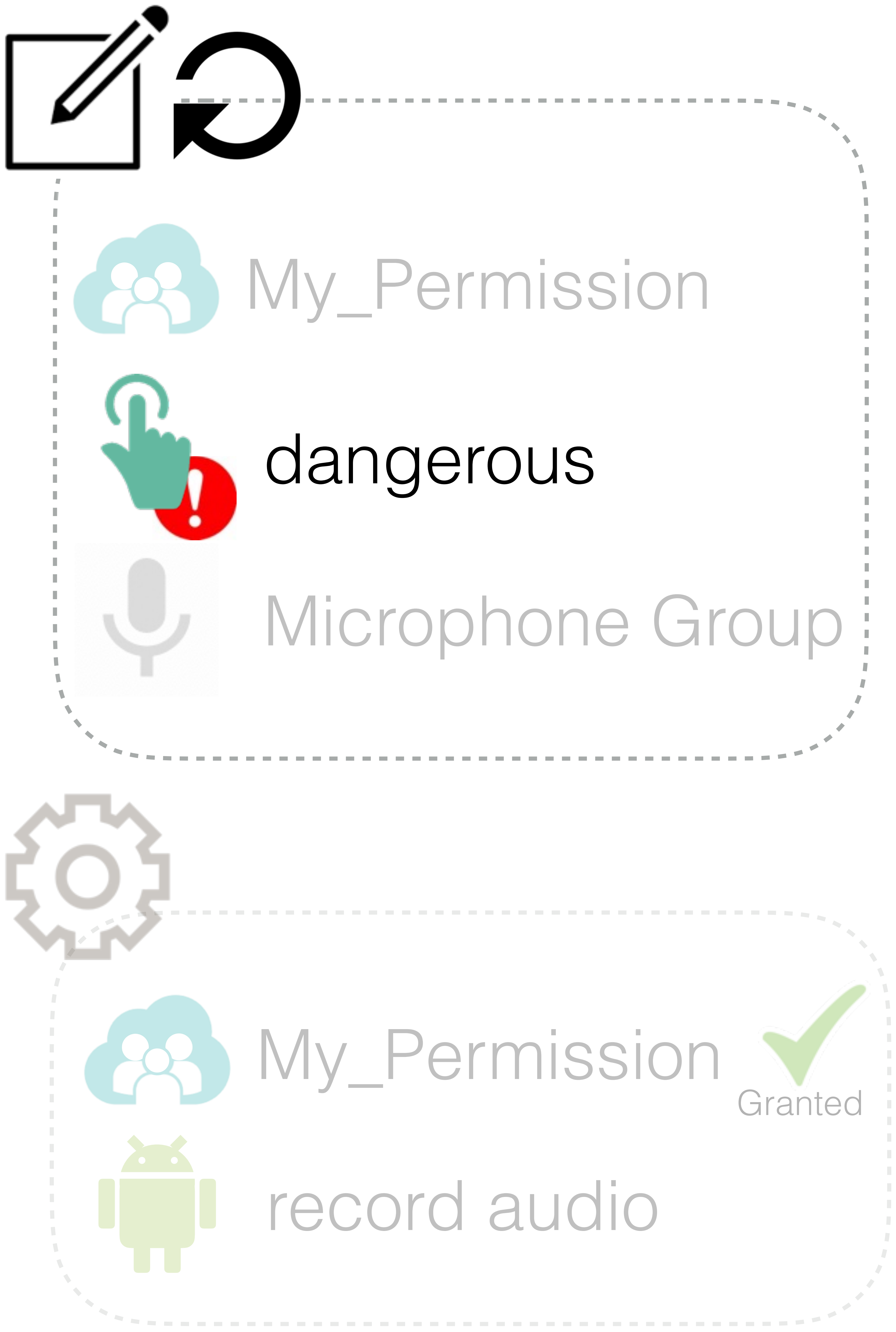
record audio

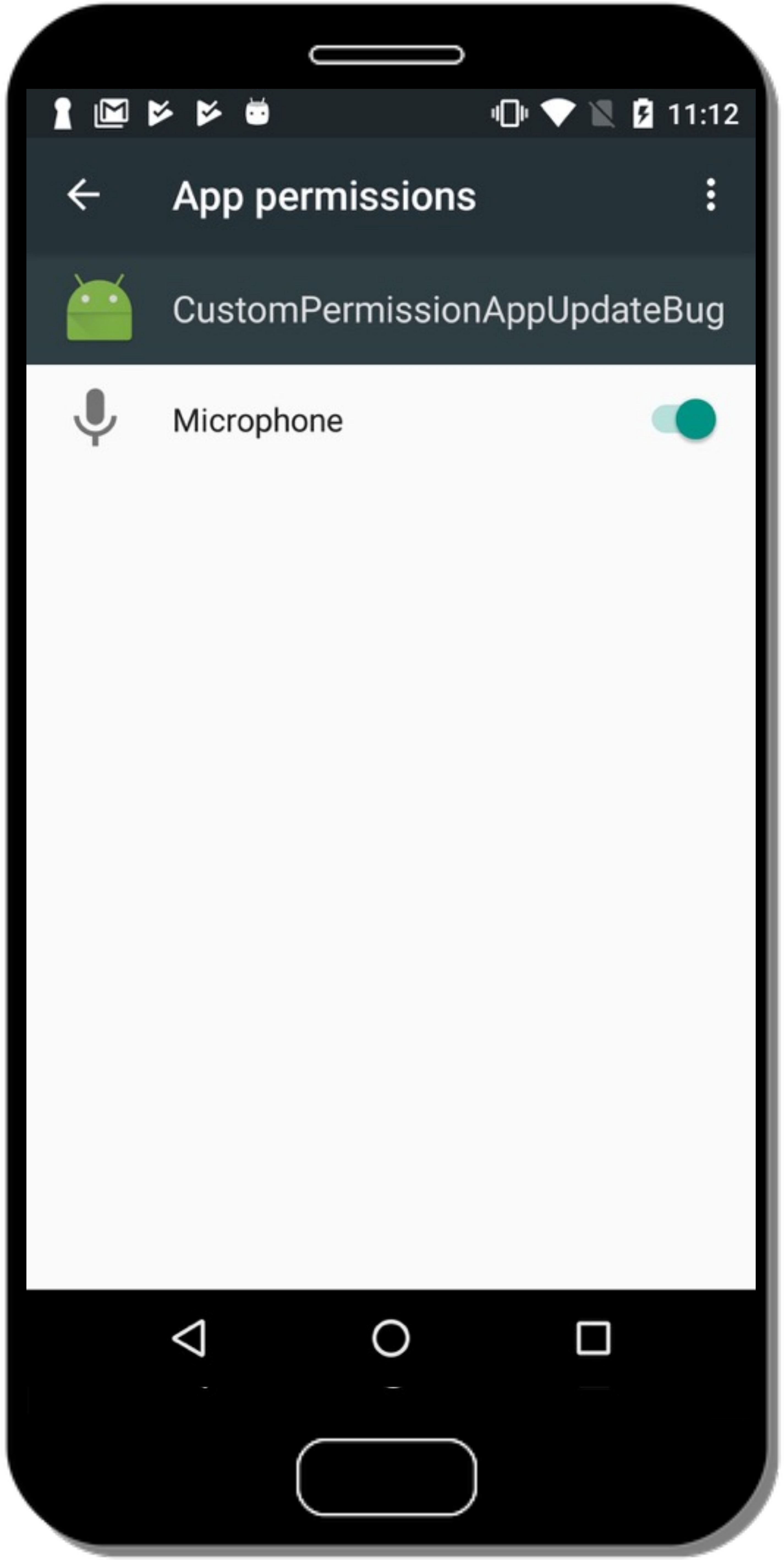


10:53

CustomPermissionAppUpdateBug

Custom permission exploit!



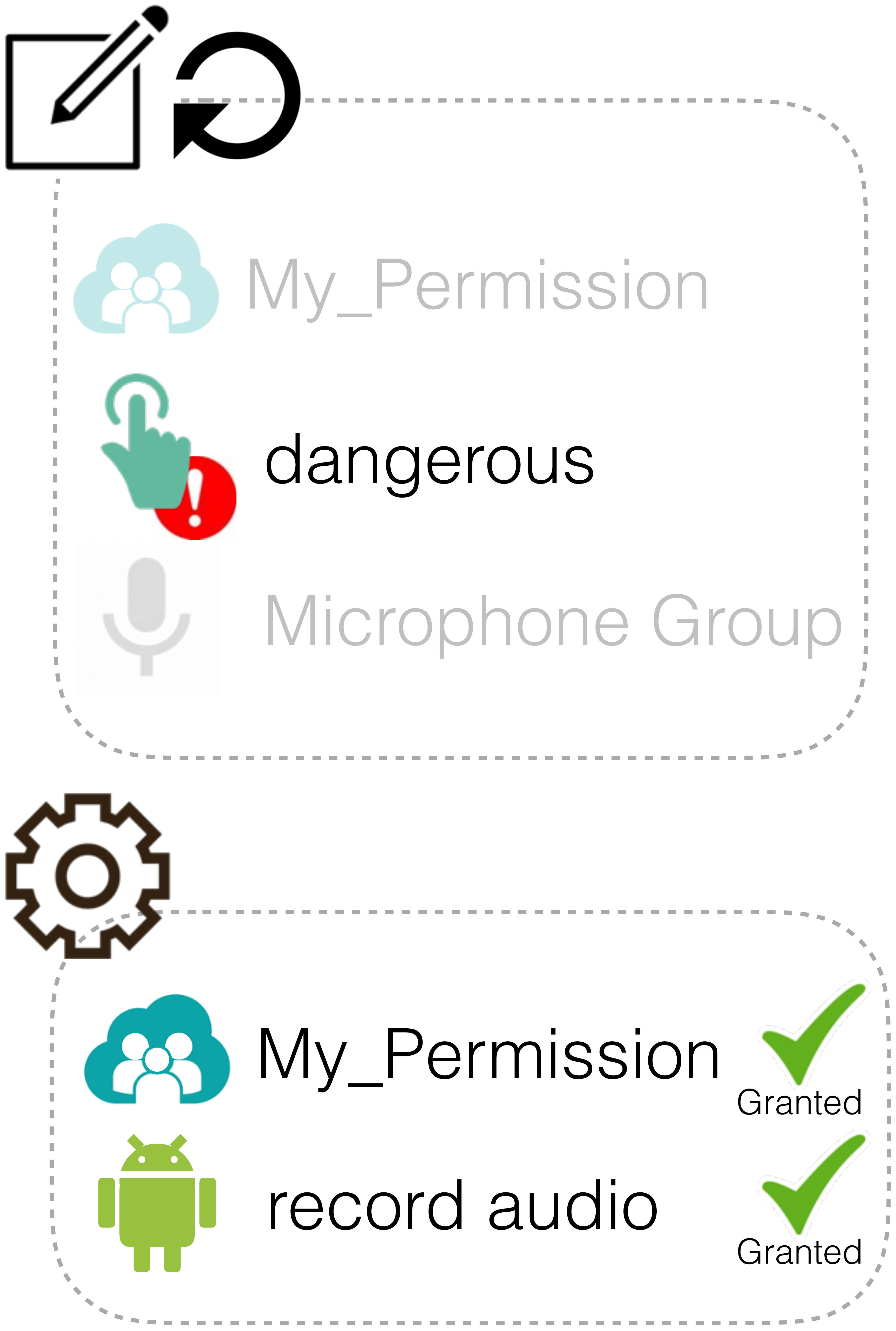


11:12

App permissions

CustomPermissionAppUpdateBug

Microphone



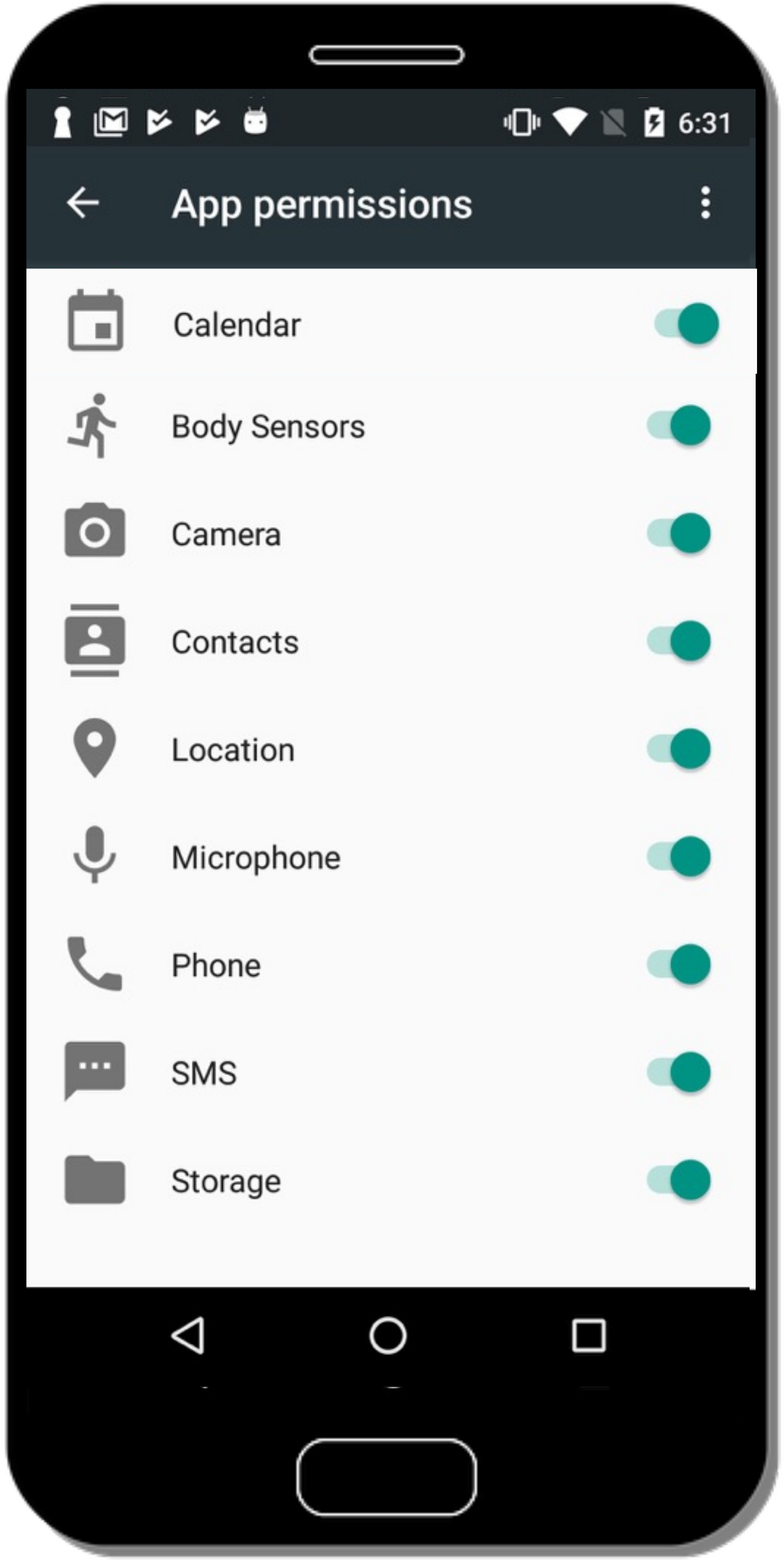
My_Permission

dangerous

Microphone Group

My_Permission ✓ Granted

record audio ✓ Granted



6:31

App permissions

Calendar

Body Sensors

Camera

Contacts

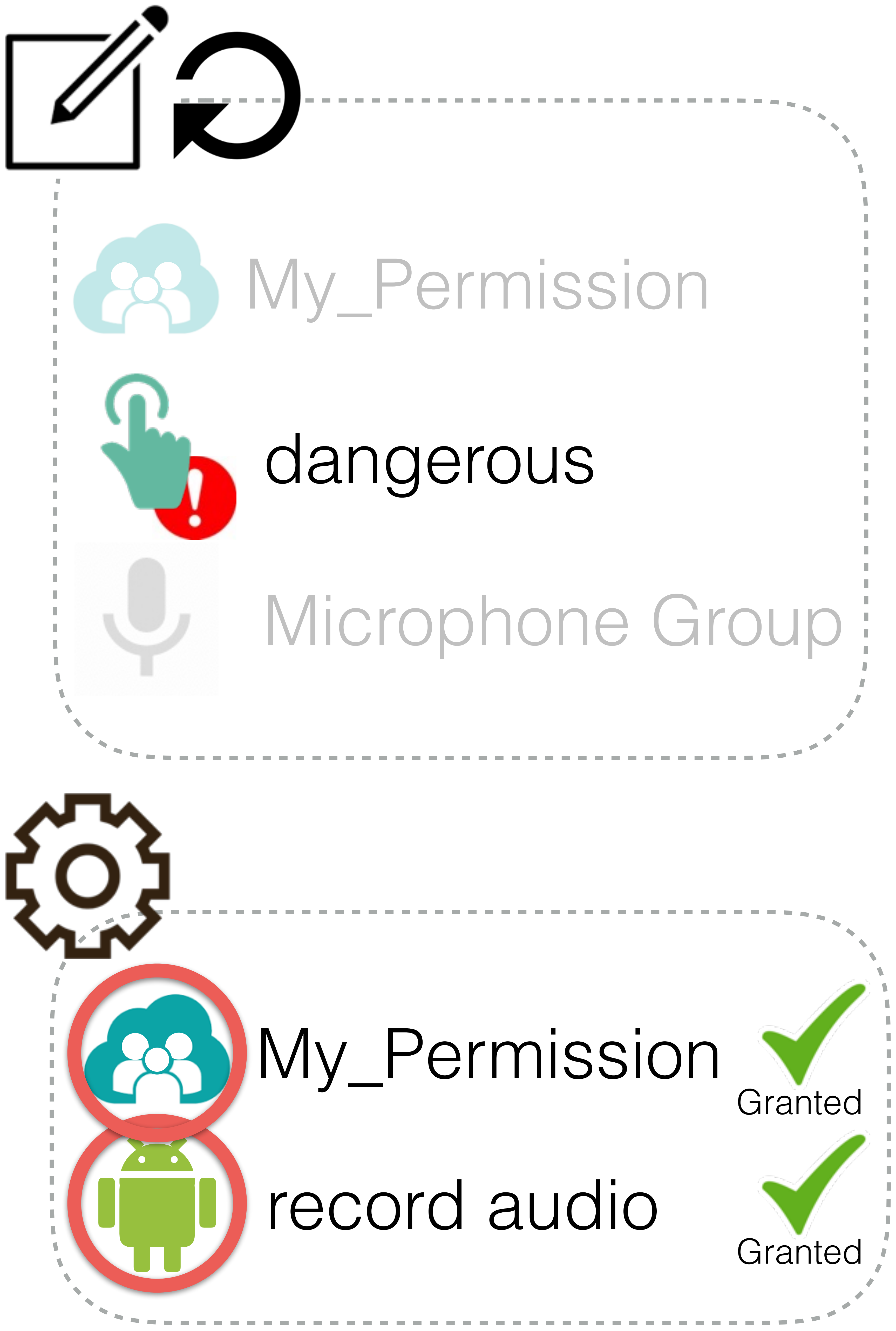
Location

Microphone

Phone

SMS

Storage



My_Permission

dangerous

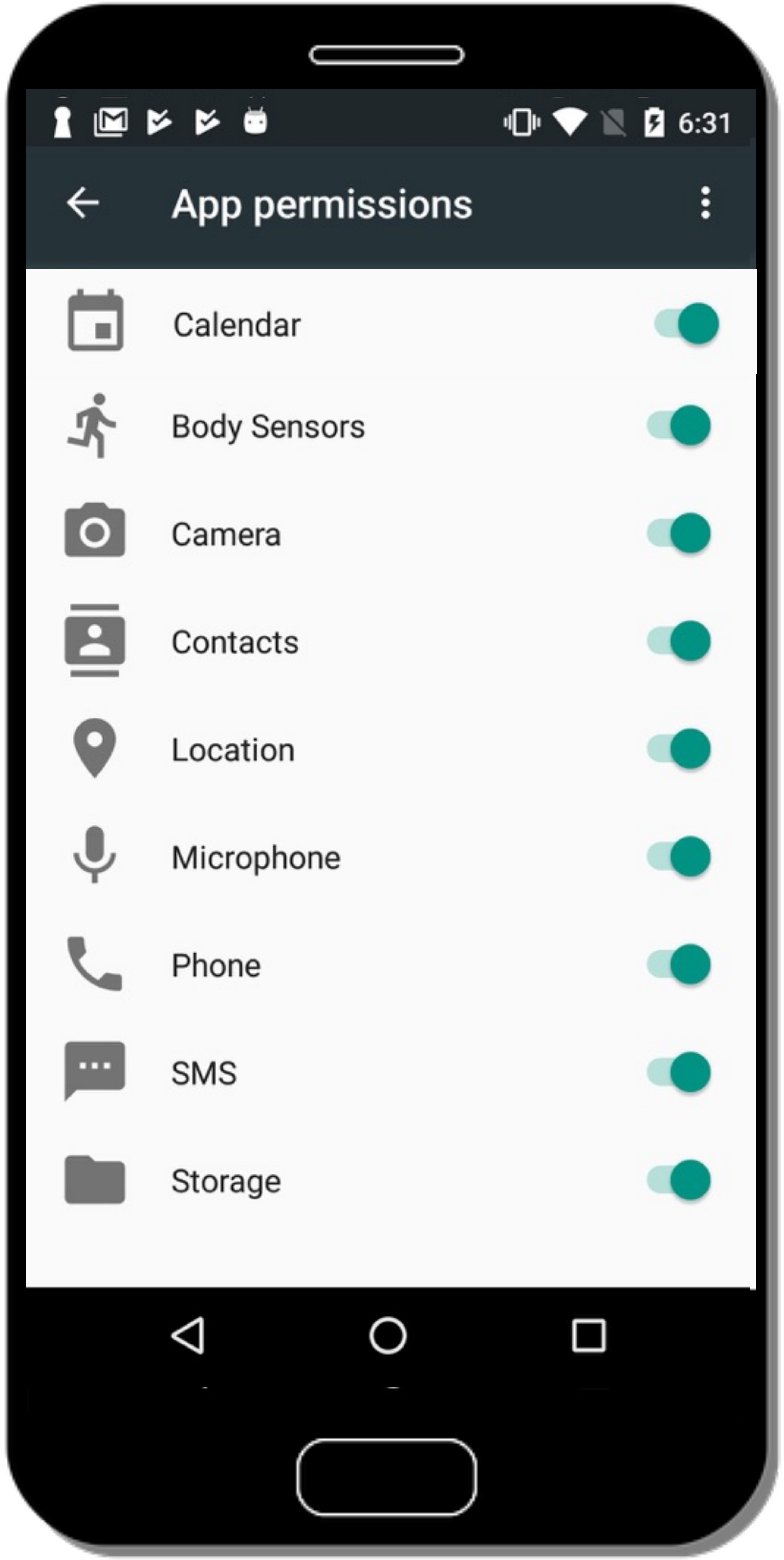
Microphone Group

My_Permission

Granted

record audio

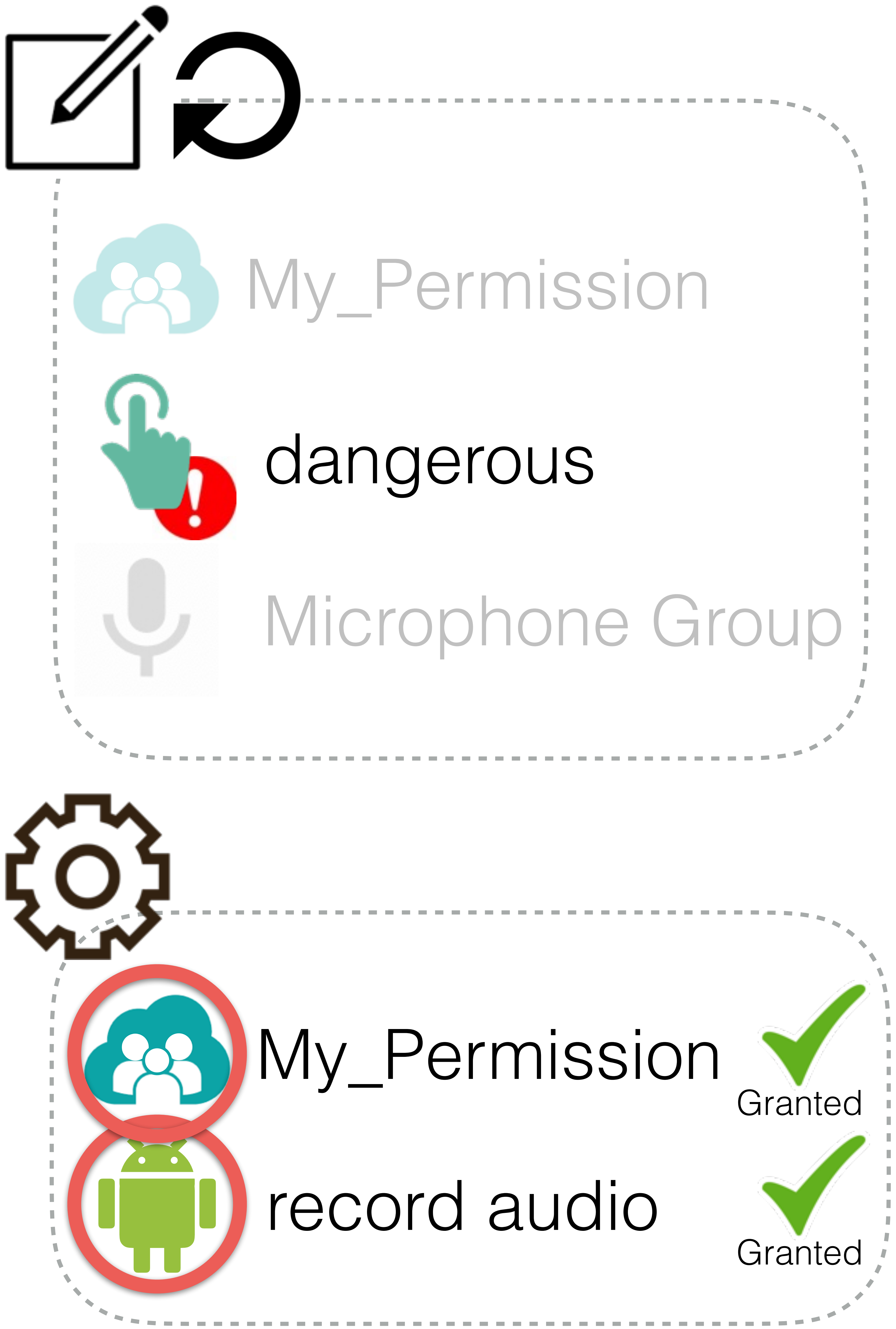
Granted



6:31

App permissions

- Calendar
- Body Sensors
- Camera
- Contacts
- Location
- Microphone
- Phone
- SMS
- Storage



My_Permission

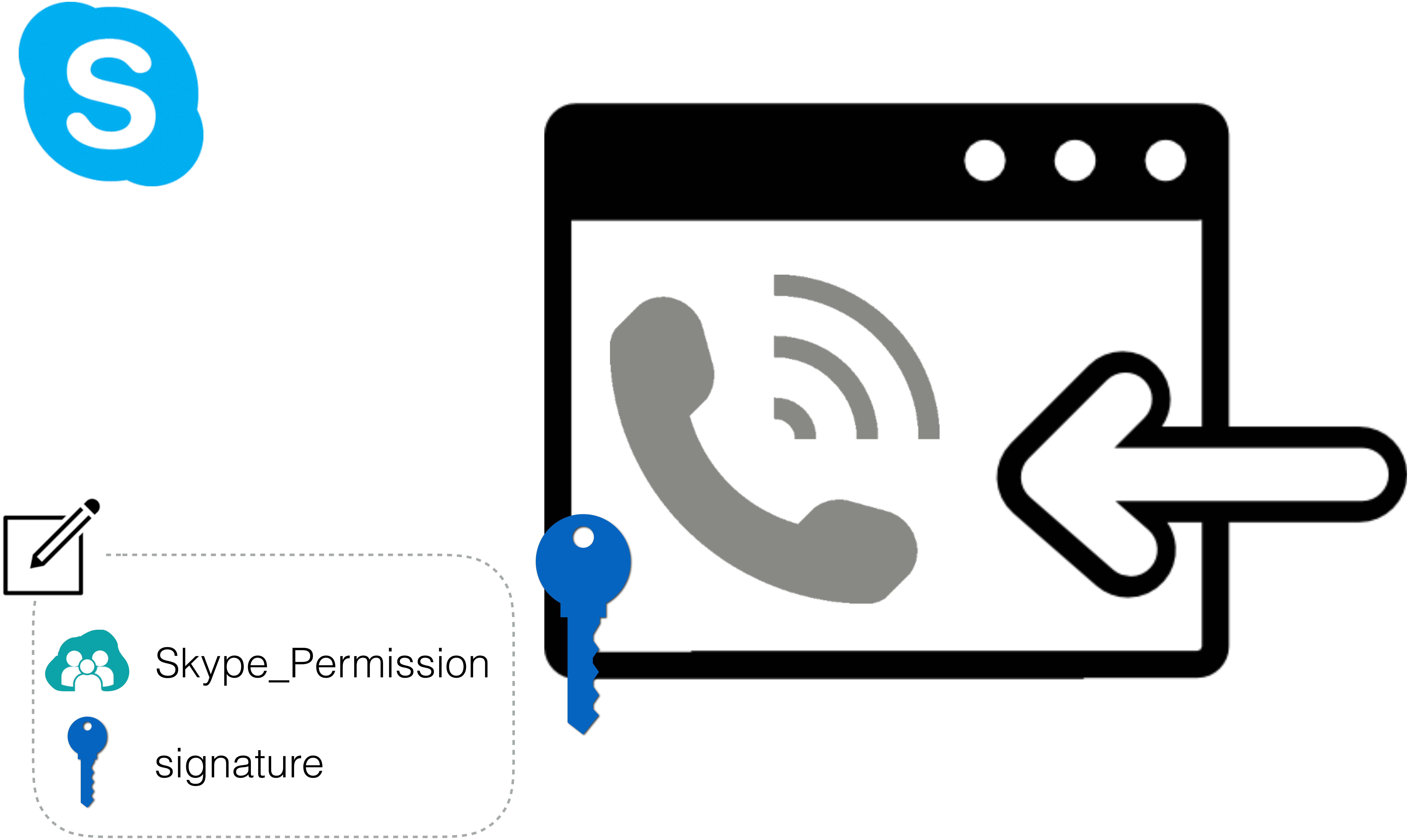
dangerous

Microphone Group

My_Permission Granted

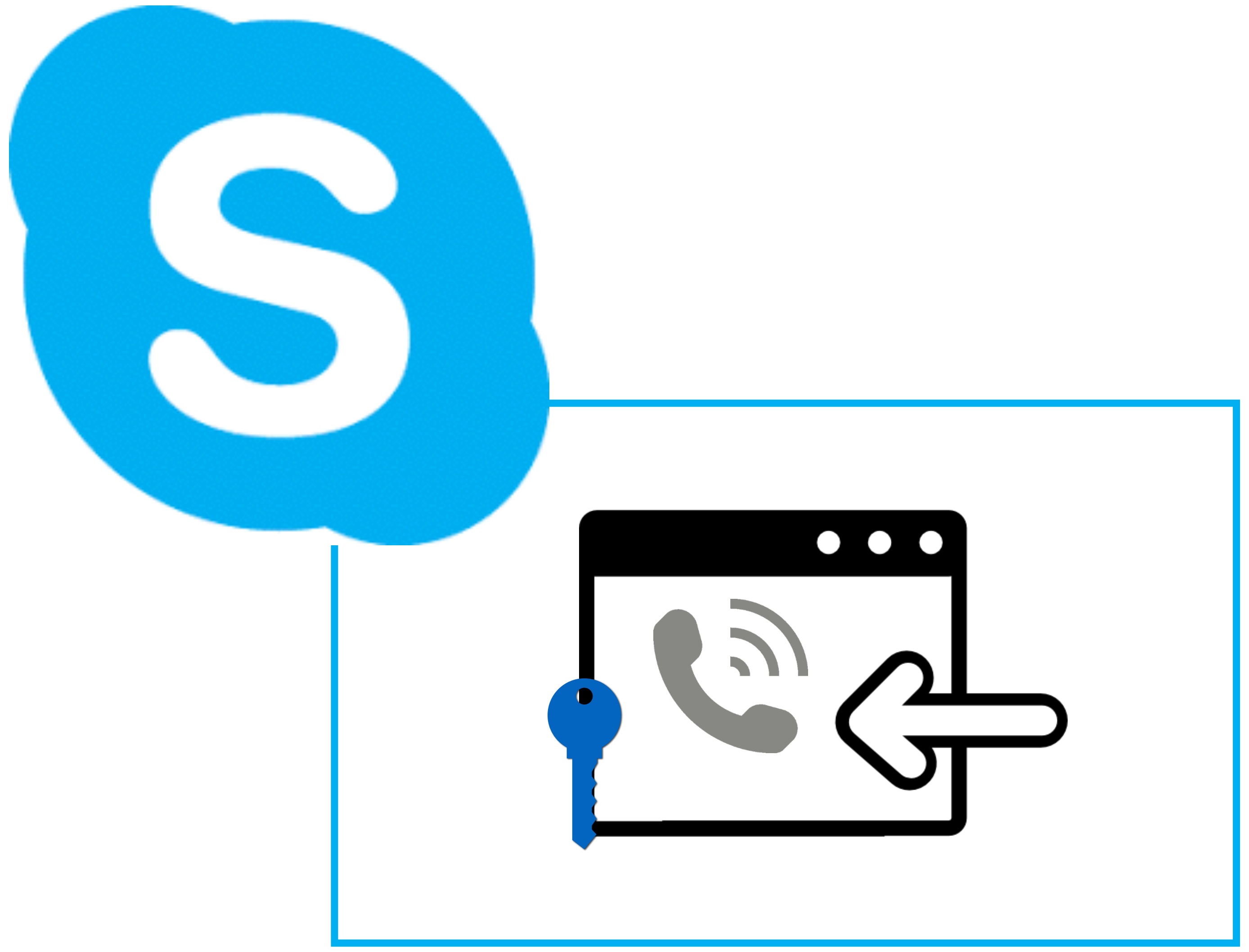
record audio Granted

⚠ No distinction between
custom permissions owners



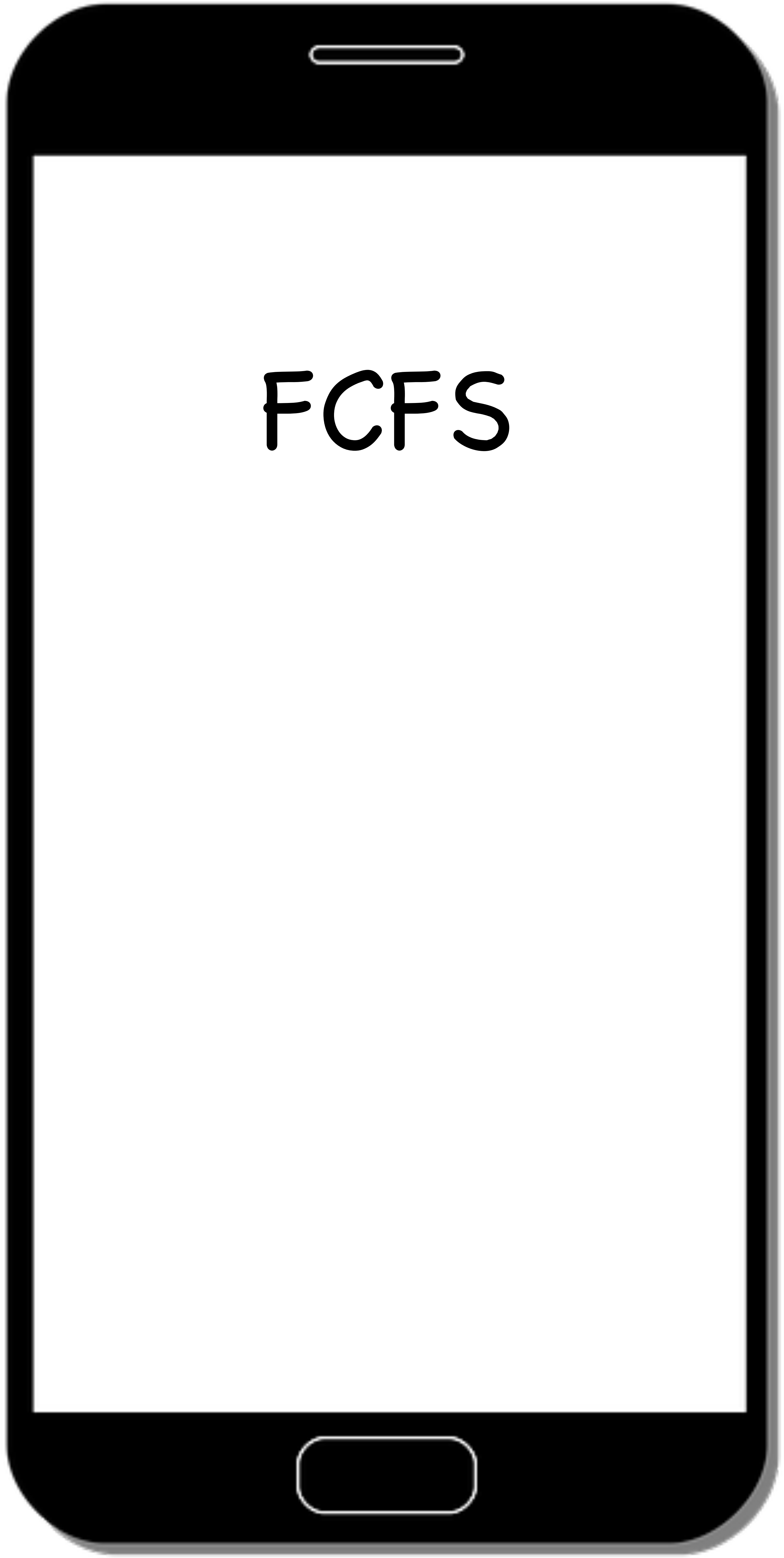
Skype_Permission

signature



Skype_Permission

signature

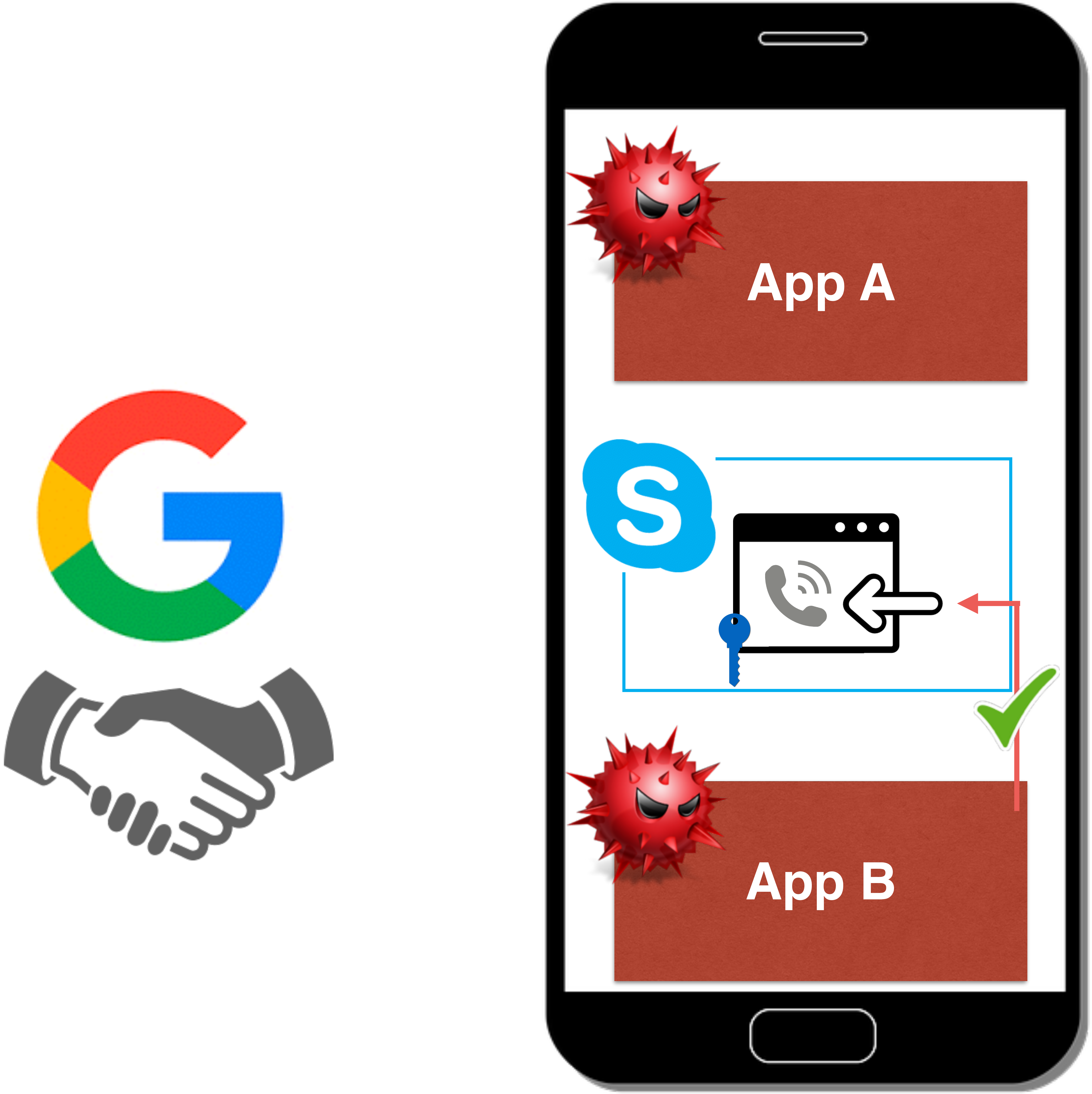


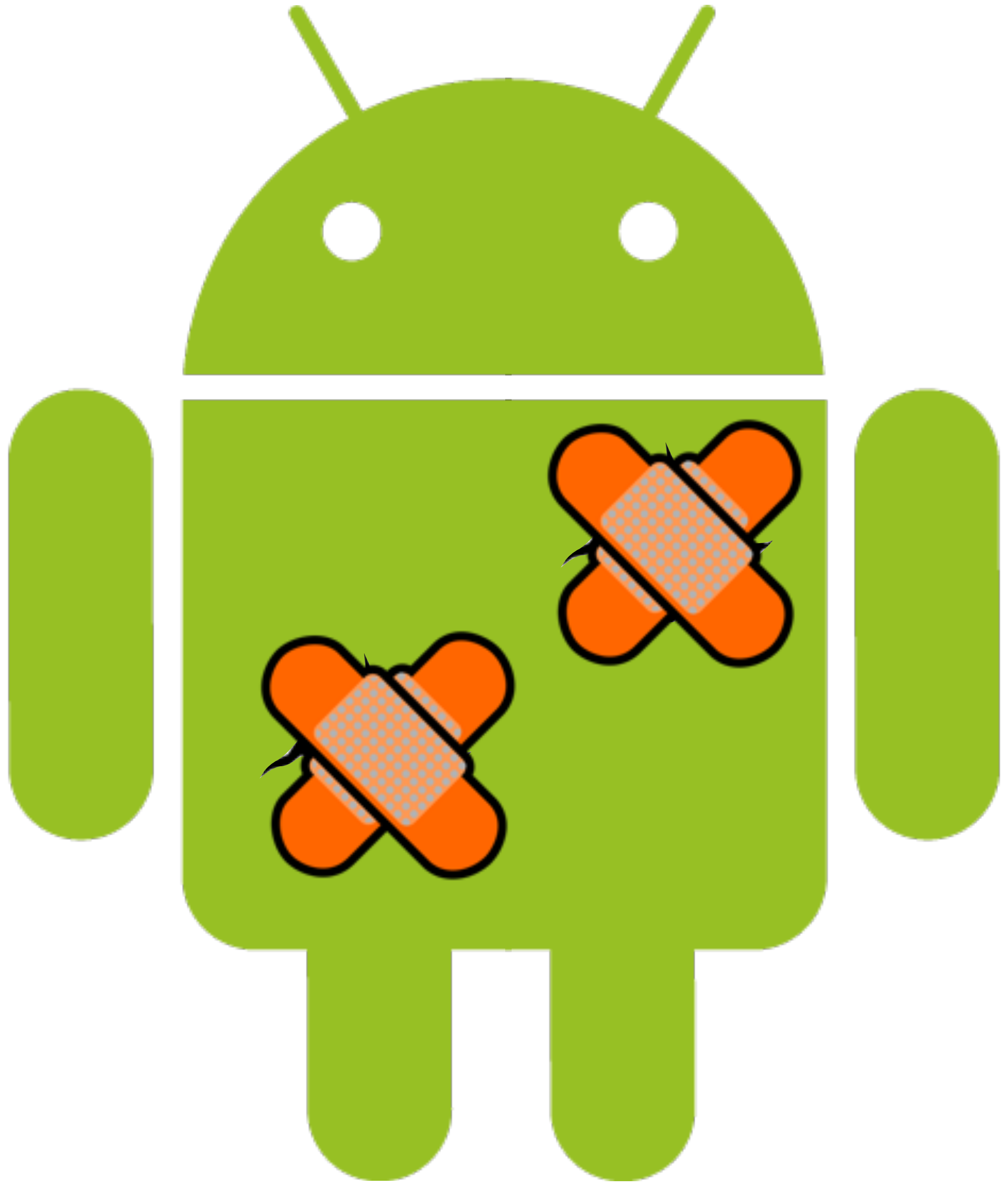
FCFS

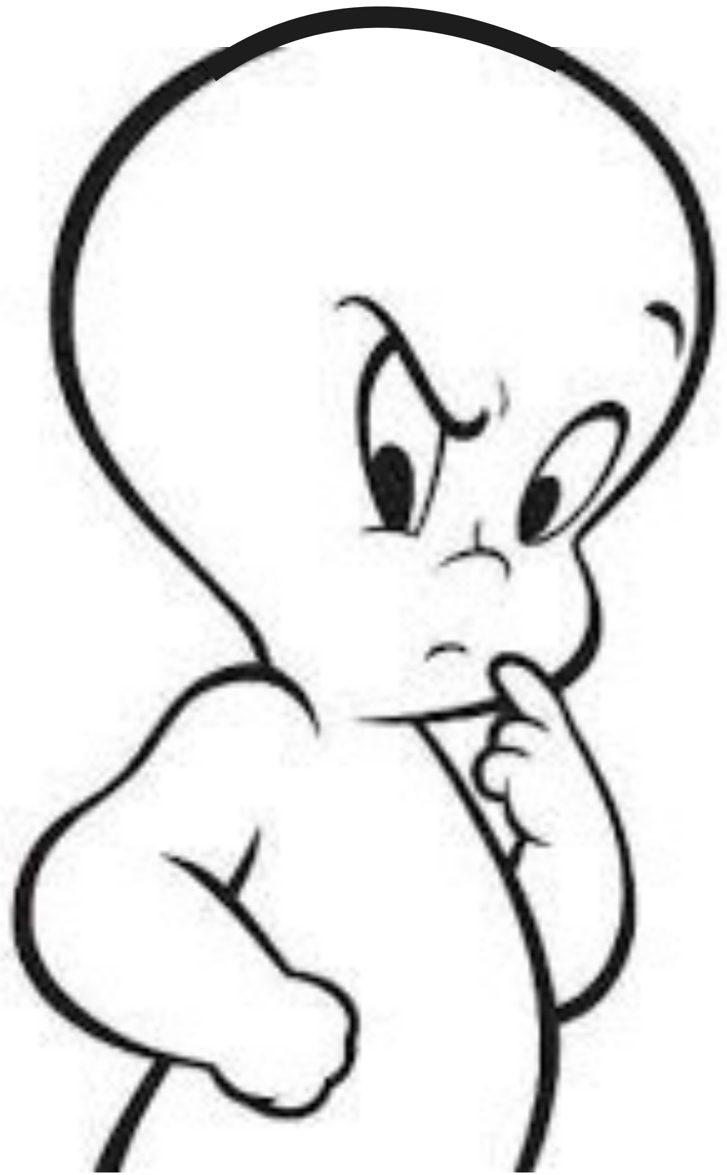
App A
App B
Skype_Permission
dangerous
Skype_Permission
Granted
Skype_Permission
signature

App A
Skype_Permission
dangerous
Skype_Permission
signature
App B
Skype_Permission
Granted

App A
Skype_Permission
dangerous
Skype_Permission
signature
App B
Skype_Permission
Granted


App A
App B





cusper

“considered to have been born on a cusp between significant generations”

cusper

“considered to have been born on a cusp between significant generations” android

cusper

Decisions made by principals outside the framework’s Trusted Compute Base affect enforcement at runtime

—> privilege escalation

→ Systematically addresses the lack of **separation** of trust by decoupling system from custom permissions

Custom permissions are claimed on a FCFS basis

—> spoofing

→ Provides a backward-compatible OS-level naming convention for tracking **ownership** of custom permissions

Software testing

→ **Formally verified** to be correct

android	cusper
Decisions made by principals outside the framework’s Trusted Compute Base affect enforcement at runtime —> privilege escalation	Systematically addresses the lack of **separation** of trust by decoupling system from custom permissions
Custom permissions are claimed on a FCFS basis —> spoofing	Provides a backward-compatible OS-level naming convention for tracking **ownership** of custom permissions
Software testing	**Formally verified** to be correct

android

cusper

Decisions made by principals outside the framework's Trusted Compute Base affect enforcement at runtime

—> privilege escalation

→ Systematically addresses the lack of **separation** of trust by decoupling system from custom permissions

Custom permissions are claimed on a FCFS basis

—> spoofing

→ Provides a backward-compatible OS-level naming convention for tracking **ownership** of custom permissions

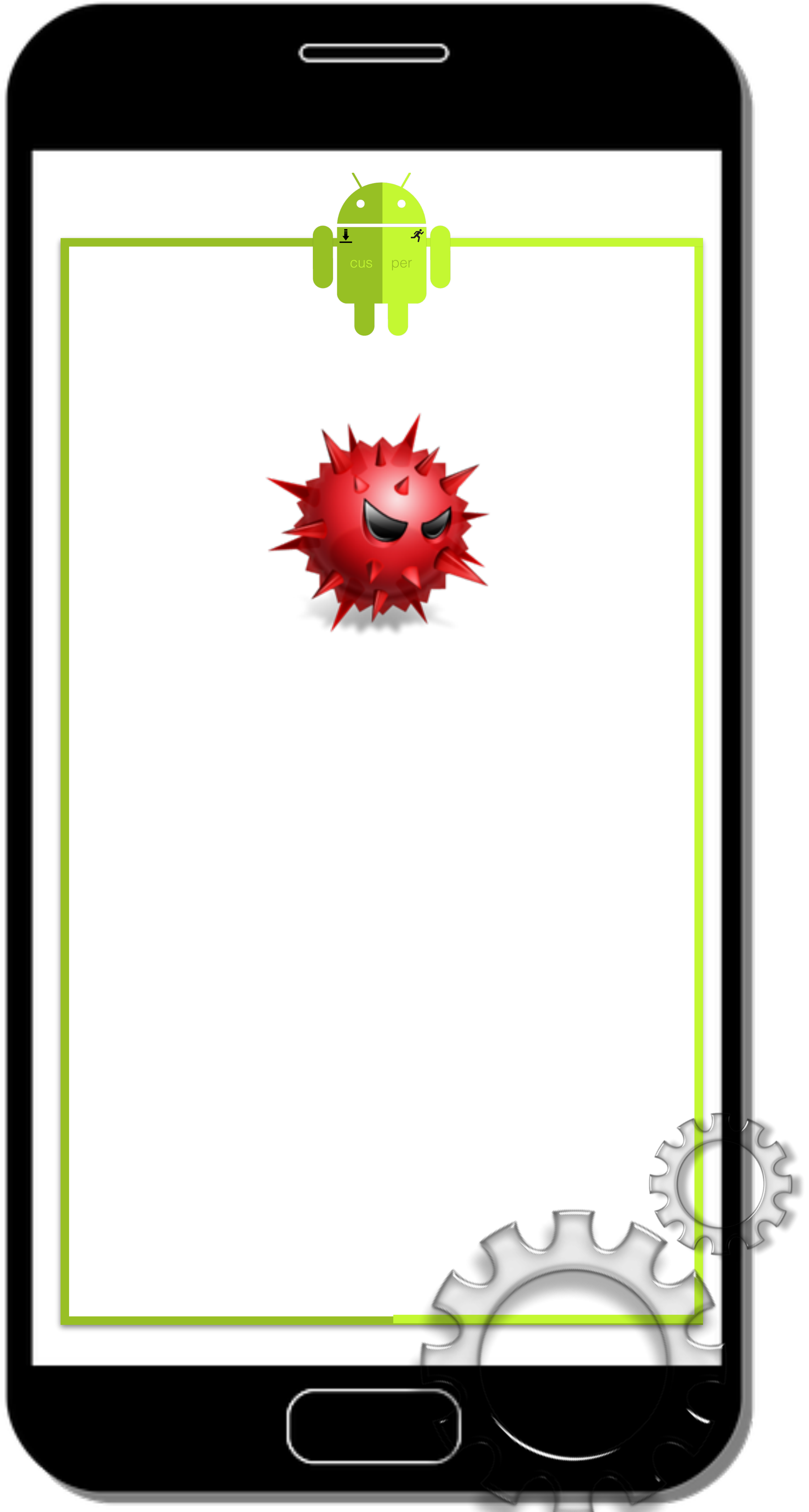
▶ Software testing

→ **Formally verified** to be correct

Cusper enhancements

declaring a custom permission

Skype_Permission

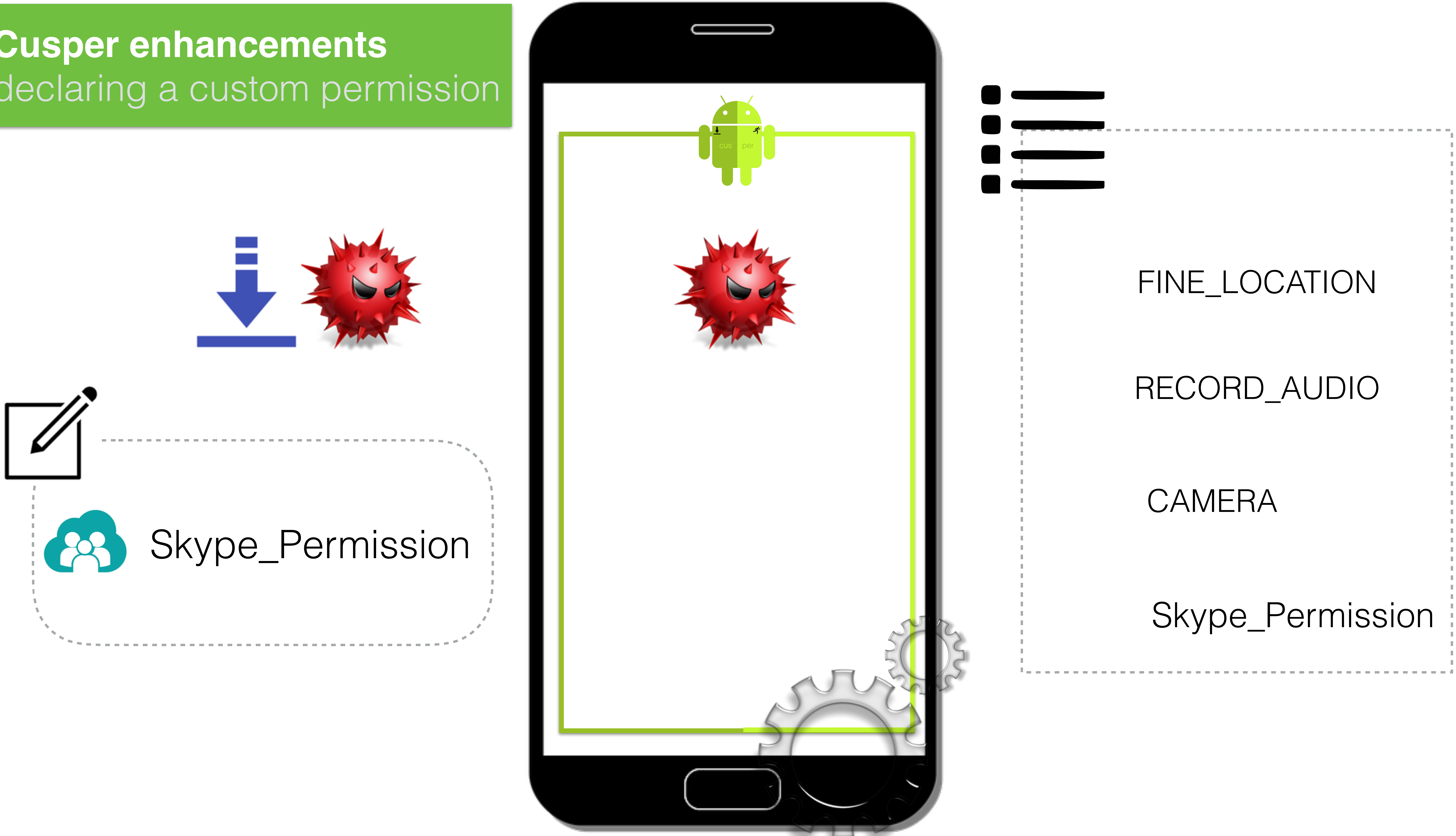


FINE_LOCATION

RECORD_AUDIO

CAMERA

Cusper enhancements
declaring a custom permission



Skype_Permission

FINE_LOCATION

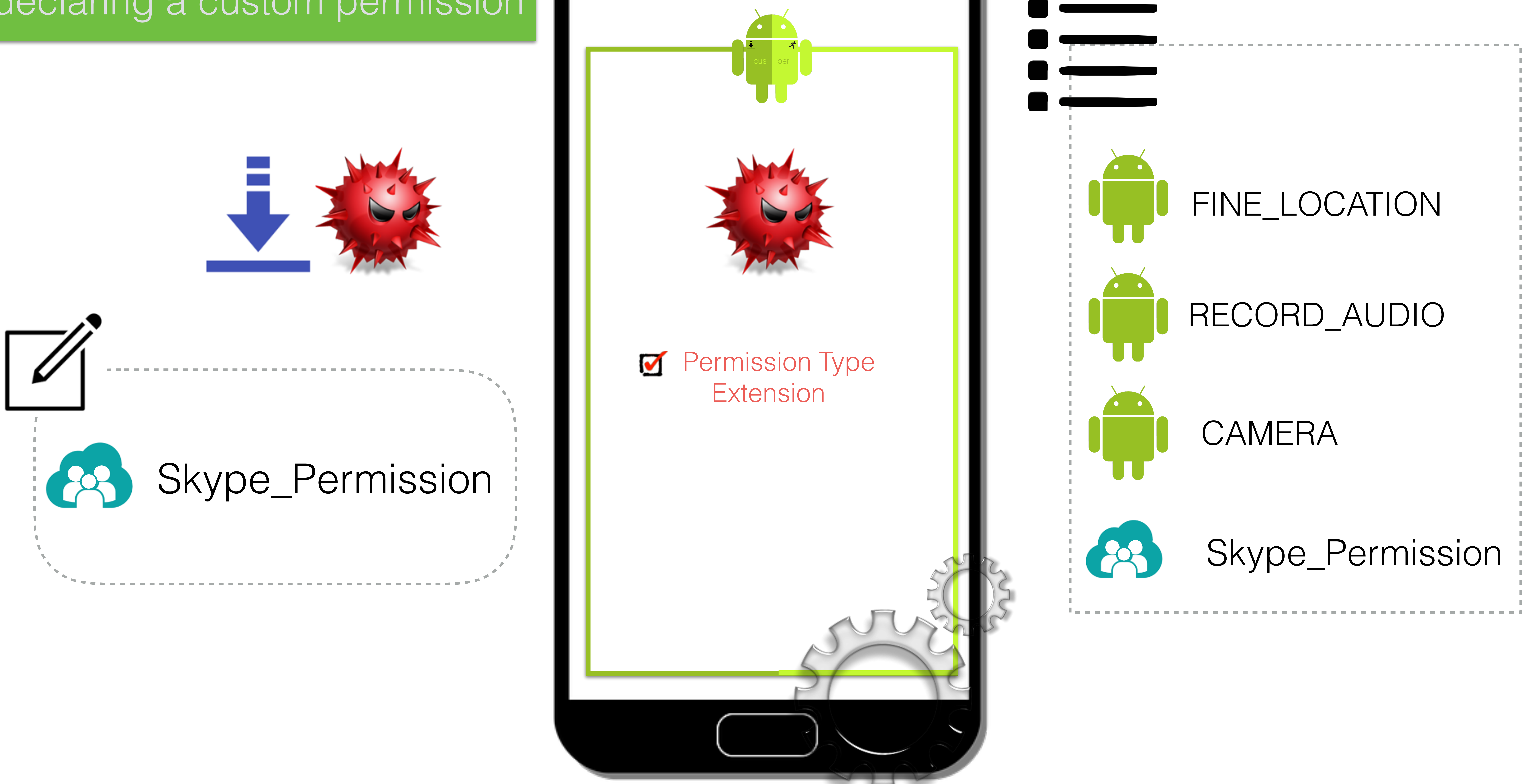
RECORD_AUDIO

CAMERA

Skype_Permission

Cusper enhancements

declaring a custom permission



Skype_Permission

☑ Permission Type Extension

FINE_LOCATION

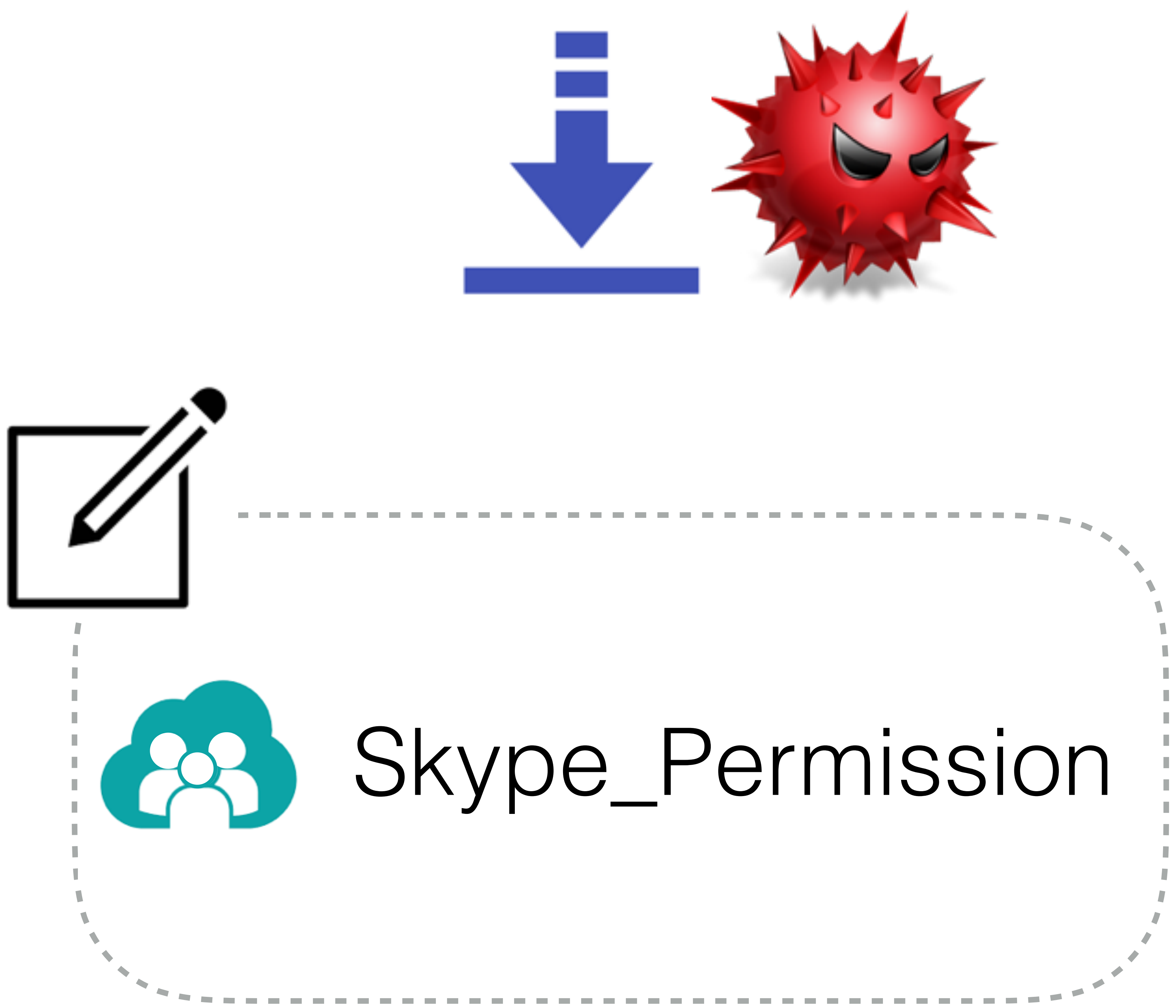
RECORD_AUDIO

CAMERA

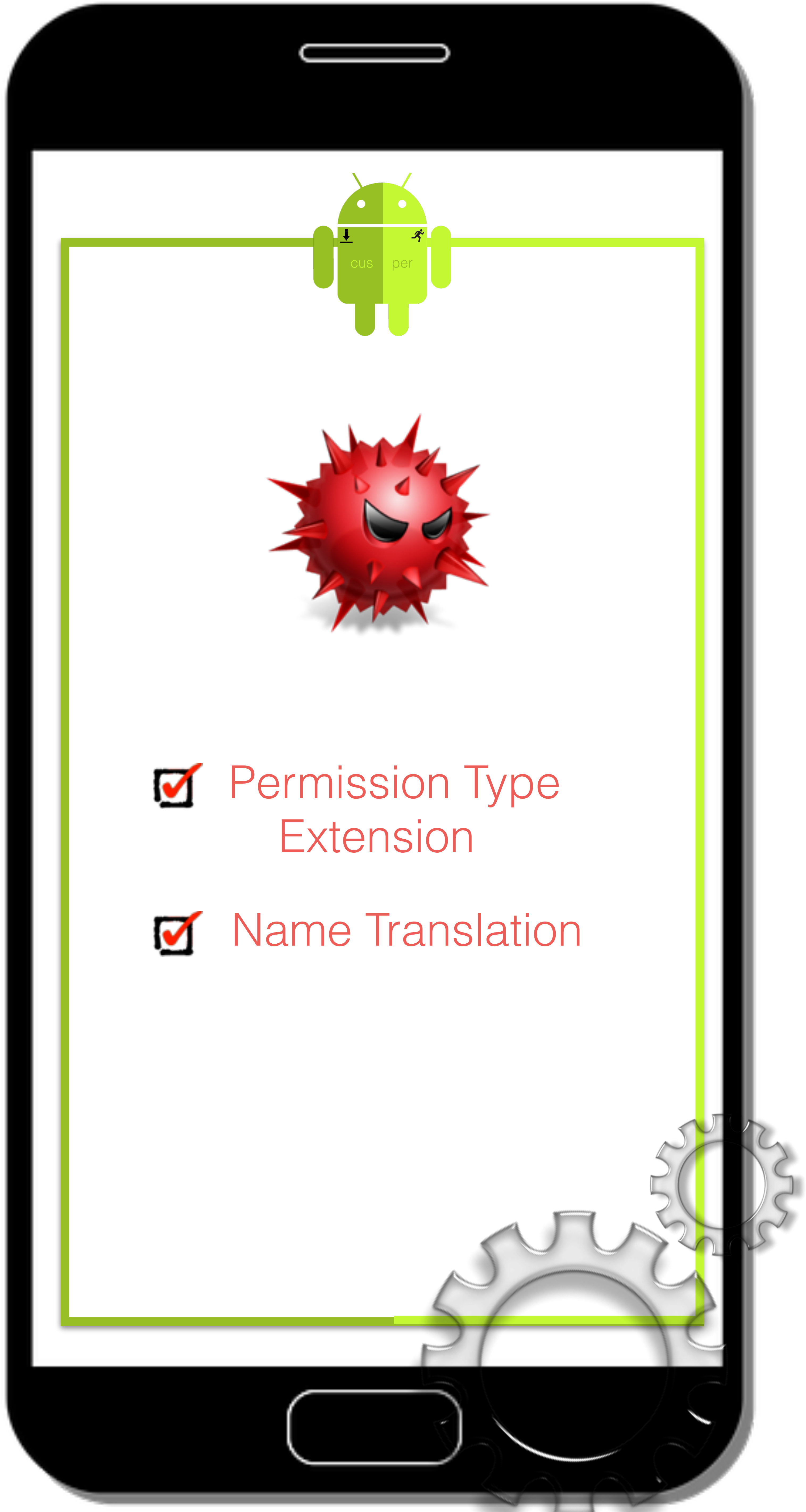
Skype_Permission

Cusper enhancements

declaring a custom permission

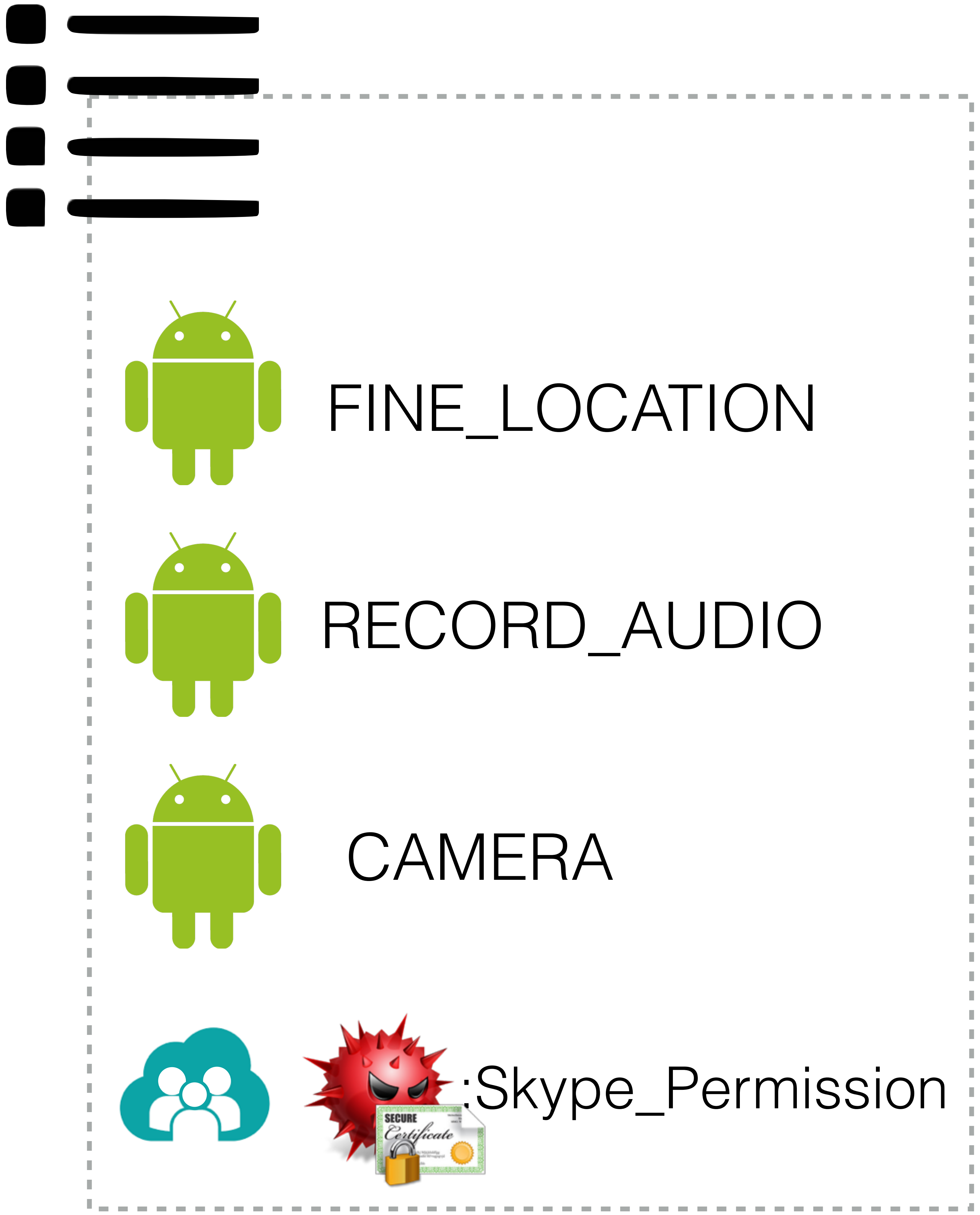


Skype_Permission



☑ Permission Type Extension

☑ Name Translation



FINE_LOCATION

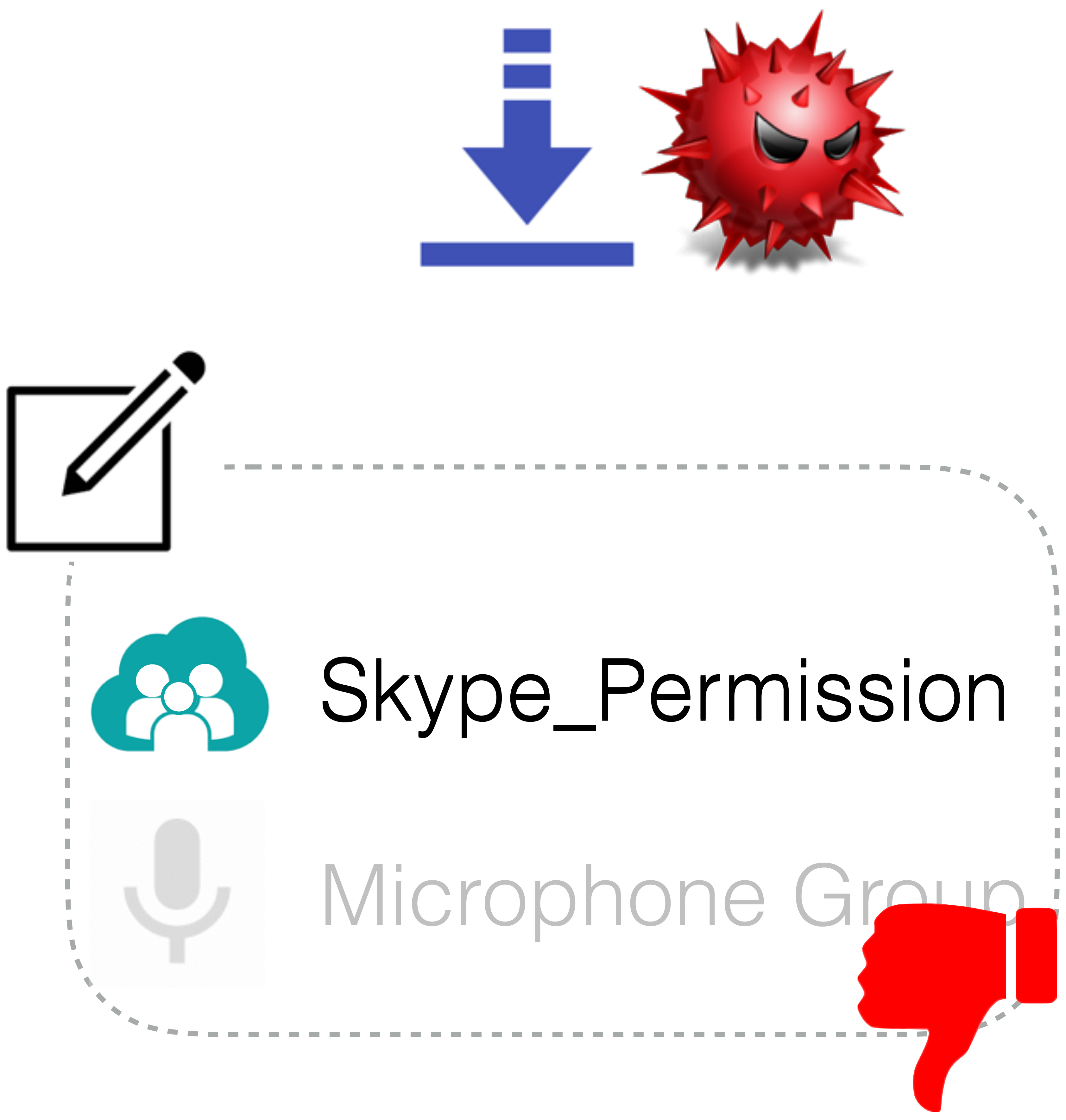
RECORD_AUDIO

CAMERA

:Skype_Permission

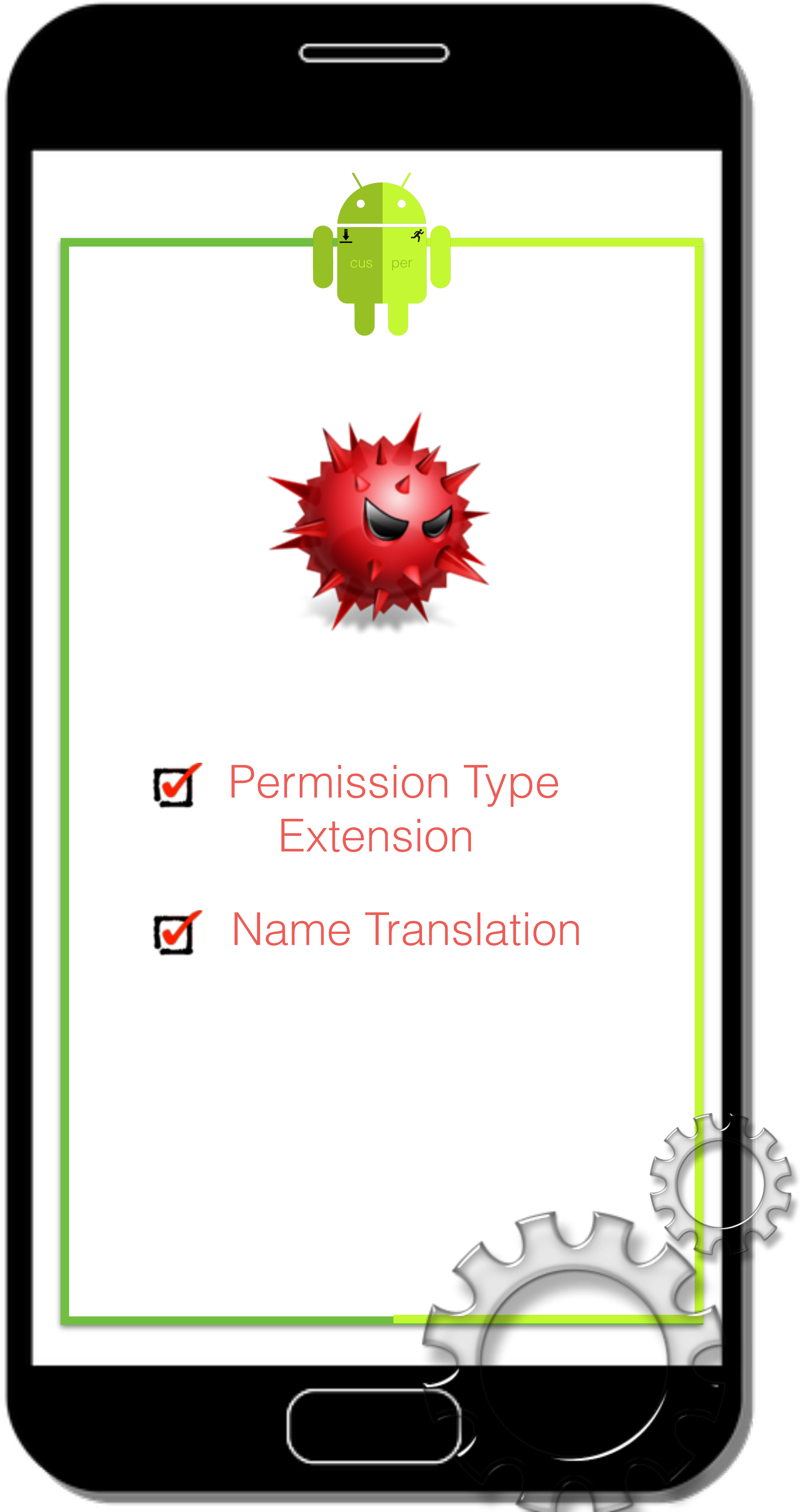
Cusper enhancements

declaring a custom permission



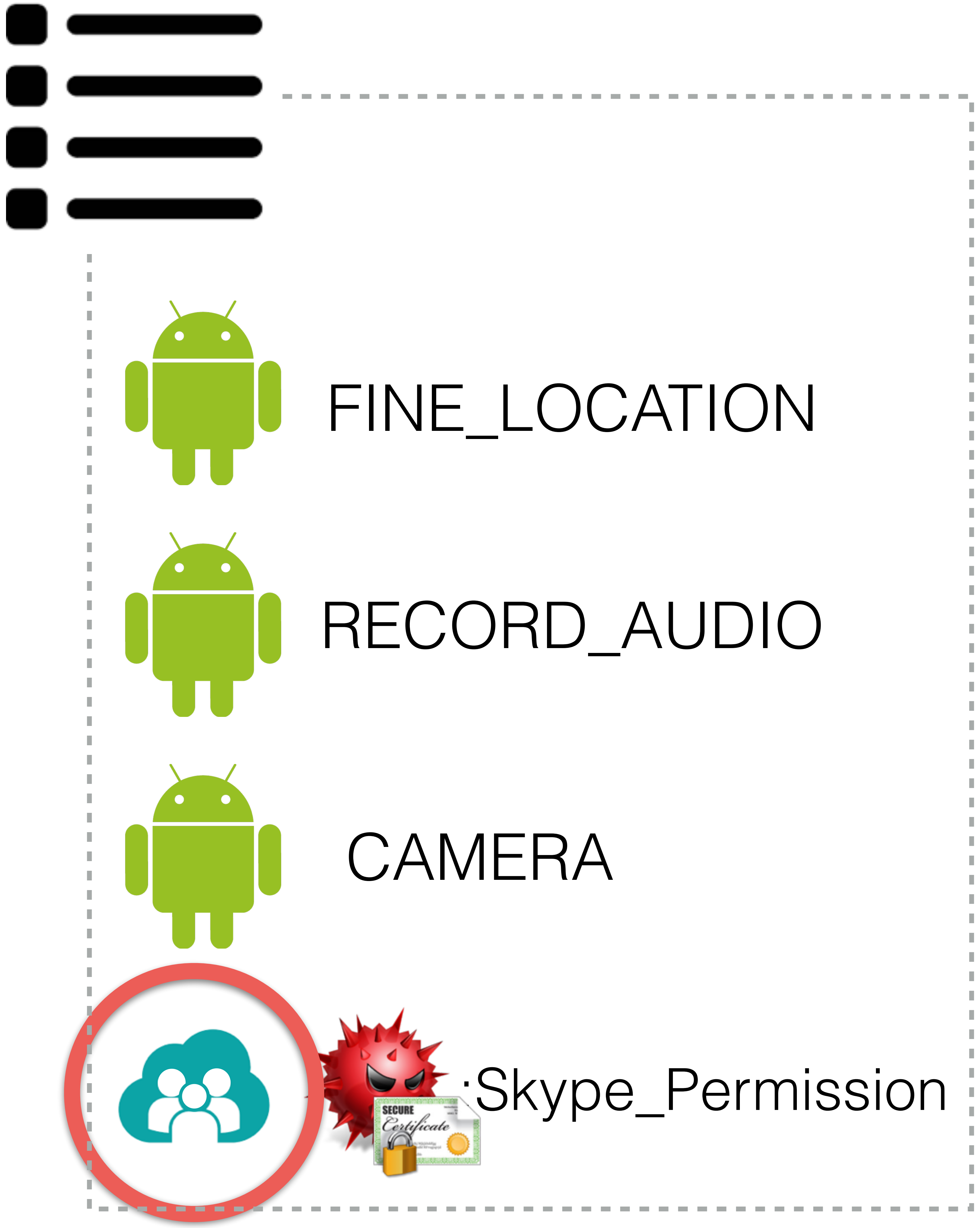
Skype_Permission

Microphone Group



☑ Permission Type Extension

☑ Name Translation



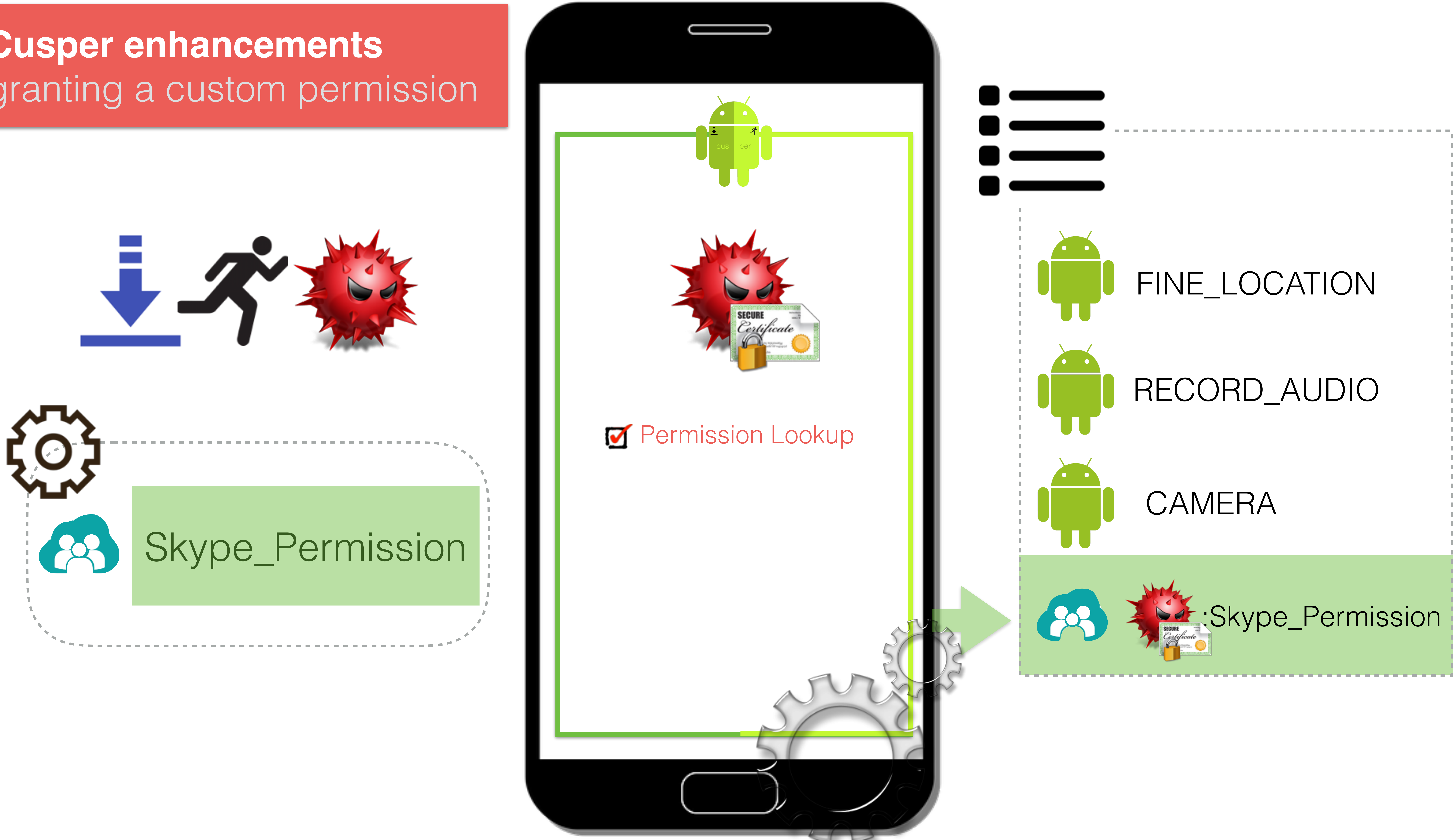
FINE_LOCATION

RECORD_AUDIO

CAMERA

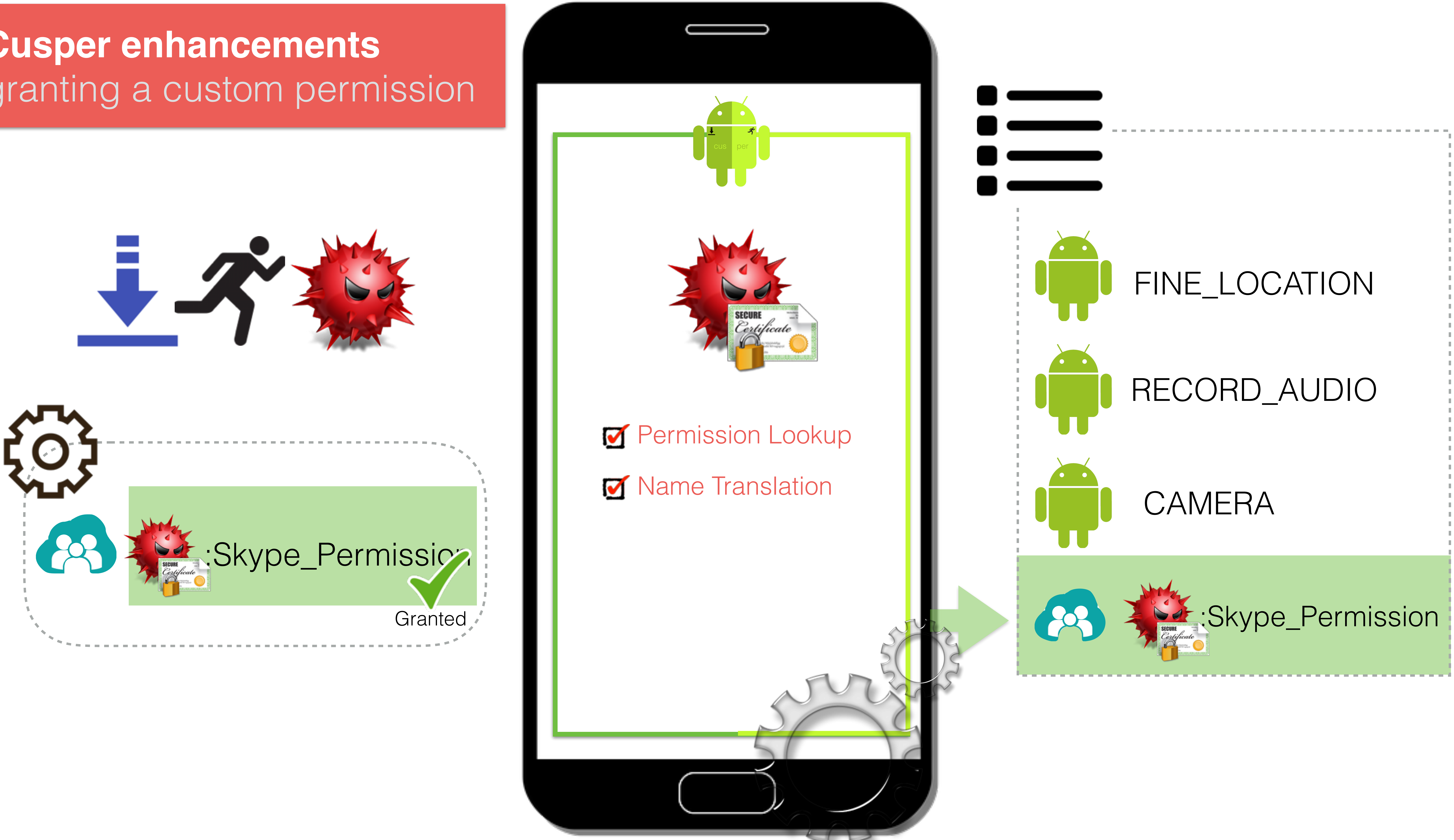
:Skype_Permission

Cusper enhancements
granting a custom permission



Cusper enhancements

granting a custom permission



☑ Permission Lookup

☑ Name Translation

:Skype_Permission

Granted

FINE_LOCATION

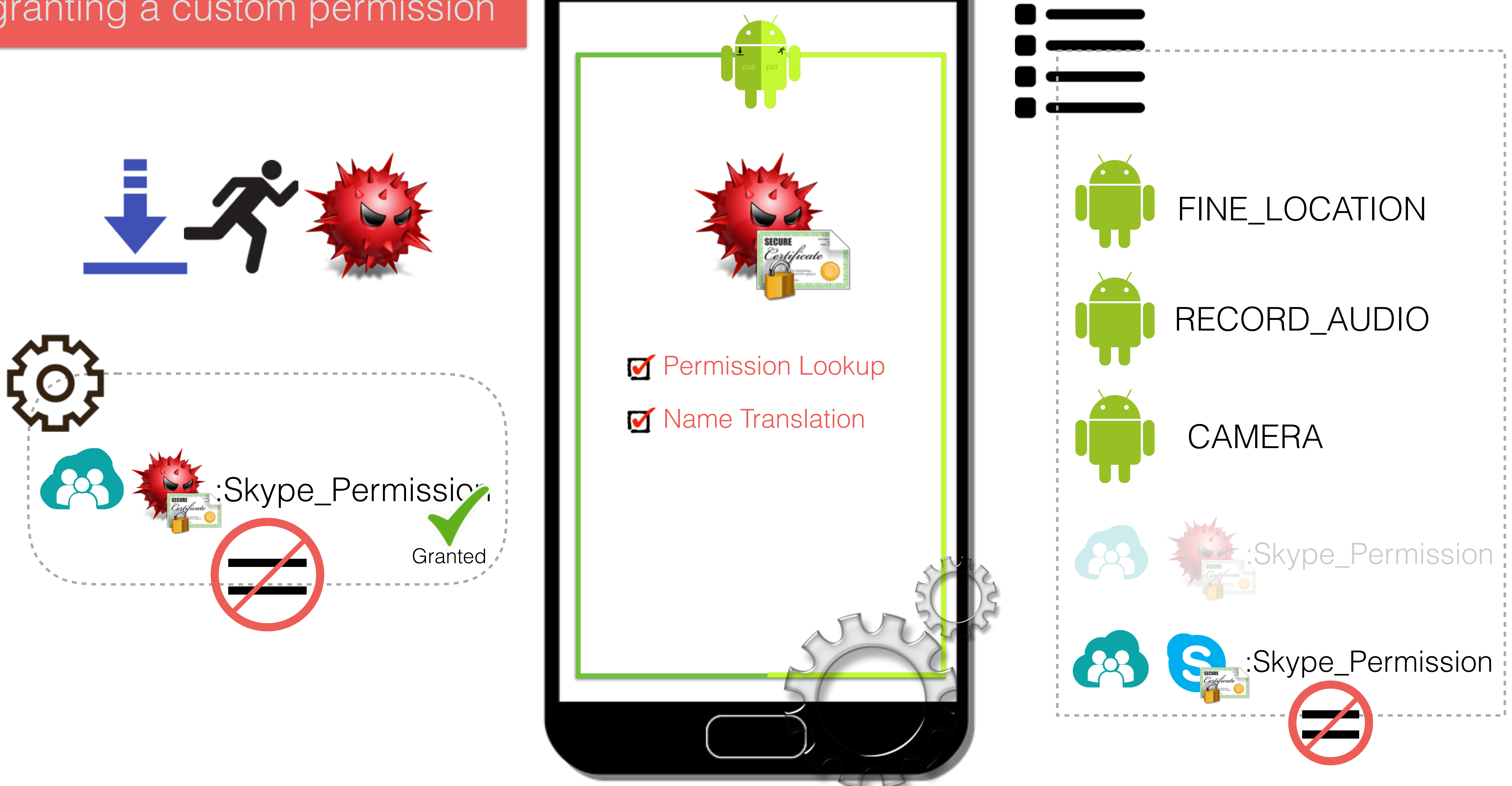
RECORD_AUDIO

CAMERA

:Skype_Permission

Cusper enhancements

granting a custom permission



:Skype_Permission

Granted

☑ Permission Lookup

☑ Name Translation

FINE_LOCATION

RECORD_AUDIO

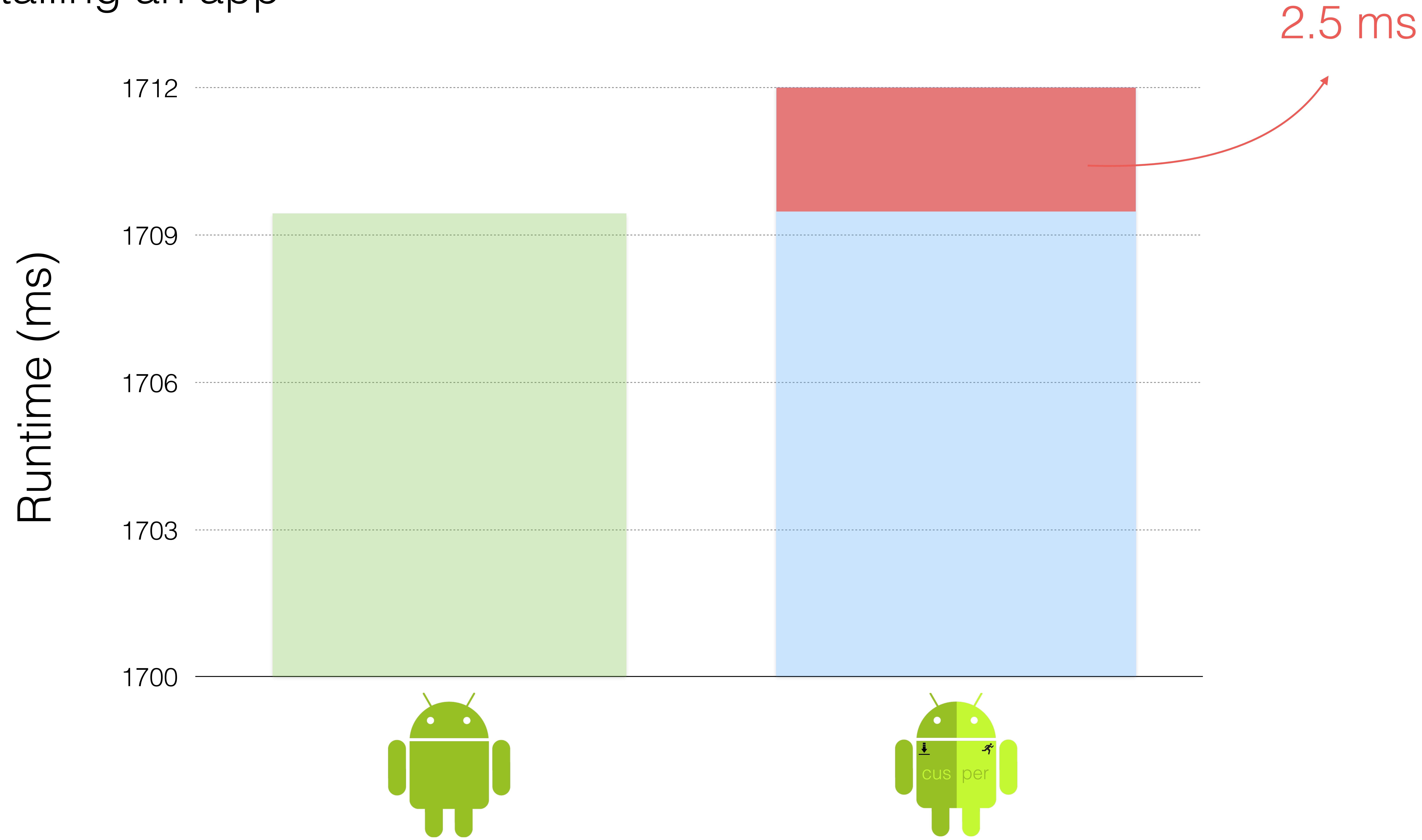
CAMERA

:Skype_Permission

:Skype_Permission

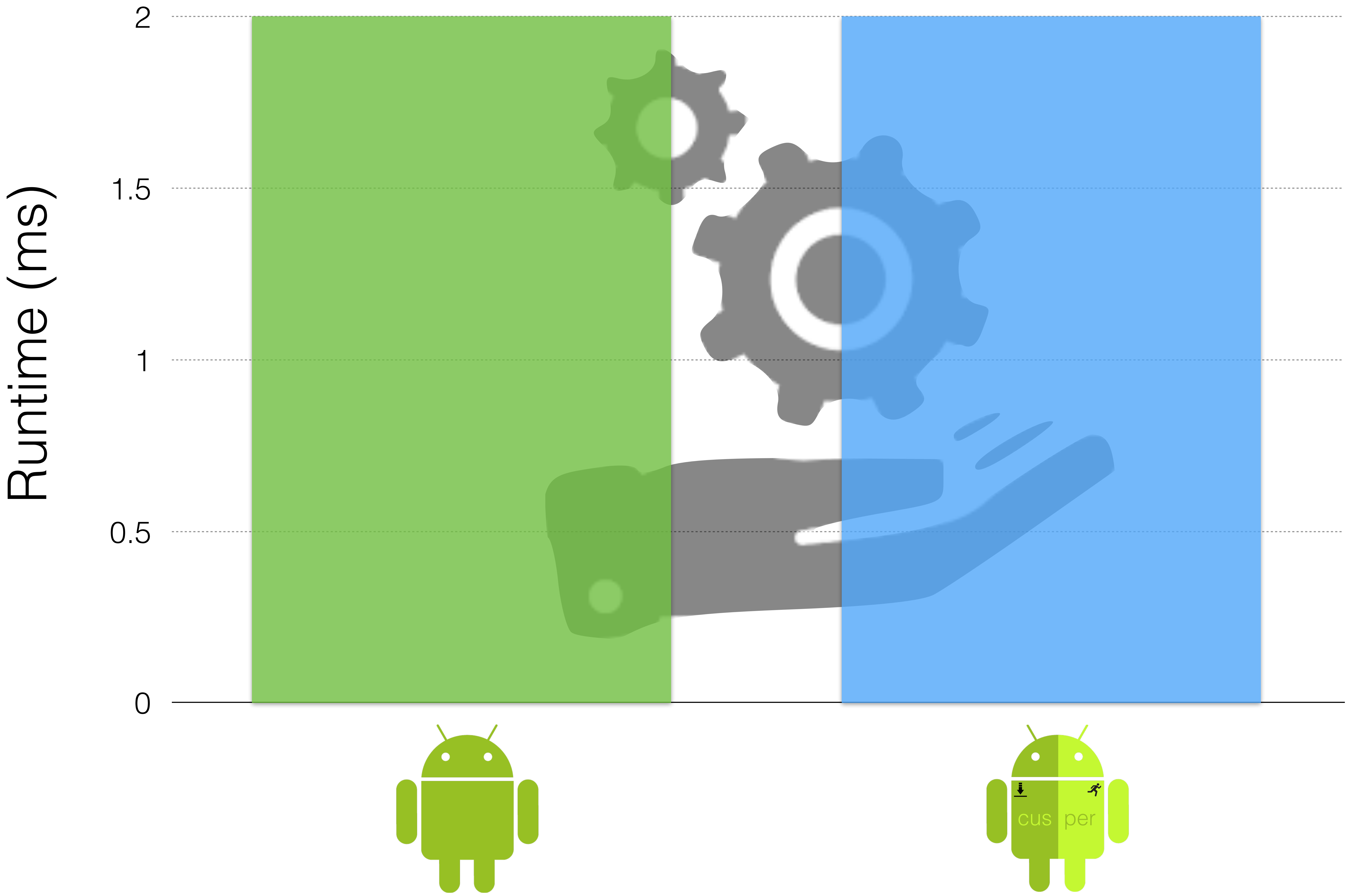
performance

installing an app

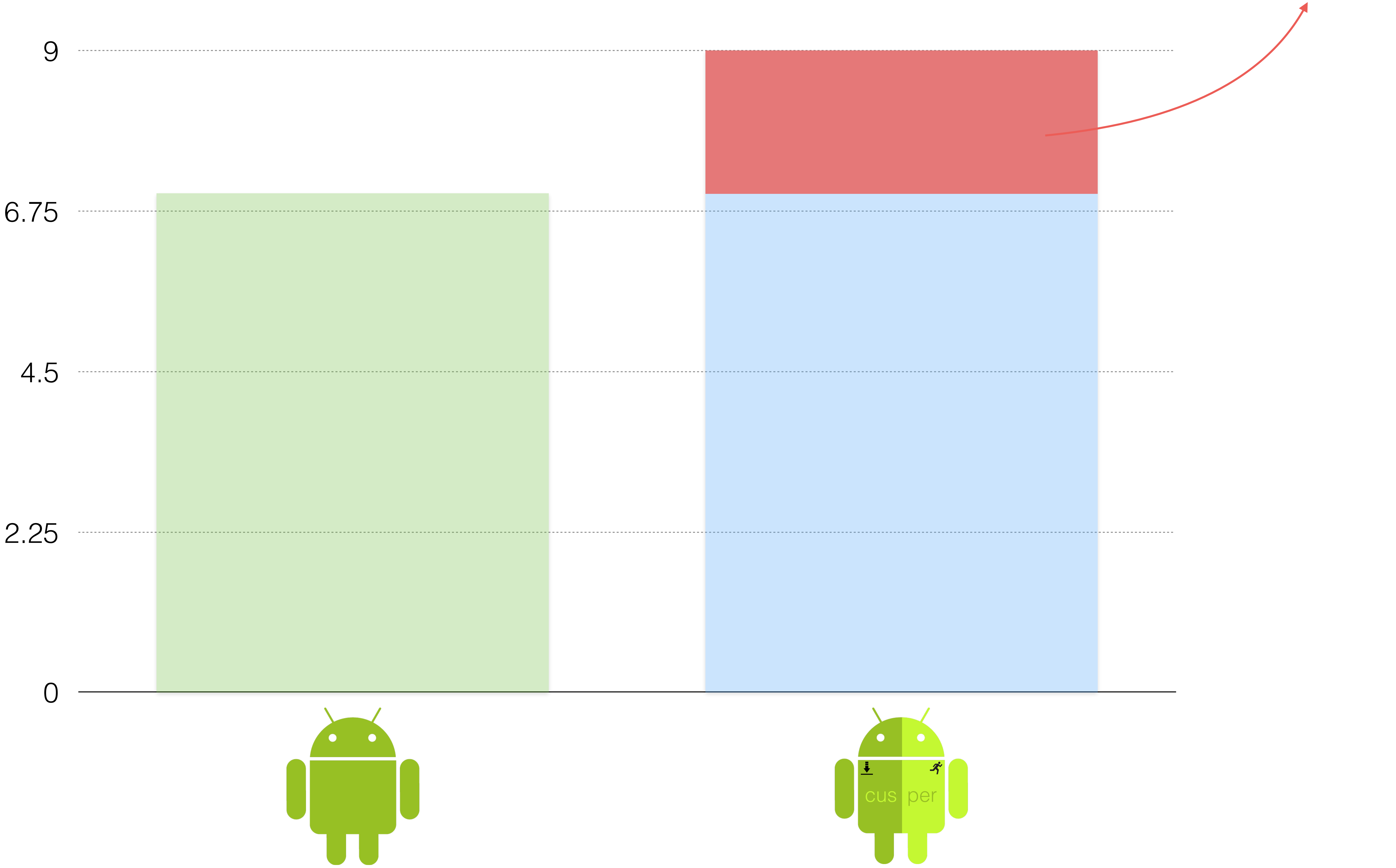


2.5 ms

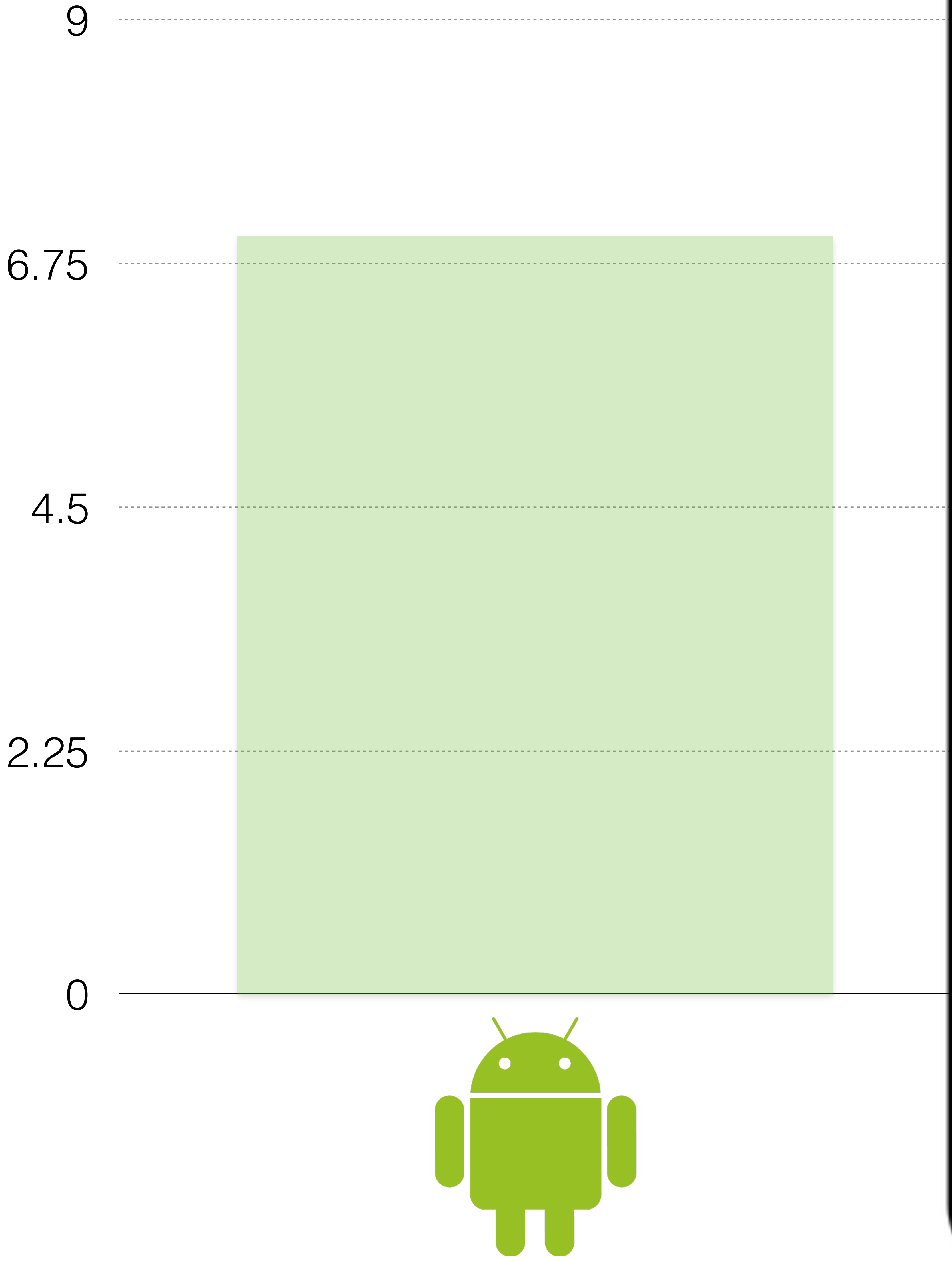
granting a signature permission to access a **service**

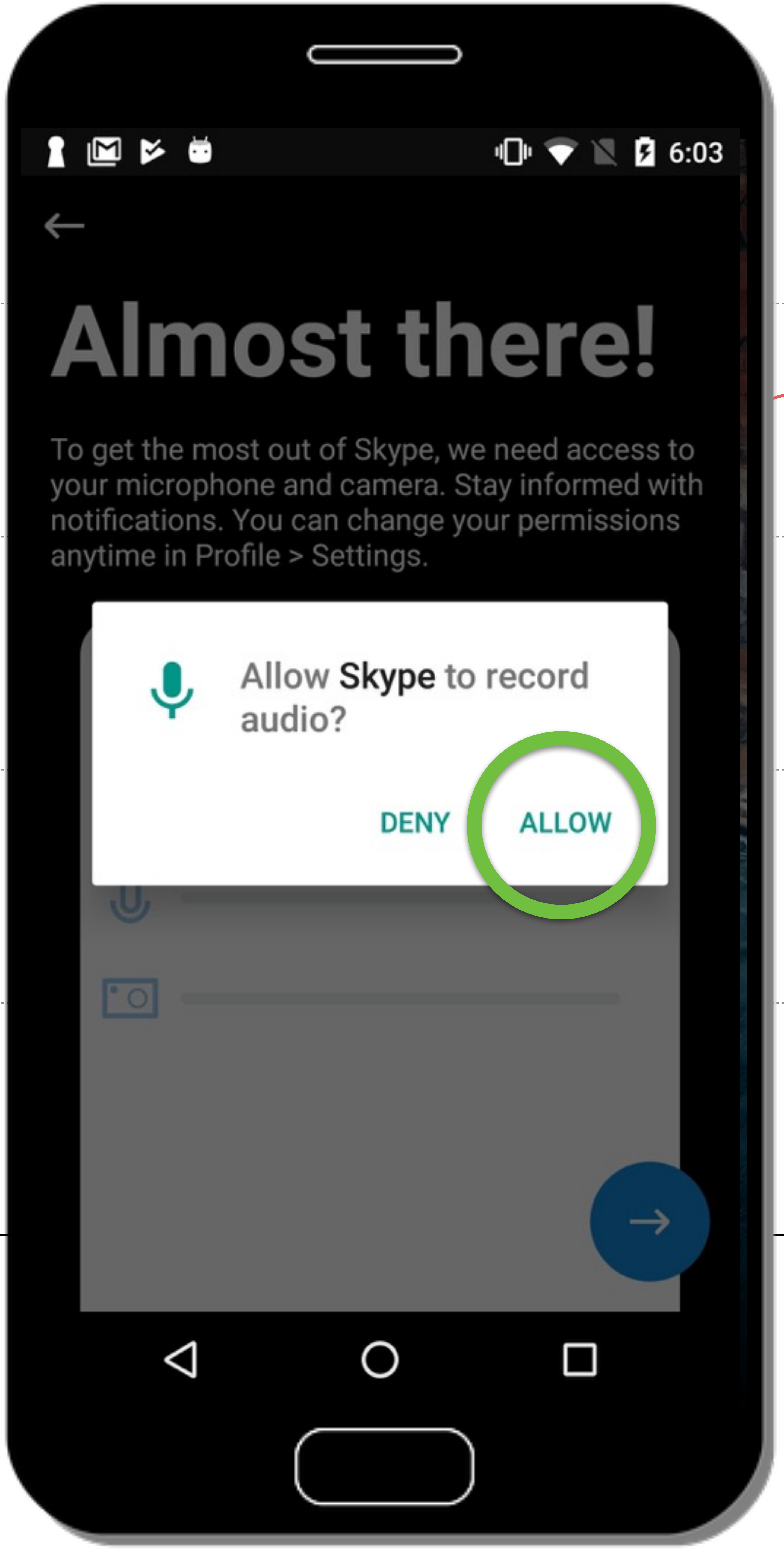


granting a dangerous permission



granting a dangerous permission





Almost there!

To get the most out of Skype, we need access to your microphone and camera. Stay informed with notifications. You can change your permissions anytime in Profile > Settings.

Allow **Skype** to record audio?

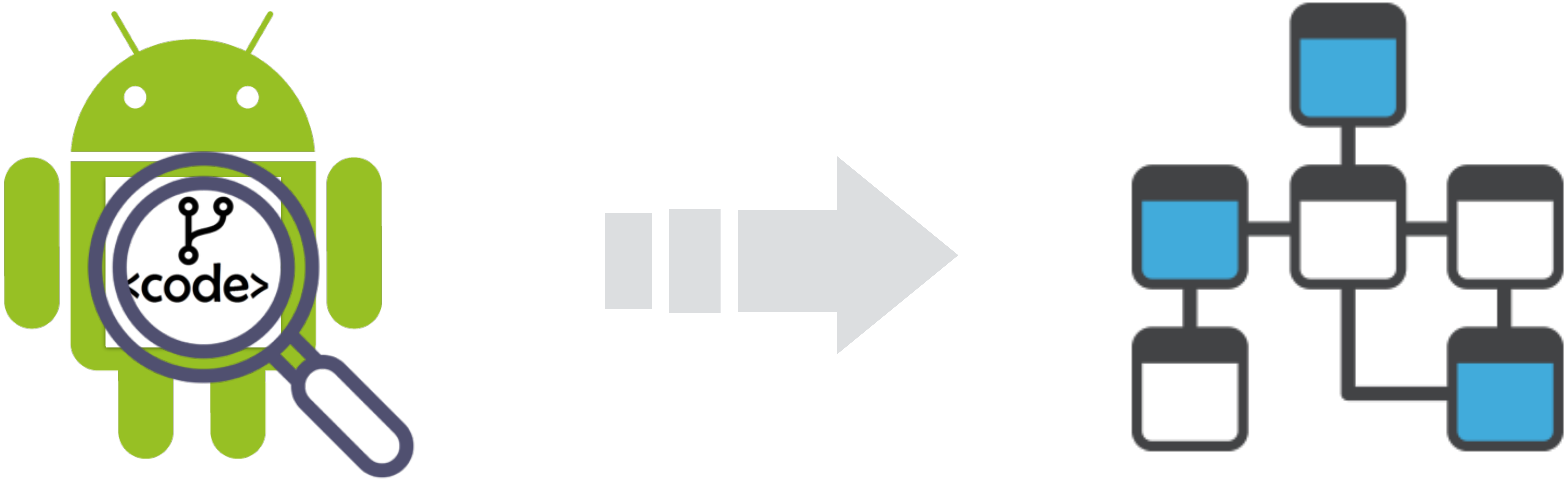
DENY ALLOW

2 ms

effectiveness

Formal Verification

formal verification



Implementation

Alloy Model

formal verification: security properties

Dangerous permissions are never granted without user interaction ✓

An app’s components cannot be accessed by other unauthorized apps ✓

Summary

- Security analysis on custom permissions revealed **serious security vulnerabilities** (acknowledged by Google)
- Designed CUSPER which introduces mechanisms for **separating system and custom permissions**.
- Introduced a strategy for **tracking permission ownership**.
- Introduced the first formal model of Android runtime permissions and used it to **formally verify correctness** of CUSPER.