

# Resolving the Predicament of Android Custom Permissions

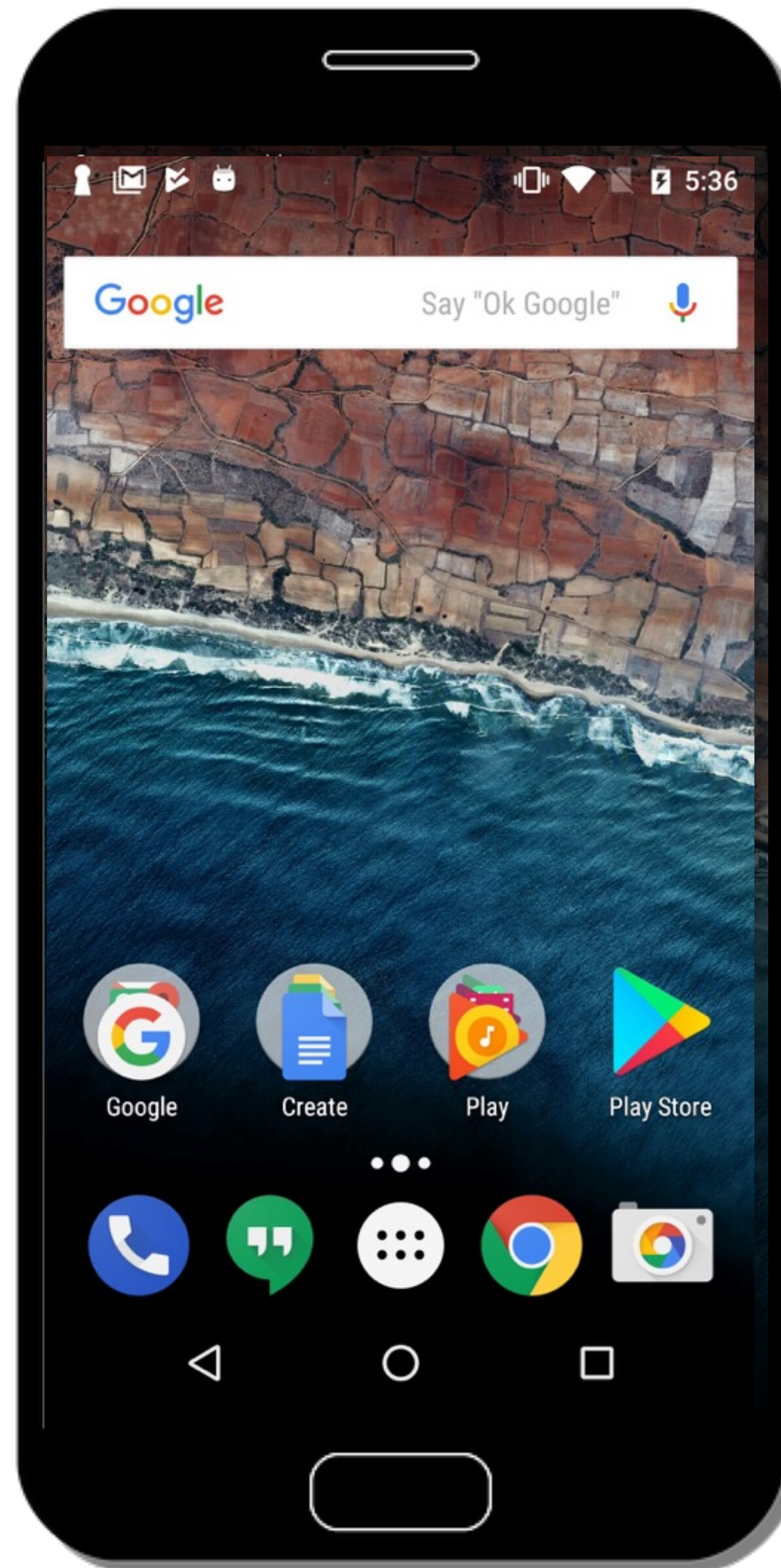
---

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

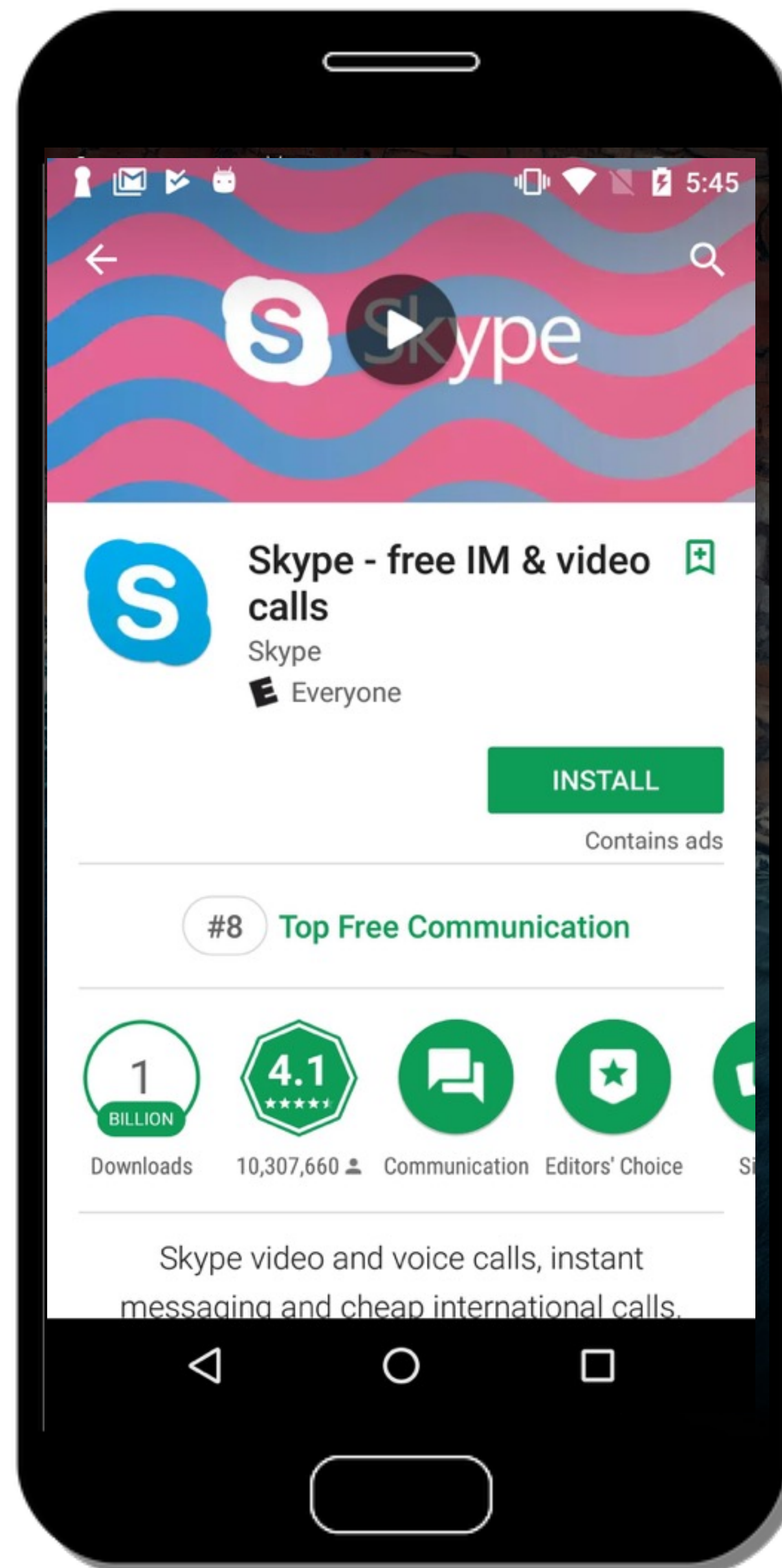
University of Illinois at Urbana - Champaign

#NDSS18

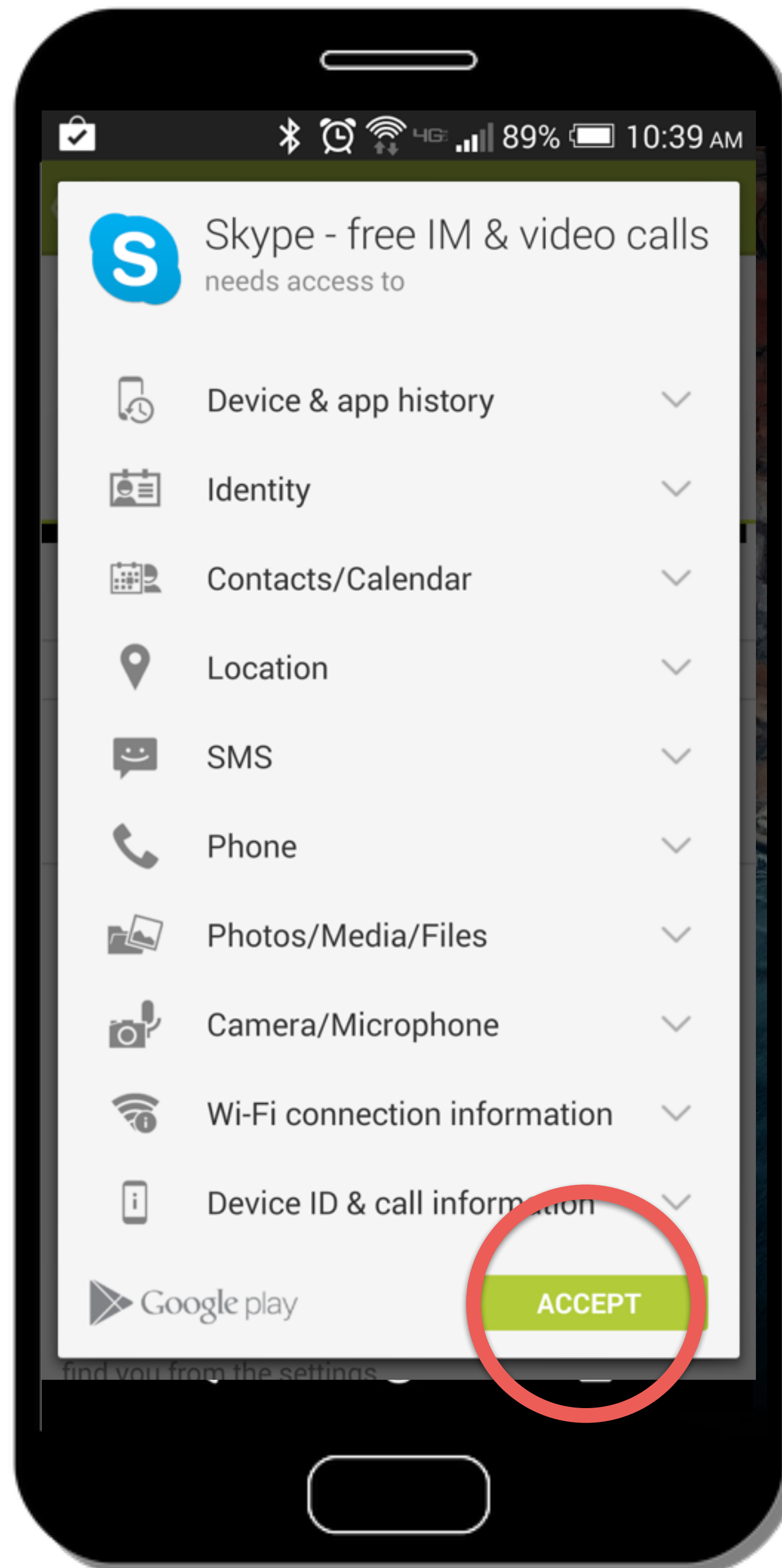
# Install-time Permissions < version 6



# Install-time Permissions < version 6



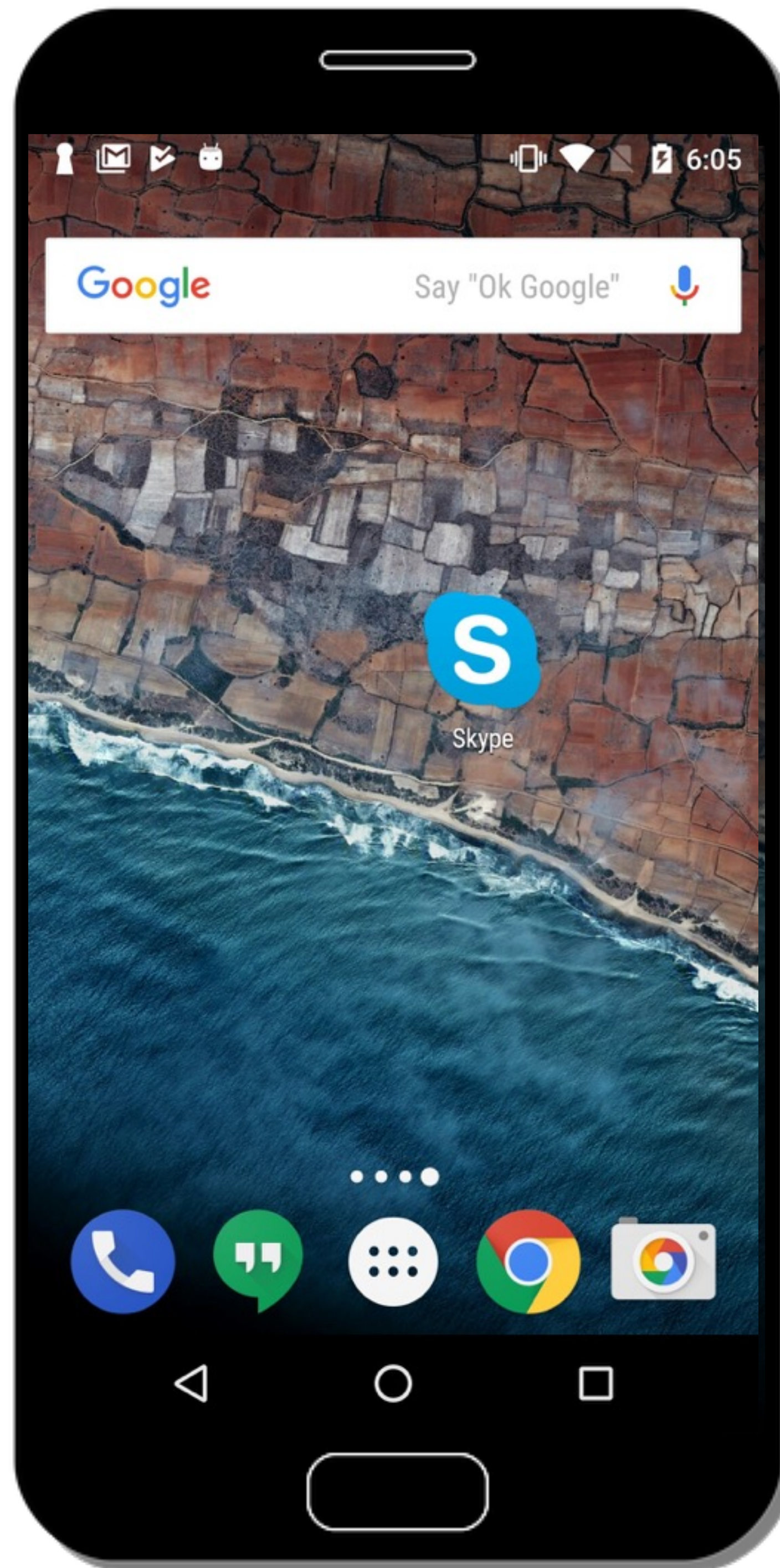
# Install-time Permissions < version 6



## Permission Types

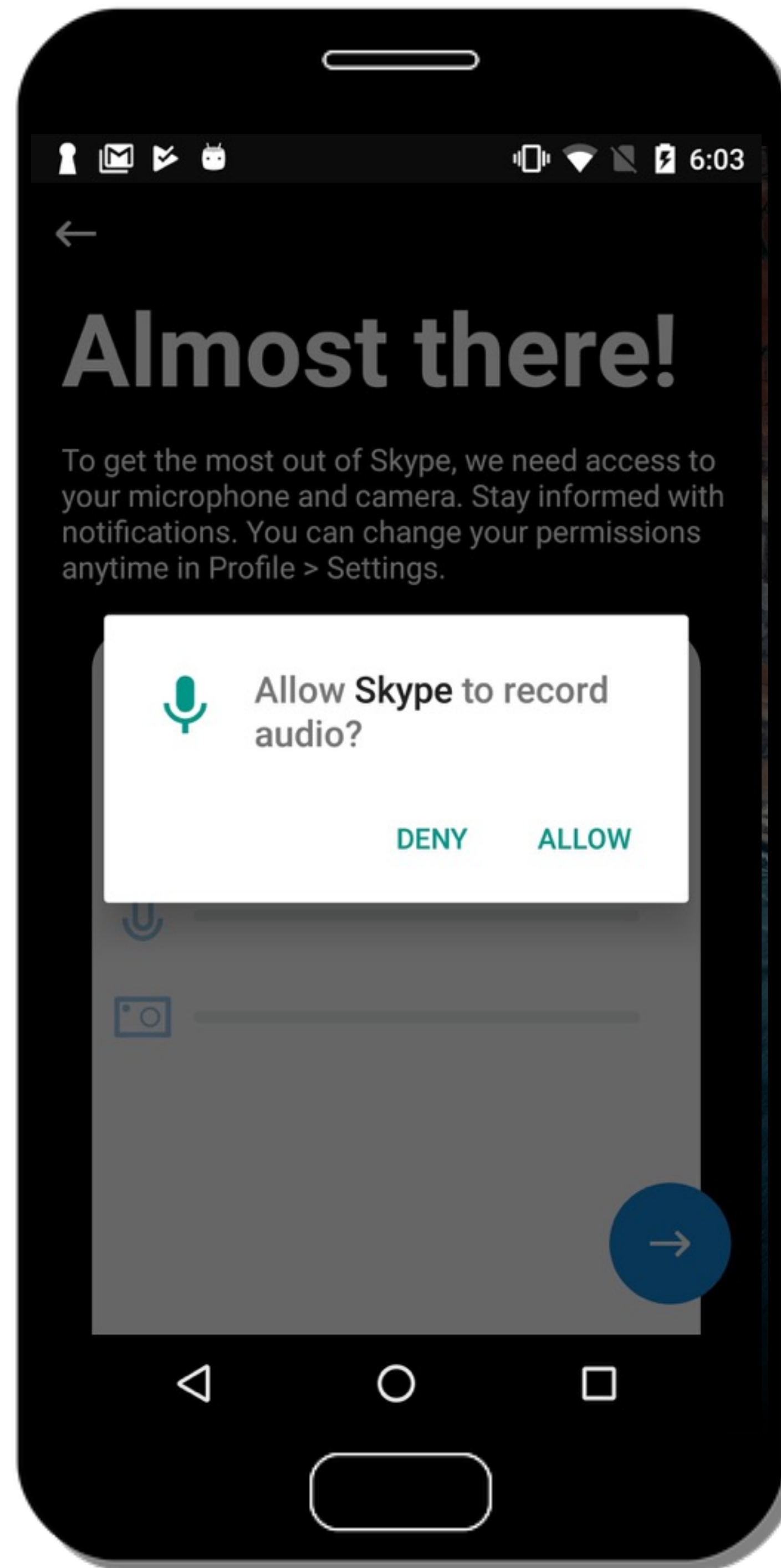
-  Normal 
-  Signature 
-  Dangerous 
-  SignatureOr System 

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



Runtime Permissions  
>= version 6

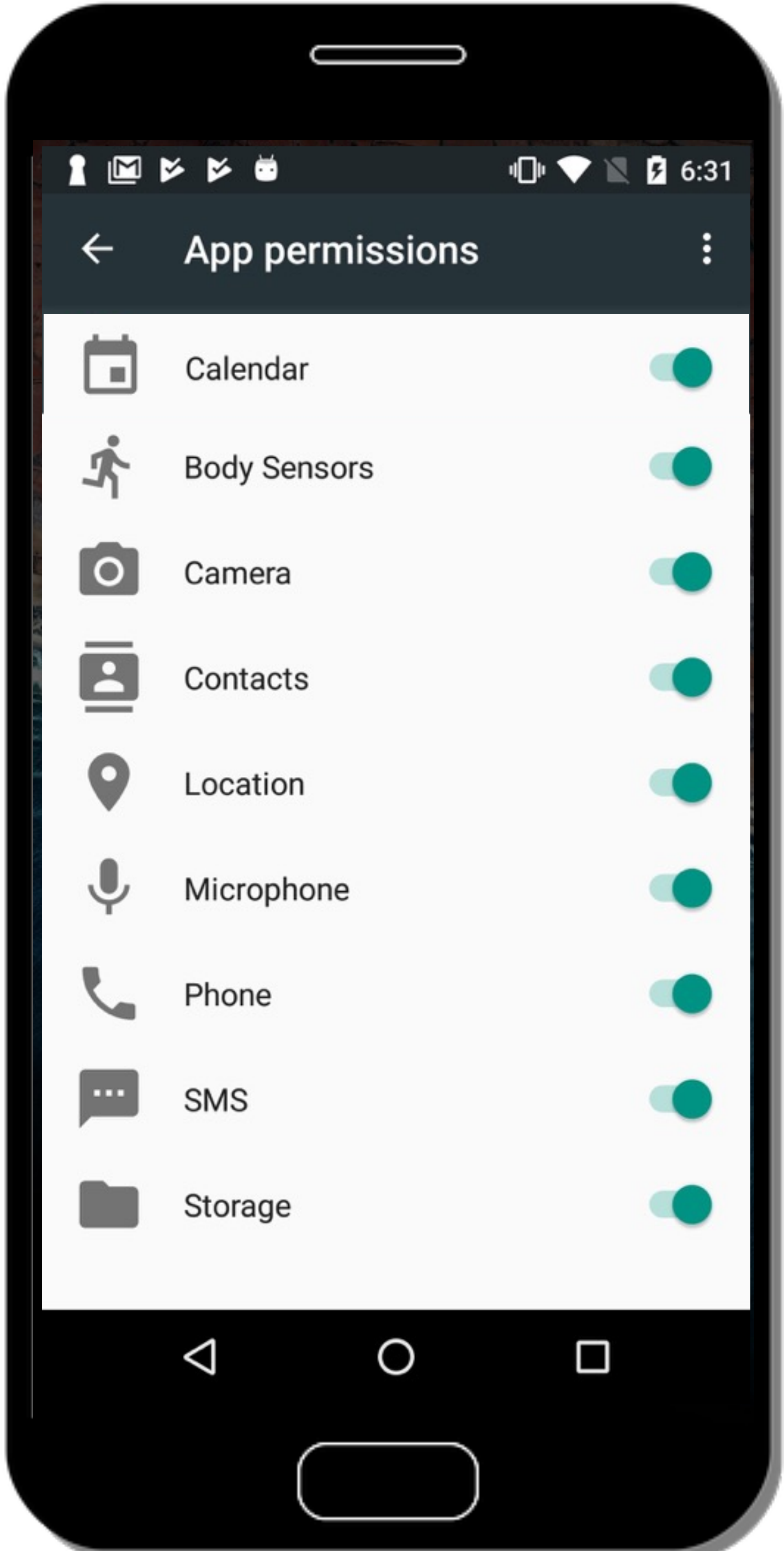
Runtime Permissions  
>= version 6



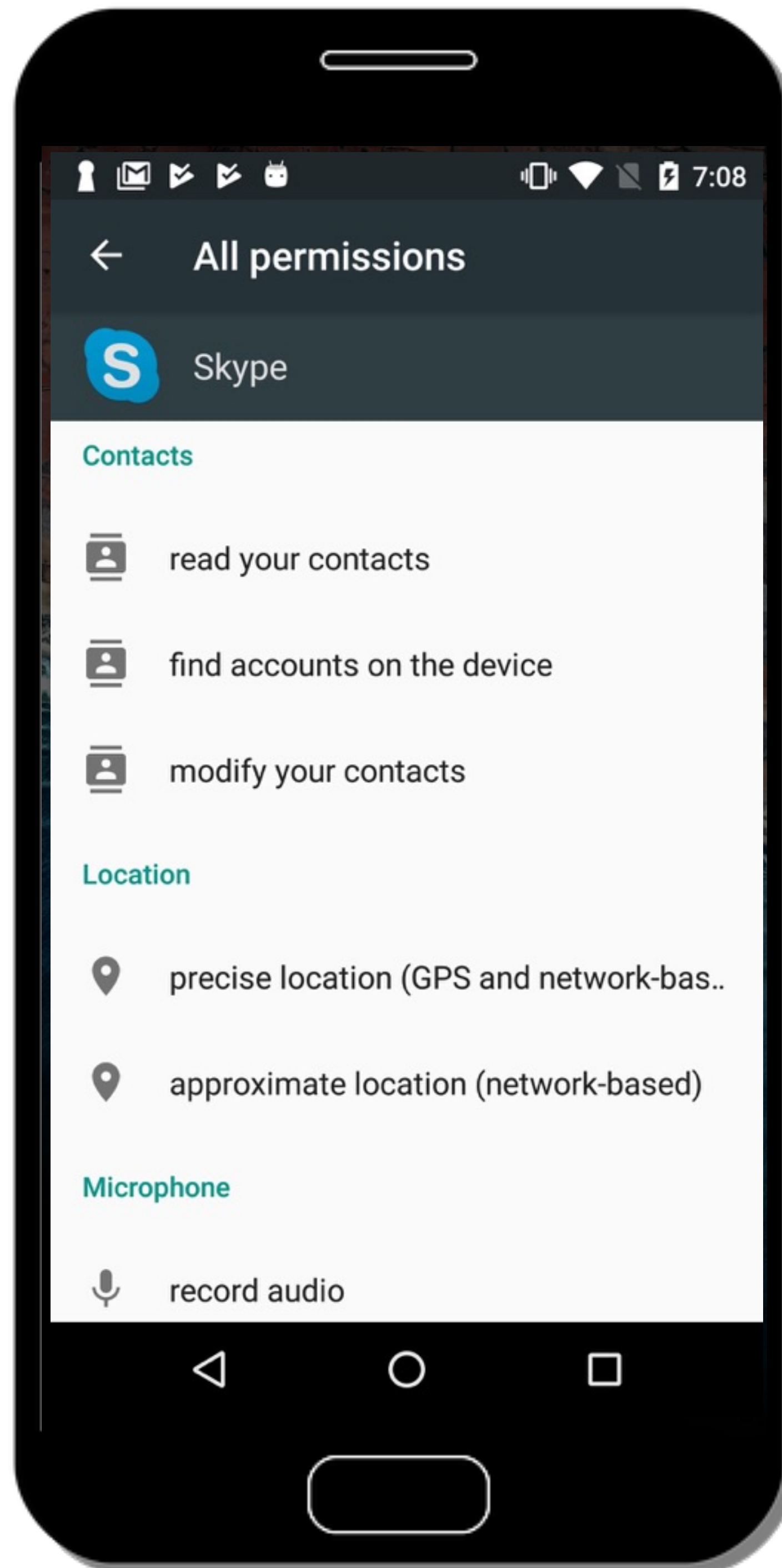
## Permission Types

- 
- |   |           |   |
|---|-----------|---|
|    | Normal    |    |
|  | Signature |  |
|  | Dangerous |  |

# Permission Groups









# Permission Groups

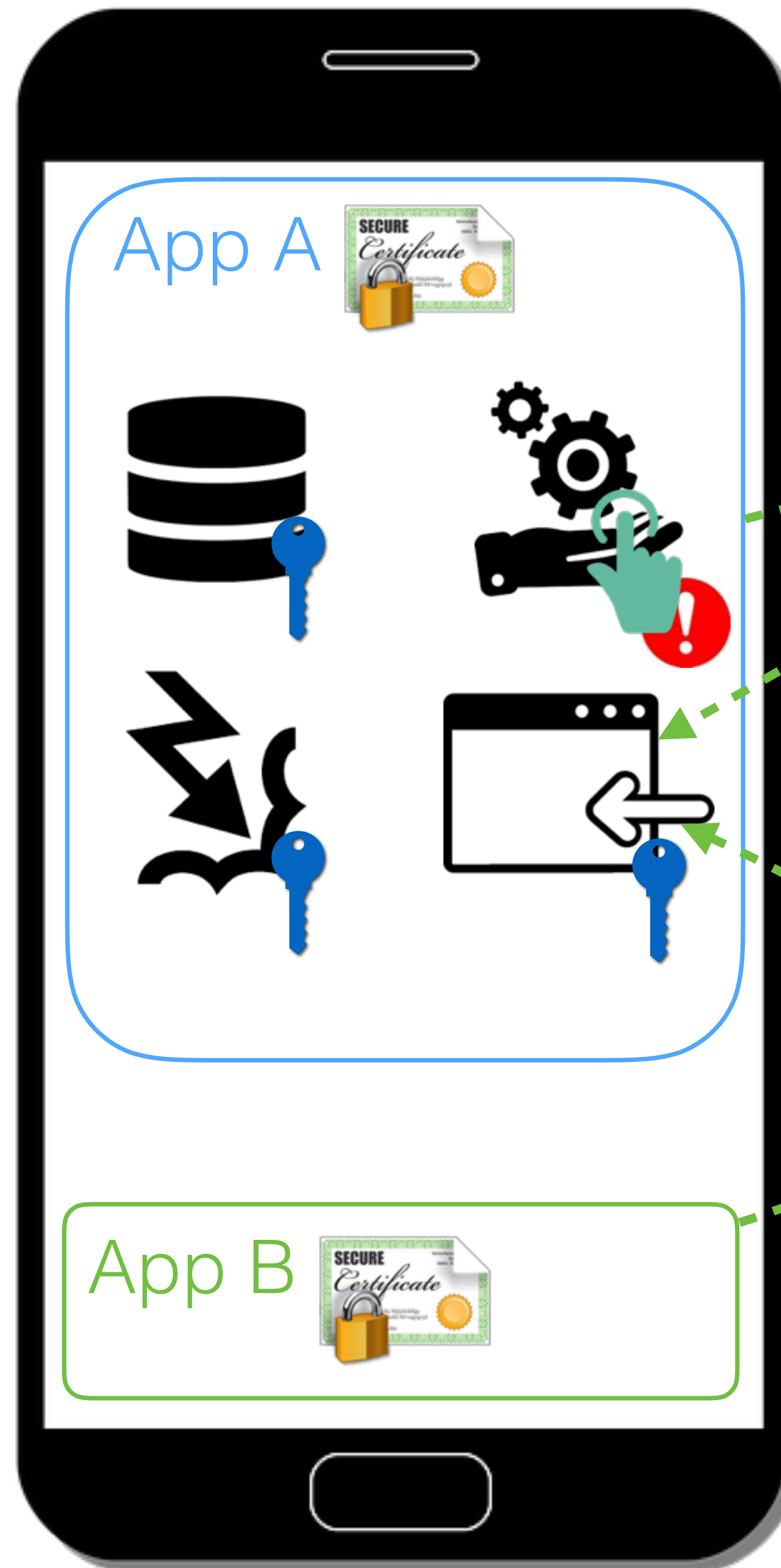




# Custom Permissions

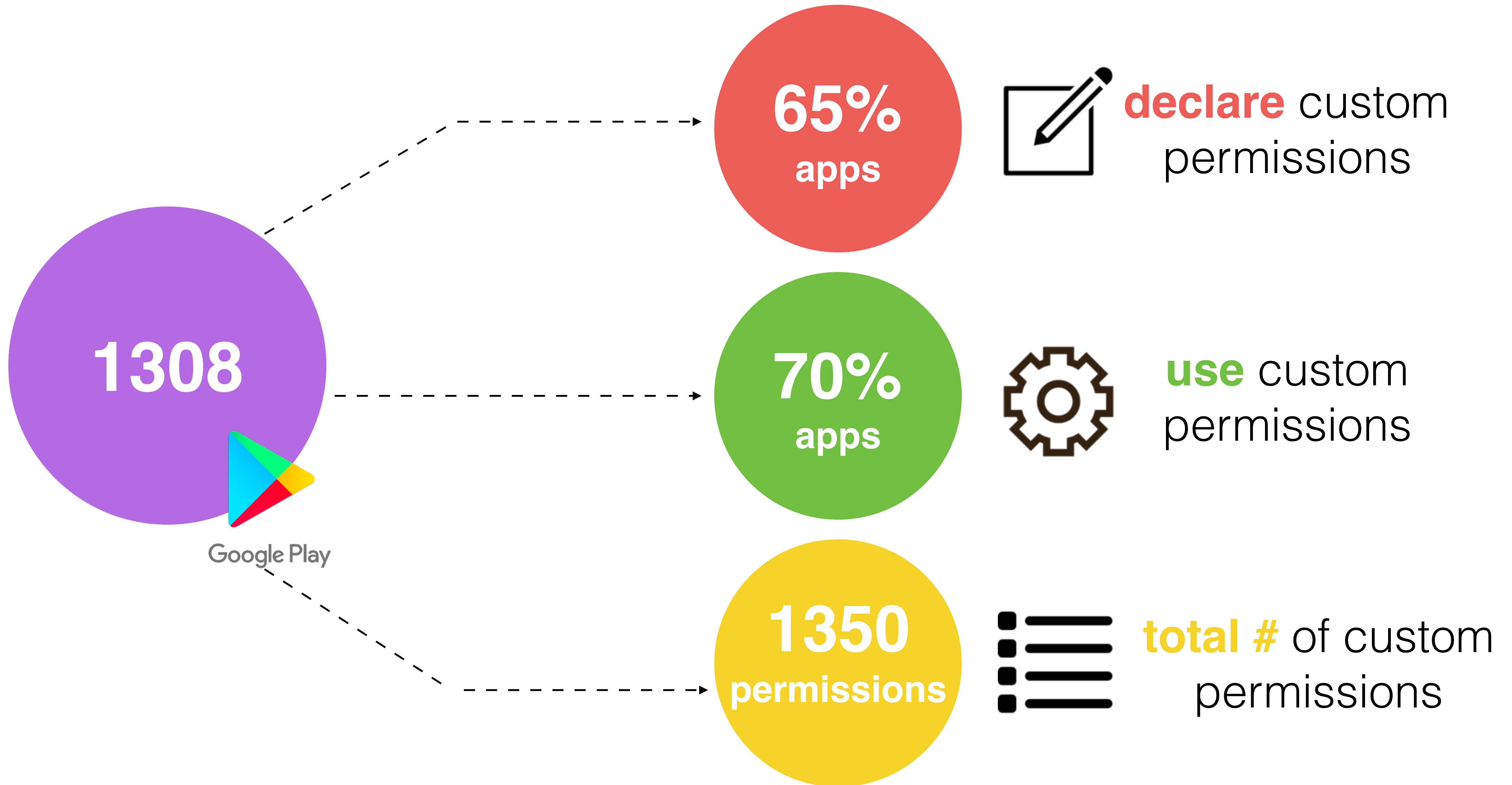
## Permission Types

-  Normal 
-  Signature 
-  Dangerous 



Protect Exported  
App Components

# Prevalence of custom permissions





No clear distinction between  
system permissions and custom permissions



# No clear distinction between system permissions and custom permissions

---

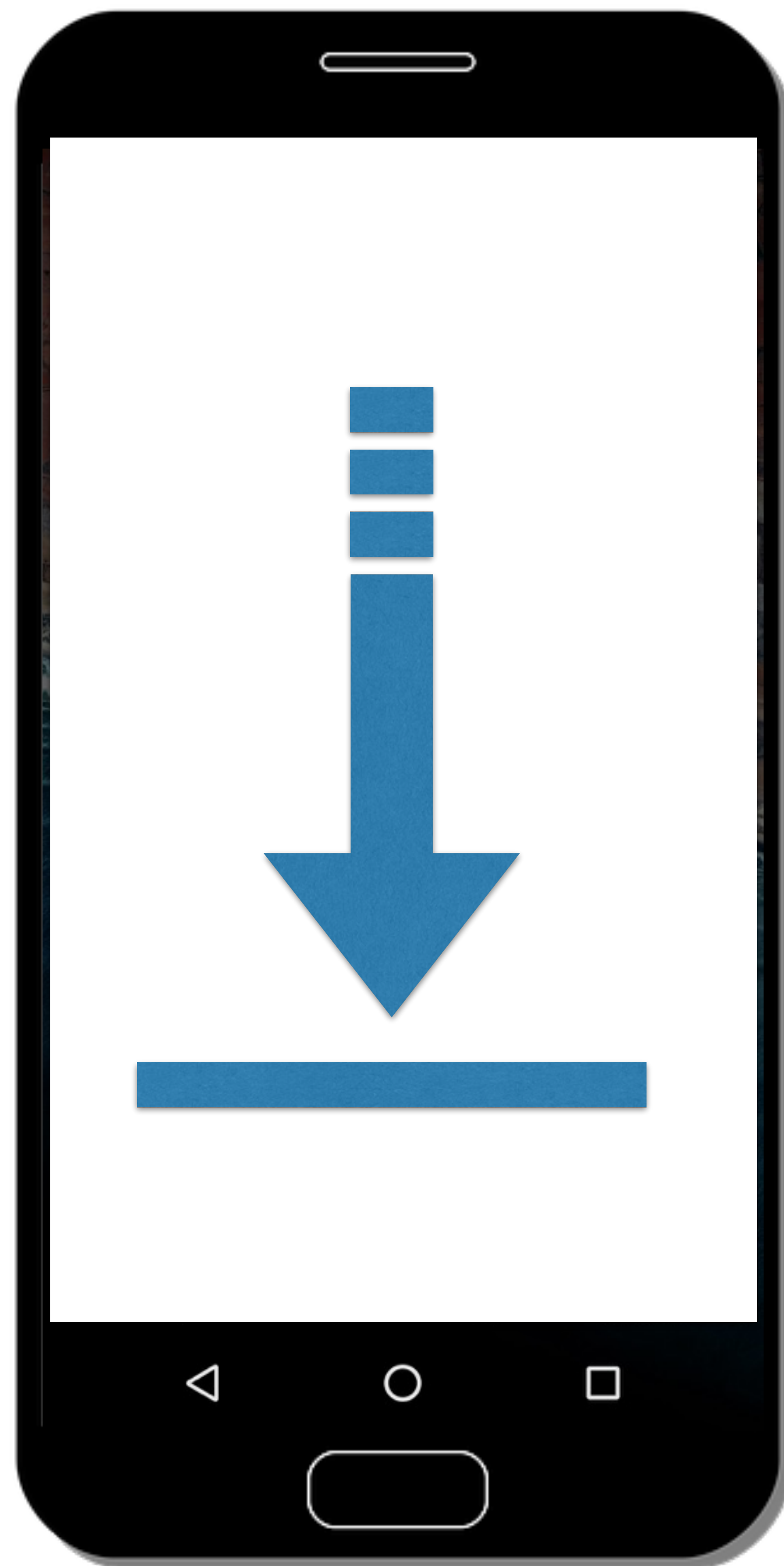


declared by the system



declared by 3rd party apps





My\_Permission



normal



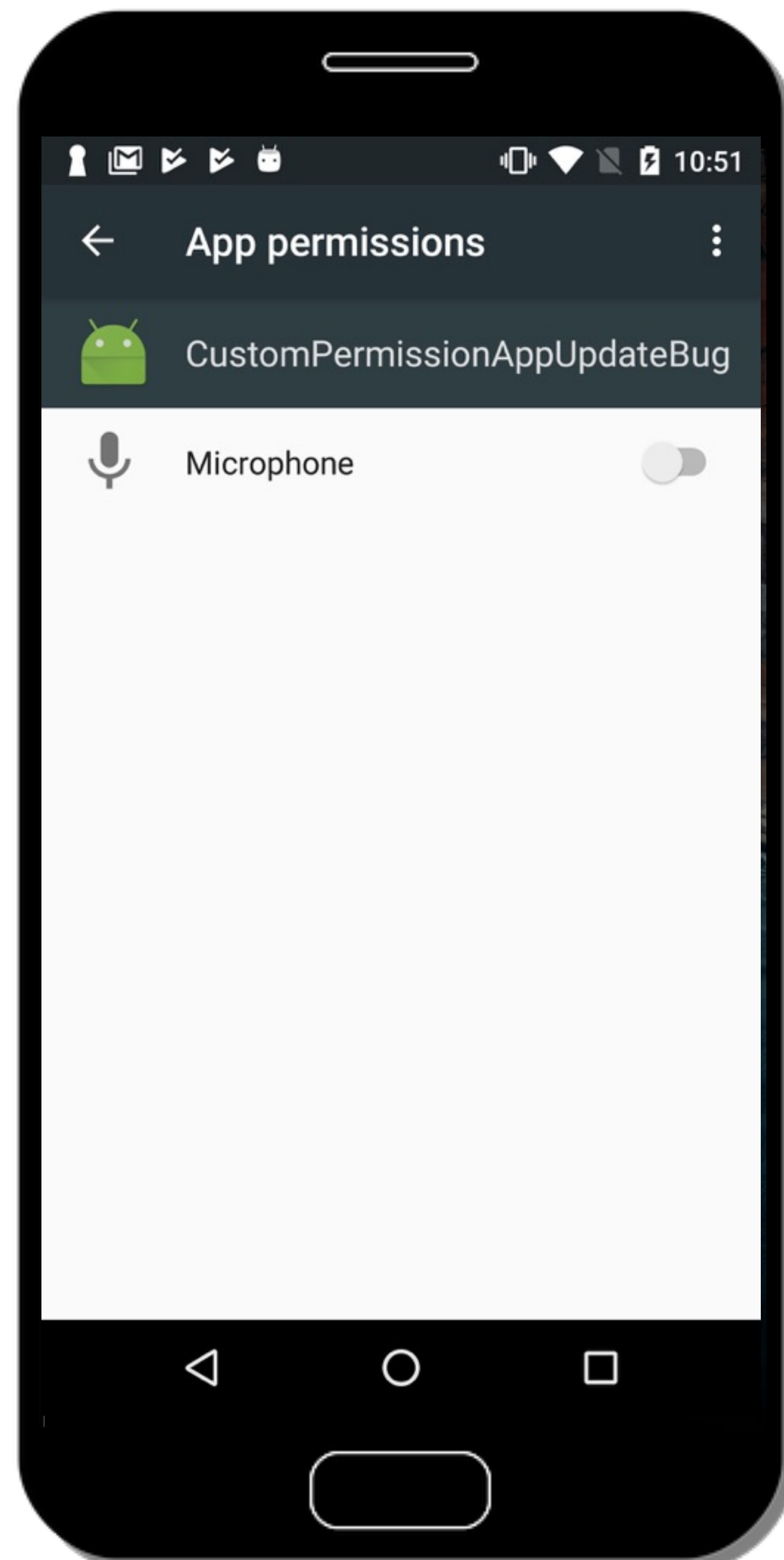
Microphone Group



My\_Permission



record audio



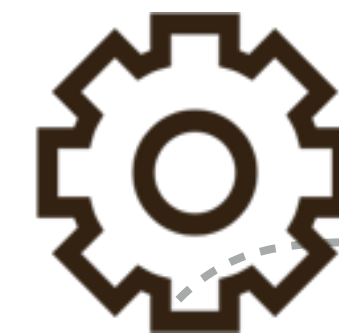
My\_Permission



normal



Microphone Group



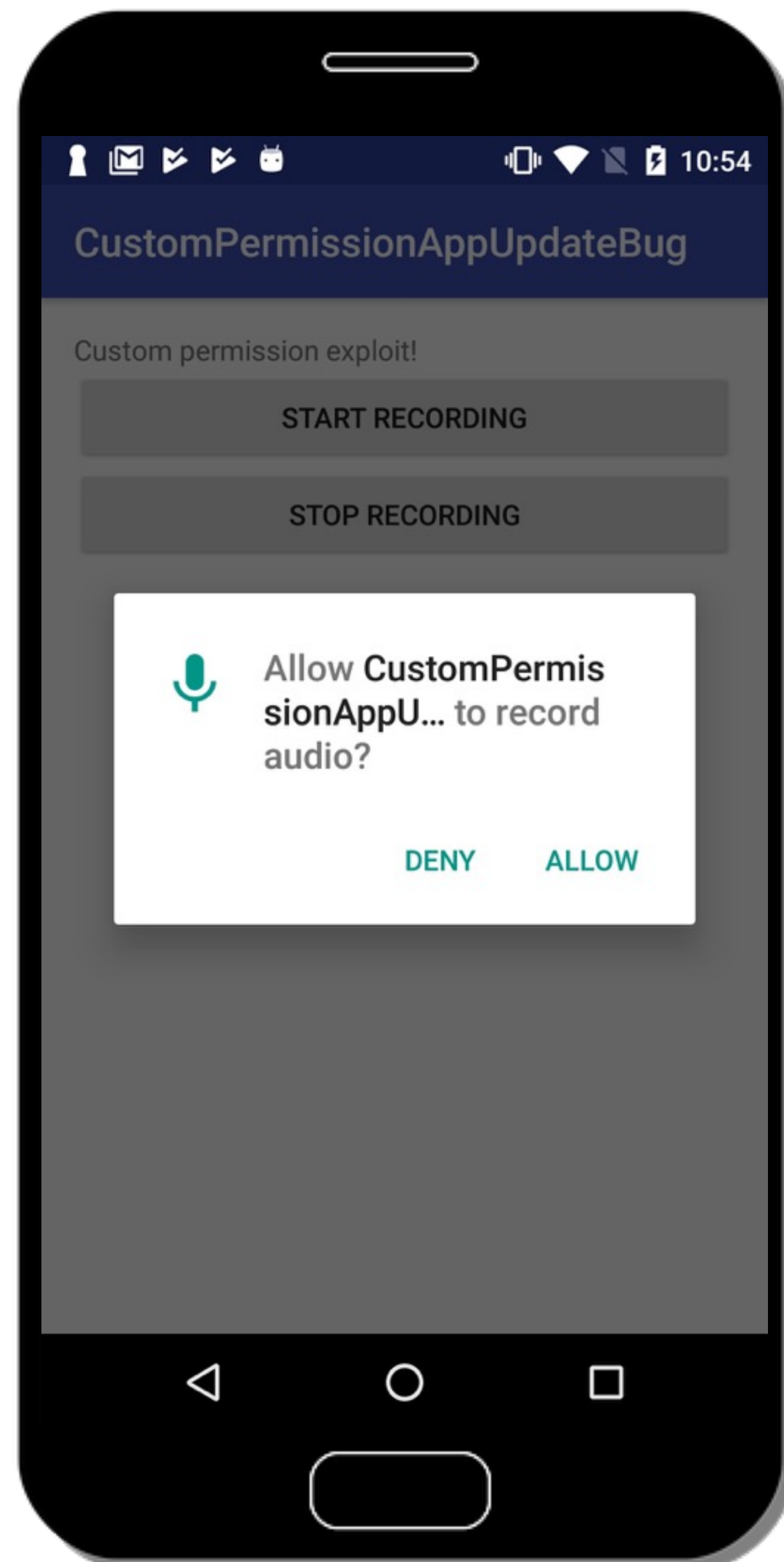
My\_Permission



Granted



record audio



My\_Permission



normal



Microphone Group



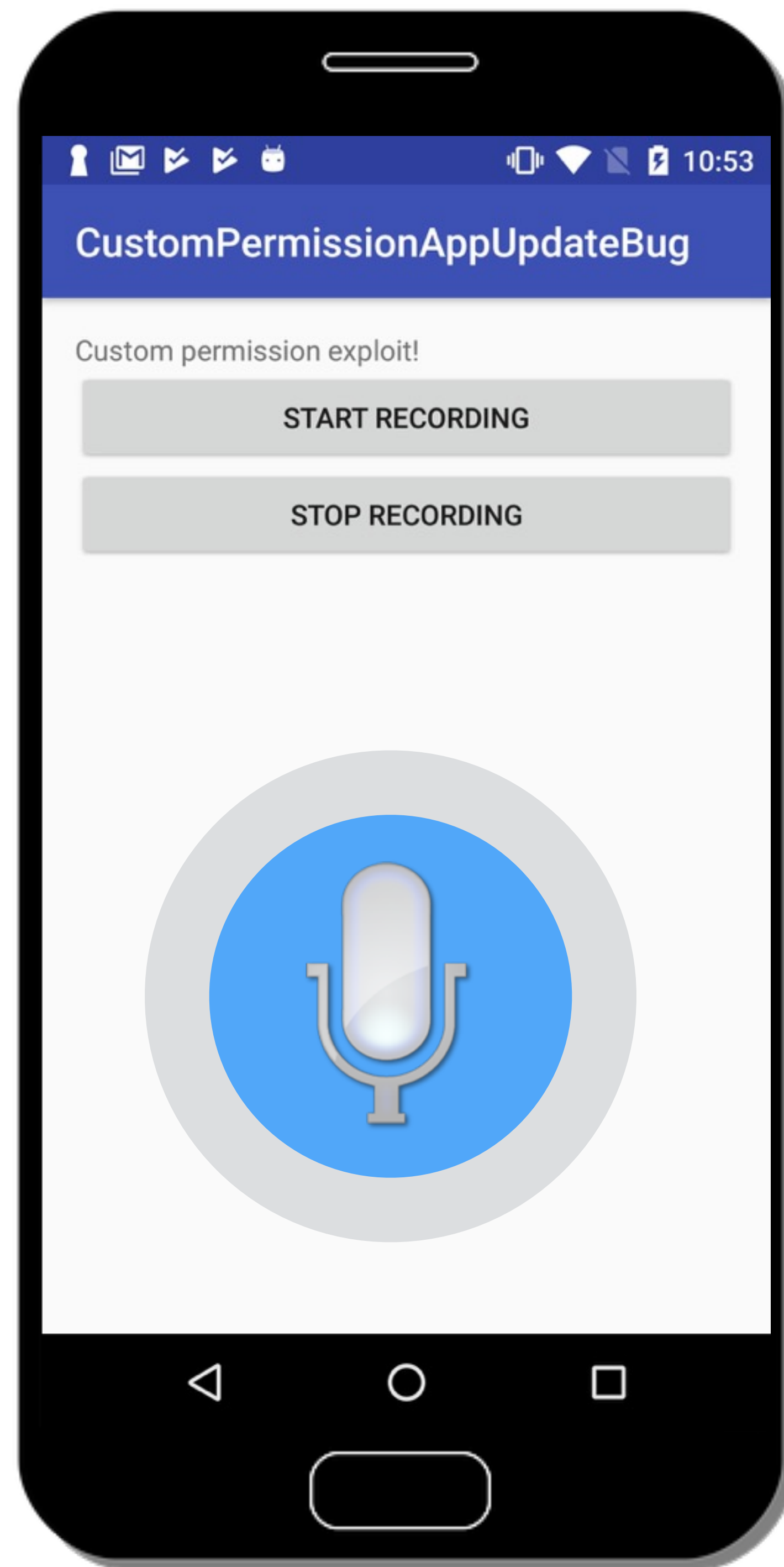
My\_Permission



Granted



record audio



My\_Permission



dangerous



Microphone Group



My\_Permission

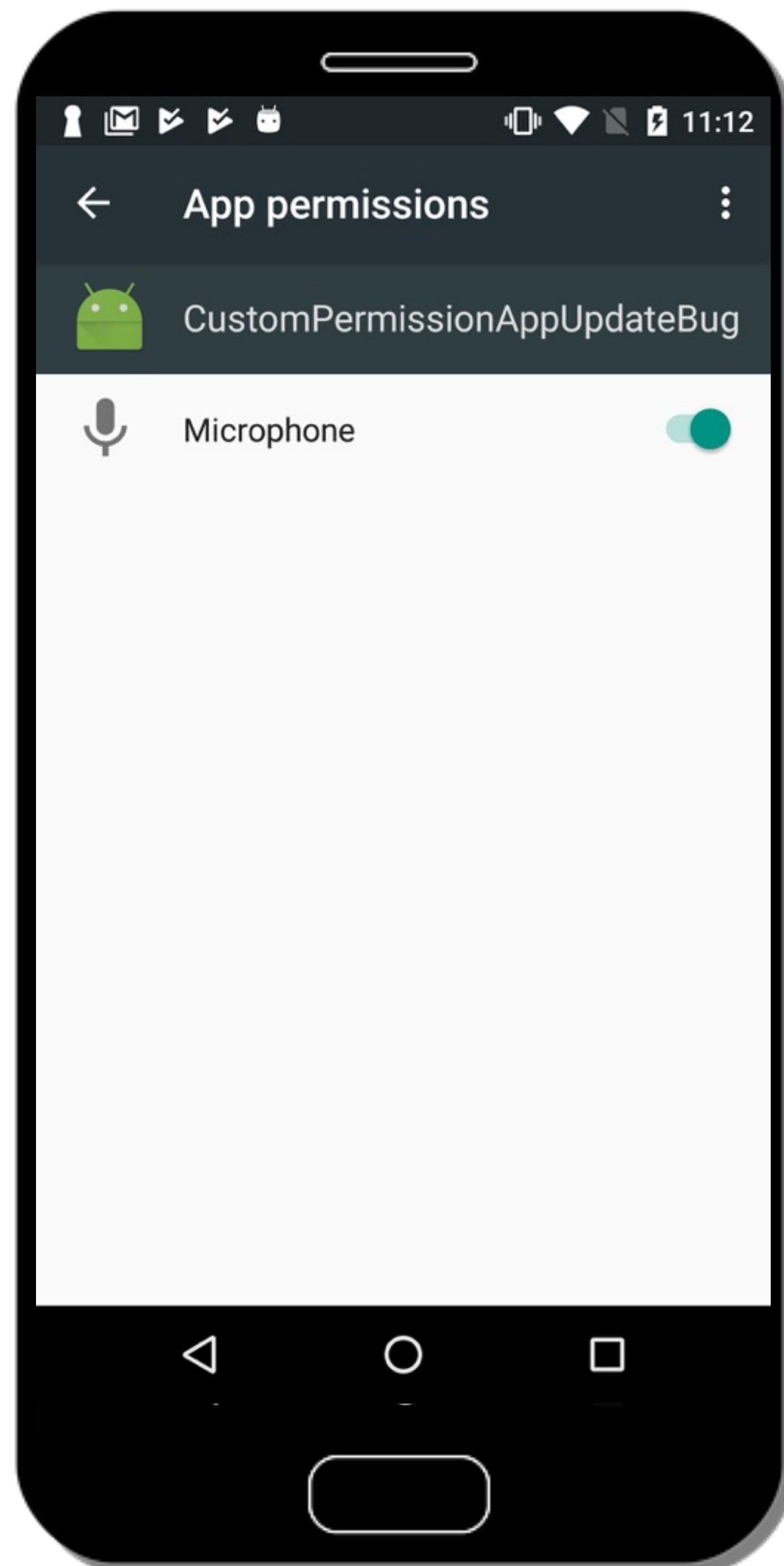


Granted



record audio





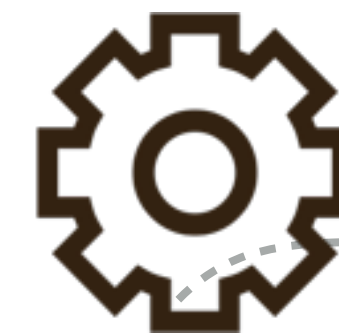
My\_Permission



dangerous



Microphone Group



My\_Permission



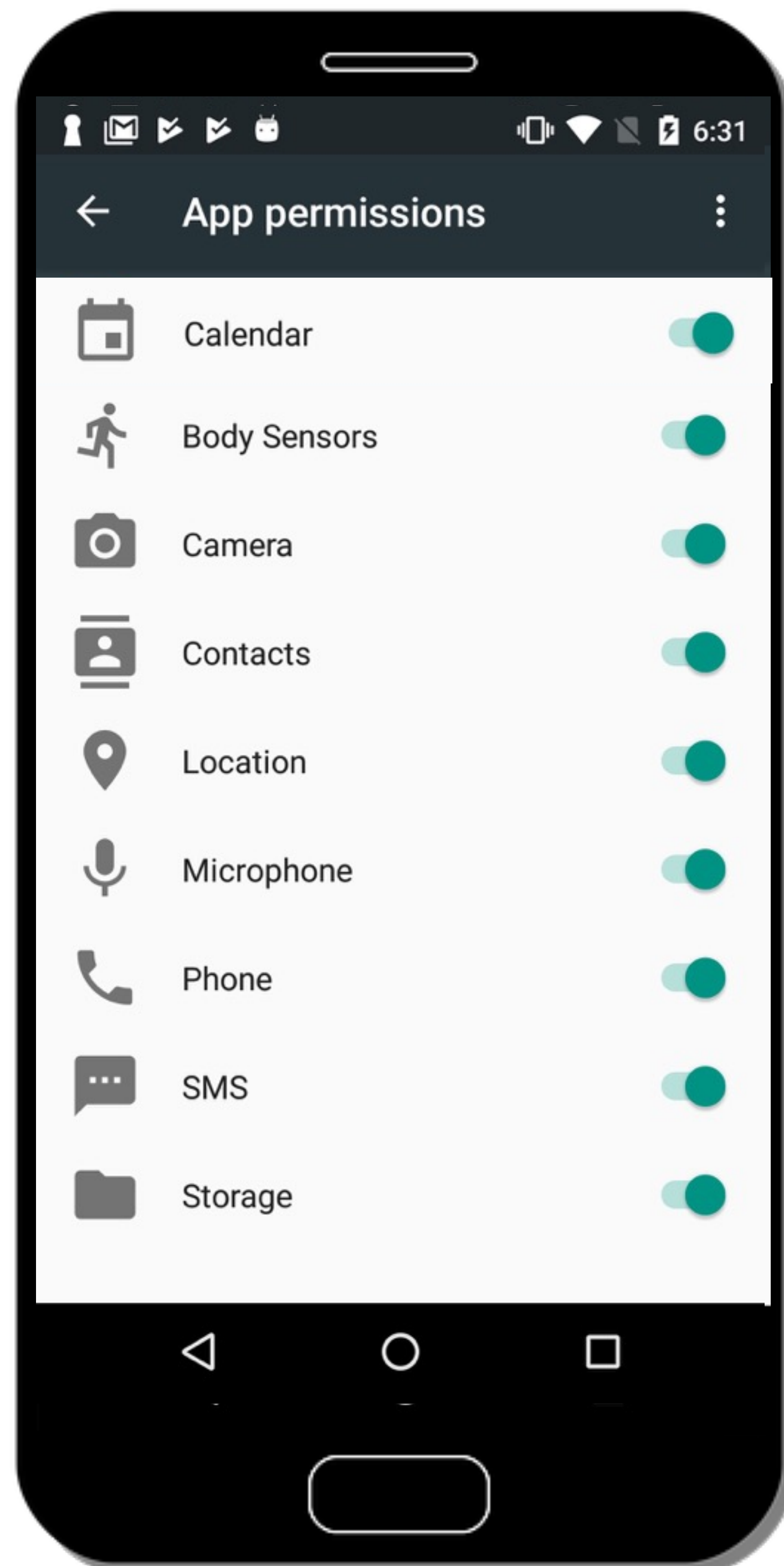
Granted



record audio



Granted



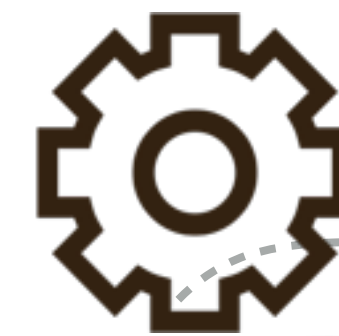
My\_Permission



dangerous



Microphone Group



My\_Permission



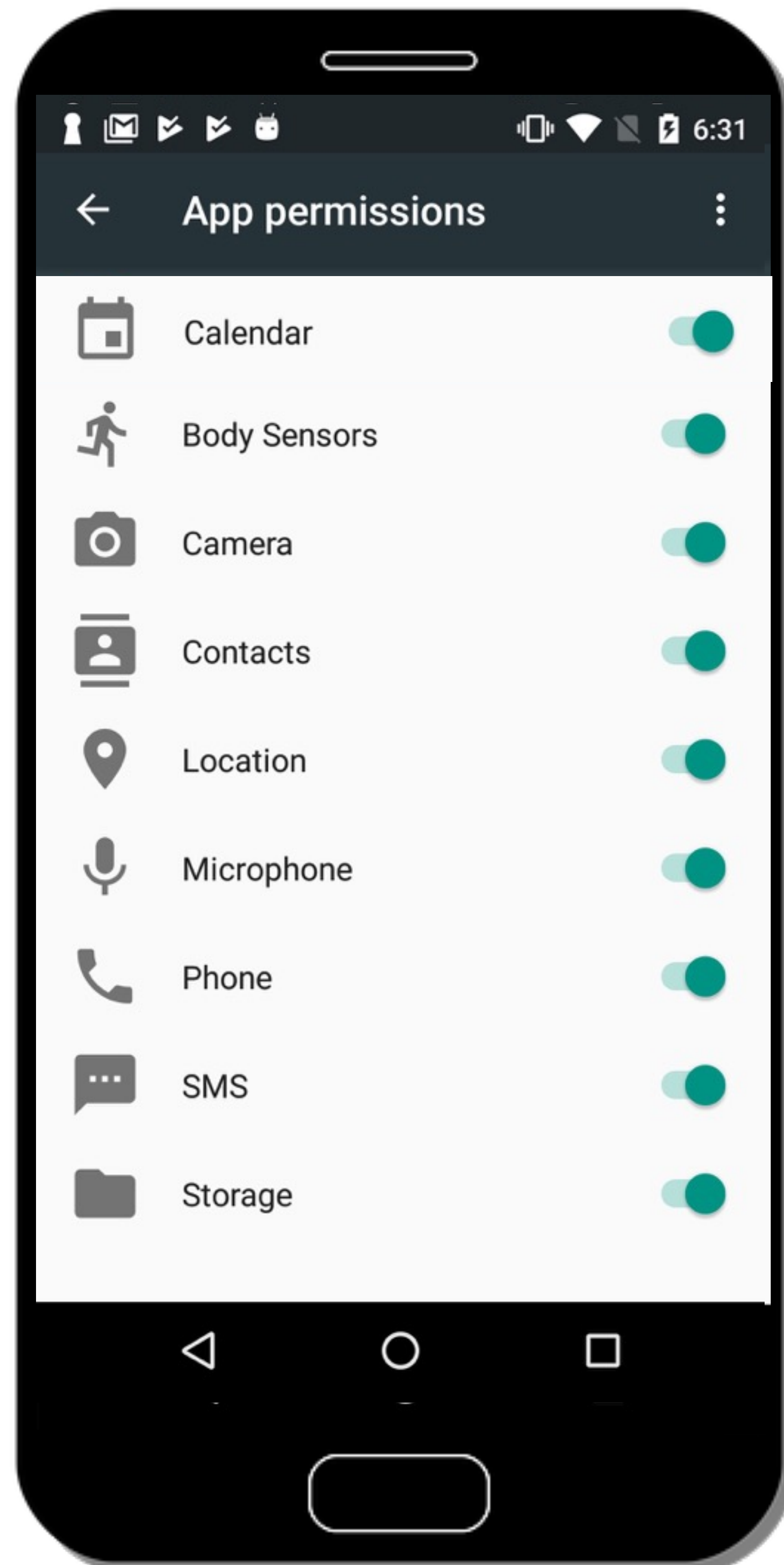
Granted



record audio



Granted



My\_Permission



dangerous



Microphone Group



My\_Permission



Granted



record audio



Granted



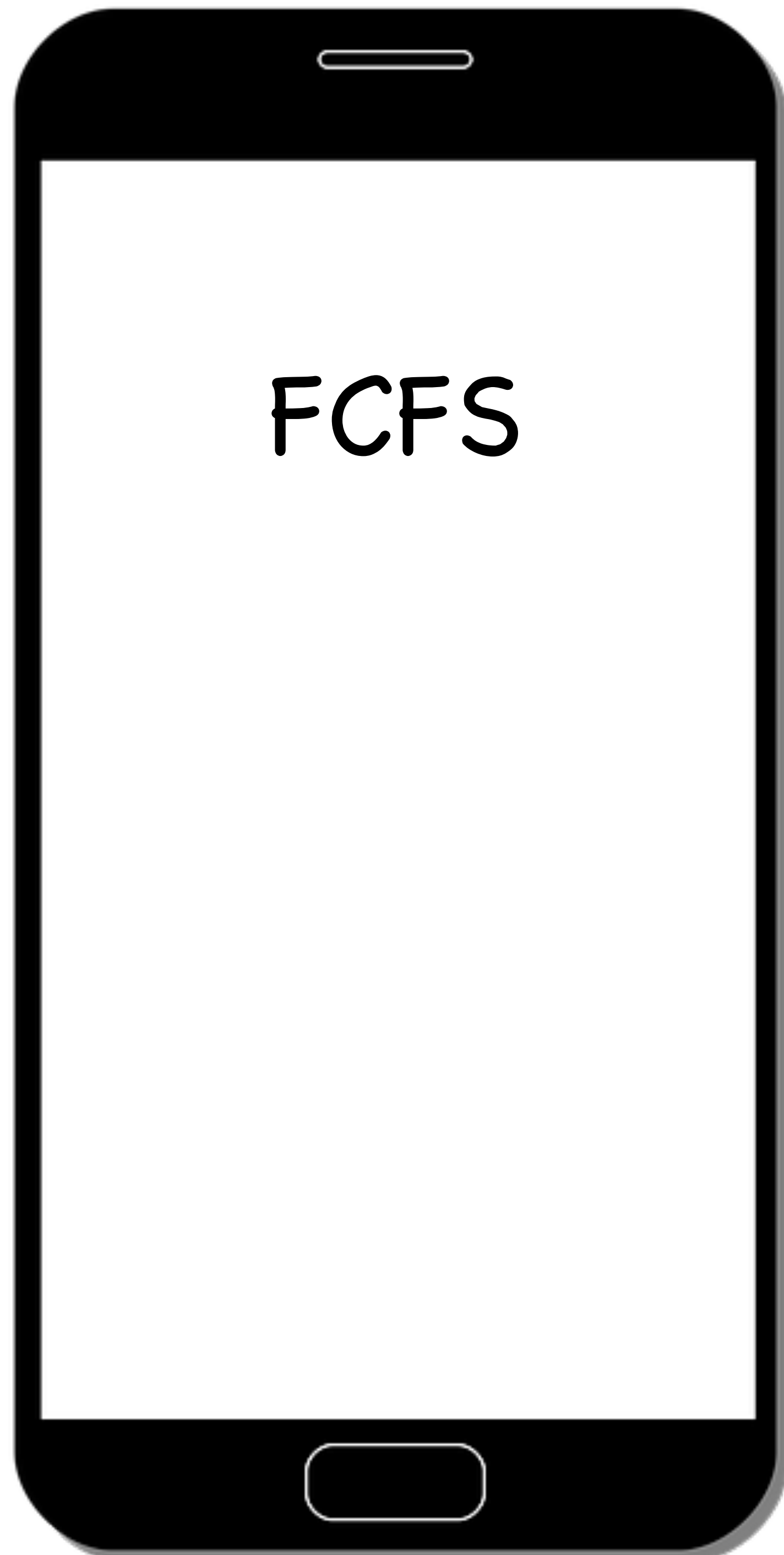
No distinction between  
custom permissions owners



Skype\_Permission



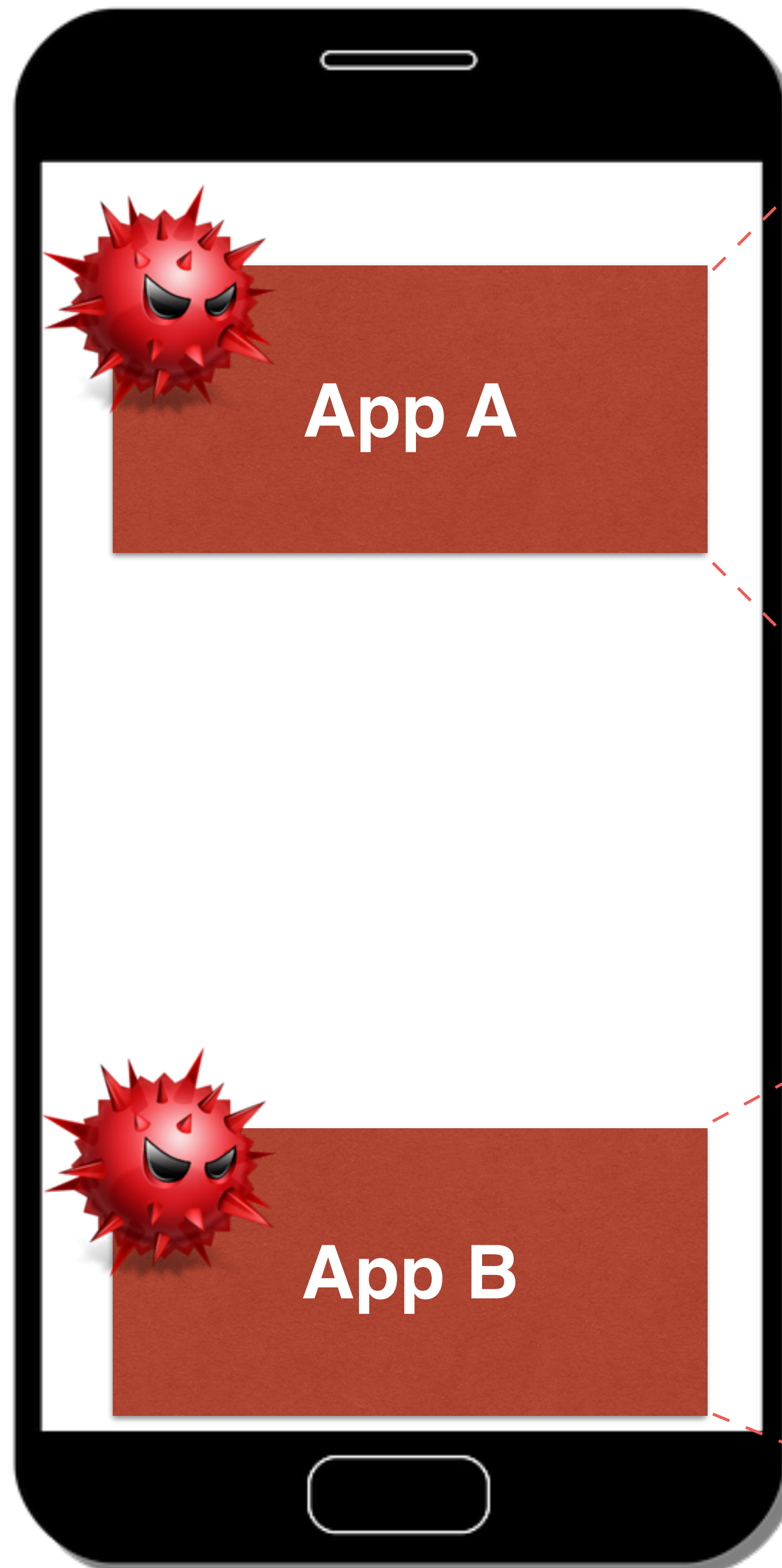
signature



Skype\_Permission



signature



App A

App B



Skype\_Permission



dangerous



Skype\_Permission



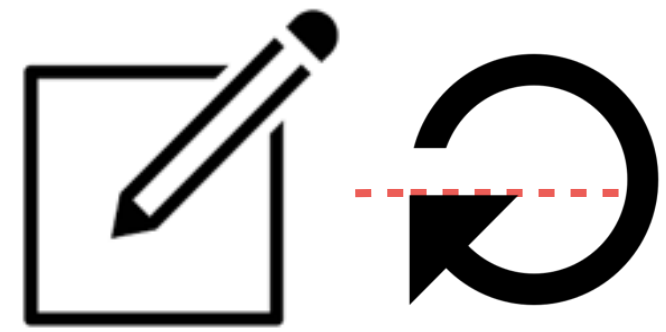
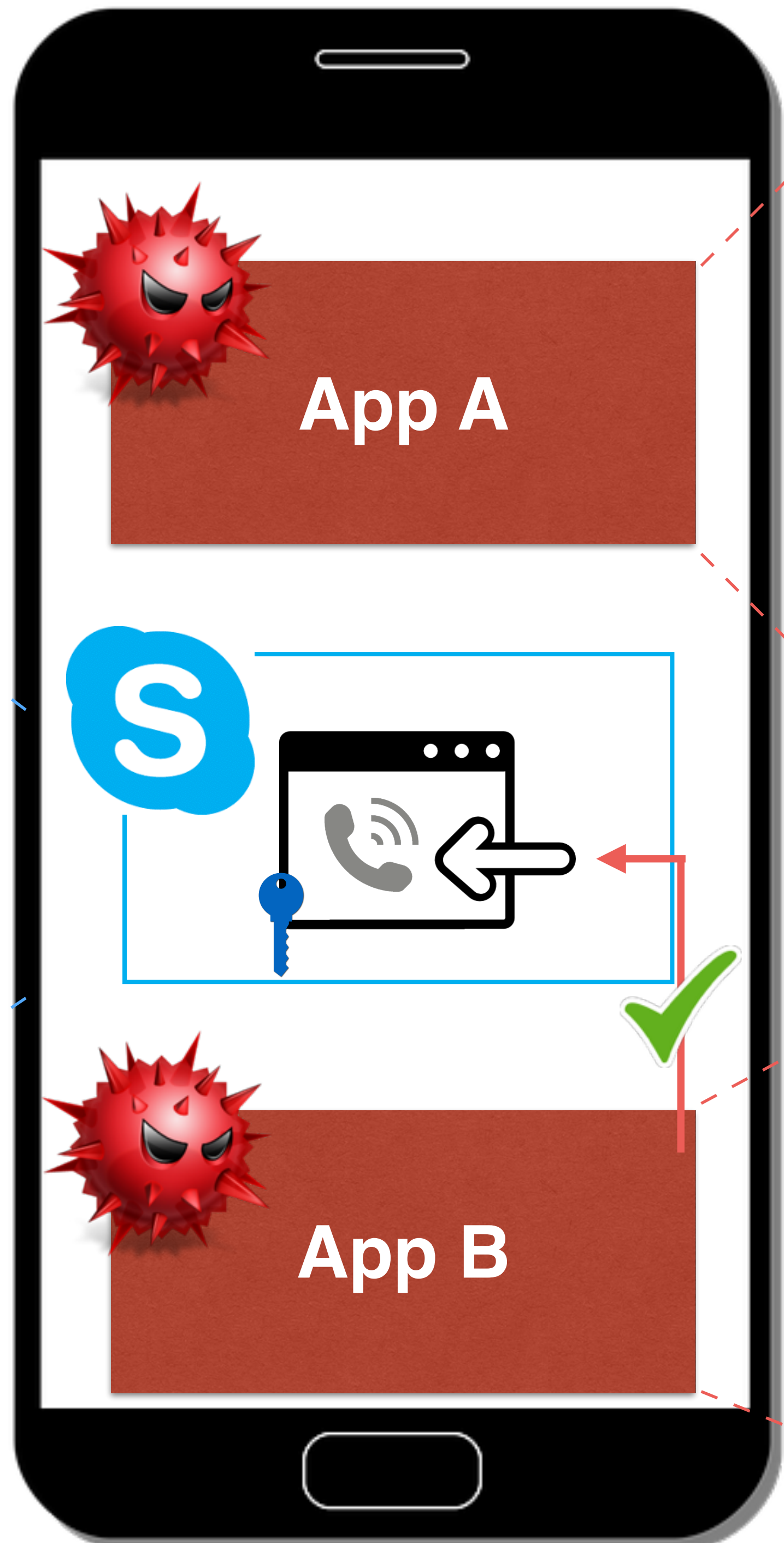
Granted



Skype\_Permission



signature



Skype\_Permission



dangerous



Skype\_Permission



signature

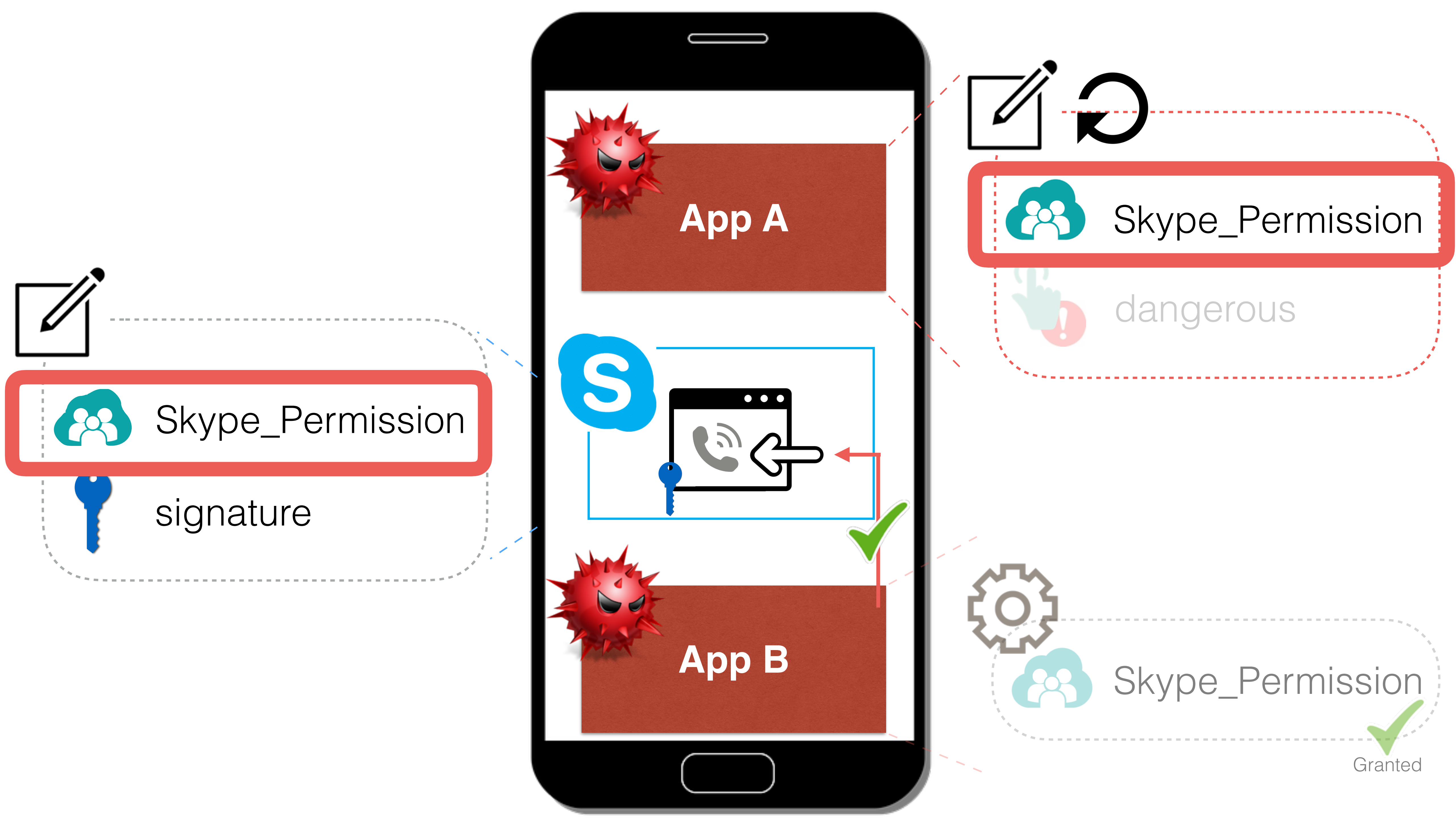


Skype\_Permission



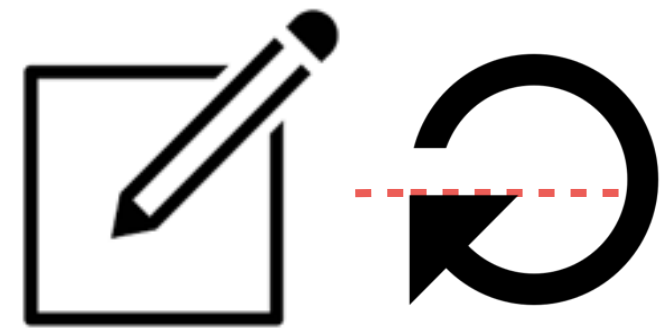
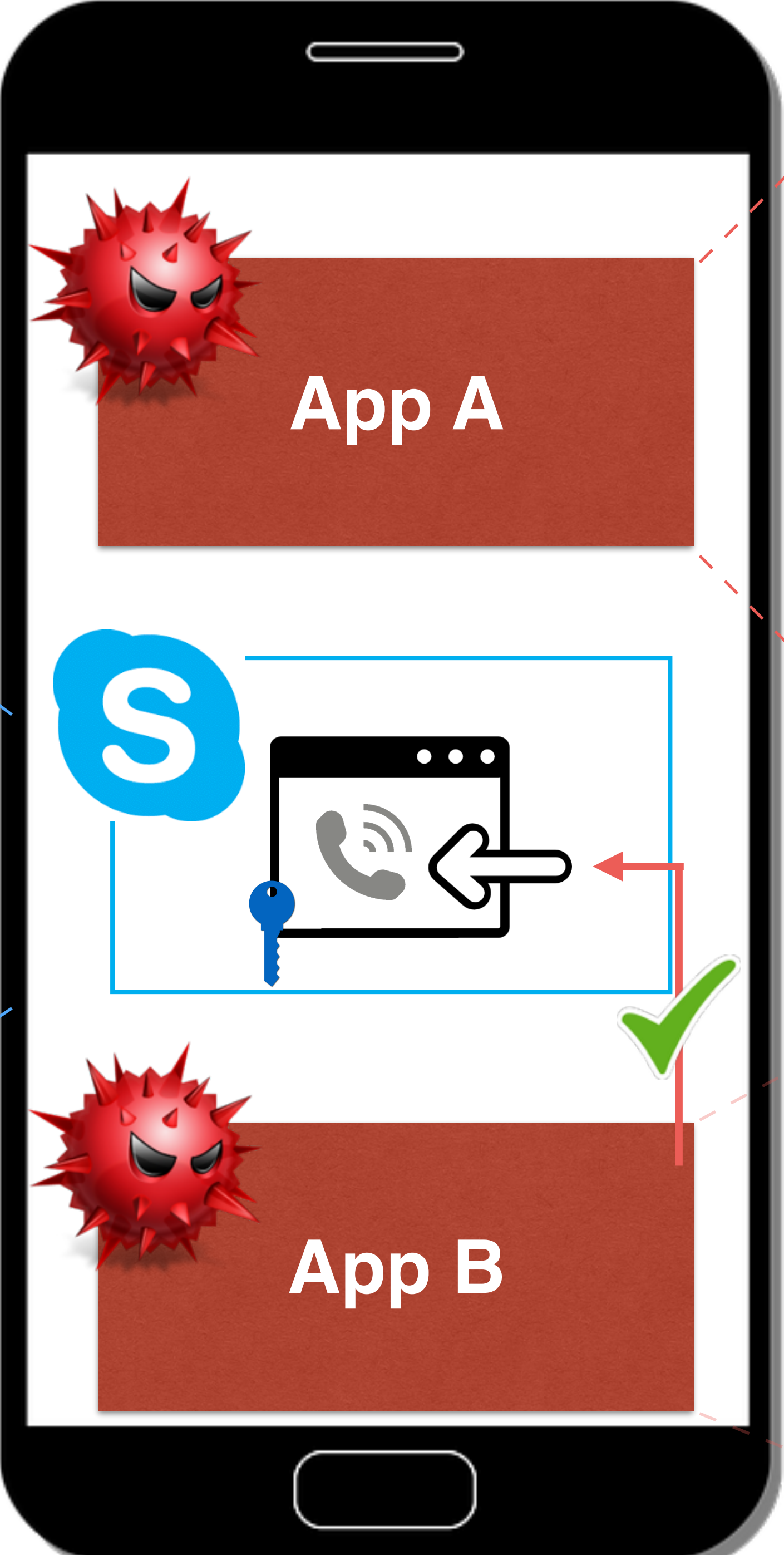
Granted





Skype\_Permission

signature



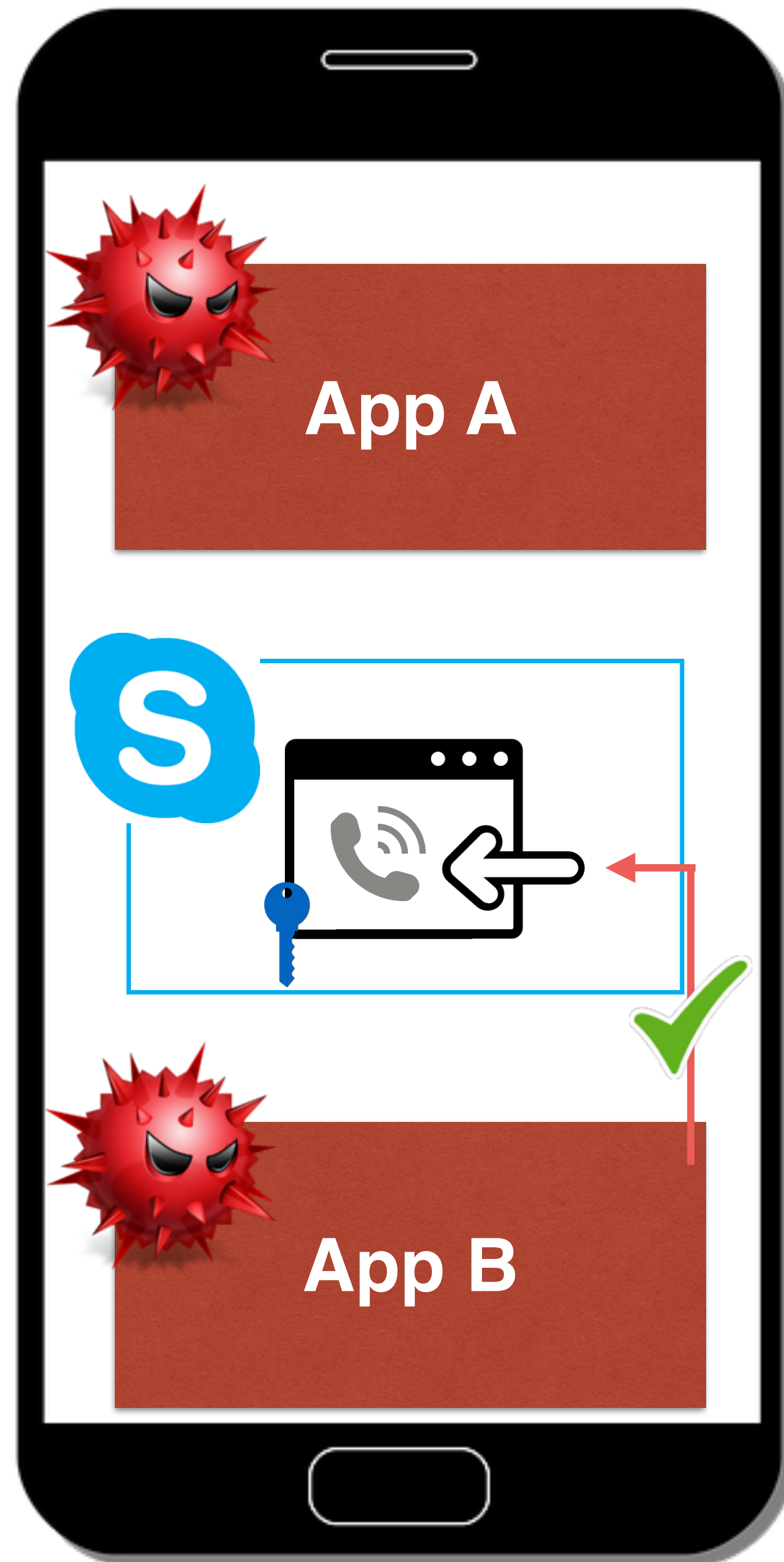
Skype\_Permission

dangerous



Skype\_Permission

Granted







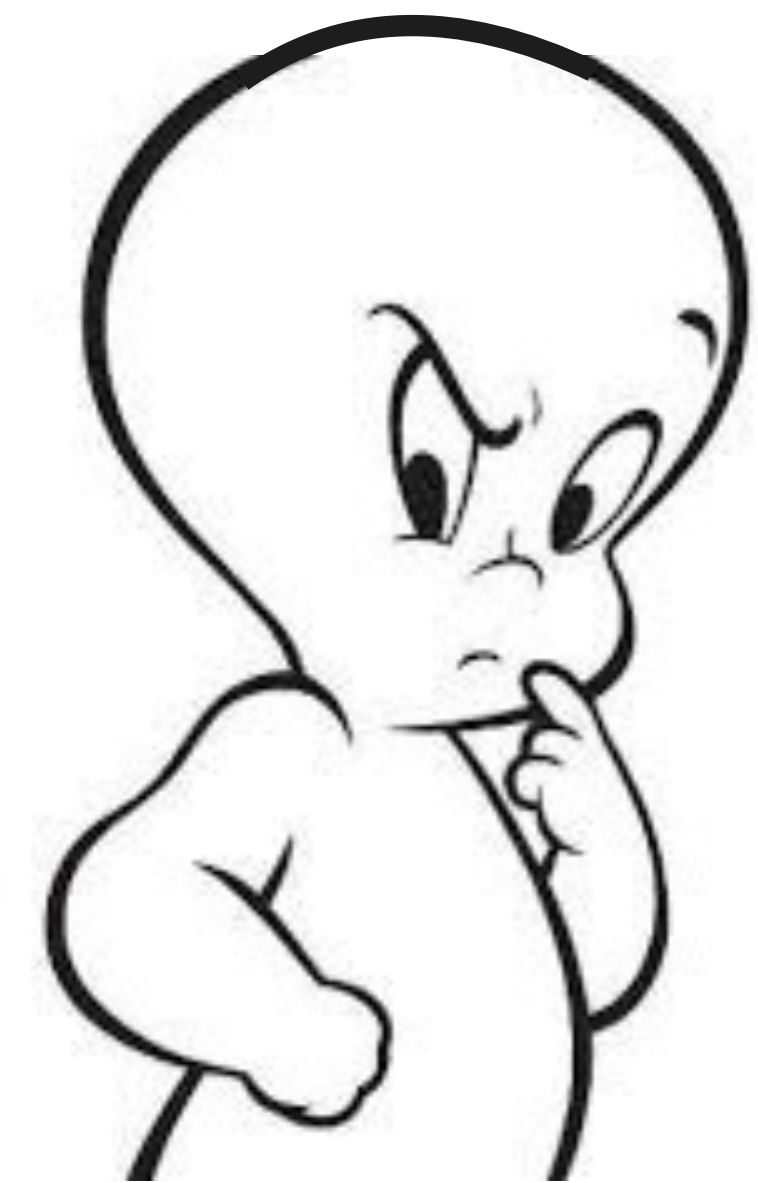






cusper

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





cusper

“considered to have been born on a **cus**p between significant generations”





android



cusper

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

—> **privilege escalation**

Custom permissions are claimed on a FCFS basis

—> **spoofing**

Software testing

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

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

**Formally verified** to be correct



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

—> **privilege escalation**

Custom permissions are claimed on a FCFS basis

—> **spoofing**

Software testing

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

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

**Formally verified** to be correct



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

—> **privilege escalation**

Custom permissions are claimed on a FCFS basis

—> **spoofing**

Software testing

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

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

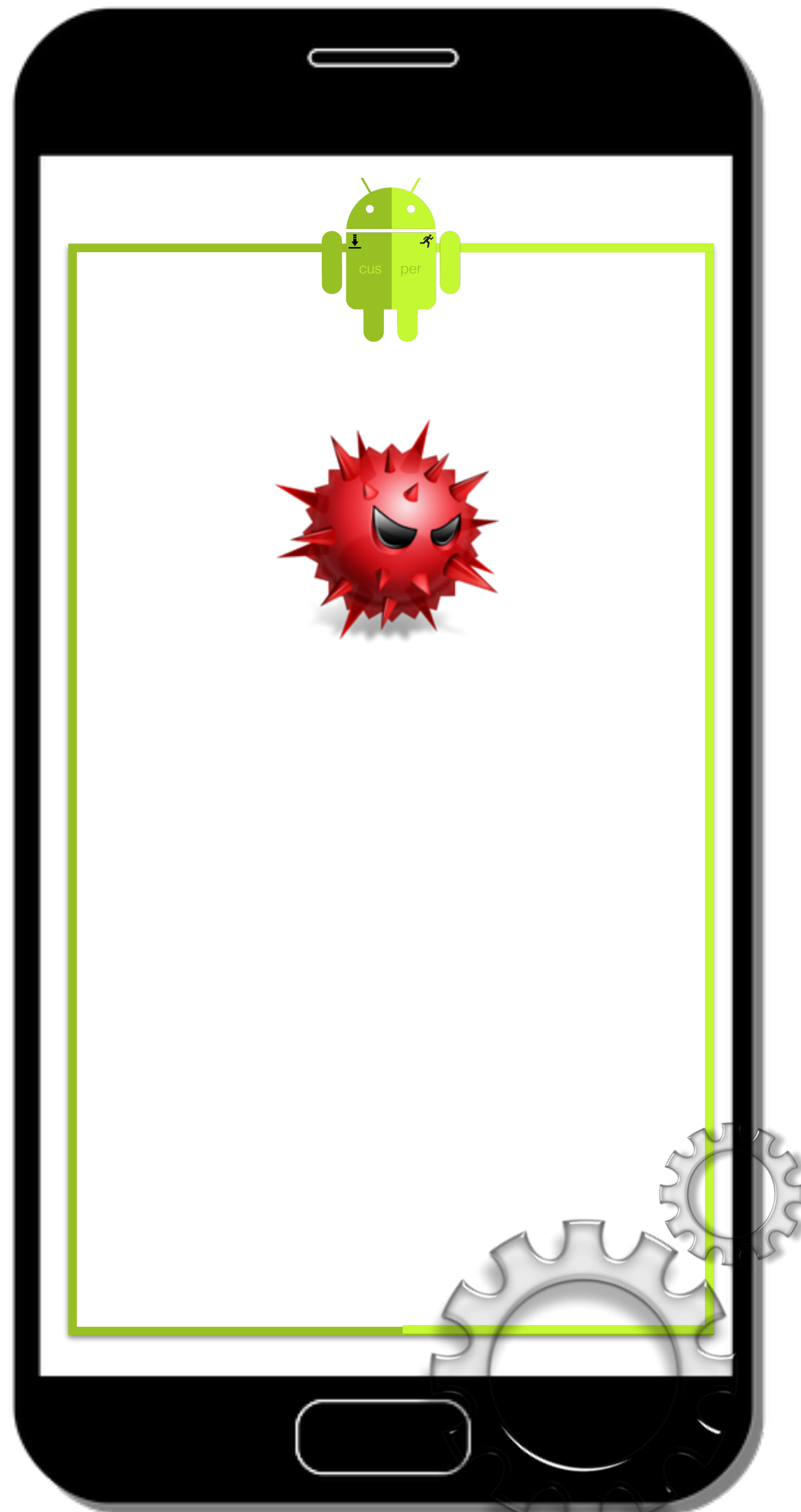
**Formally verified** to be correct

# Cusper enhancements

declaring a custom permission



Skype\_Permission



FINE\_LOCATION

RECORD\_AUDIO

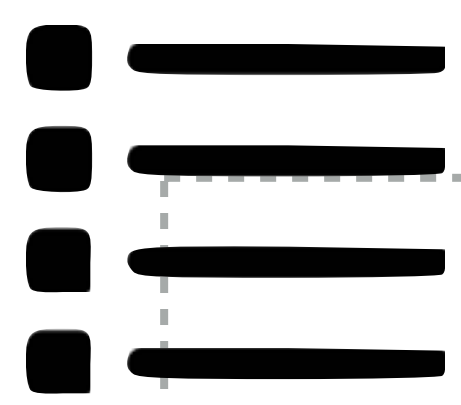
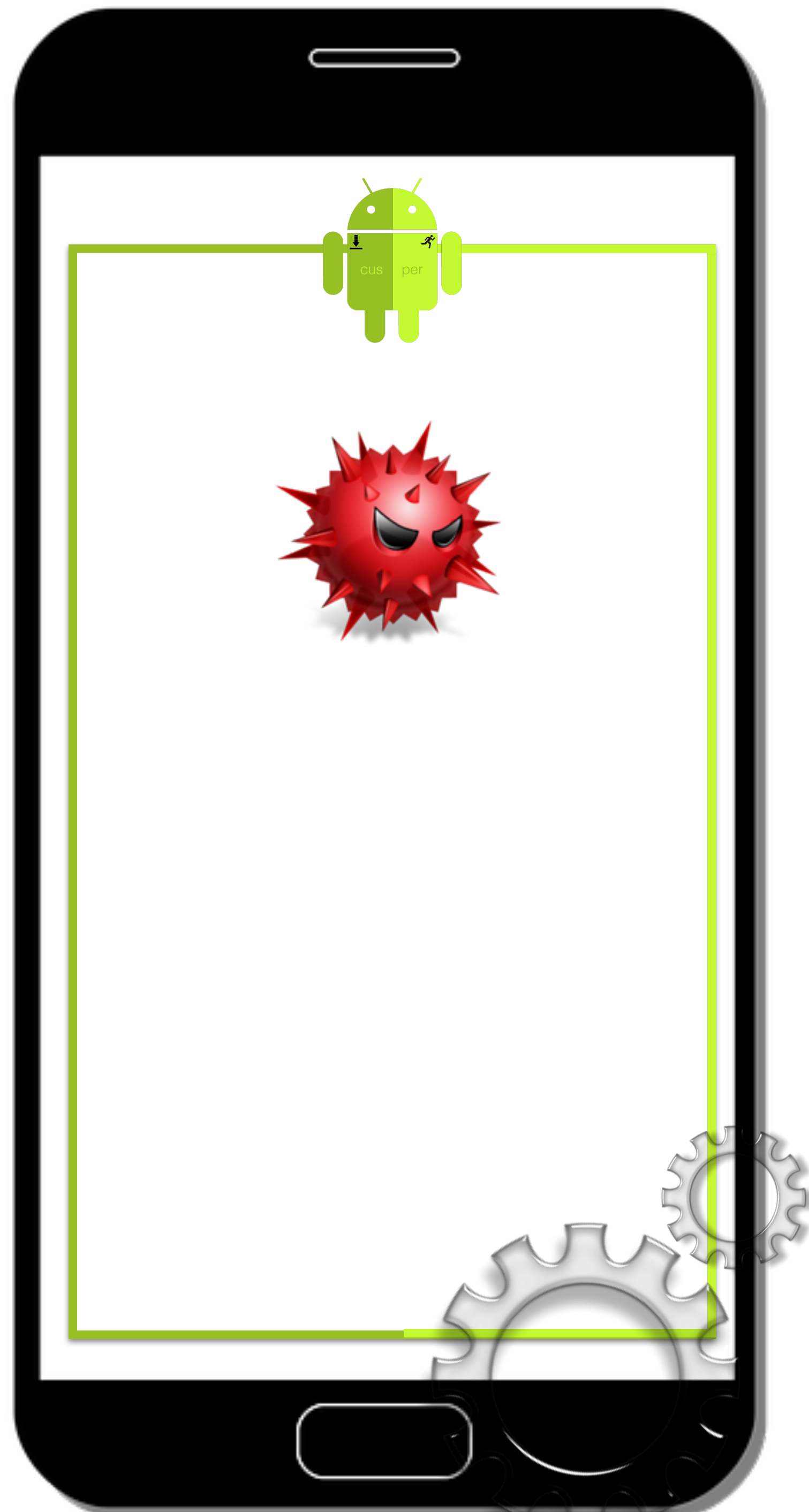
CAMERA

# Cusper enhancements

declaring a custom permission



Skype\_Permission



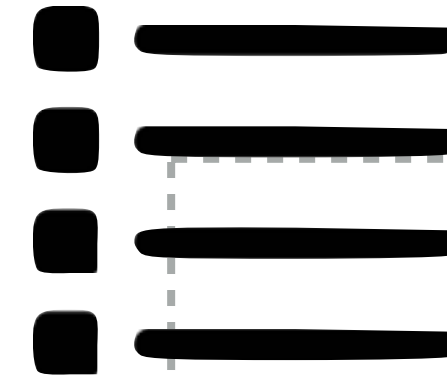
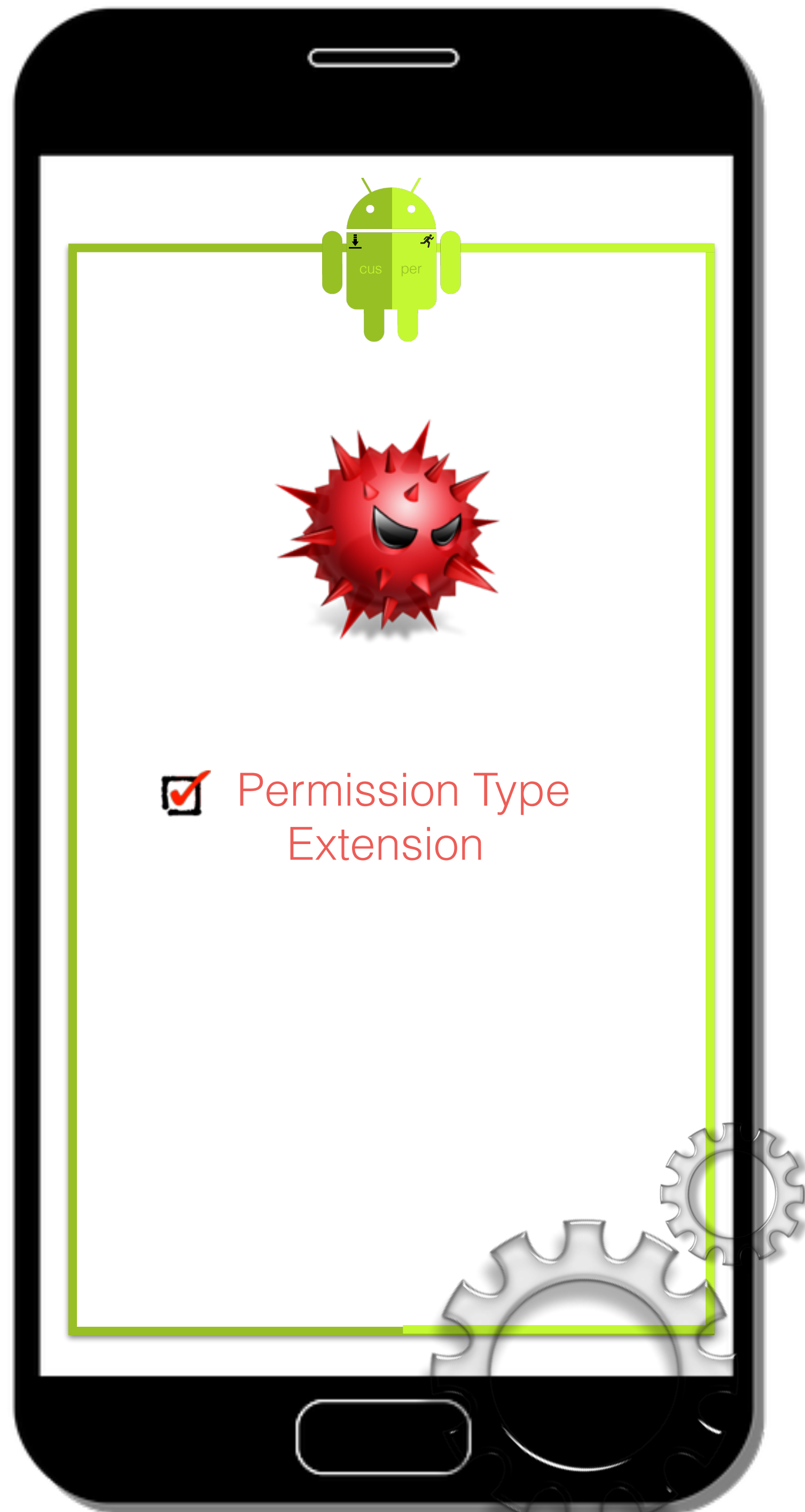
- FINE\_LOCATION
- RECORD\_AUDIO
- CAMERA
- Skype\_Permission

# Cusper enhancements

declaring a custom permission



Skype\_Permission



FINE\_LOCATION



RECORD\_AUDIO



CAMERA



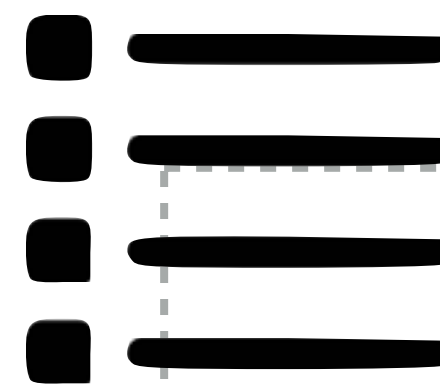
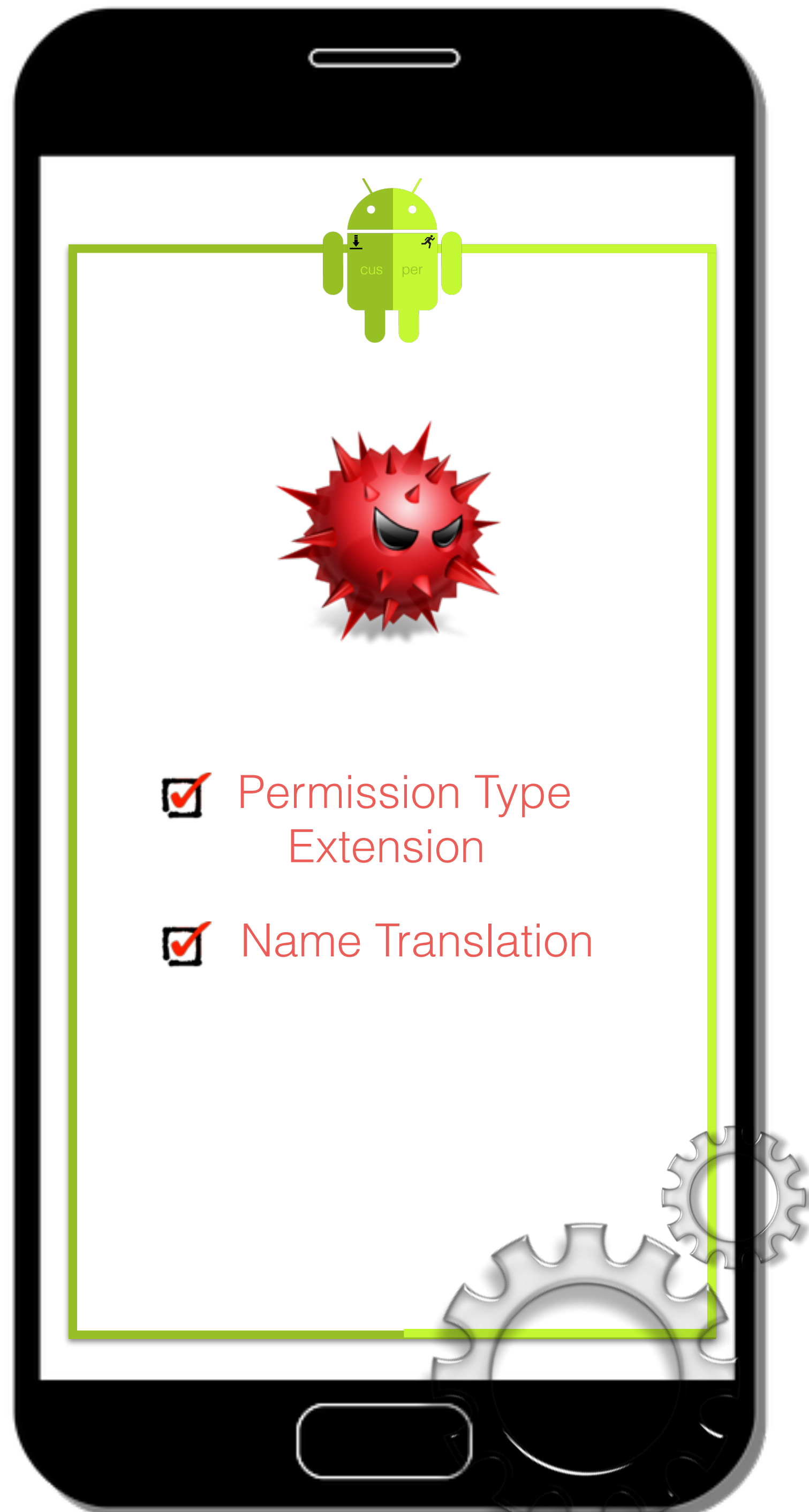
Skype\_Permission

# Cusper enhancements

declaring a custom permission



Skype\_Permission



FINE\_LOCATION



RECORD\_AUDIO



CAMERA



:Skype\_Permission

# Cusper enhancements

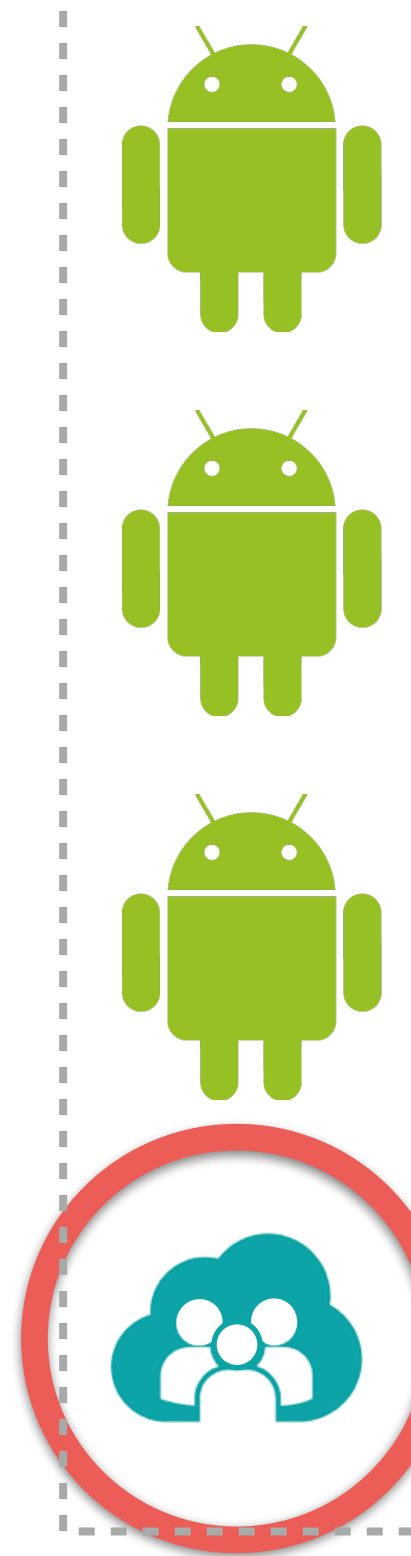
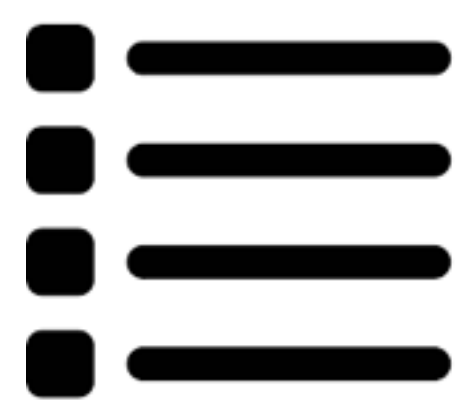
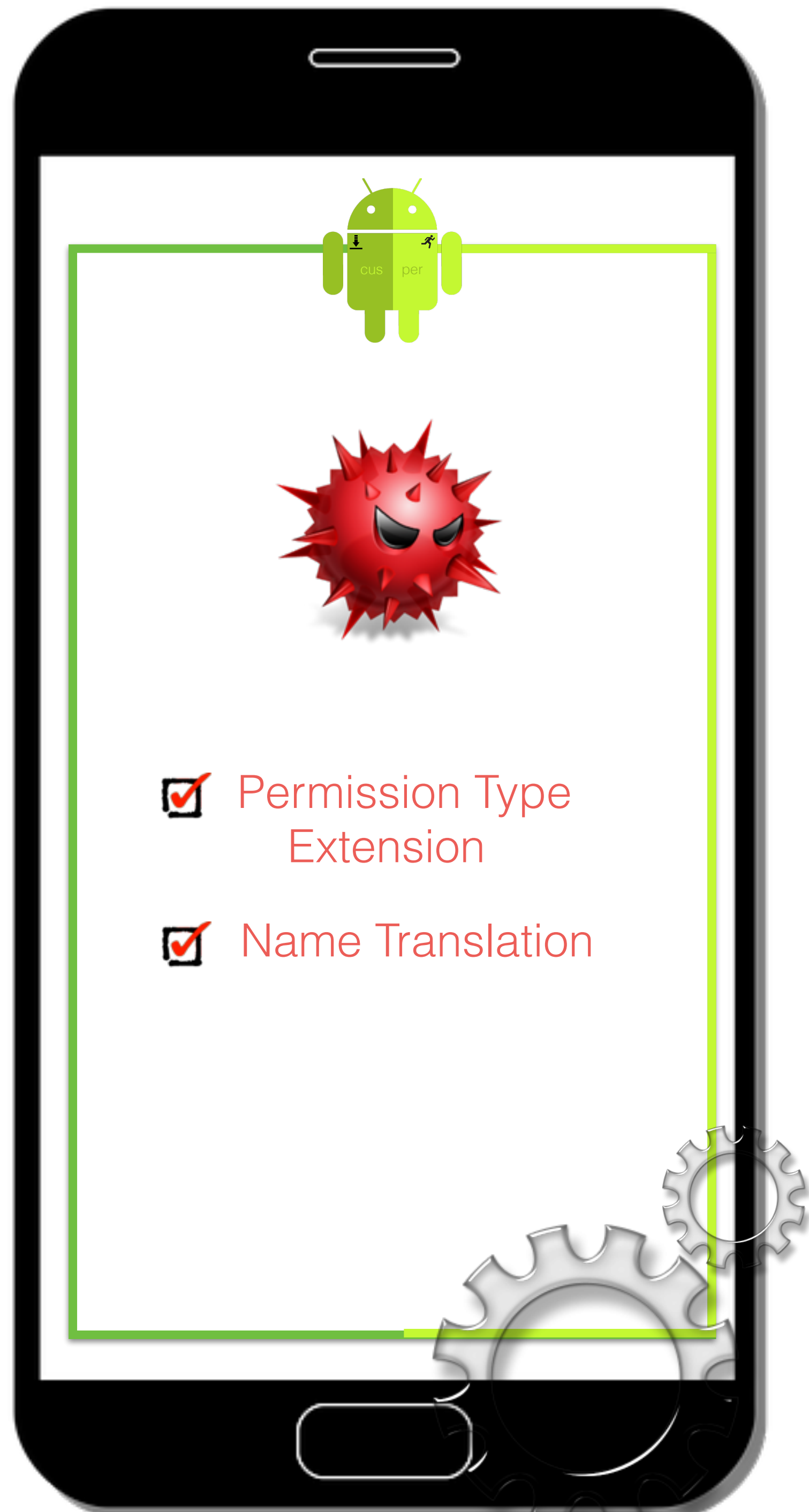
declaring a custom permission



Skype\_Permission



Microphone Group



FINE\_LOCATION

RECORD\_AUDIO

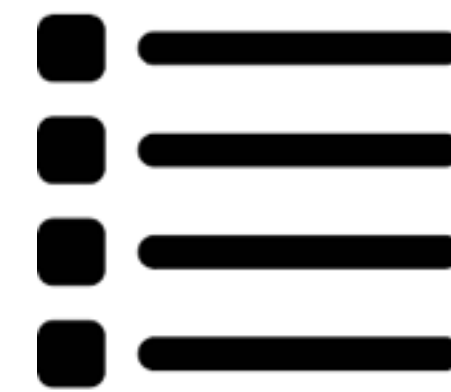
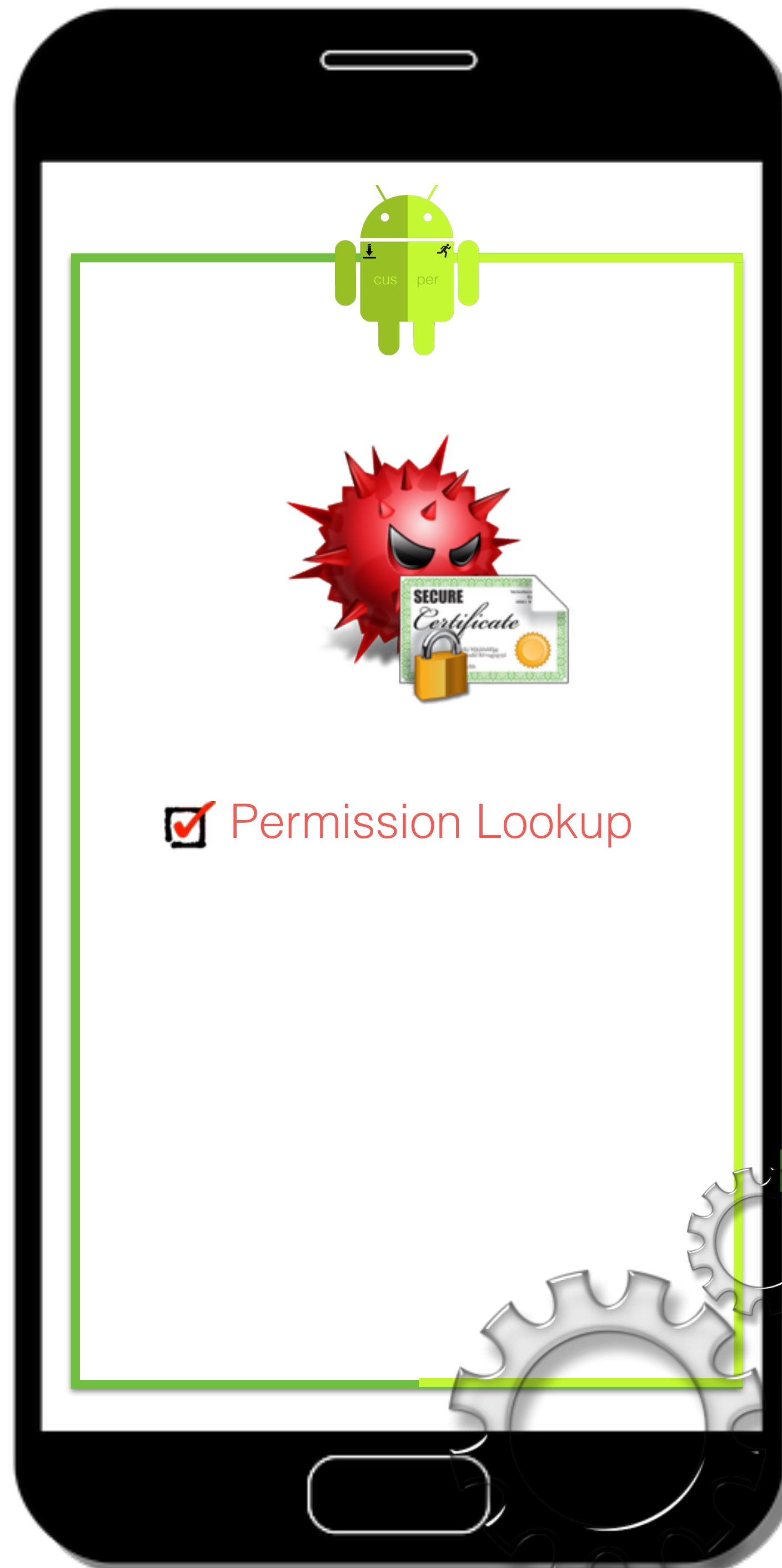
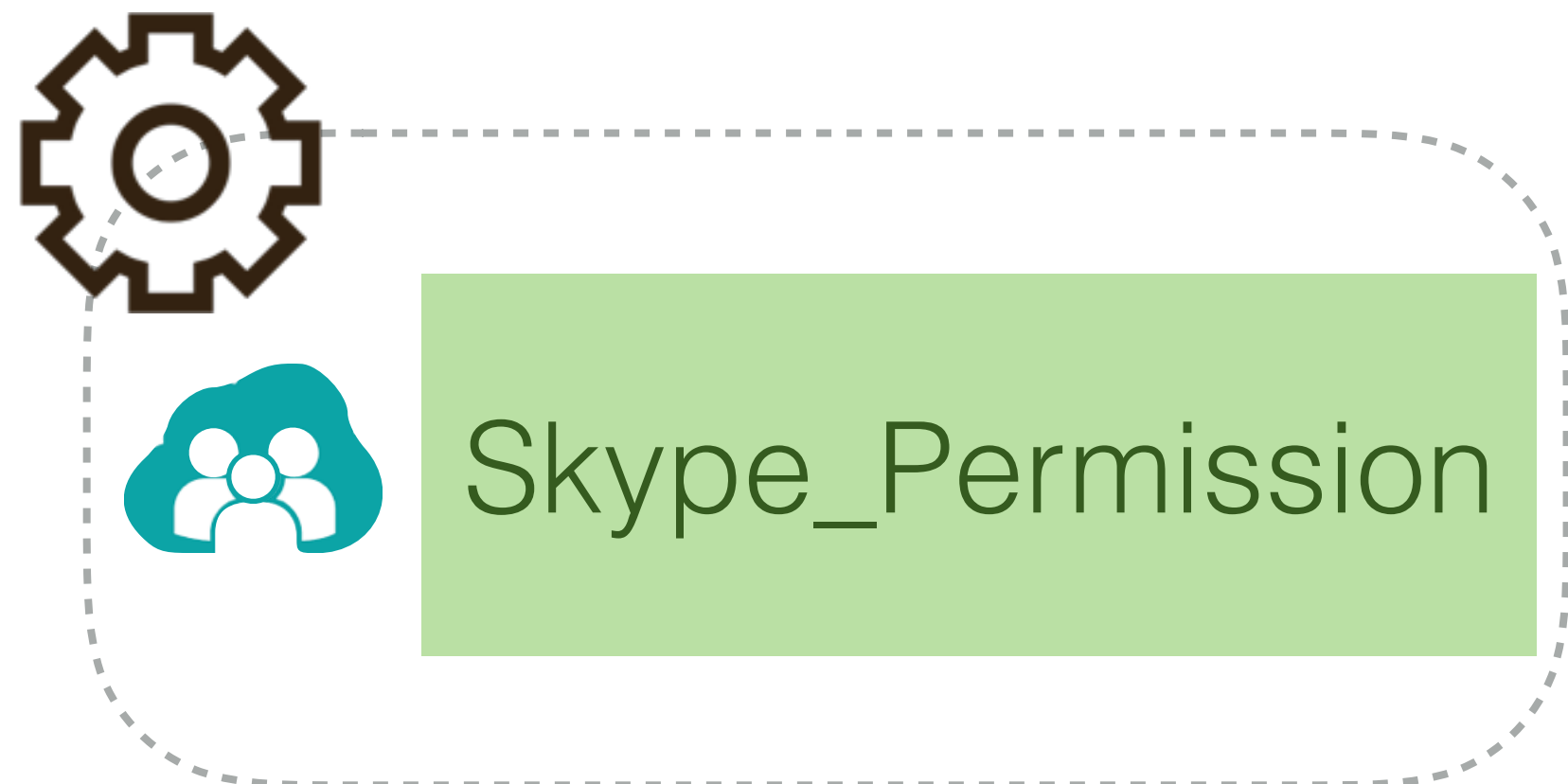
CAMERA






Skype\_Permission



# Cusper enhancements

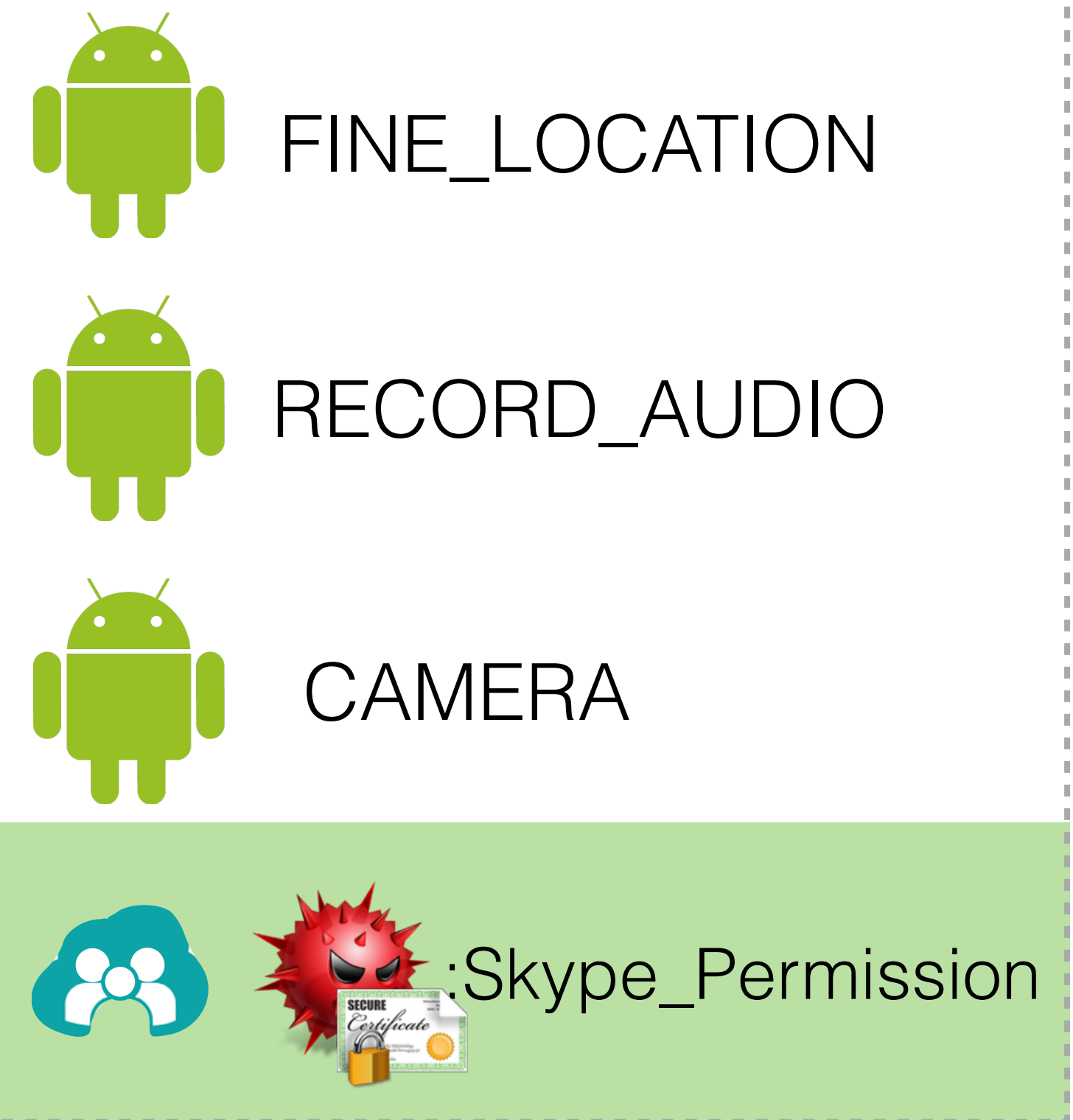
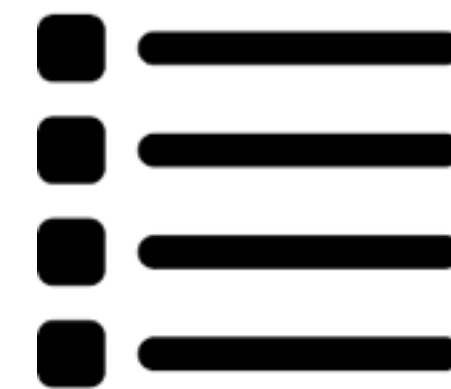
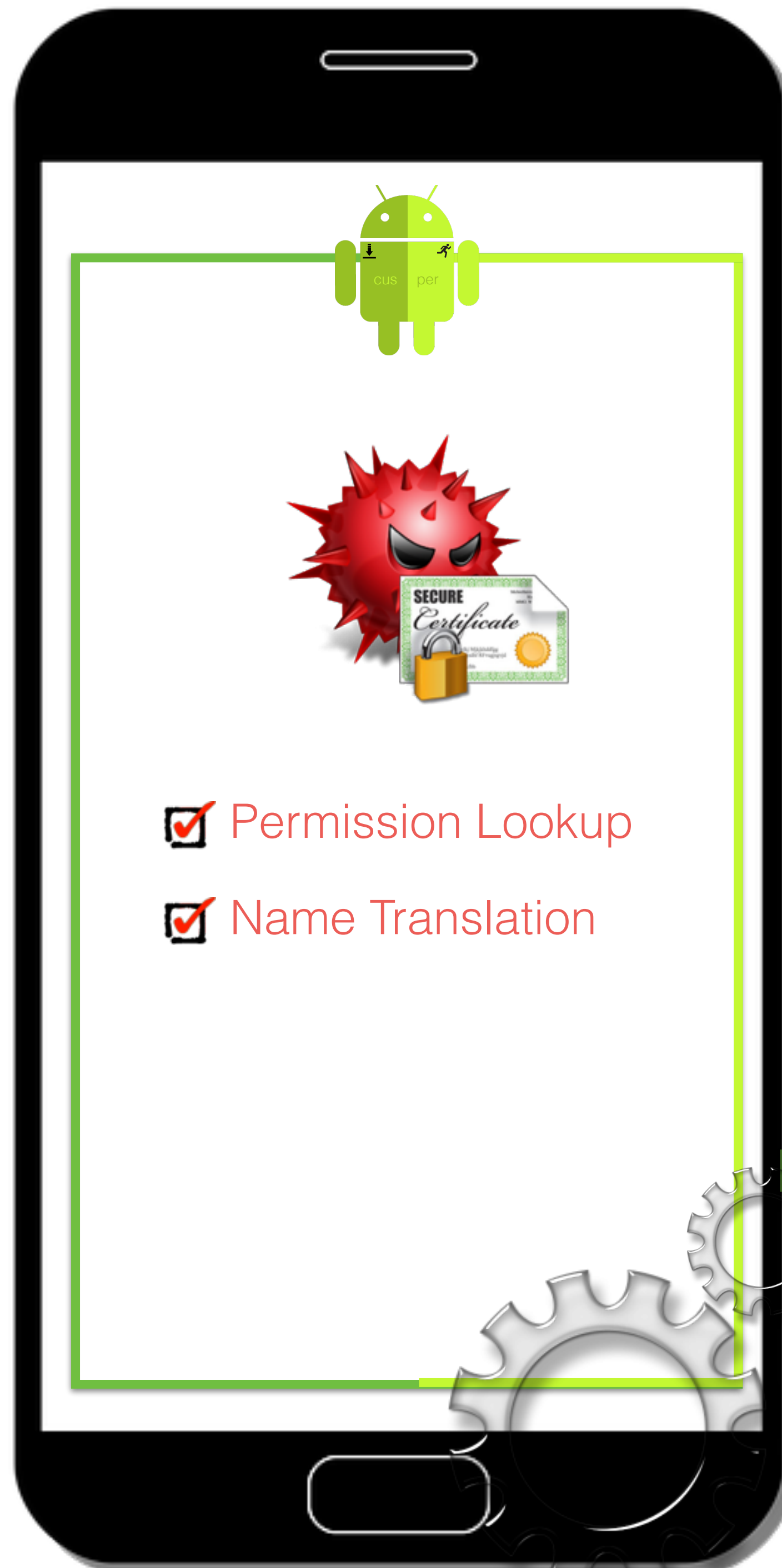
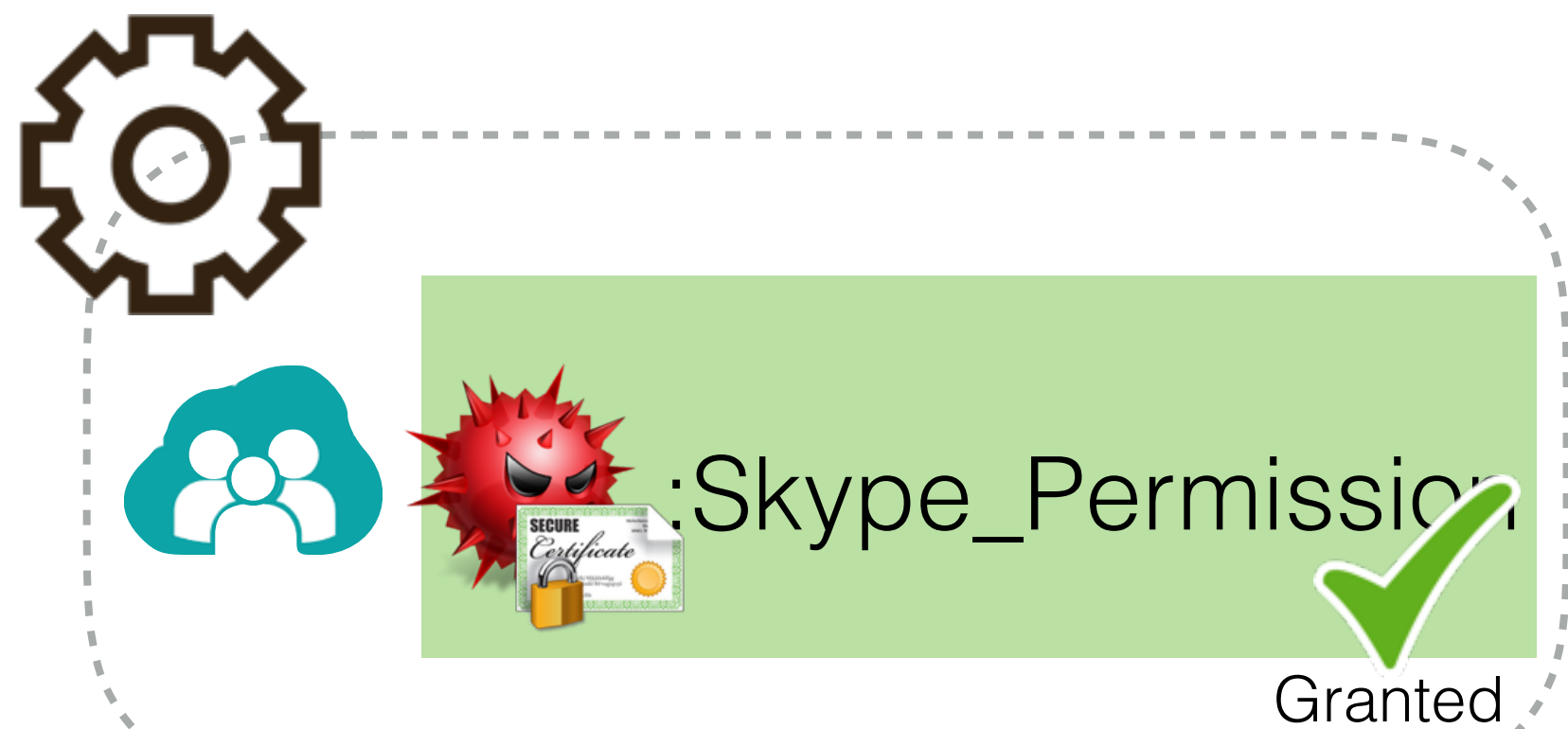
granting a custom permission



-  FINE\_LOCATION
-  RECORD\_AUDIO
-  CAMERA
-   :Skype\_Permission

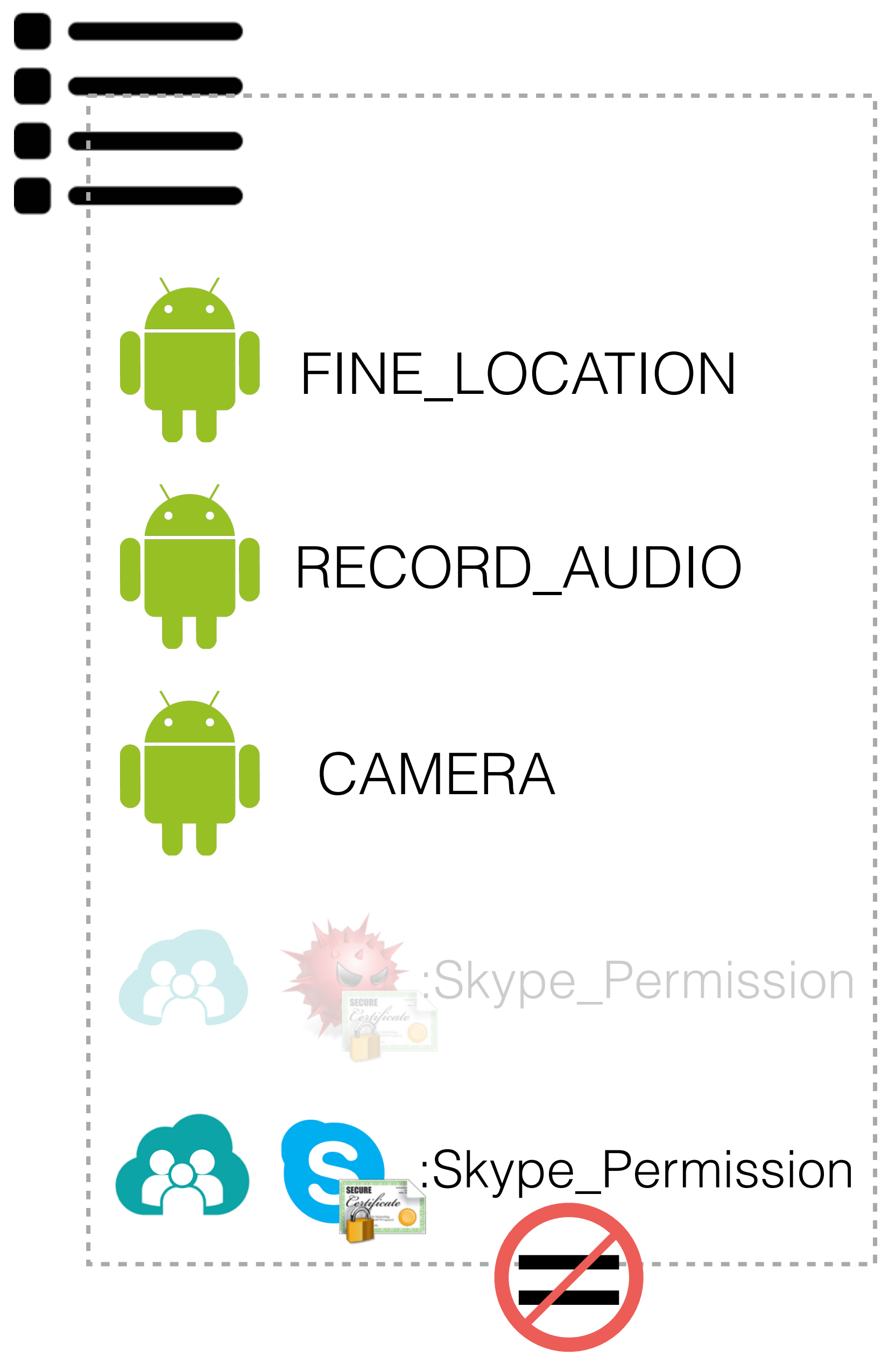
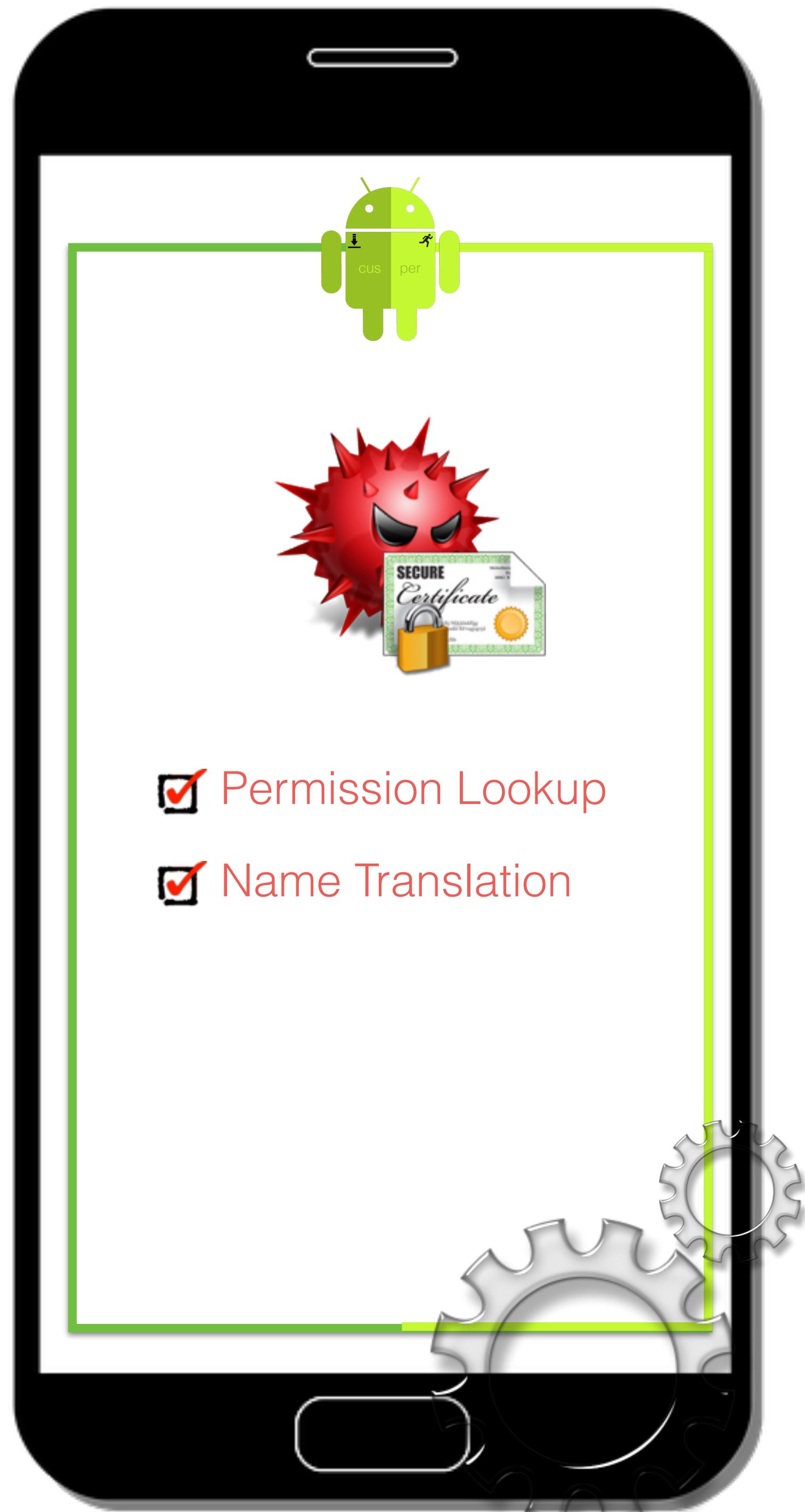
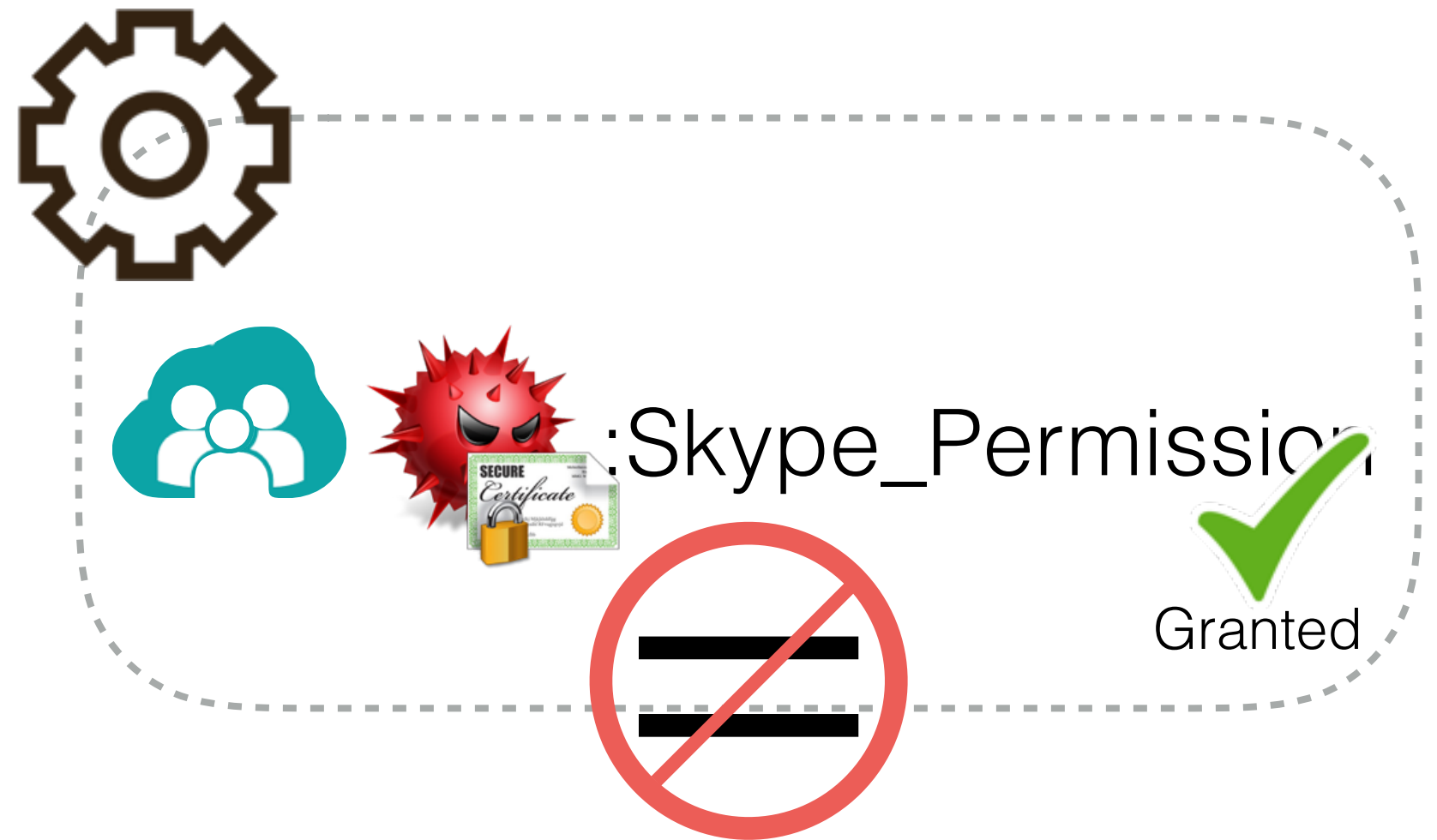
# Cusper enhancements

granting a custom permission



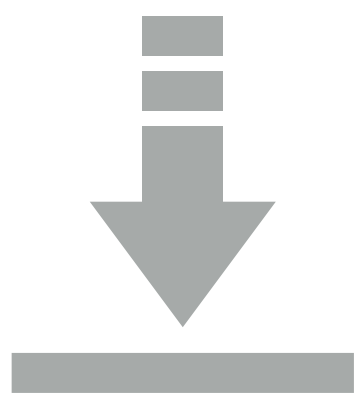
# Cusper enhancements

granting a custom permission

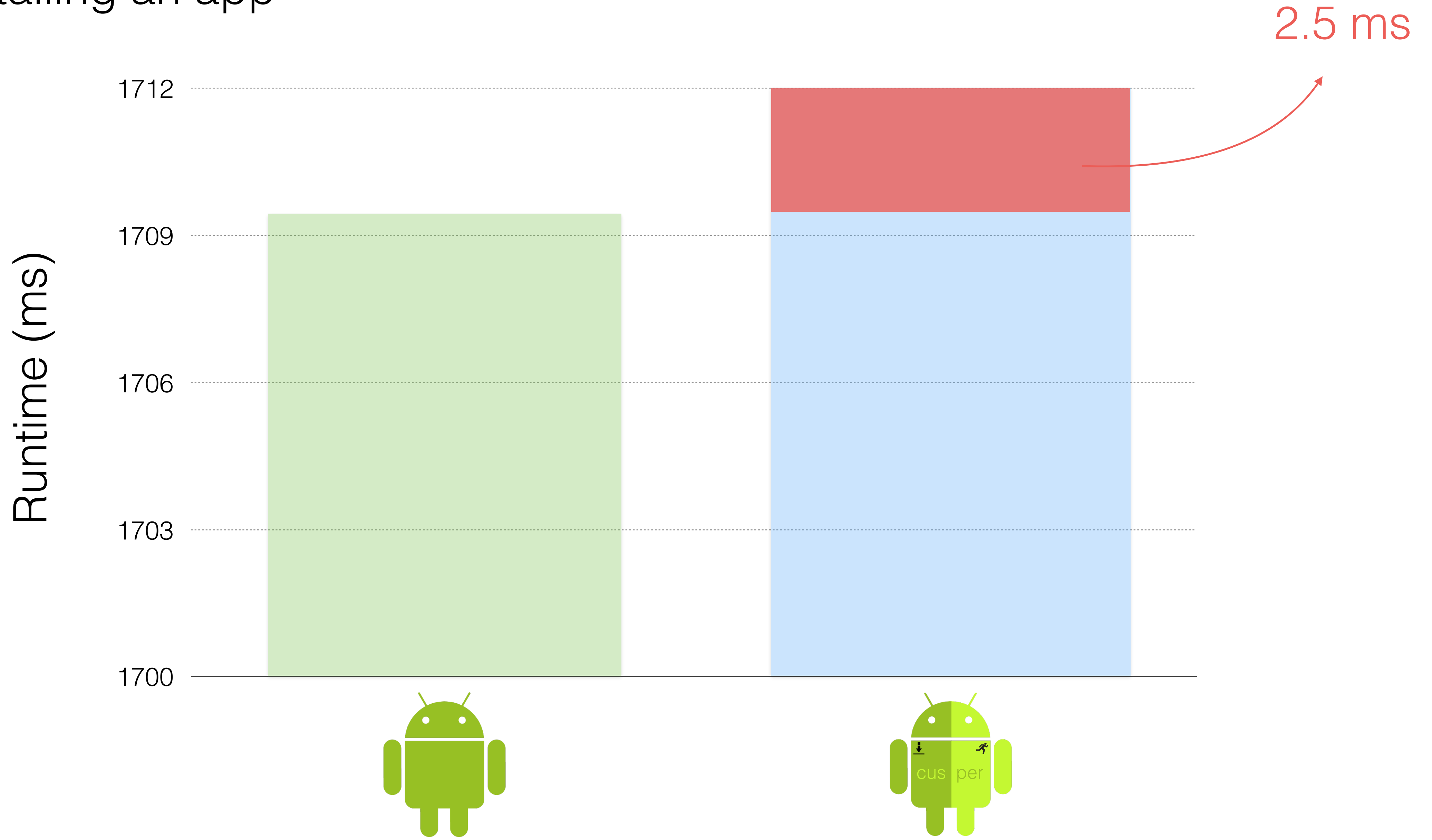




performance

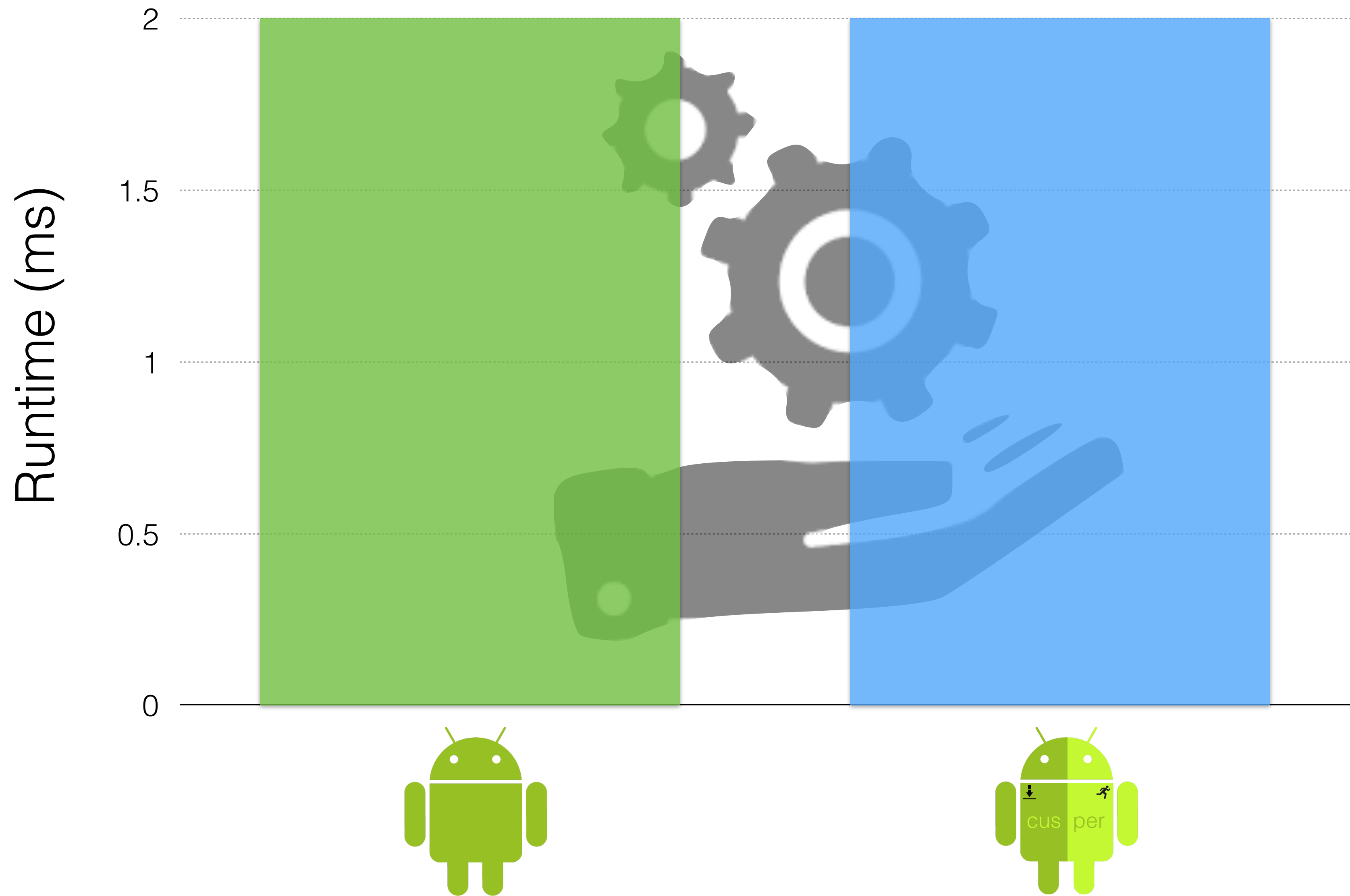


installing an app



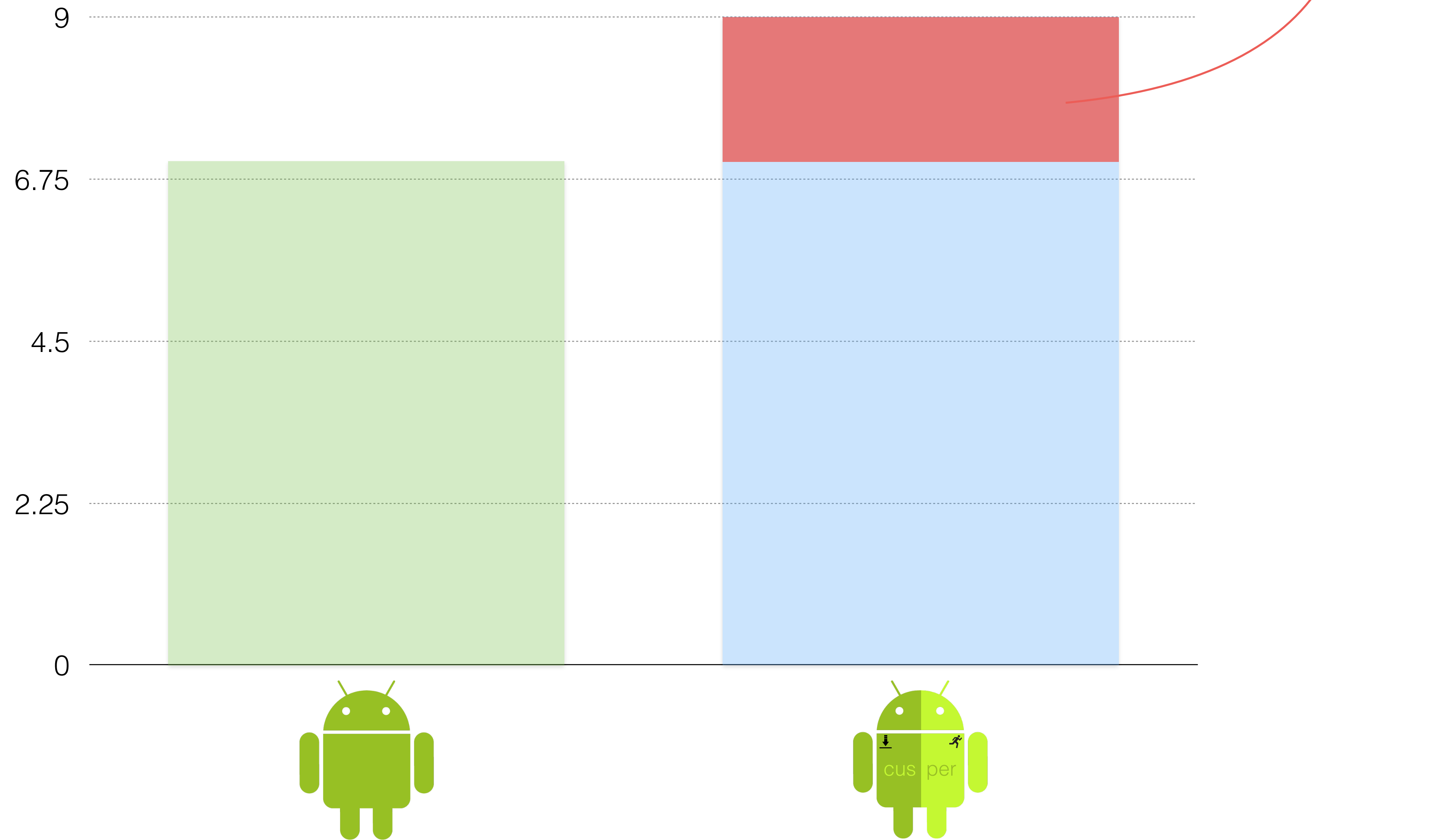


granting a signature permission to access a **service**



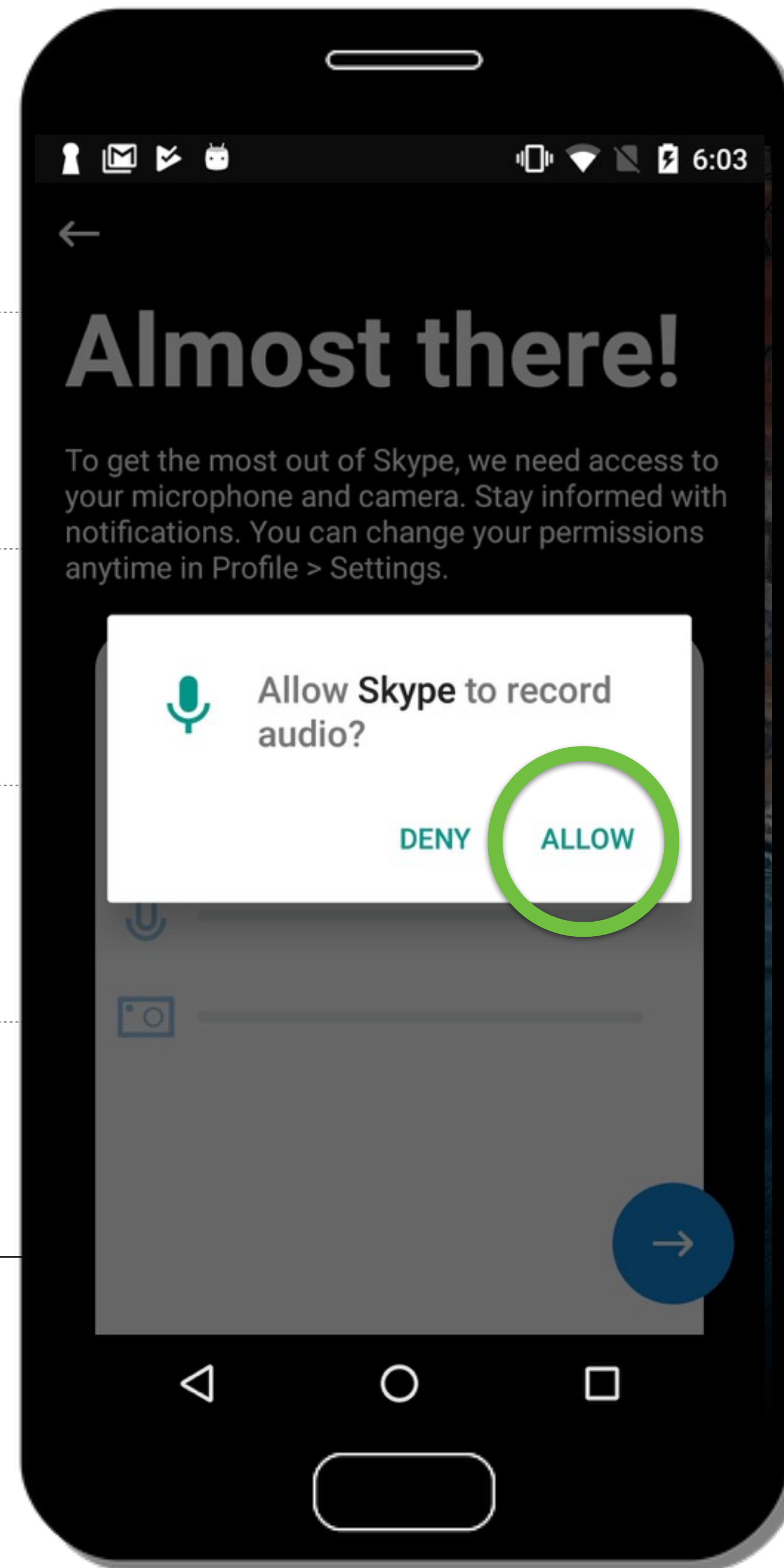
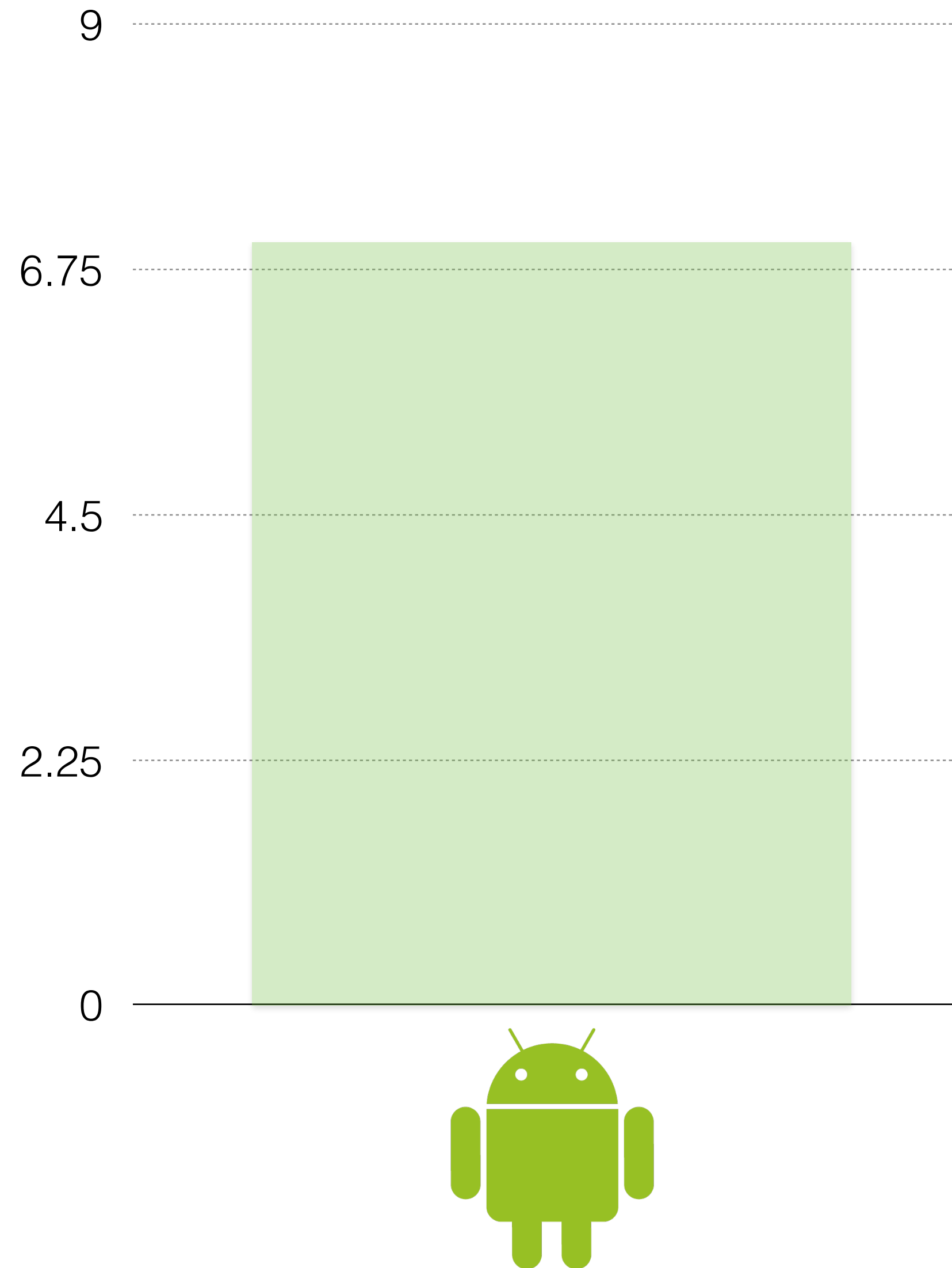


# granting a dangerous permission





granting a dangerous permission



2 ms





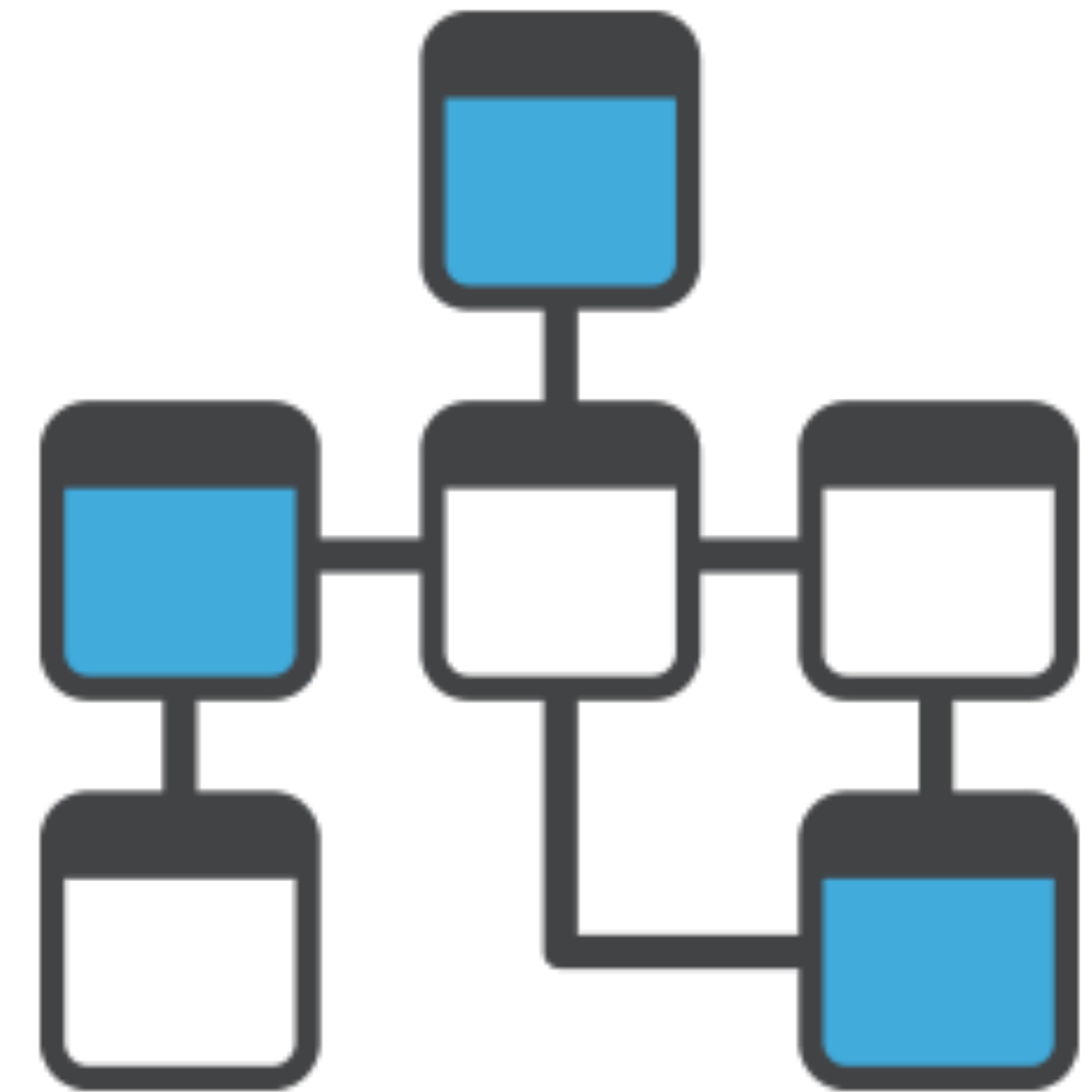
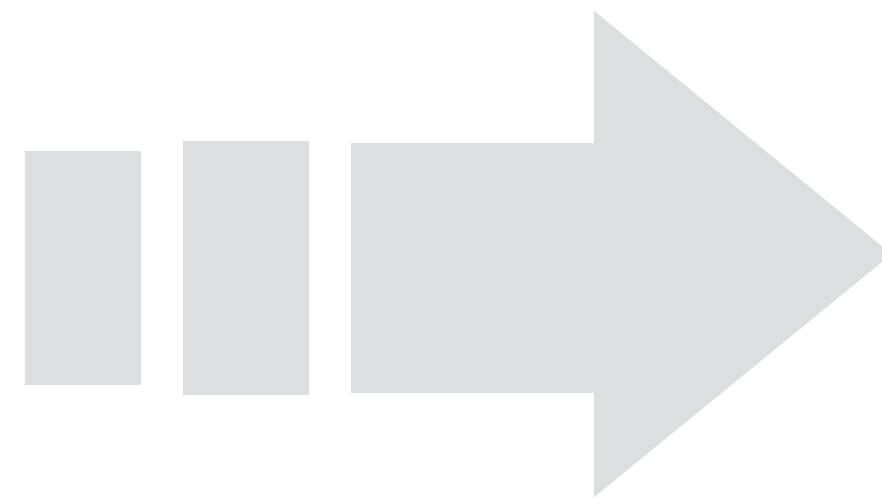
effectiveness

Formal Verification

formal verification



Implementation

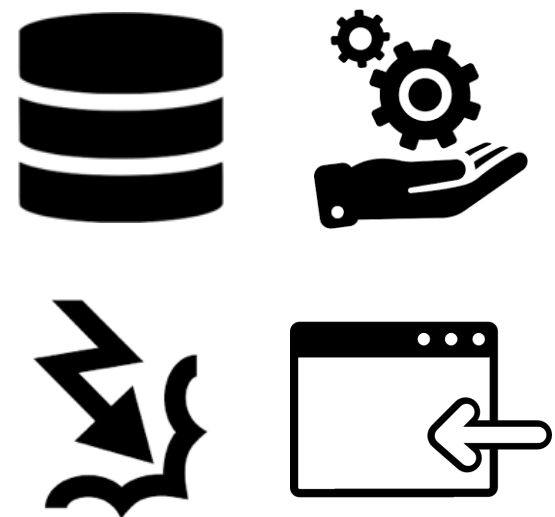


Alloy Model

# 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.

