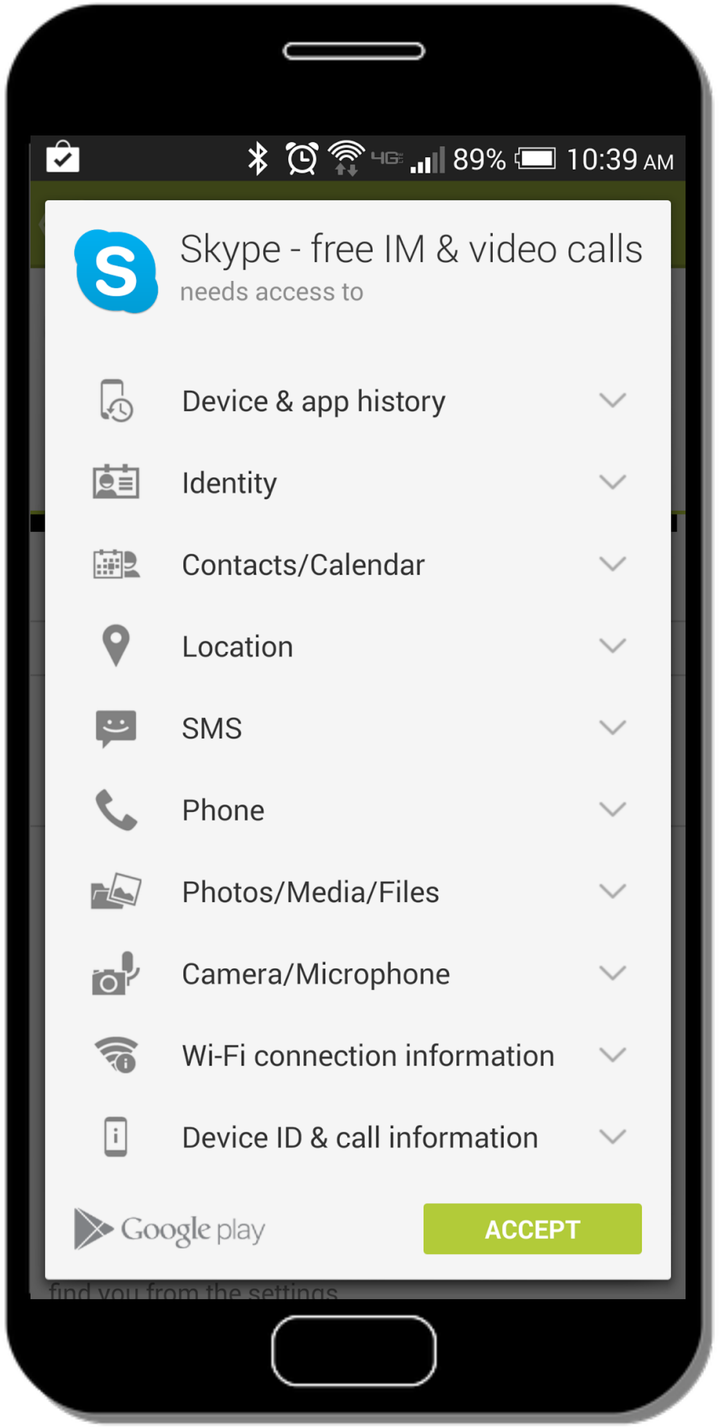
See No Evil: Phishing for Permissions with False Transparency

Güliz Seray Tuncay*†, Jingyu Qian†, Carl A. Gunter†

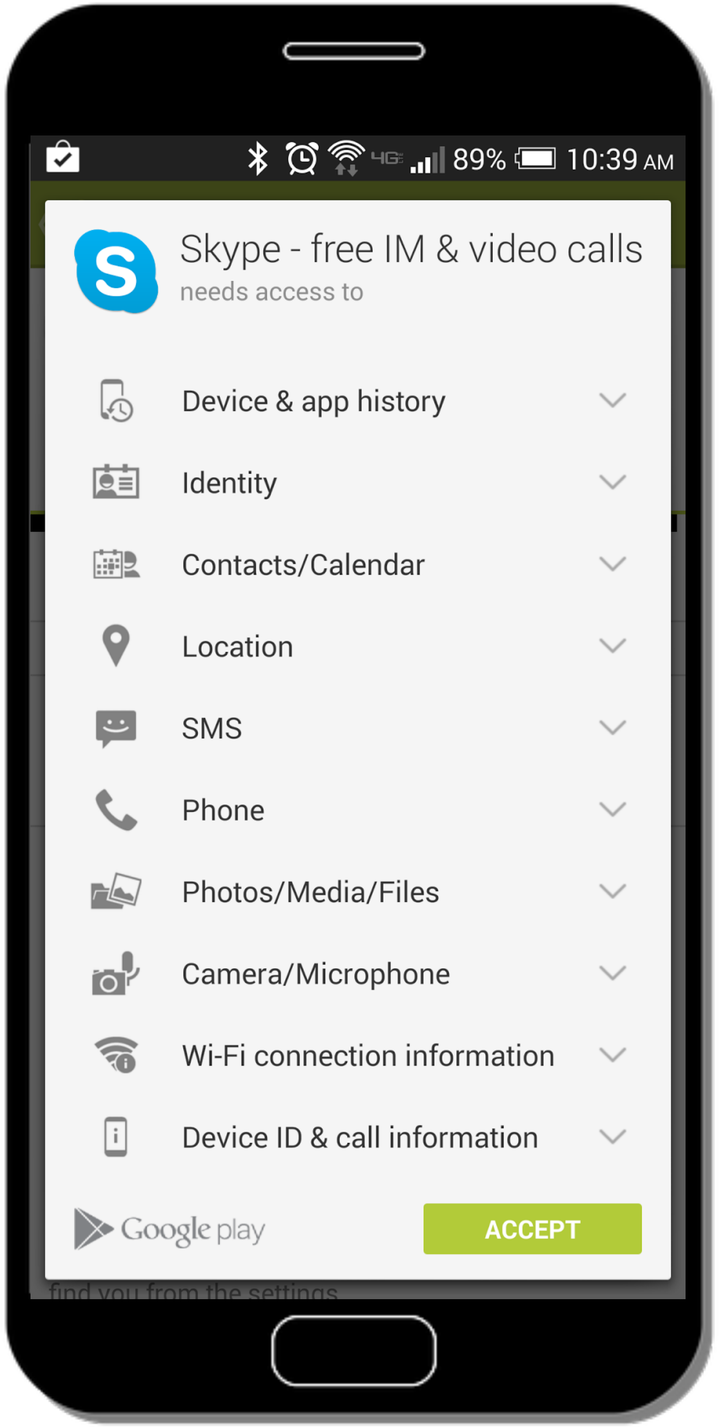
*Google, †University of Illinois at Urbana-Champaign

Install-time Permissions
< Android 6.0



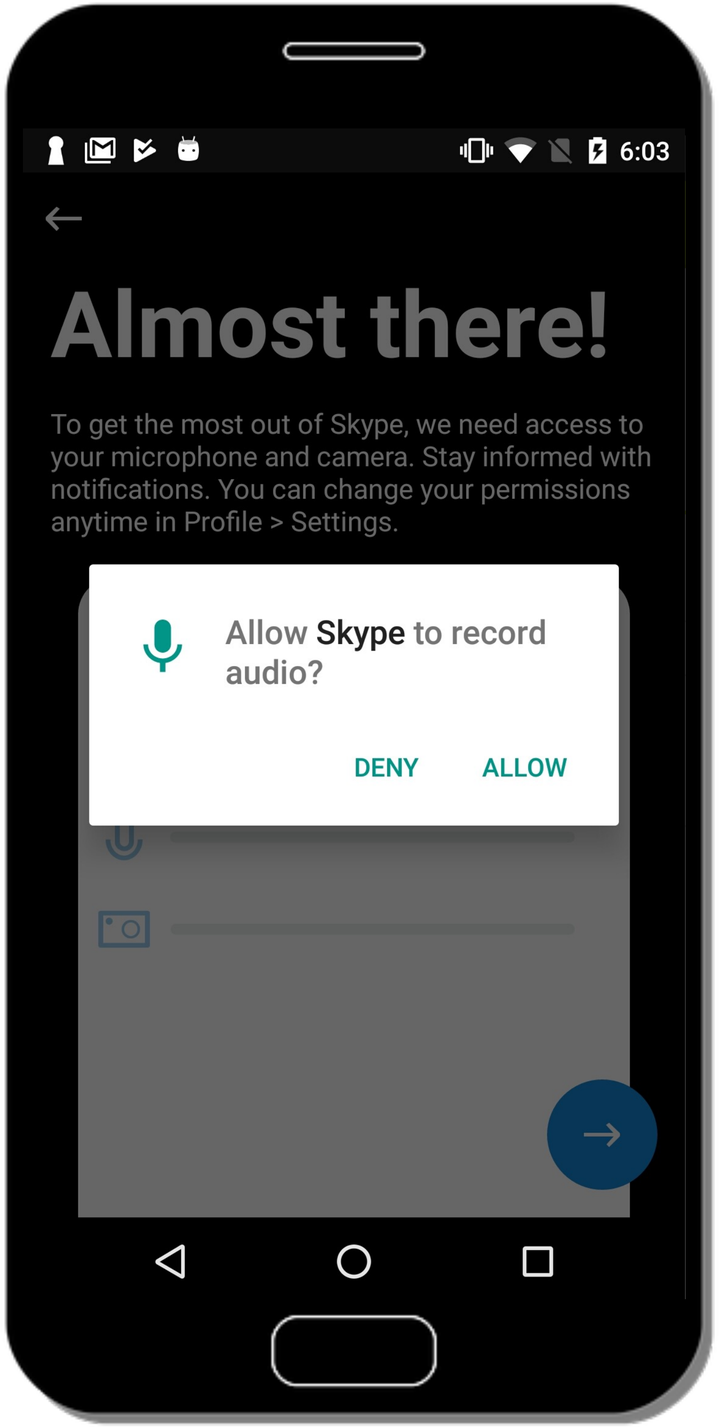
Install-time Permissions
< Android 6.0

lack of context



Install-time Permissions
< Android 6.0

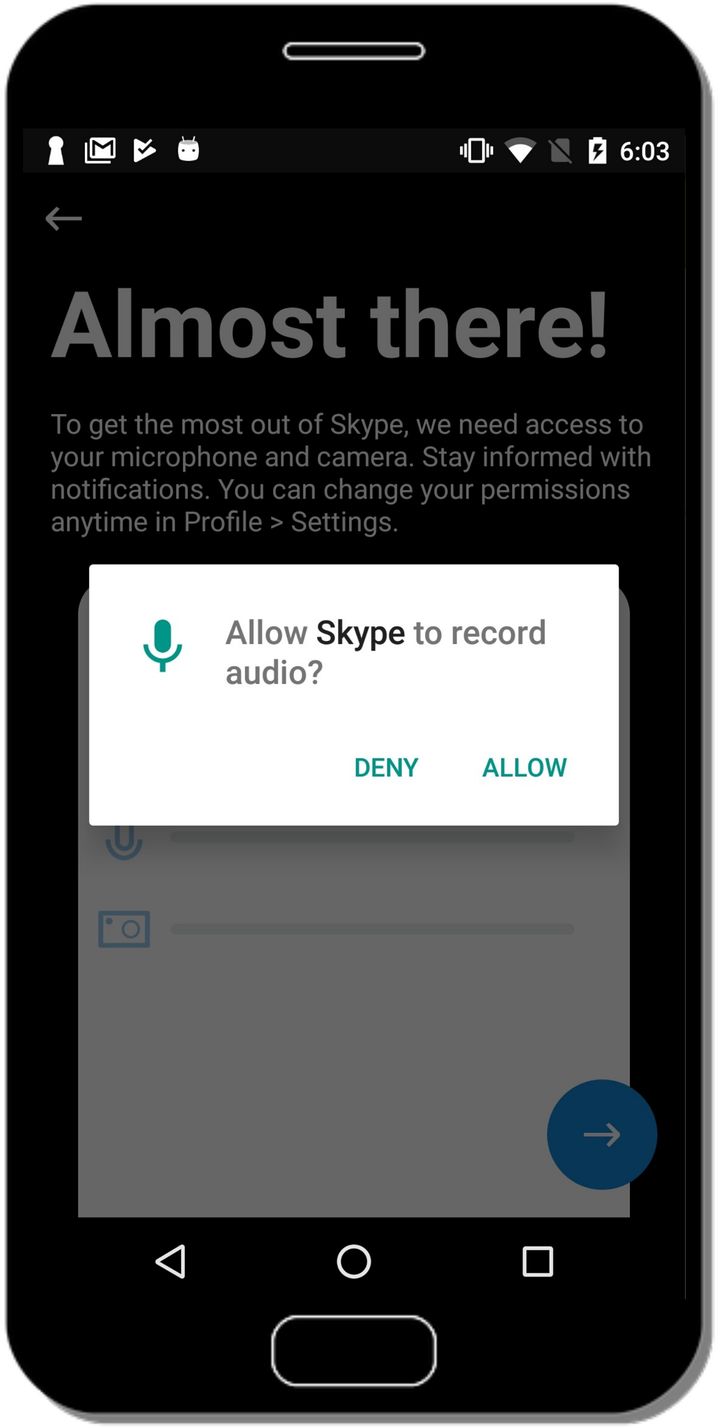
lack of context



Runtime Permissions
>= Android 6.0

Install-time Permissions
< Android 6.0

lack of context

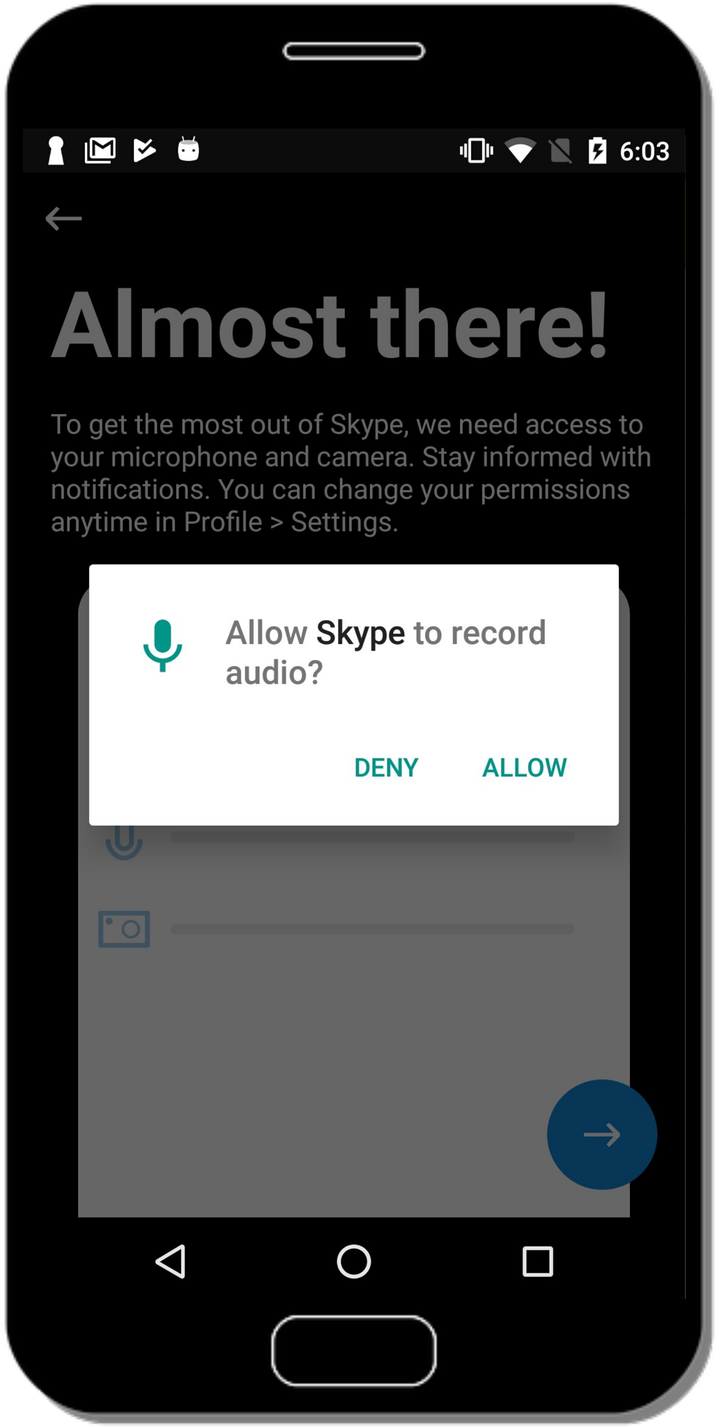


Runtime Permissions
>= Android 6.0

more context

Install-time Permissions
< Android 6.0

lack of context



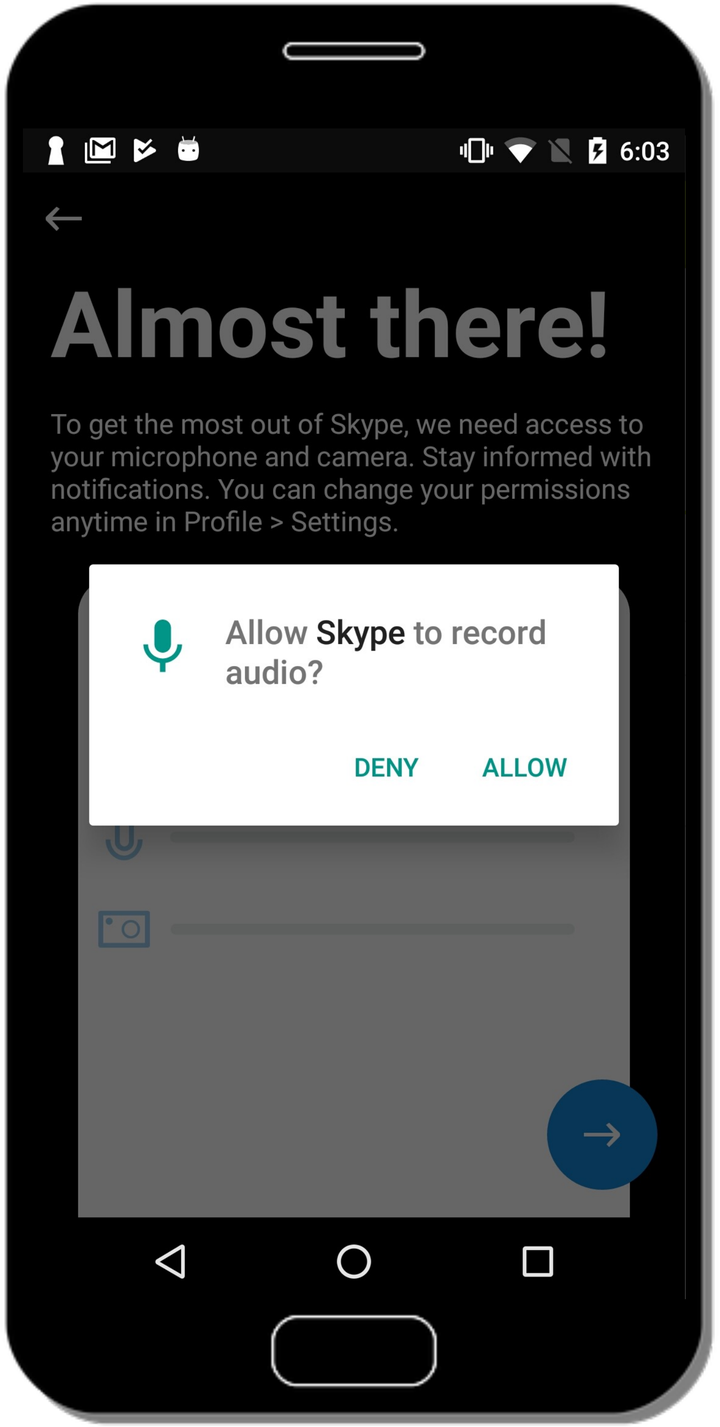
Runtime Permissions
>= Android 6.0

more context

ask on first use from
the foreground

Install-time Permissions
< Android 6.0

lack of context



Runtime Permissions
>= Android 6.0

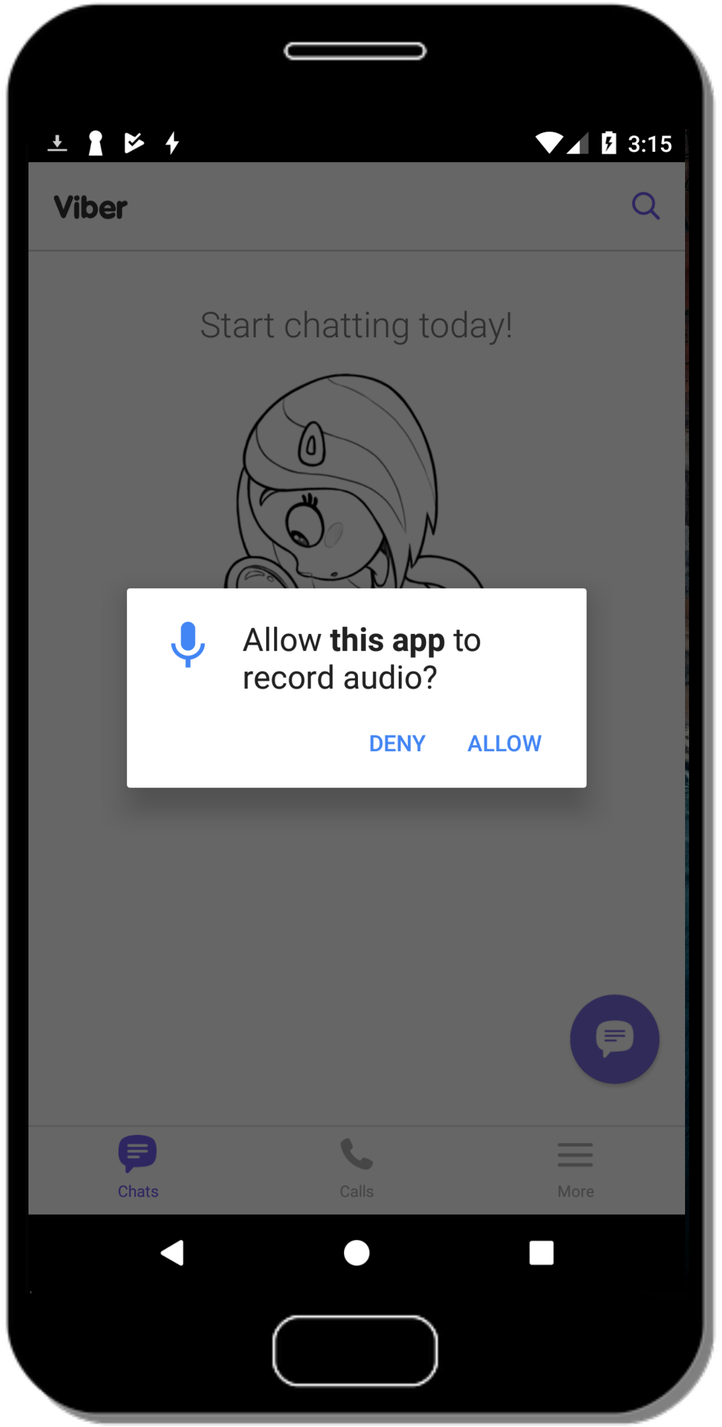
more context

ask on first use from the foreground

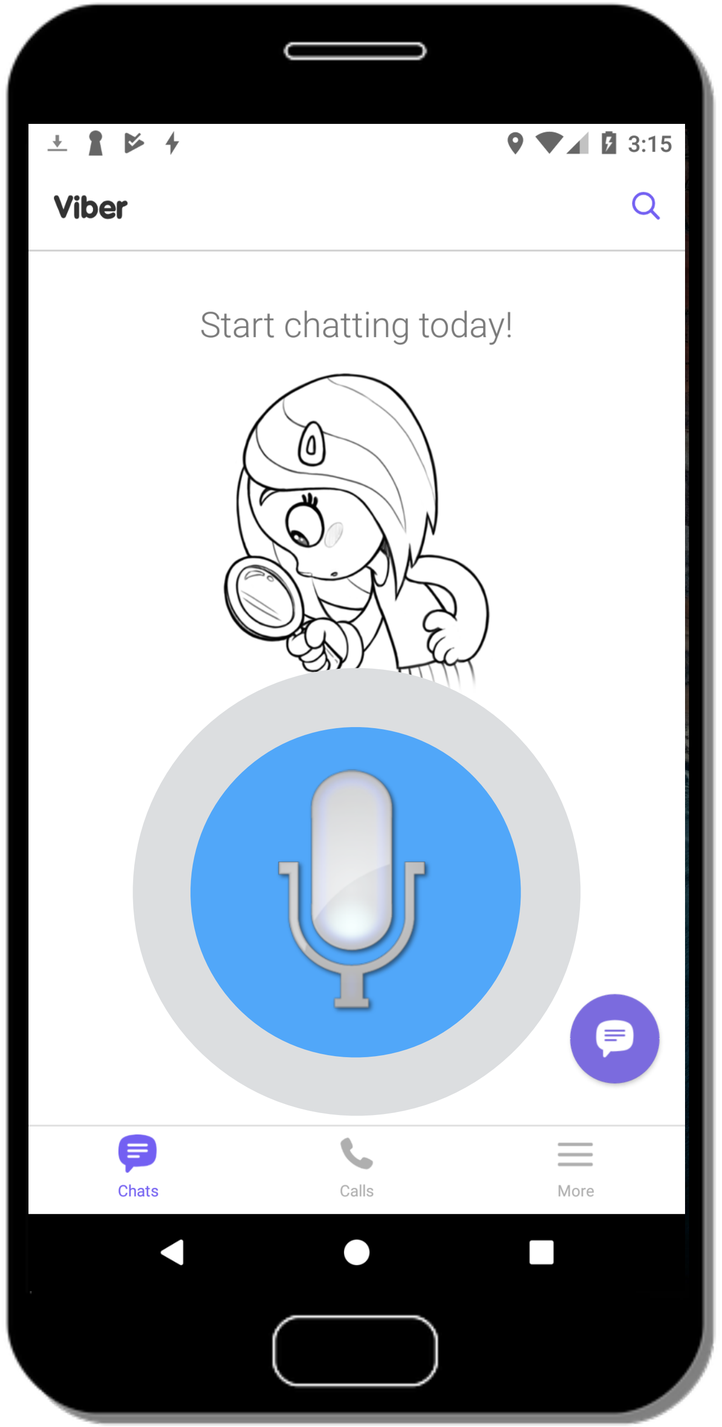
>75% of the market now uses runtime permissions

Viber requesting

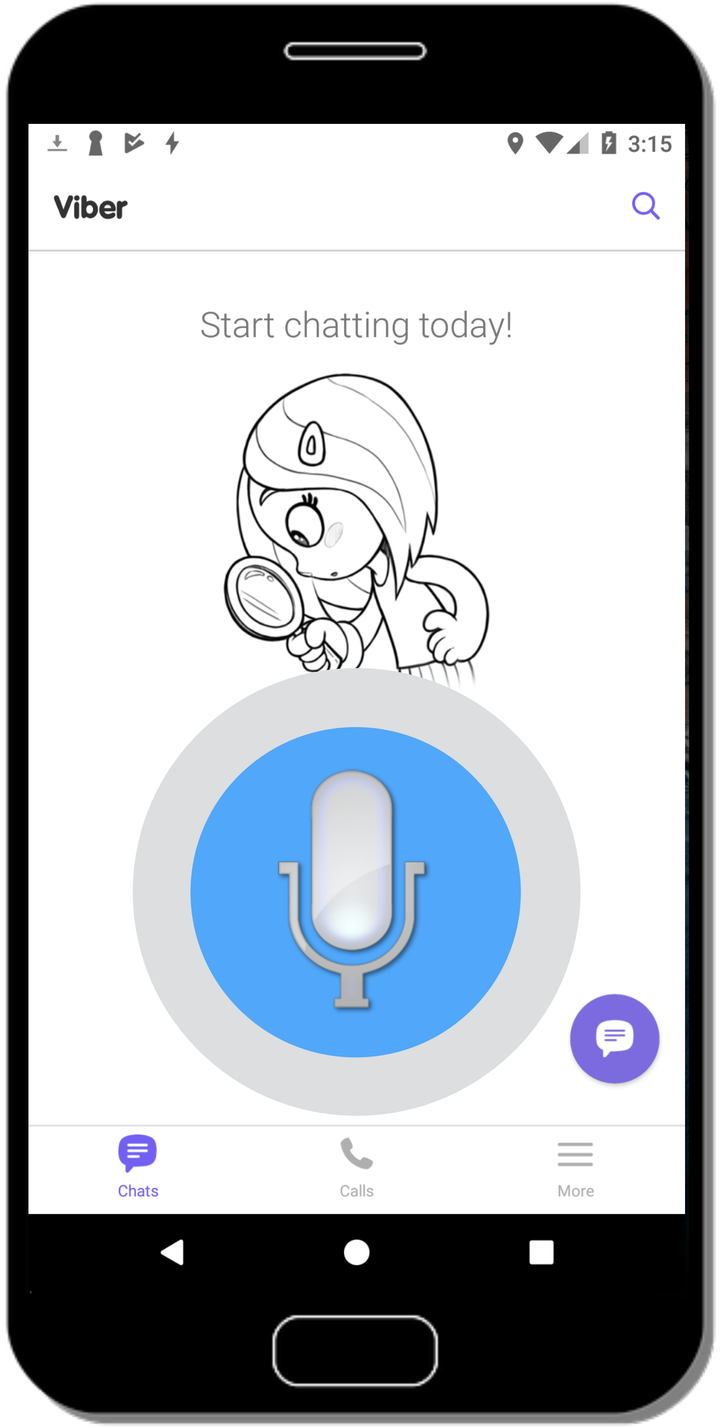
Viber requesting



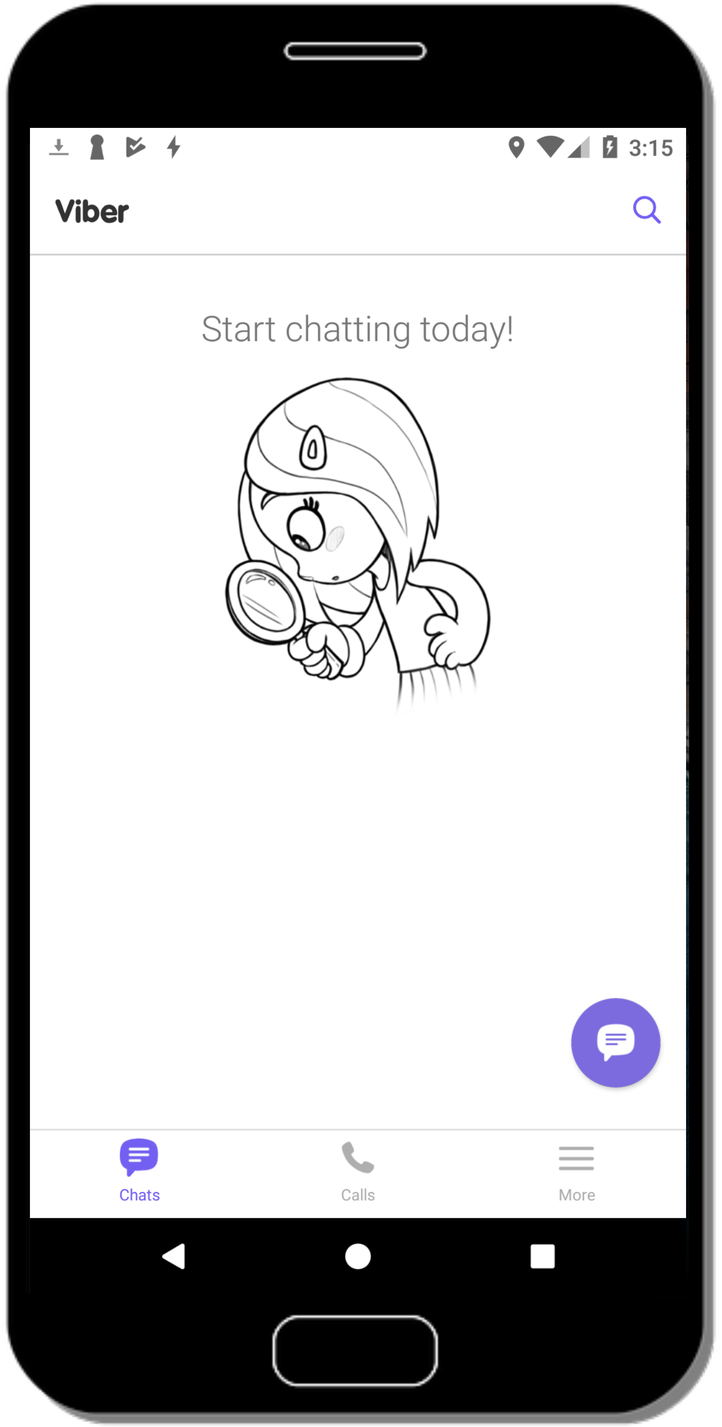
Viber requesting

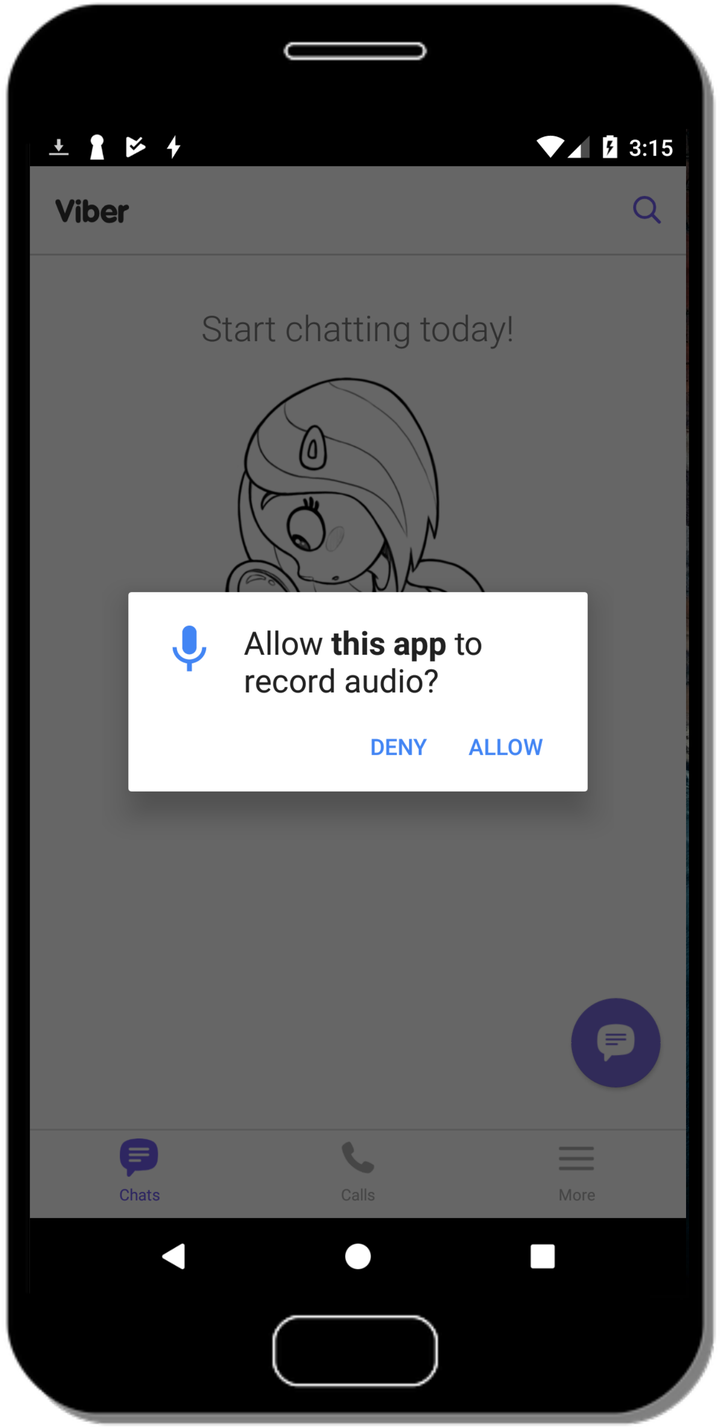


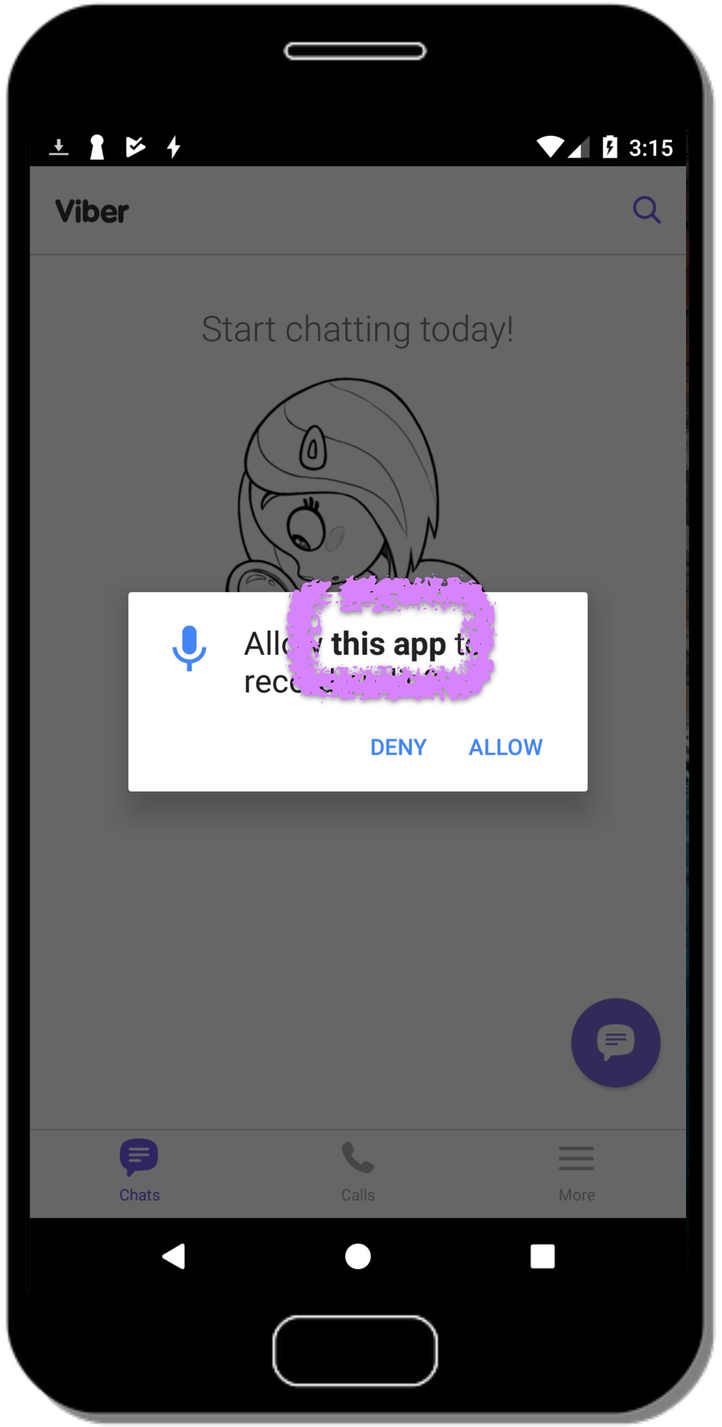
Viber requesting



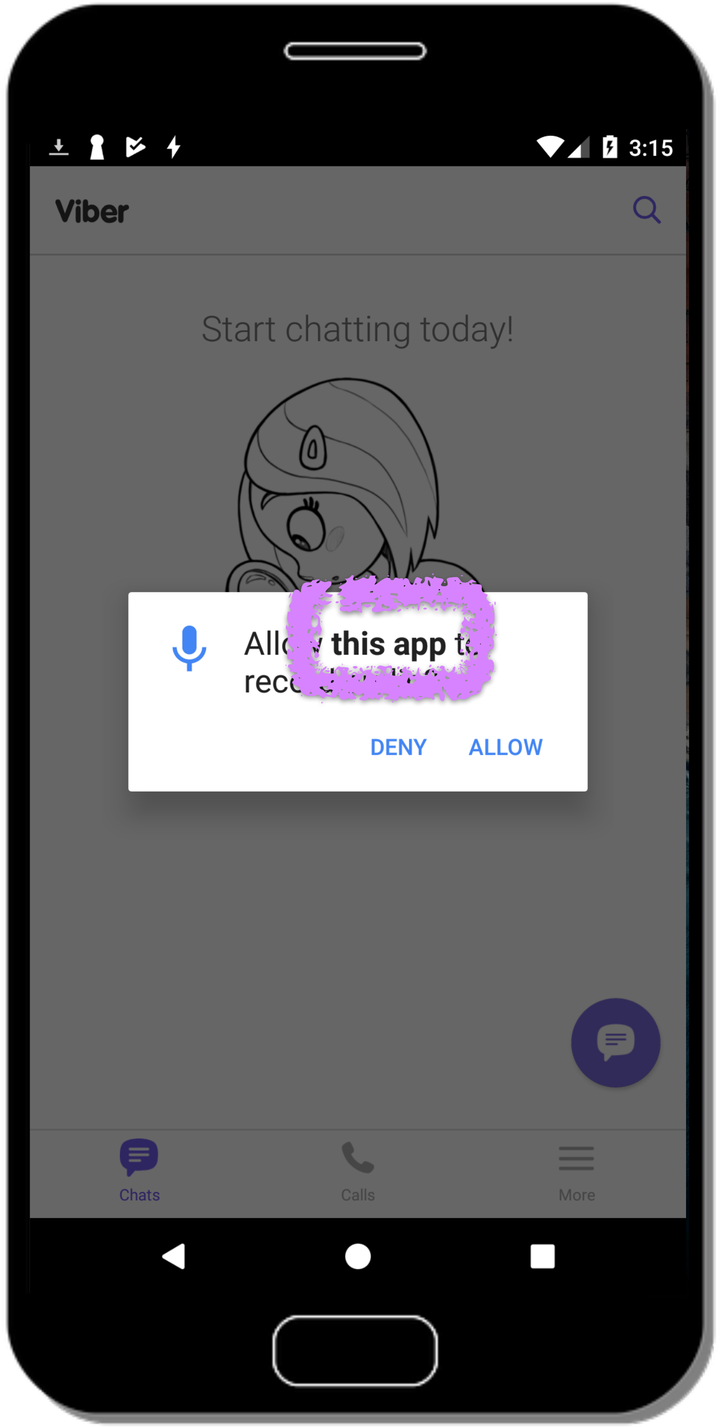
So far so good


3:15
Viber
Start chatting today!
Chats
Calls
More

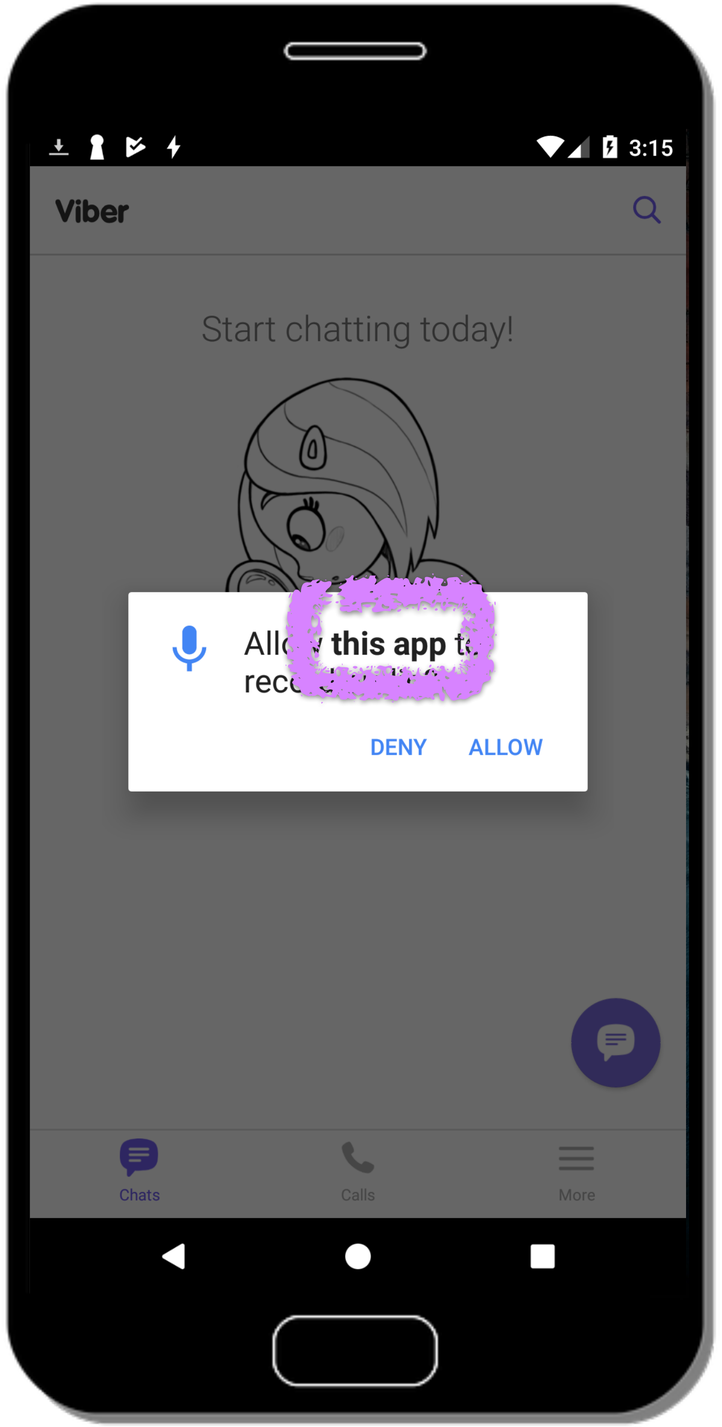

3:15
Viber
Start chatting today!
Allow this app to record audio?
DENY
ALLOW
Chats
Calls
More


3:15
Viber
Start chatting today!
this app t
DENY
ALLOW
Chats
Calls
More

Viber requesting?

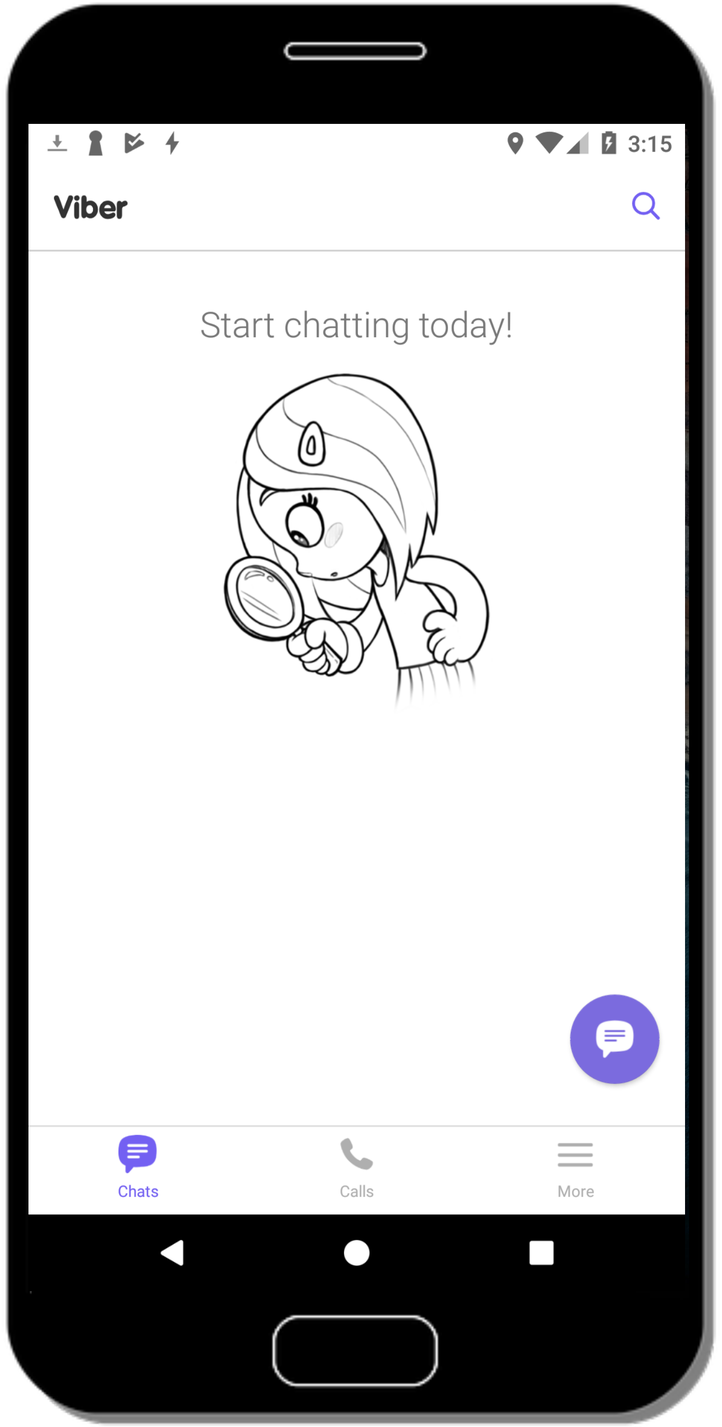


Viber requesting?

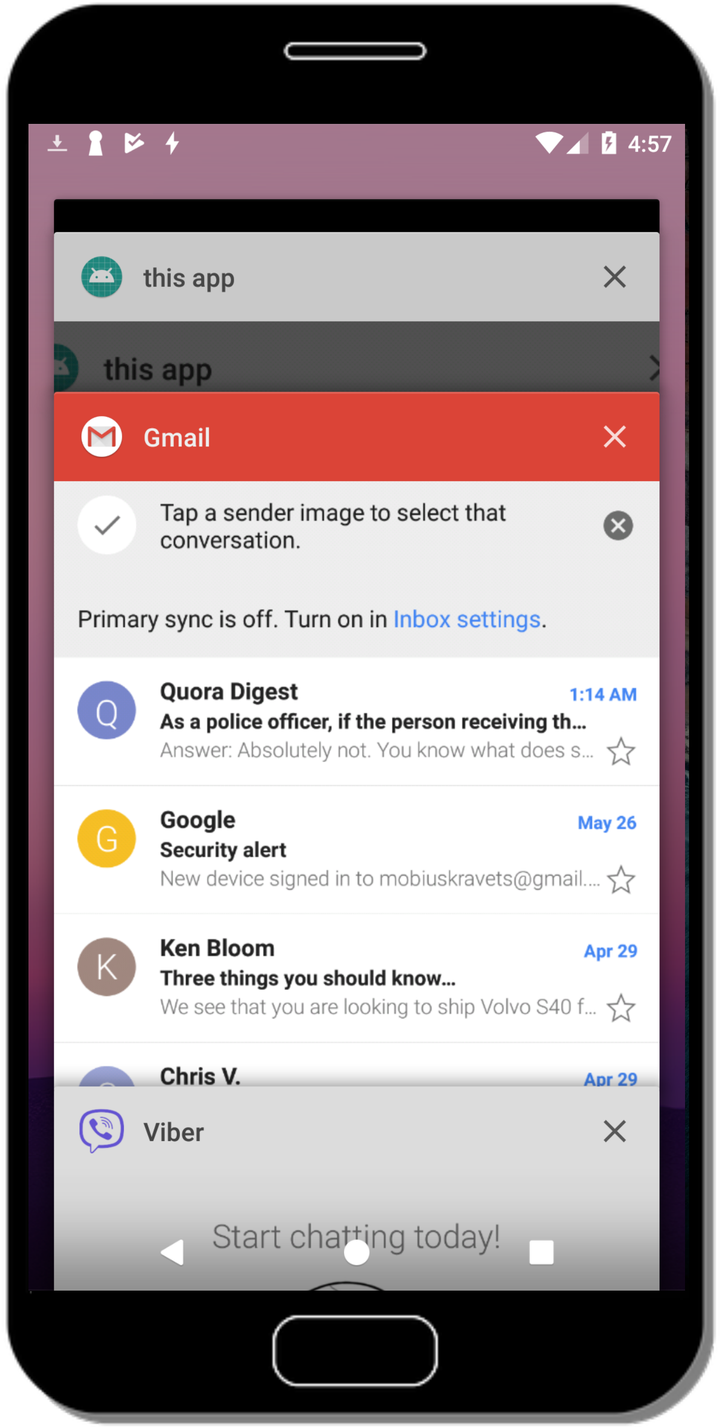


No?!

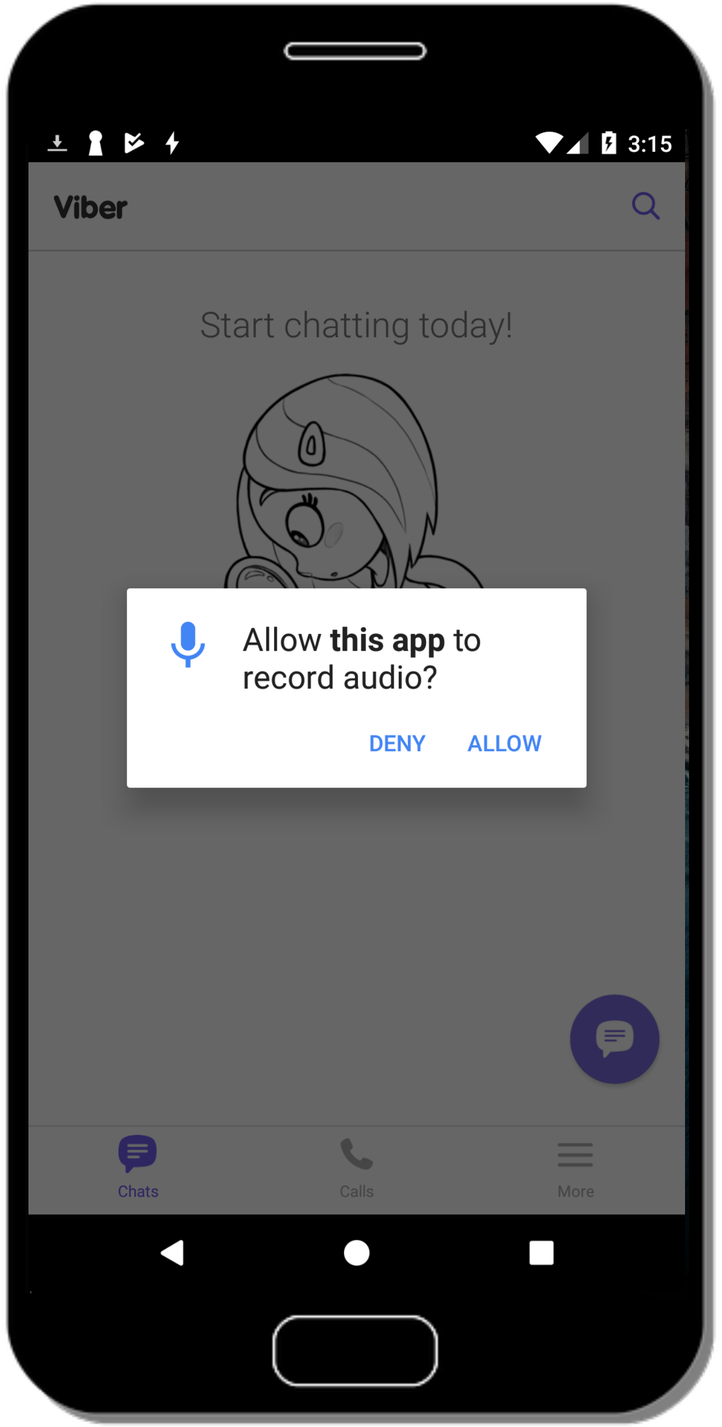
Viber requesting?



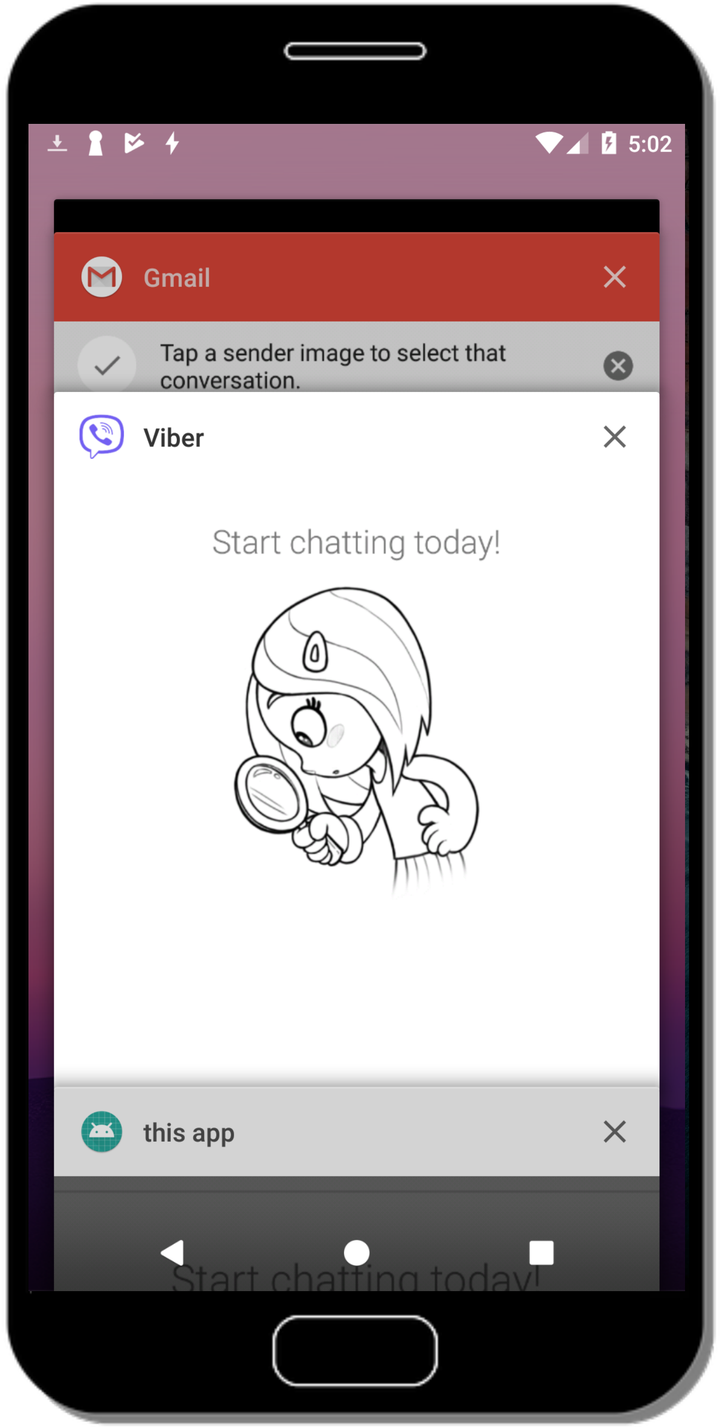
Viber requesting?



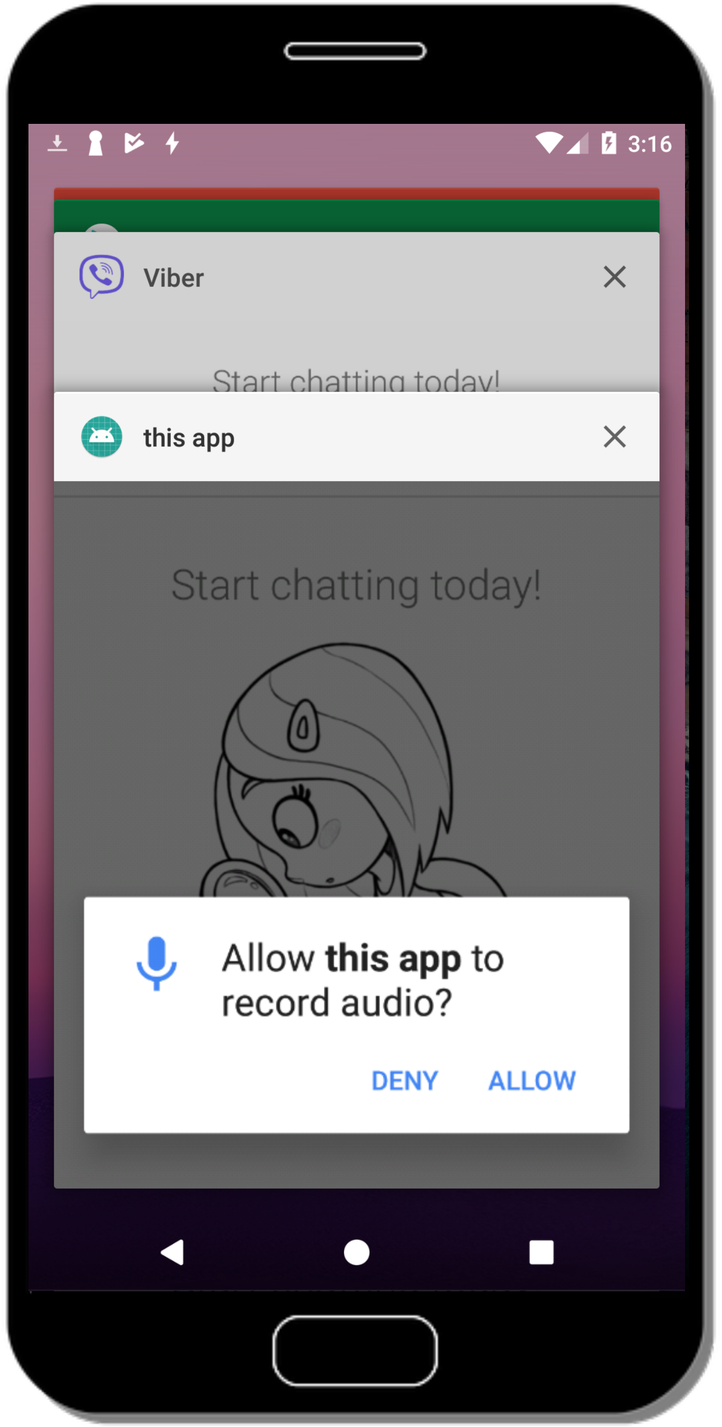
Viber requesting?



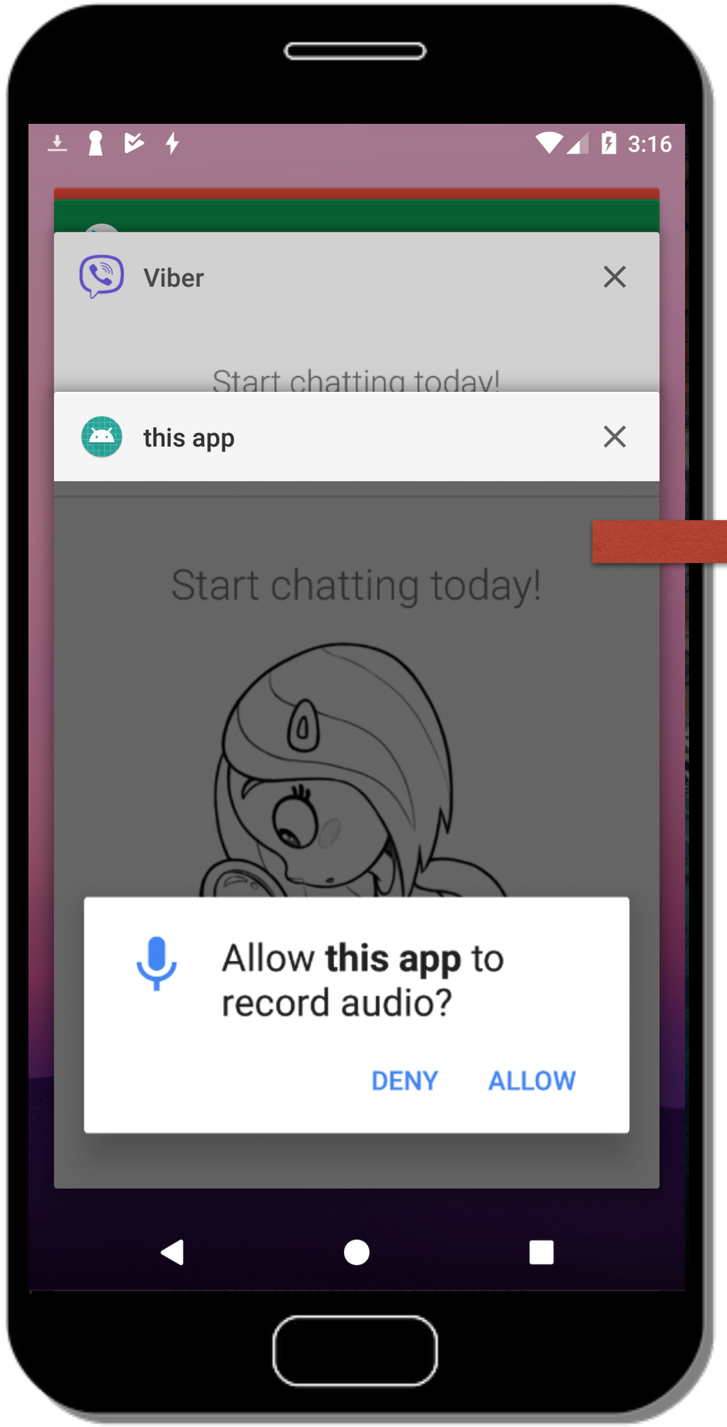
Viber requesting?



Viber requesting?



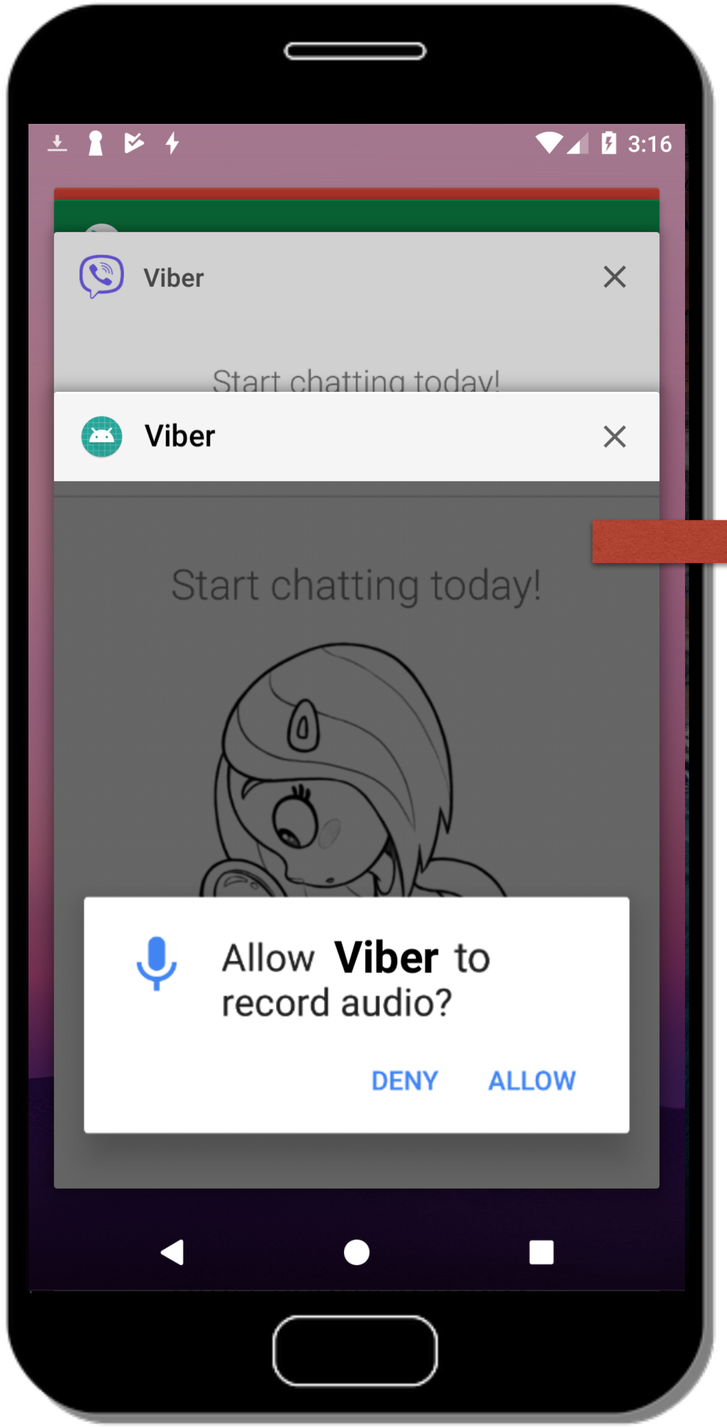
Viber requesting?



Invisible background app requests permission!

False transparency attacks on runtime permissions

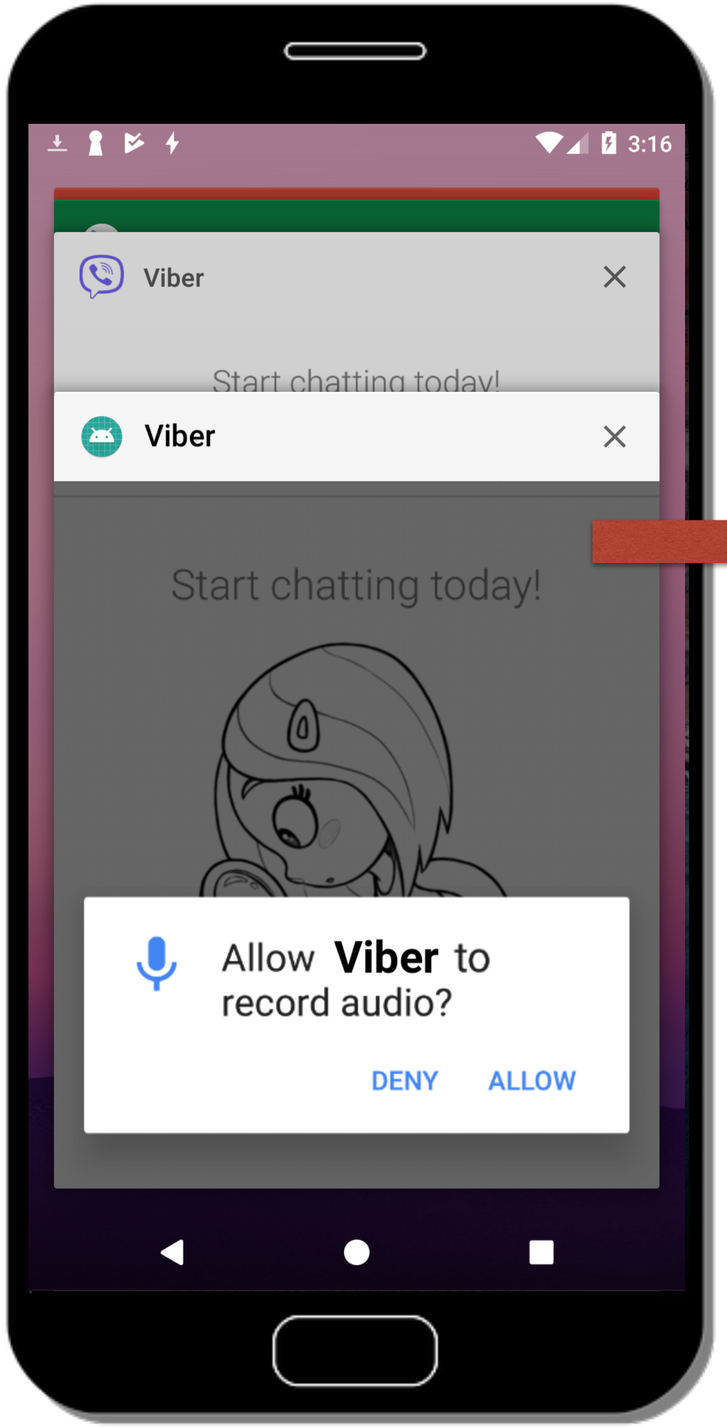
Viber requesting?



Invisible background app requests permission!

False transparency attacks on runtime permissions

Viber requesting?

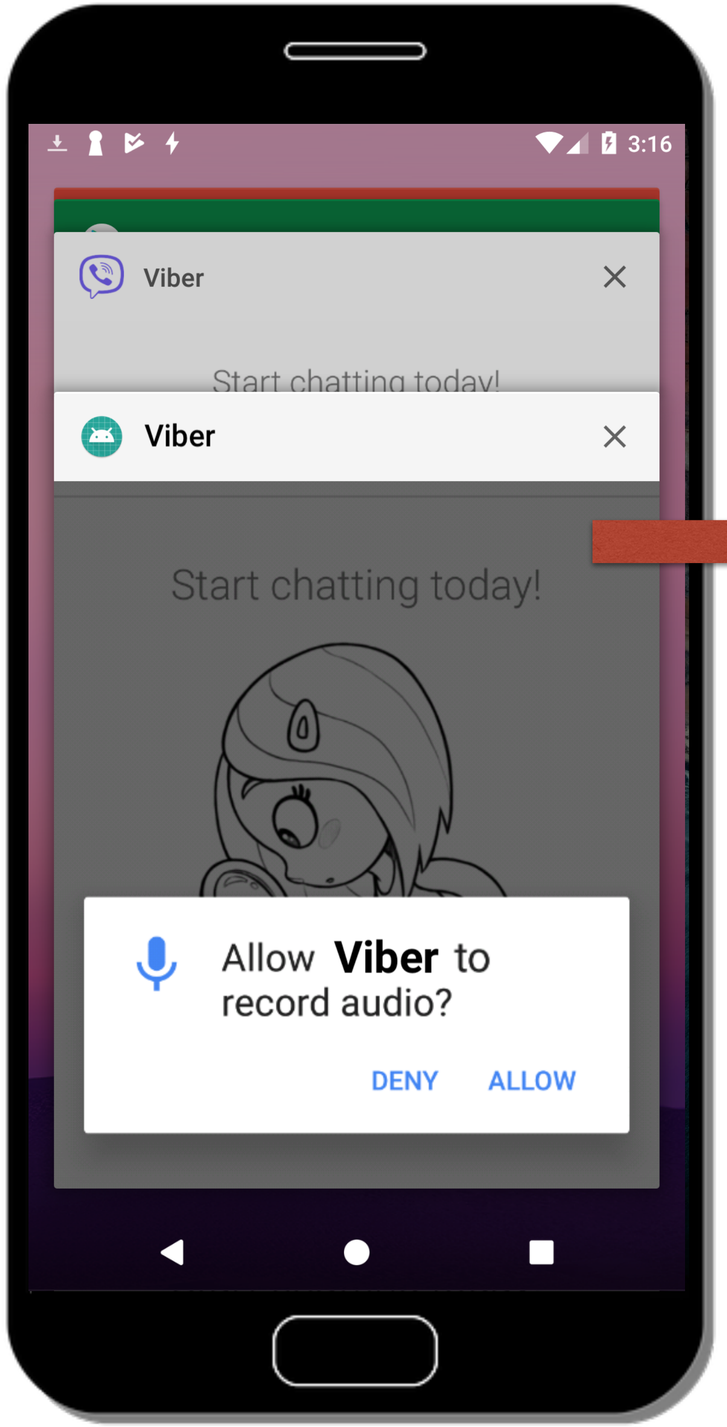


Invisible background app requests permission!

False transparency attacks on runtime permissions

Affects Android 6-11

What's going on?



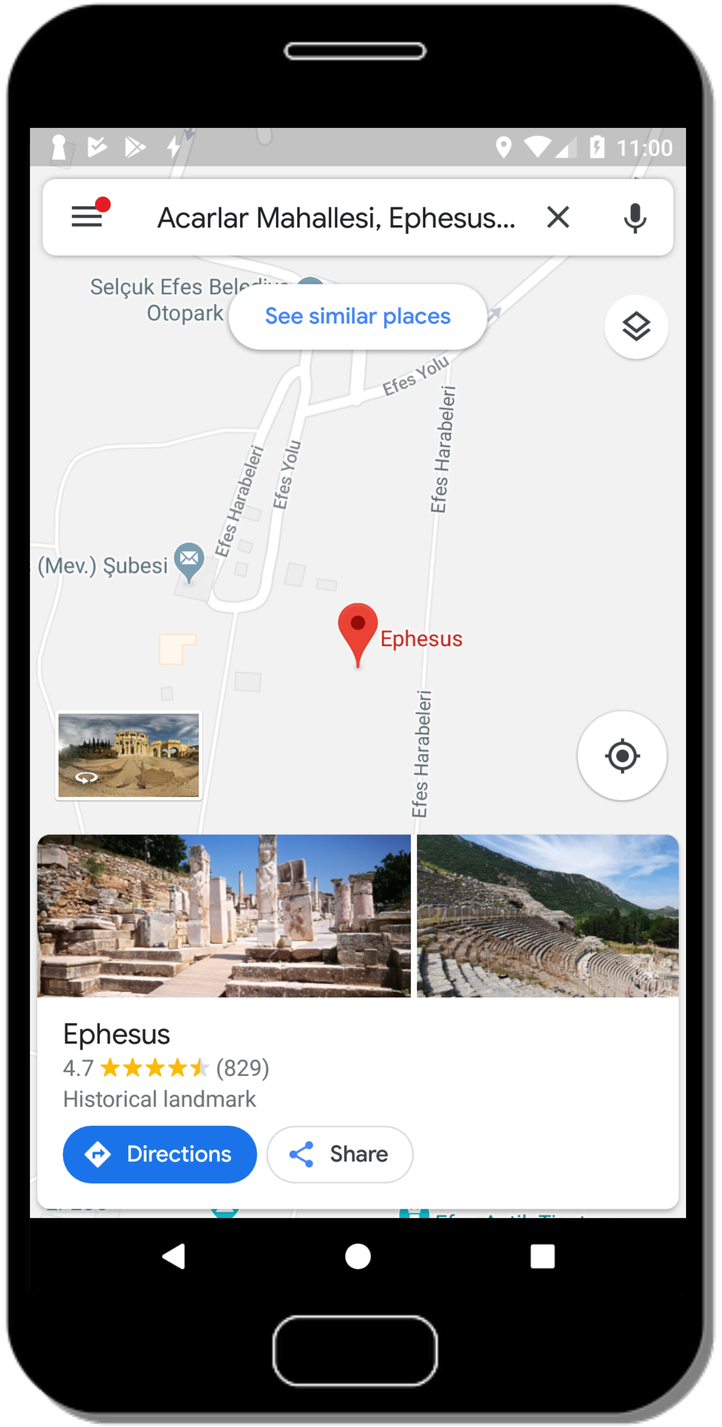
Invisible background app requests permission!

False transparency attacks on runtime permissions

Affects Android 6-11

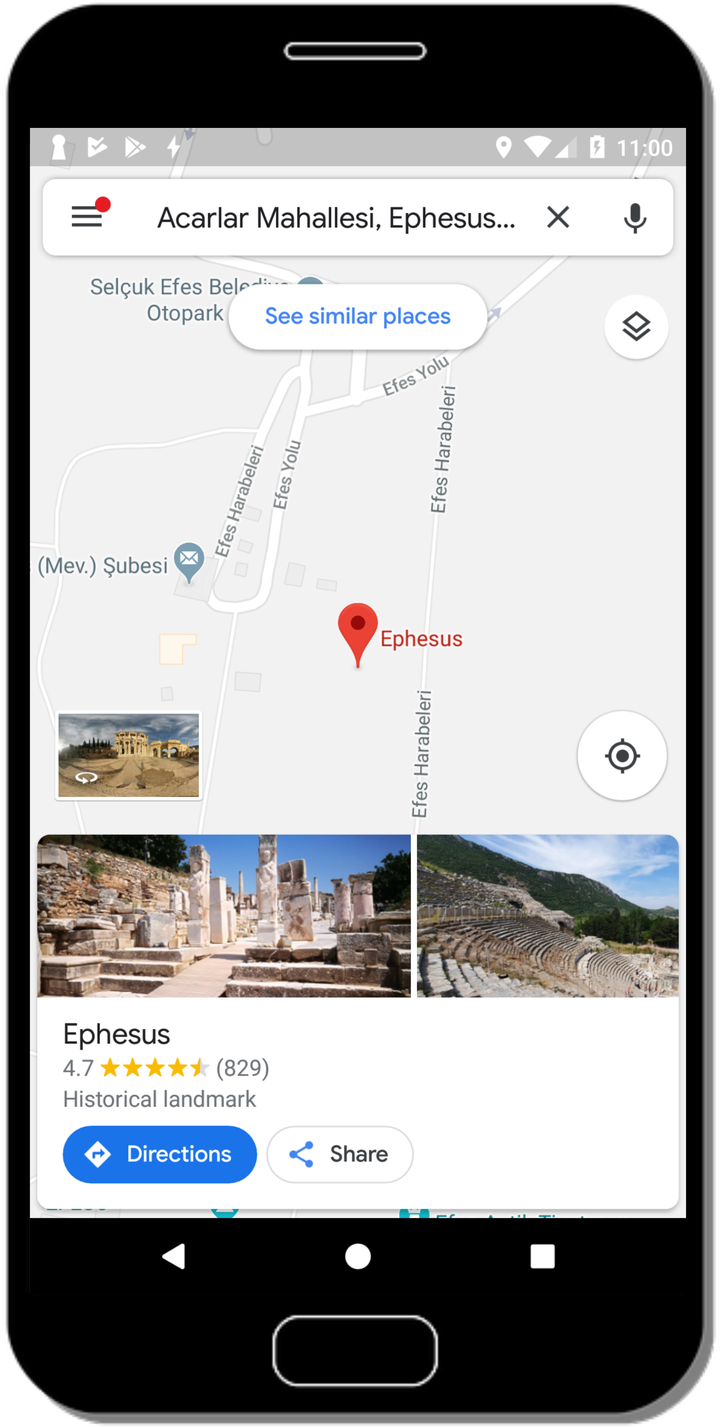
Breaking the security guarantees of runtime permissions

Contextual Guarantee



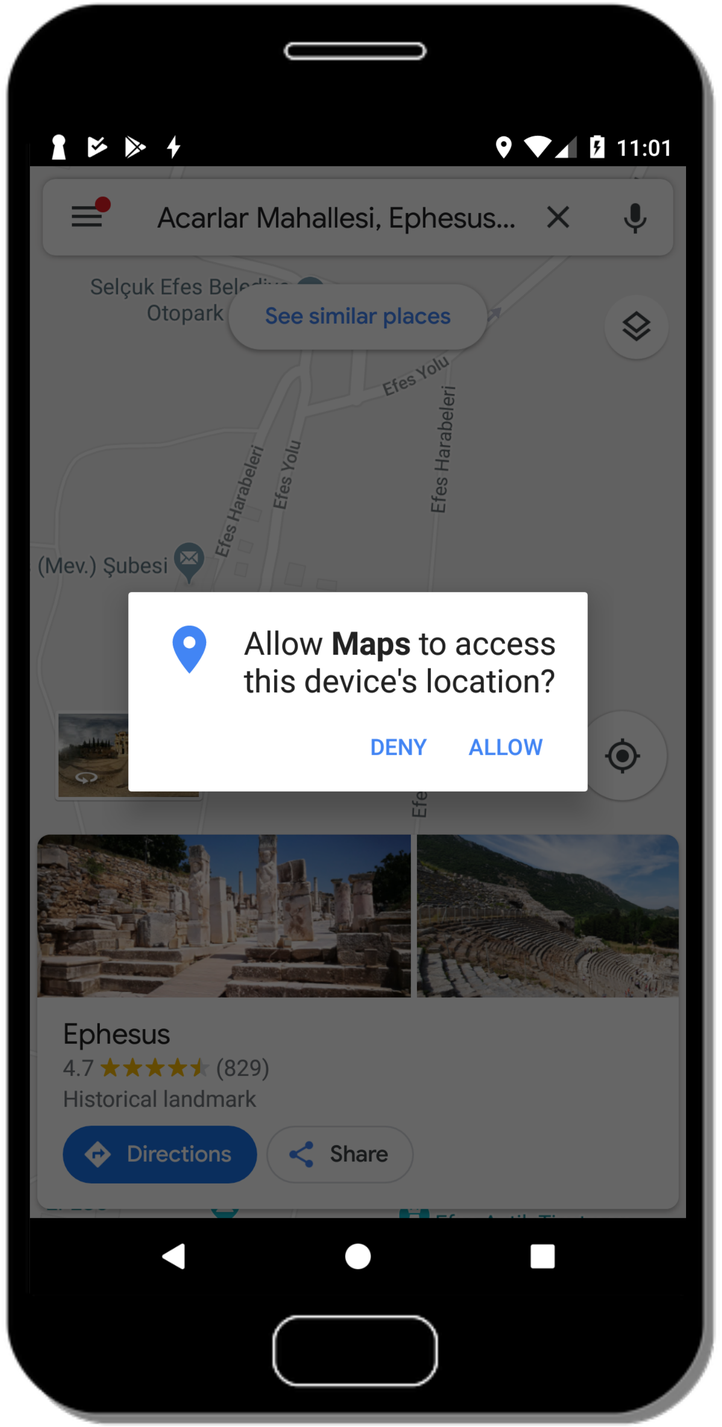
Contextual Guarantee

- Users will always be provided with context



Contextual Guarantee

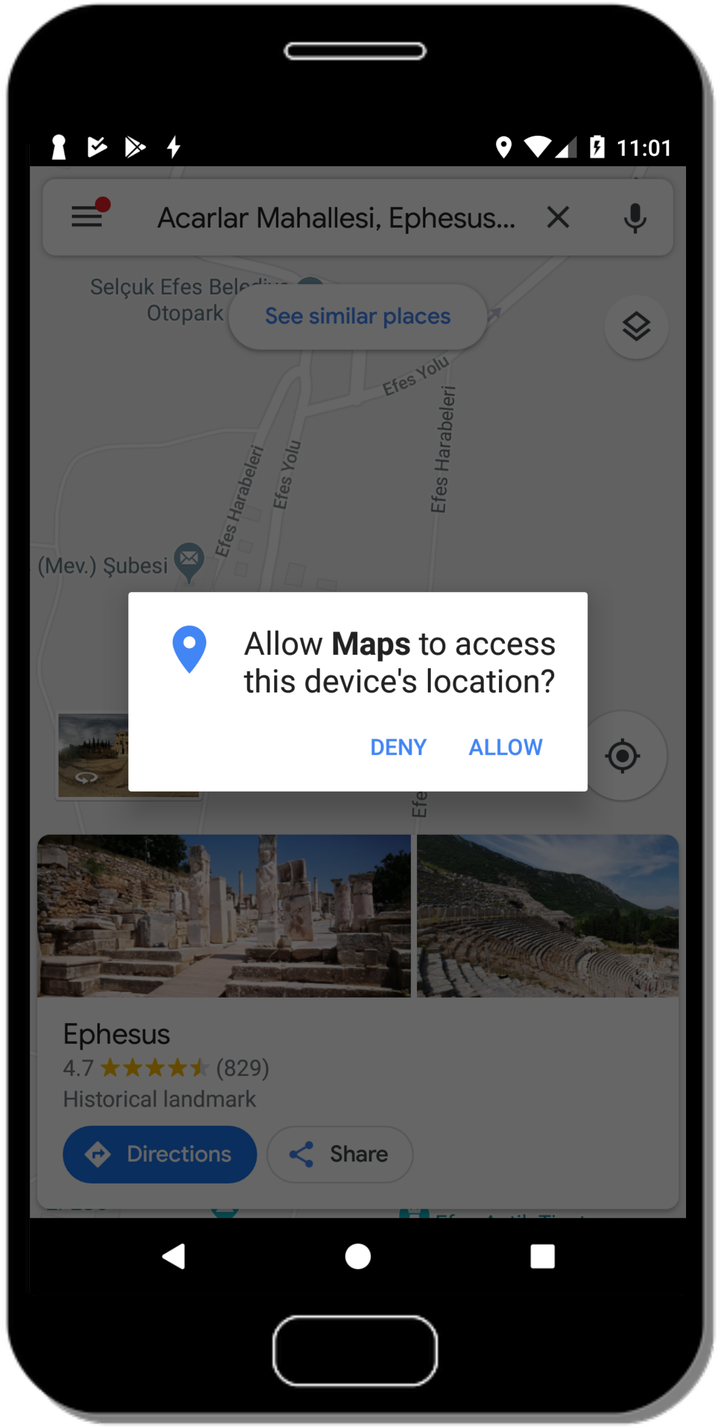
- Users will always be provided with context
  - Allow permission requests to be made only from the foreground



Contextual Guarantee

- Users will always be provided with context
  - Allow permission requests to be made only from the foreground

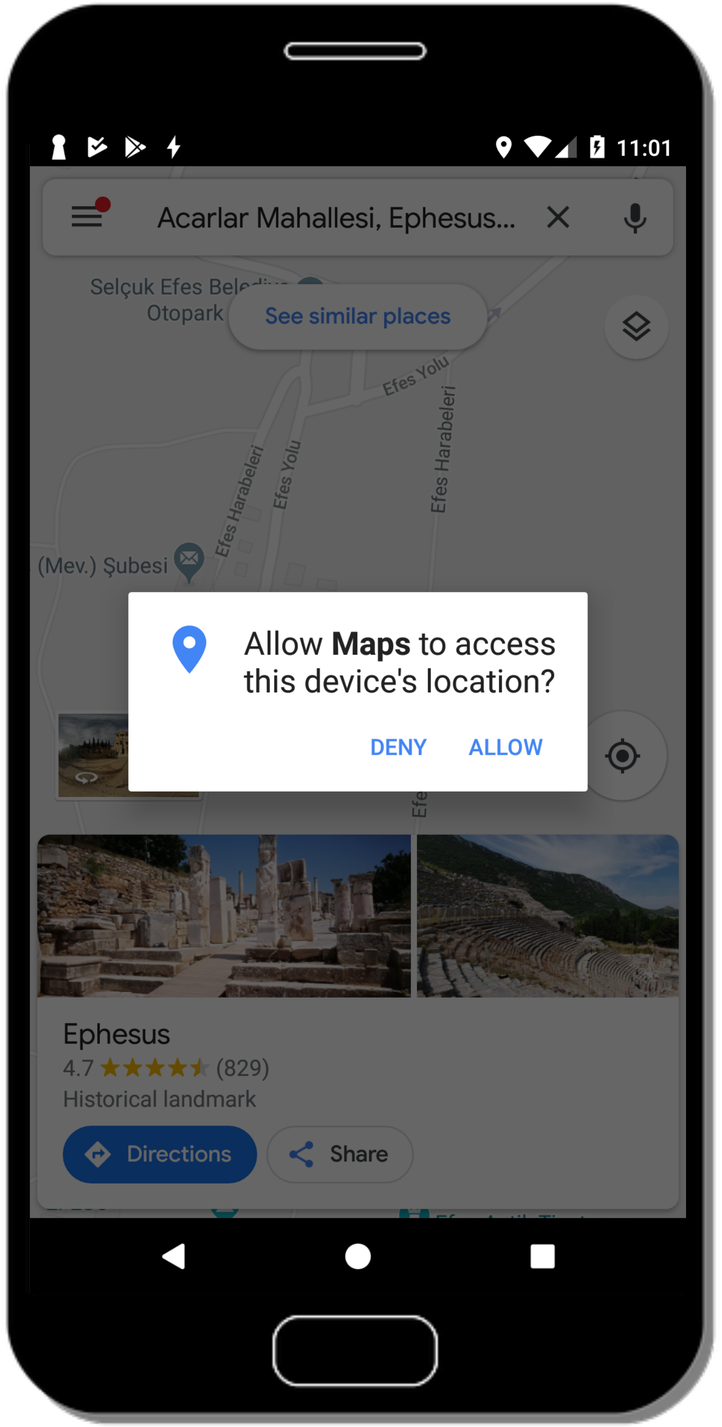
Assumption:
Context provided by the FG app is legitimate



Contextual Guarantee

- Users will always be provided with context
  - Allow permission requests to be made only from the foreground

Assumption:
Context provided by the FG app is legitimate



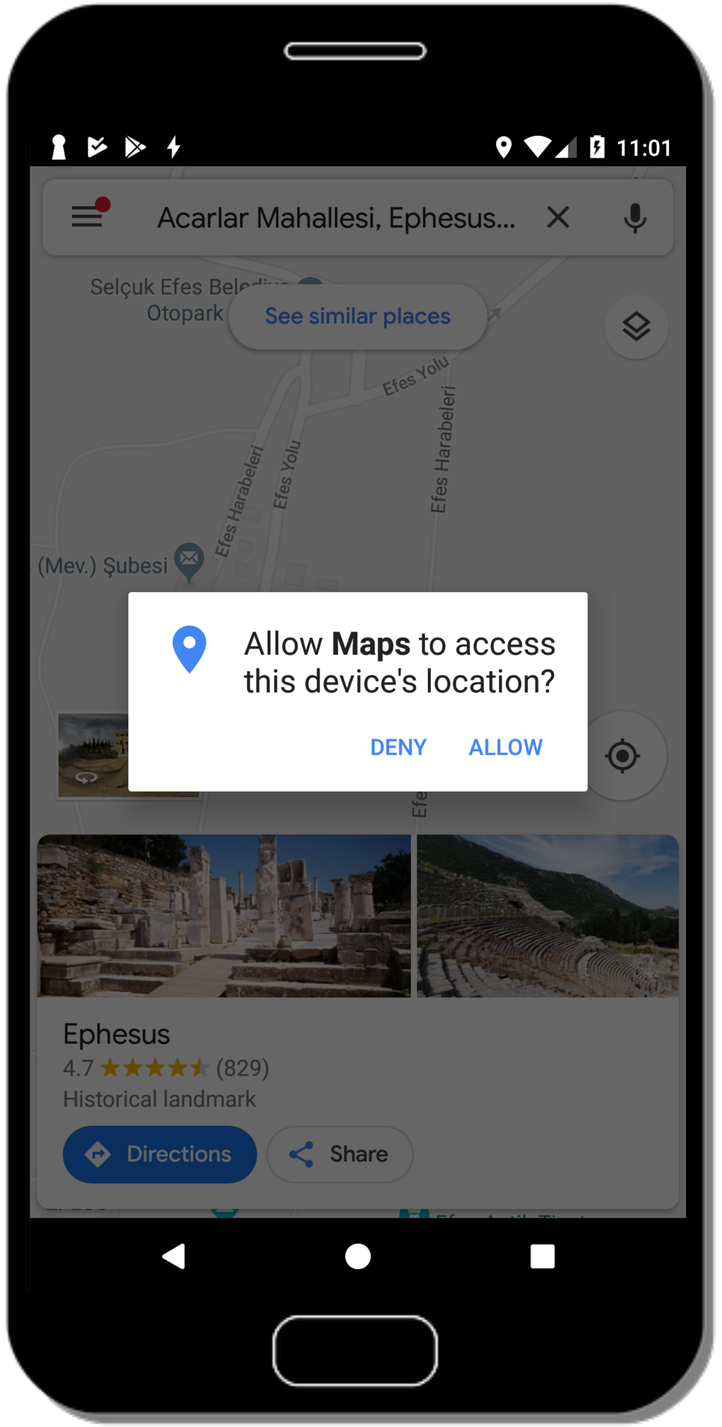
APIs to move within the task stack!

- moveTaskToFront()
- moveTaskToBack()
- startActivity()
- requestPermissions()

Contextual Guarantee

- Users will always be provided with context
  - Allow permission requests to be made only from the foreground

Assumption:
Context provided by the FG app is legitimate



APIs to move within the task stack!

- moveTaskToFront()
- moveTaskToBack()
- startActivity()
- requestPermissions()

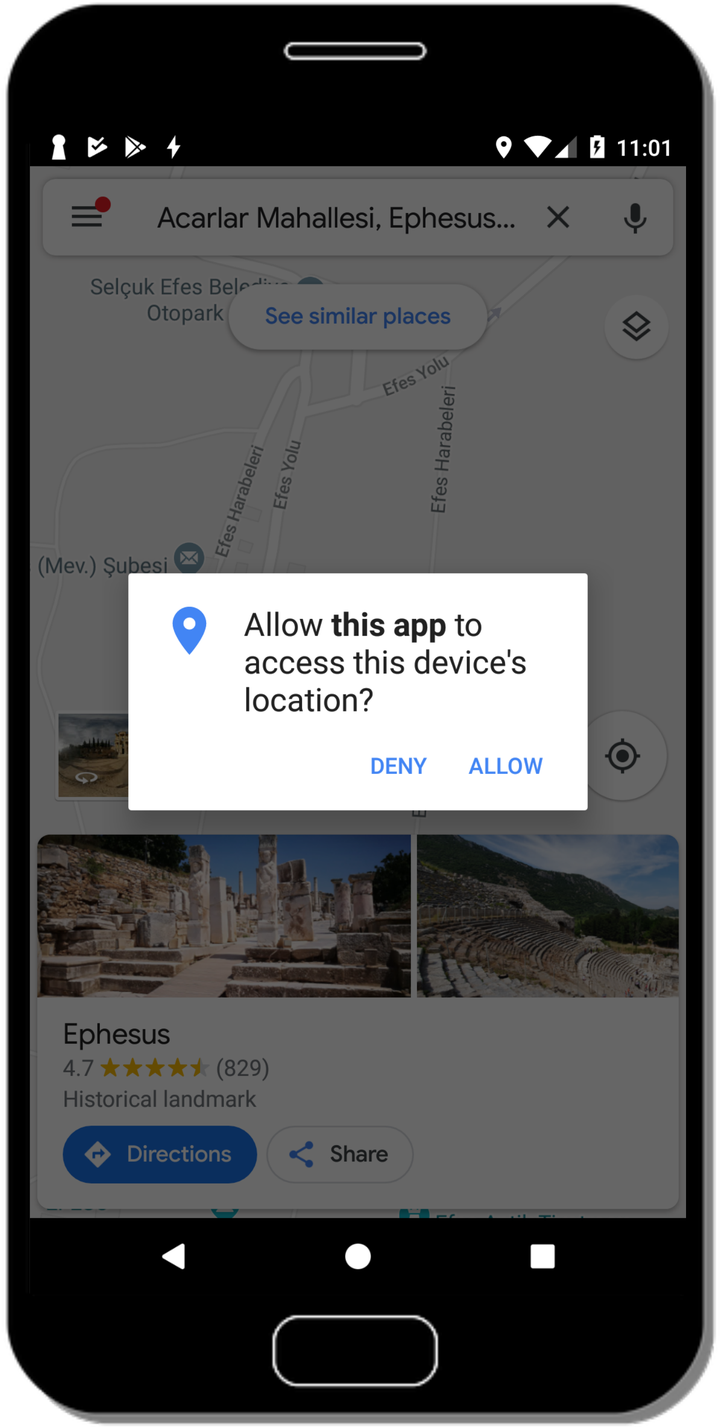
+

transparency

Contextual Guarantee

- Users will always be provided with context
  - Allow permission requests to be made only from the foreground

Assumption:
Context provided by the FG app is legitimate



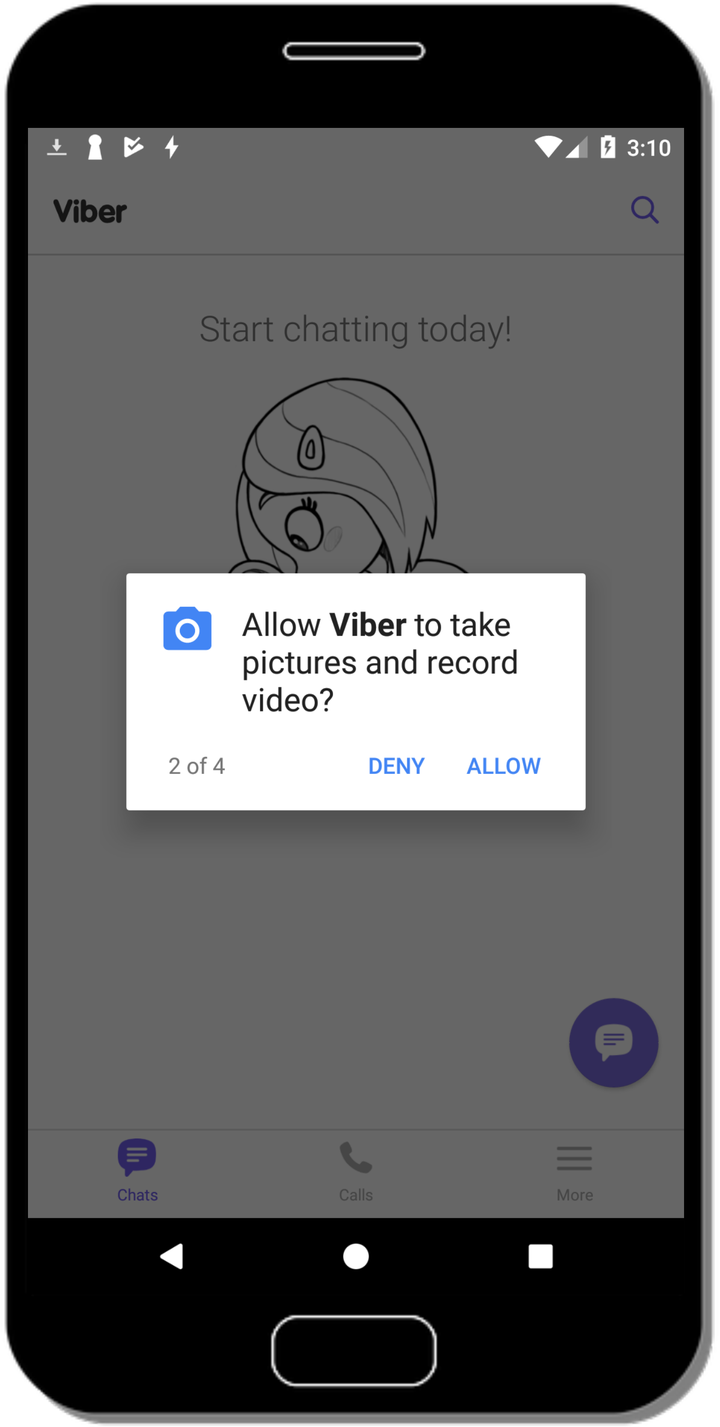
APIs to move within the task stack!

- moveTaskToFront()
- moveTaskToBack()
- startActivity()
- requestPermissions()

+

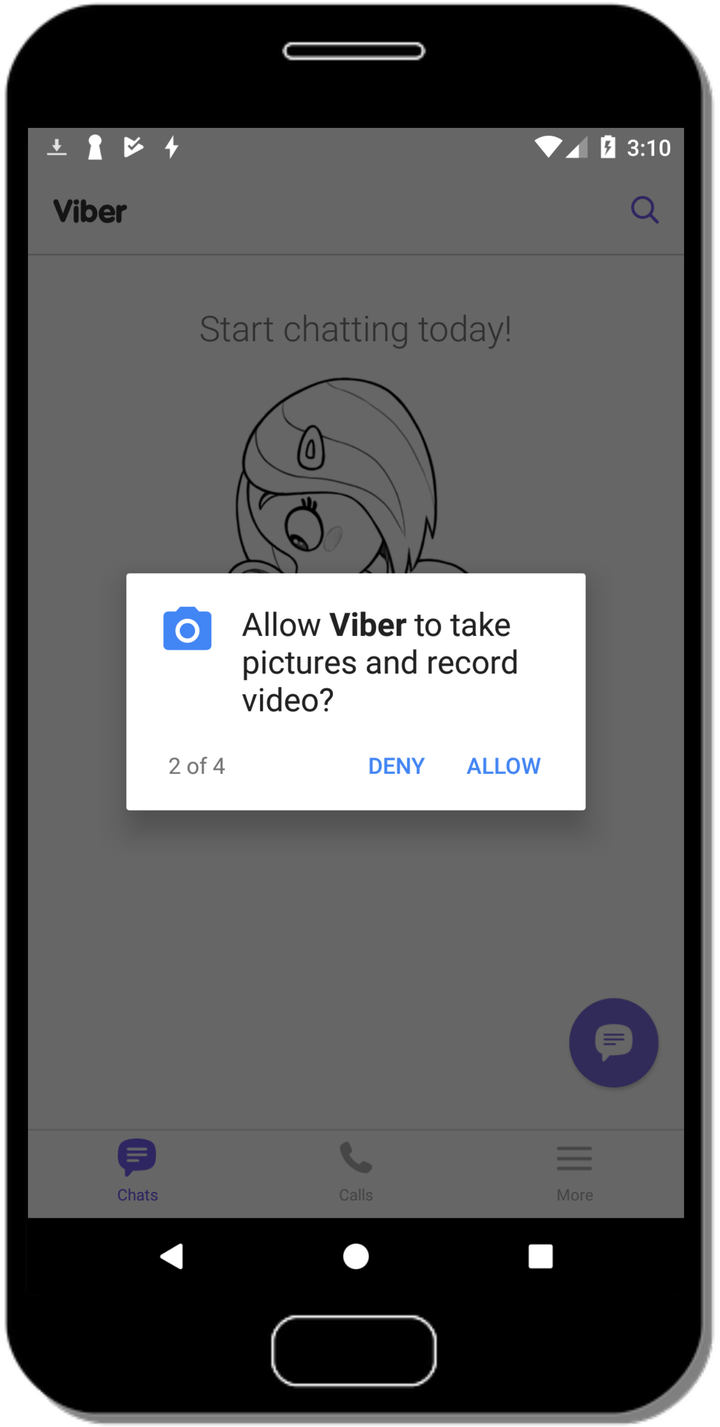
transparency

Identity Guarantee



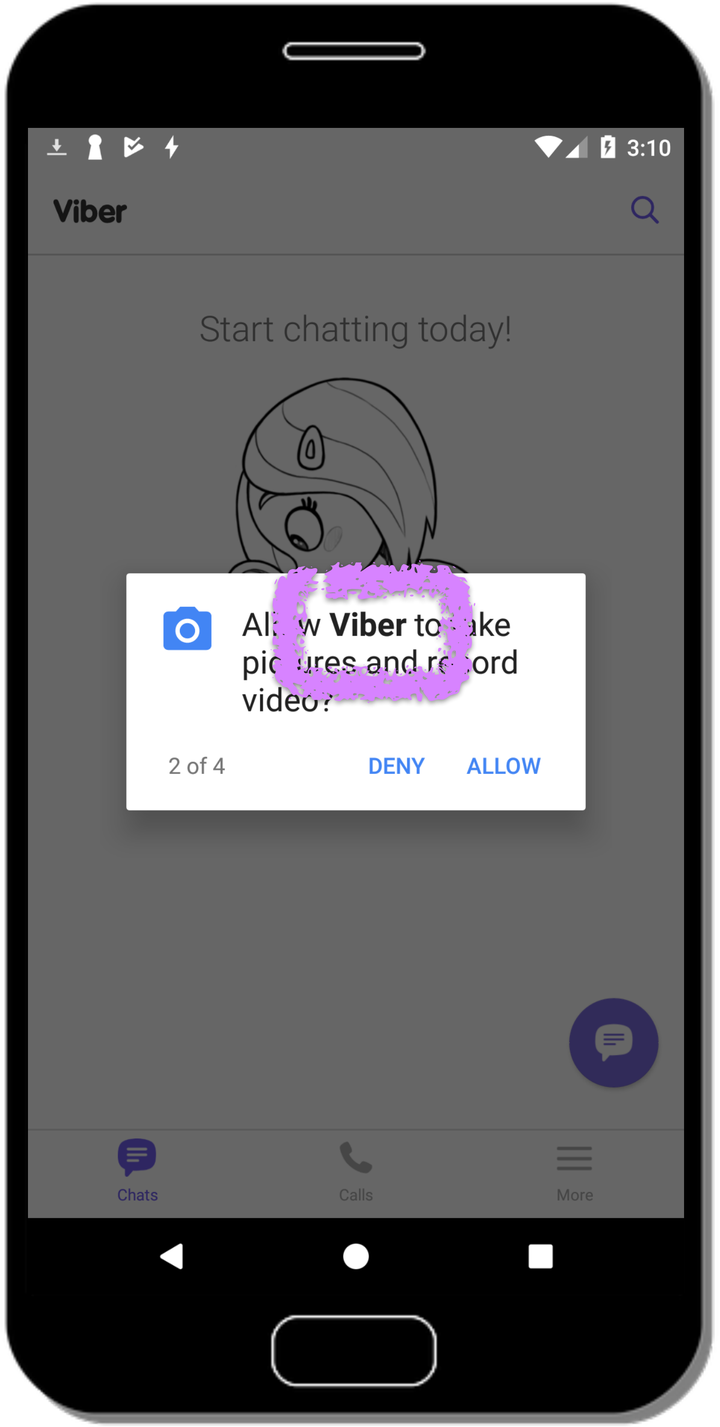
Identity Guarantee

- Users should be made aware of the identity of requesting app



Identity Guarantee

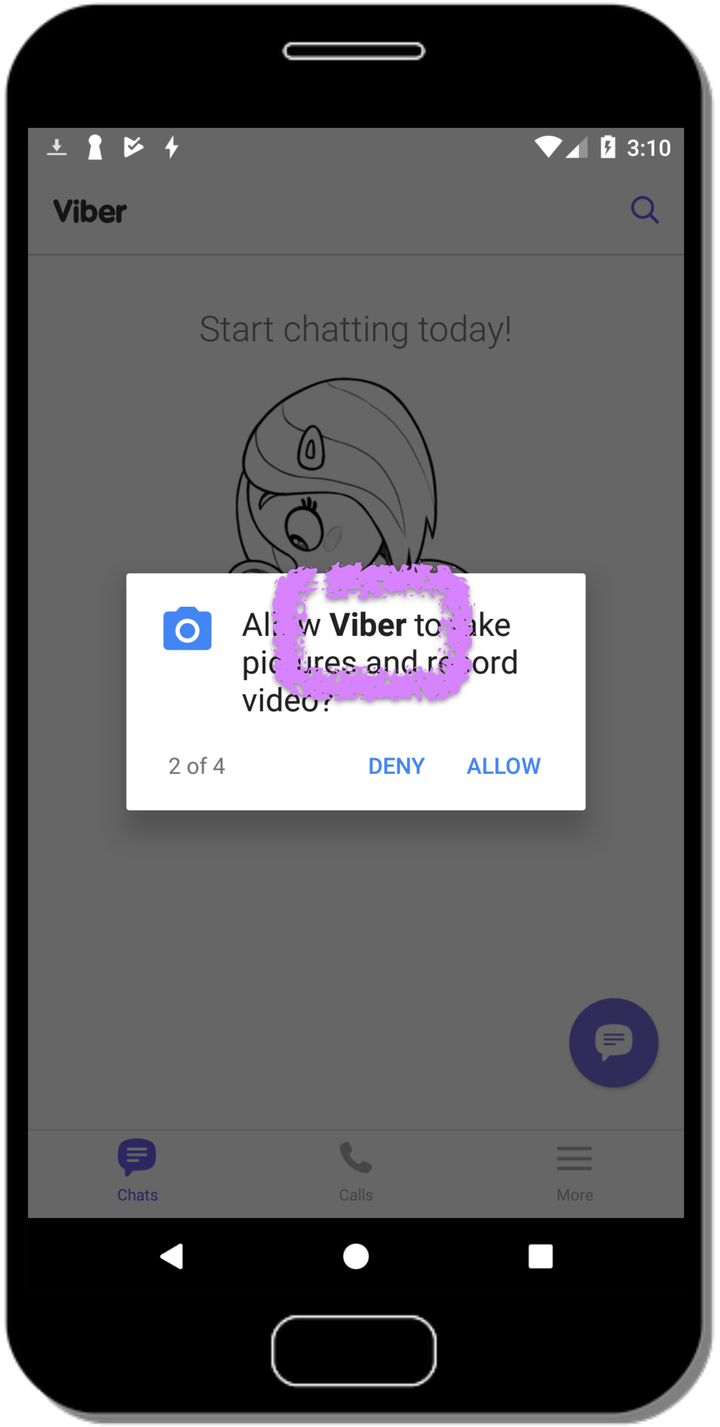
- Users should be made aware of the identity of requesting app
  - Show app name in the permission dialog



Identity Guarantee

- Users should be made aware of the identity of requesting app
  - Show app name in the permission dialog

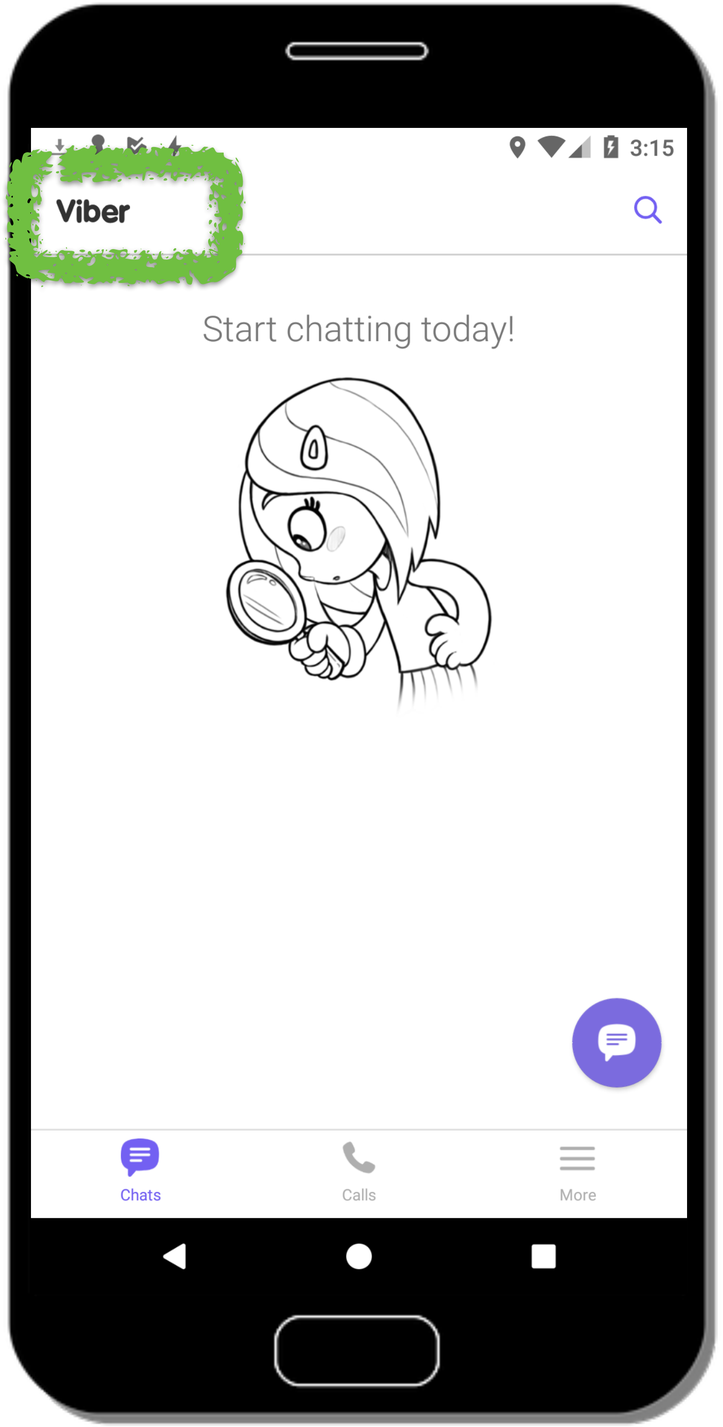
Assumption:
Uniquely identifying app names



Identity Guarantee

- Users should be made aware of the identity of requesting app
  - Show app name in the permission dialog

Assumption:
Uniquely identifying
app names

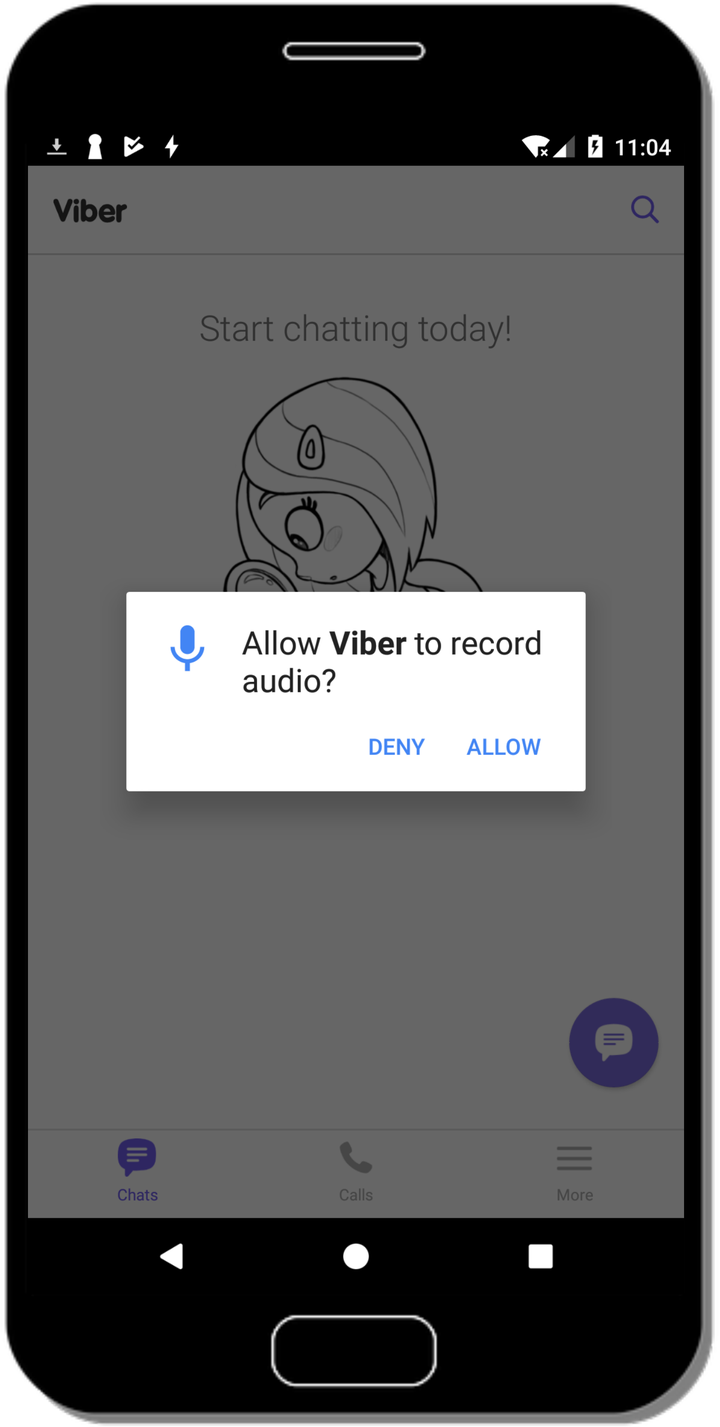


App name
- no rules!

Identity Guarantee

- Users should be made aware of the identity of requesting app
  - Show app name in the permission dialog

Assumption:
Uniquely identifying app names



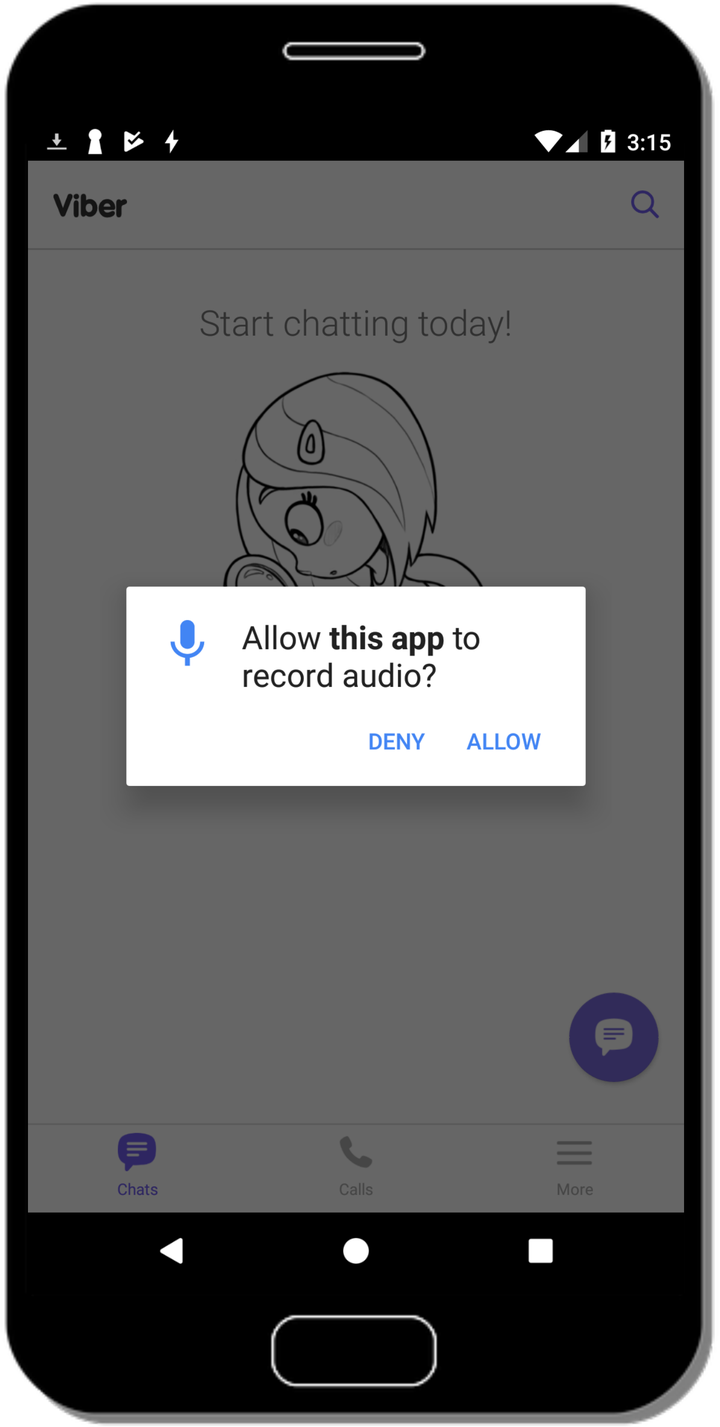
App name
- no rules!

✓ Viber

Identity Guarantee

- Users should be made aware of the identity of requesting app
  - Show app name in the permission dialog

Assumption:
Uniquely identifying app names



App name
- no rules!

✓ Viber
✓ this app

Background apps can request permissions with an illegitimate context

Background apps can request permissions with an illegitimate context

Apps can exploit users' trust and request permissions impersonating other apps

Realizing the Attacks

Realizing the Attacks

Survey with 200 Amazon mTurk participants

Realizing the Attacks

- Is there any underlying susceptibility enabling FTAs?

Survey with 200 Amazon mTurk participants

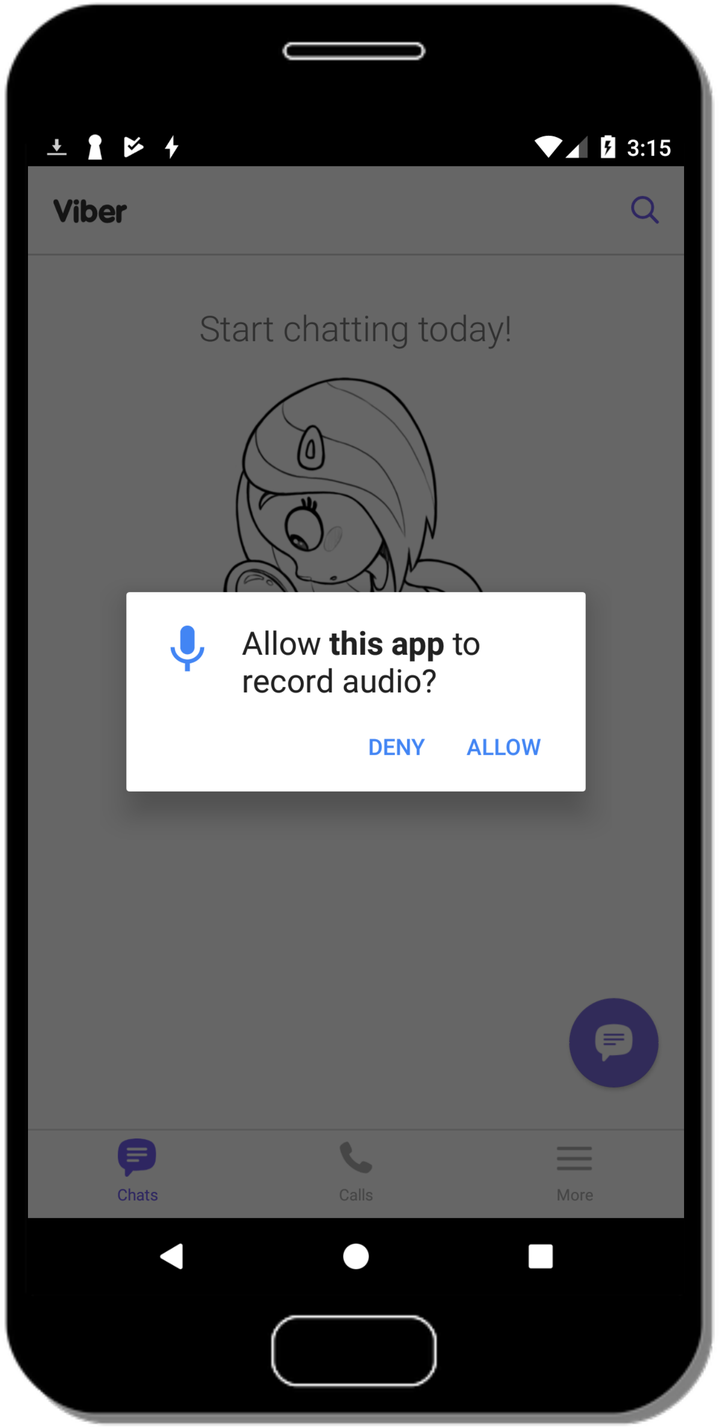
Realizing the Attacks

- Is there any underlying susceptibility enabling FTAs?
- How to make FTAs realistic and more likely to succeed?

Survey with 200 Amazon mTurk participants

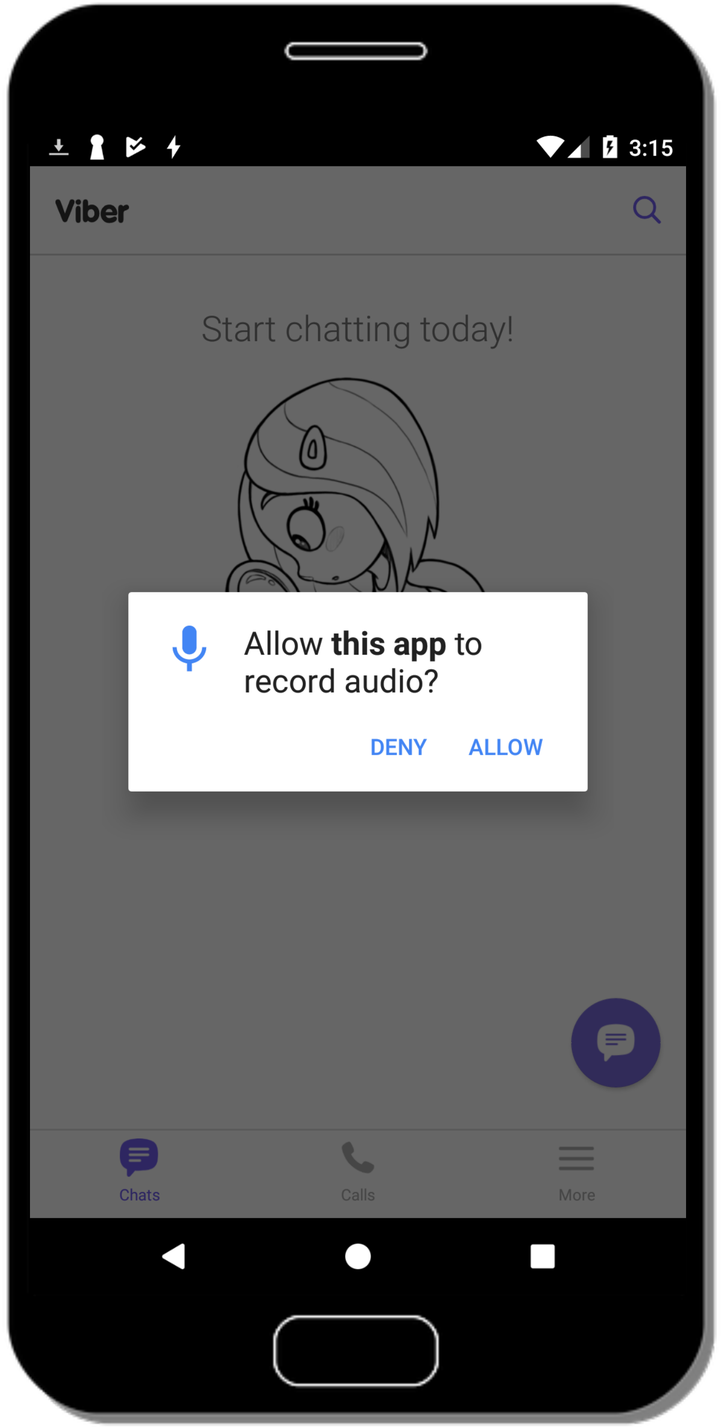
Susceptibility

Susceptibility



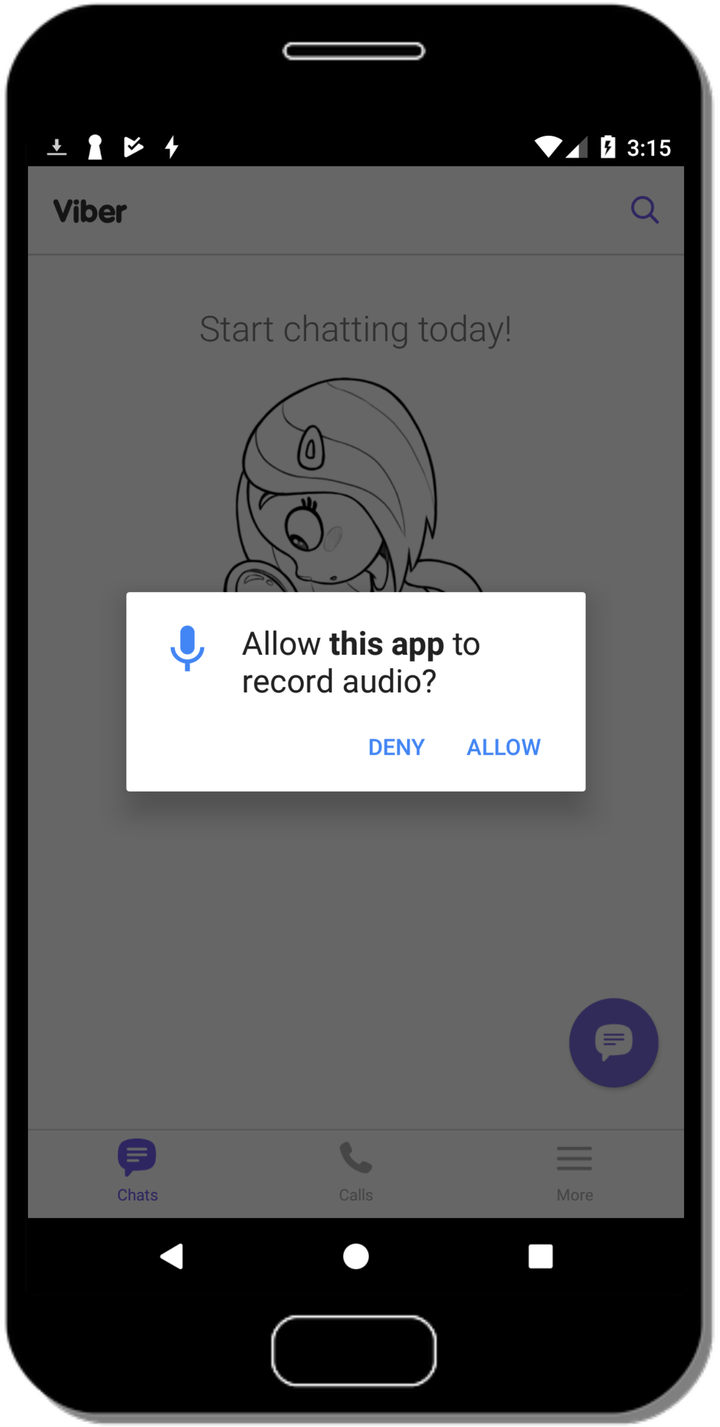
Susceptibility

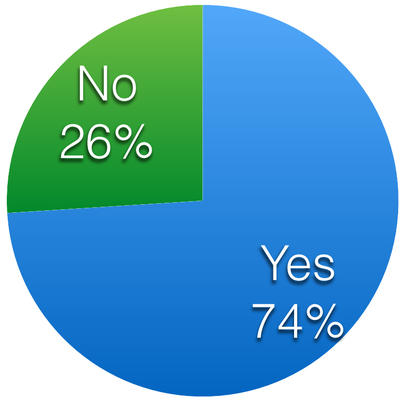
Would you grant this permission?



Susceptibility

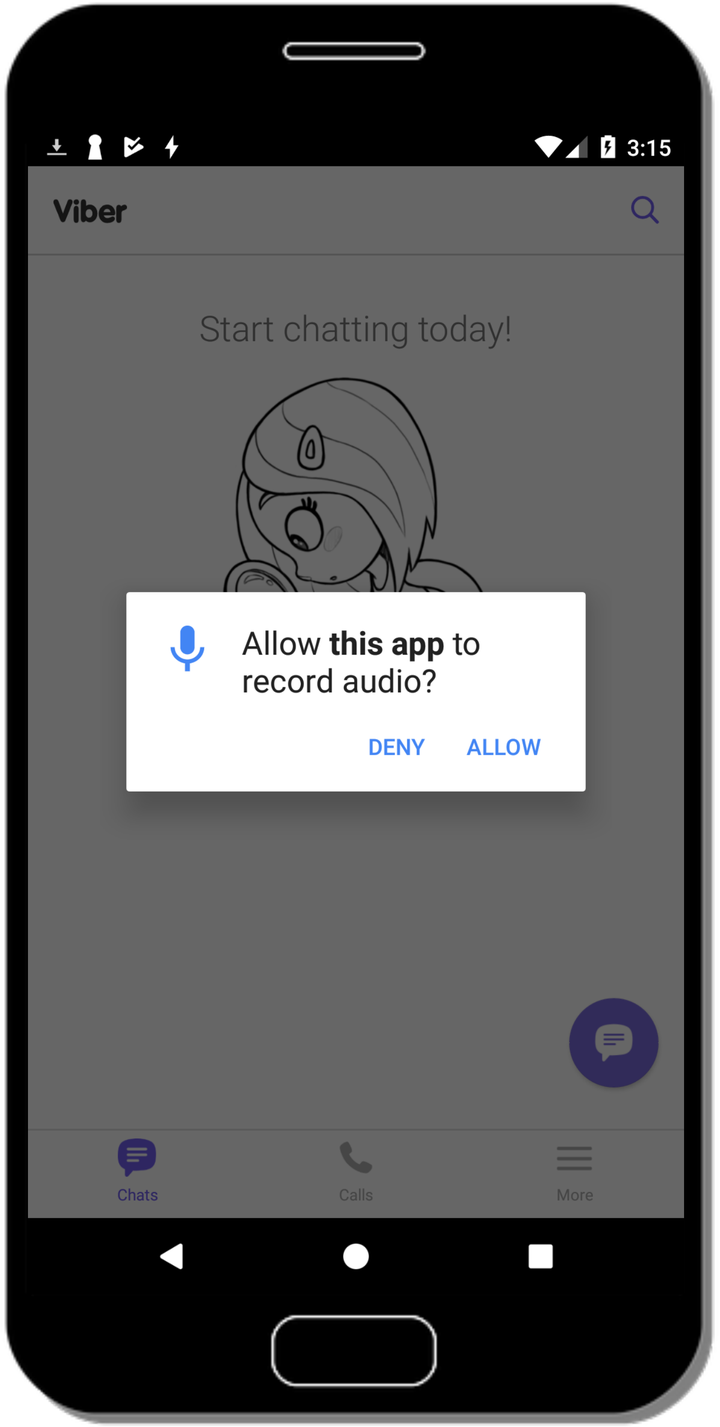
Would you grant this permission?



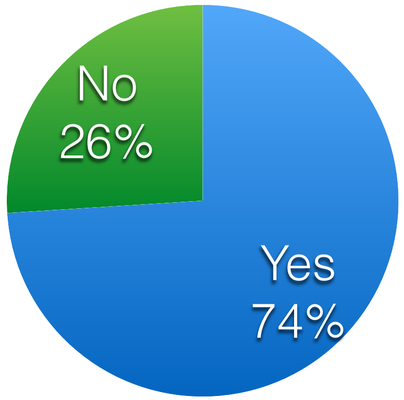


Susceptibility

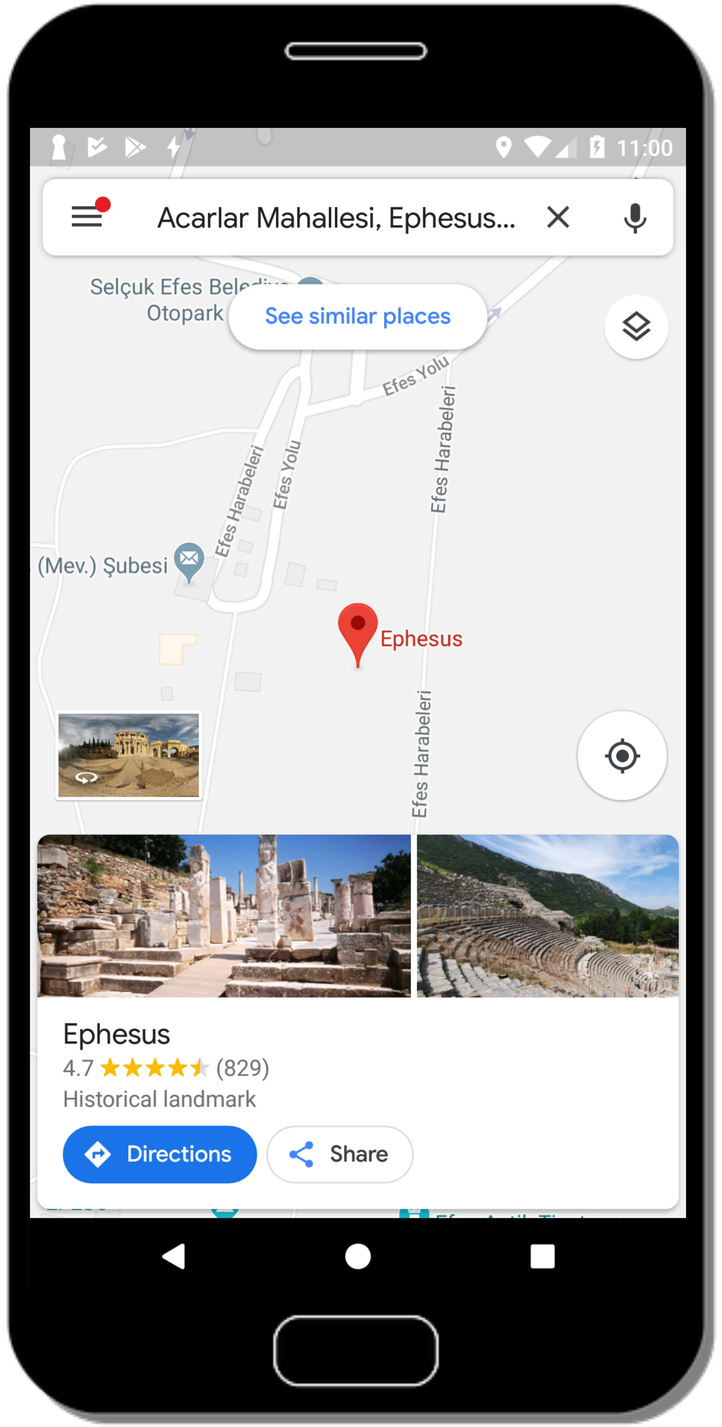
Would you grant this permission?



1 user mentioned request looking fishy

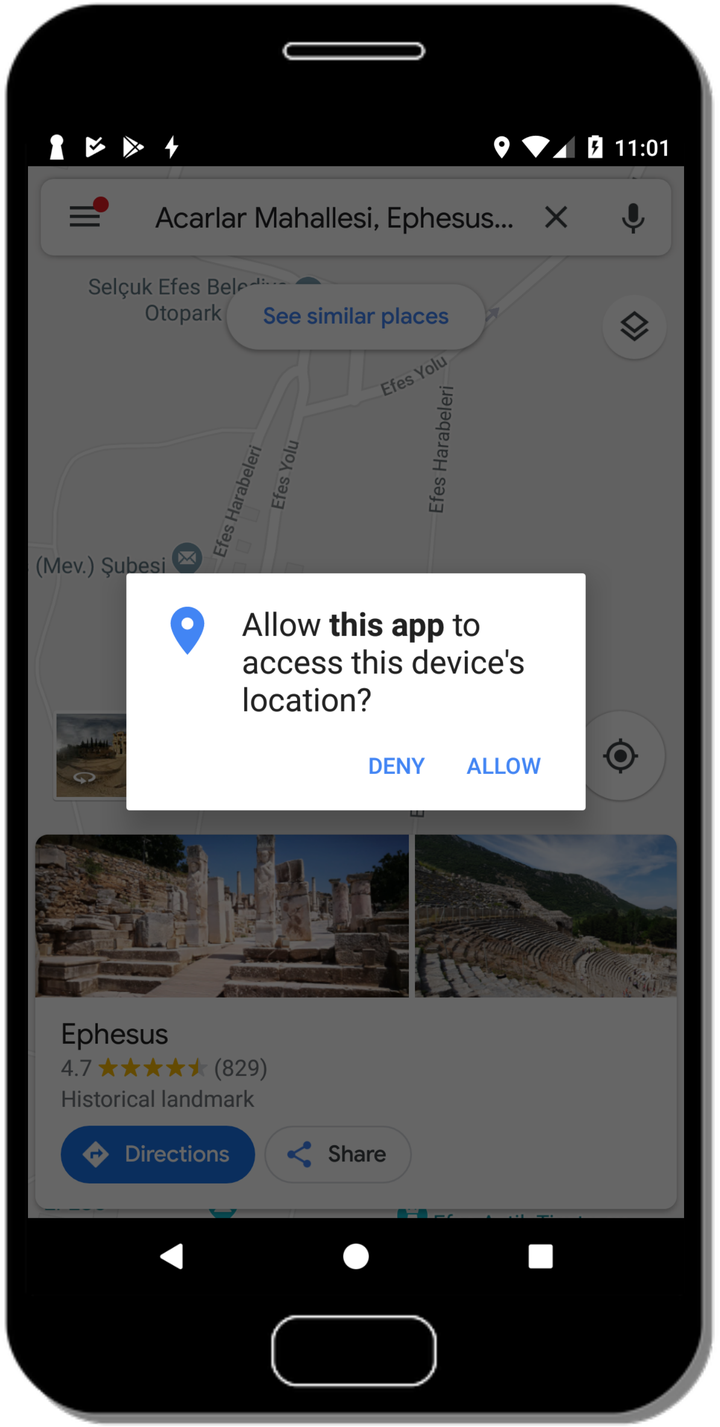


Susceptibility



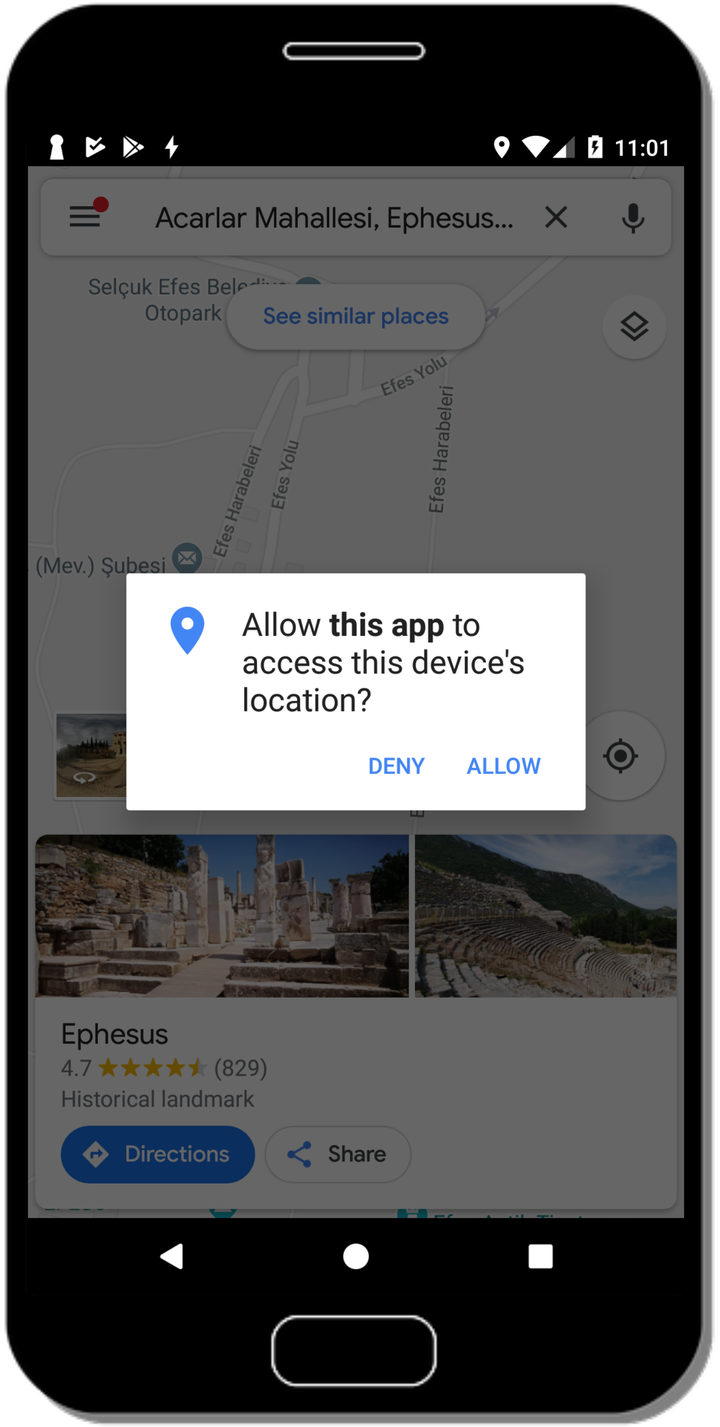
Susceptibility

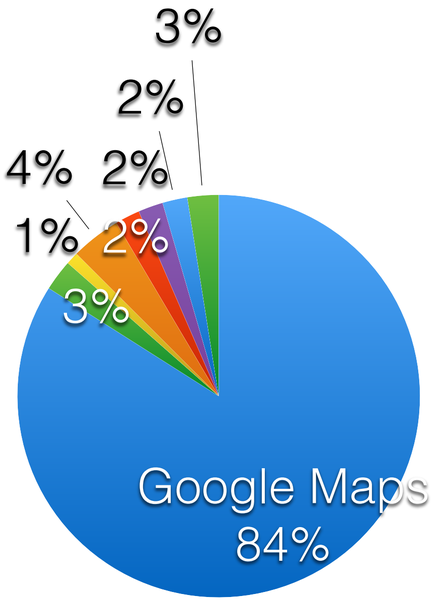
Who’s requesting this permission?



Susceptibility

Who’s requesting this permission?

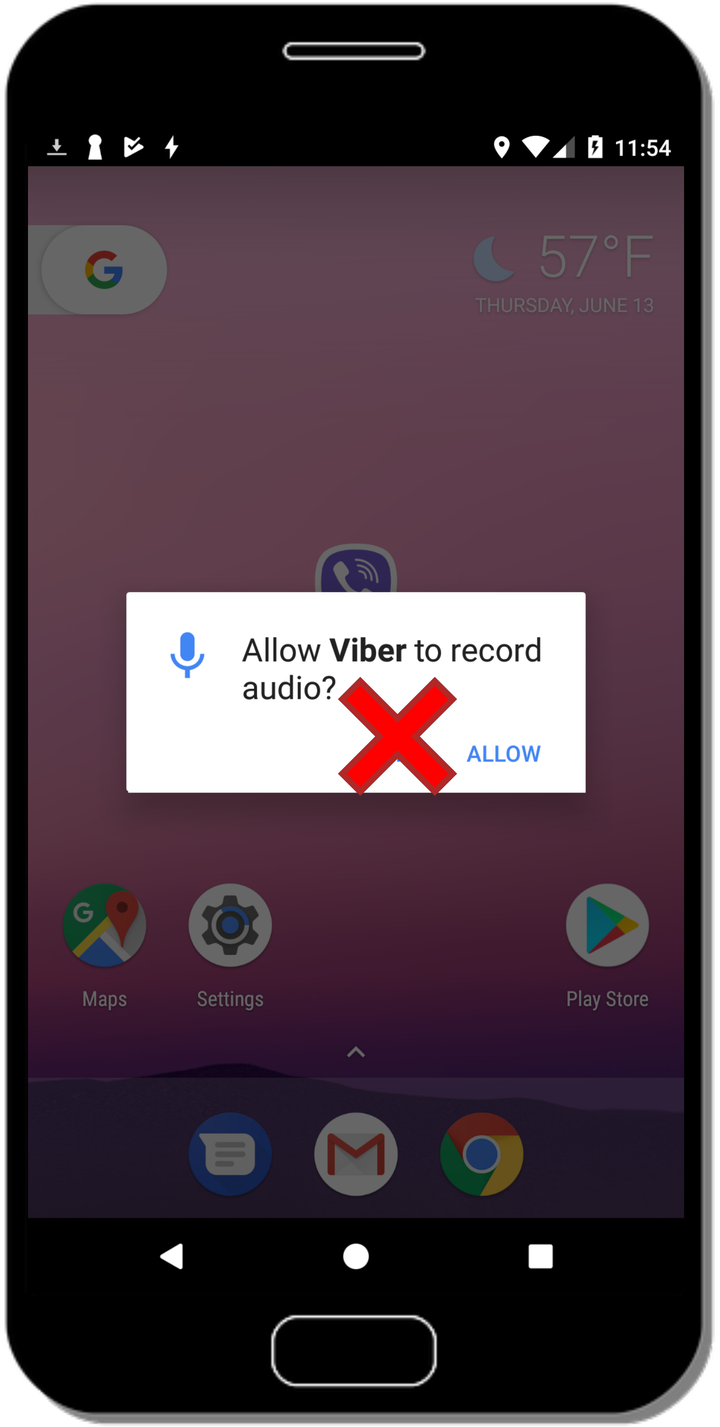




Realistic Attacks

Realistic Attacks (1)

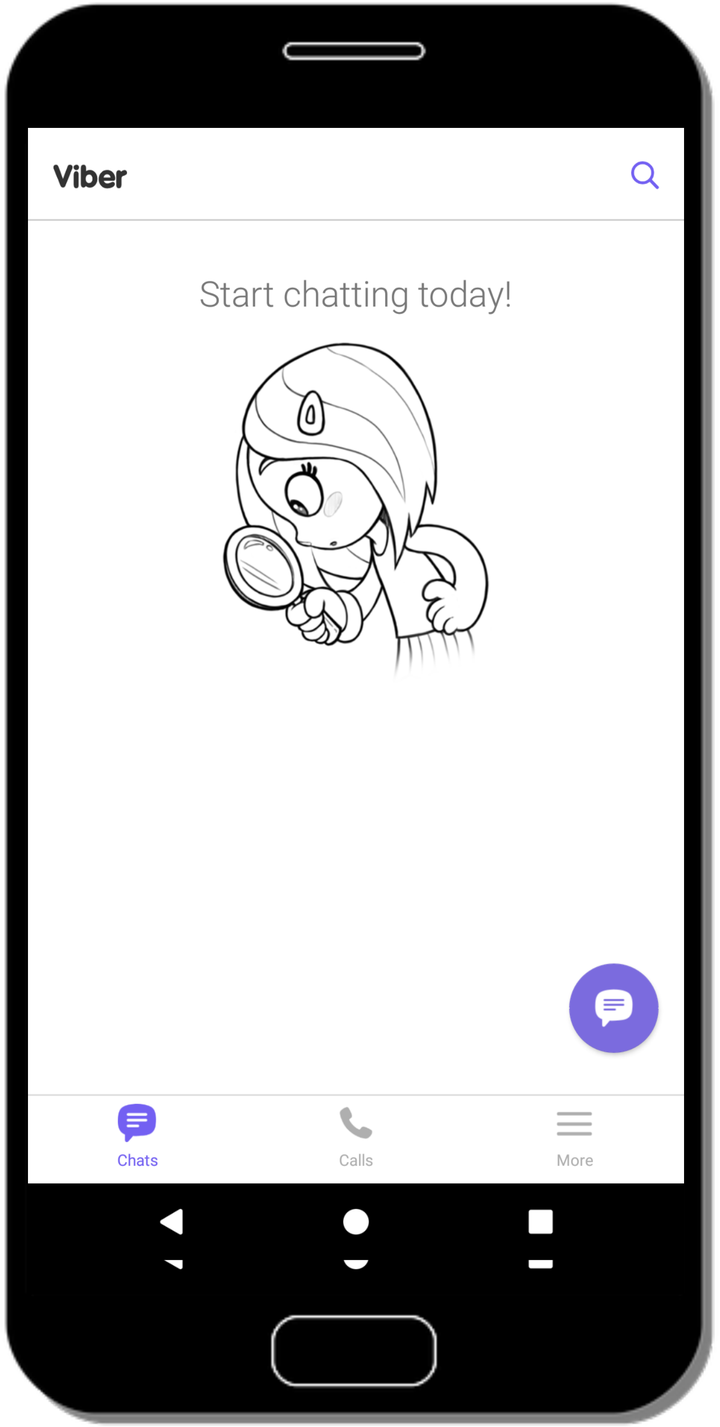
Realistic Attacks (1)



Users are more likely to deny permission requests with NO app in the foreground

WTH?

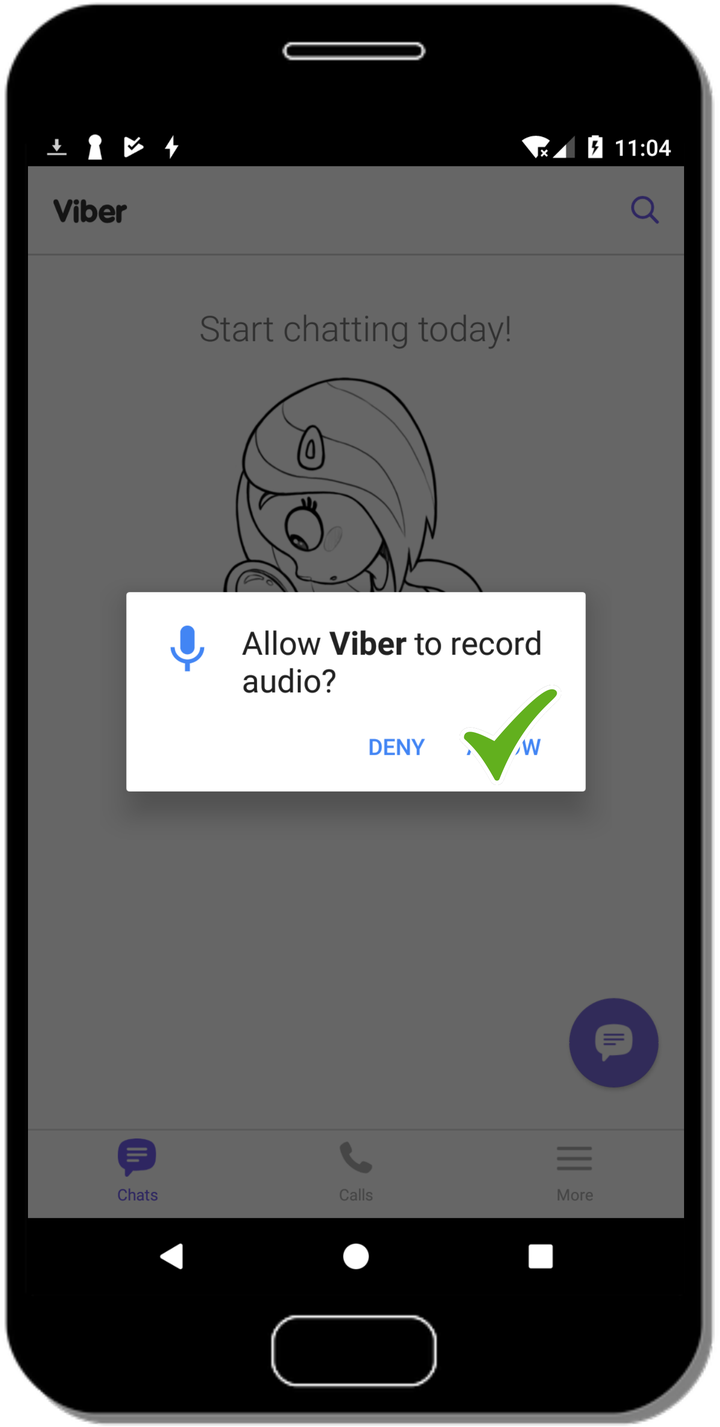
Realistic Attacks (1)



Users are more likely to deny permission requests with NO app in the foreground

Realistic Attacks (1)

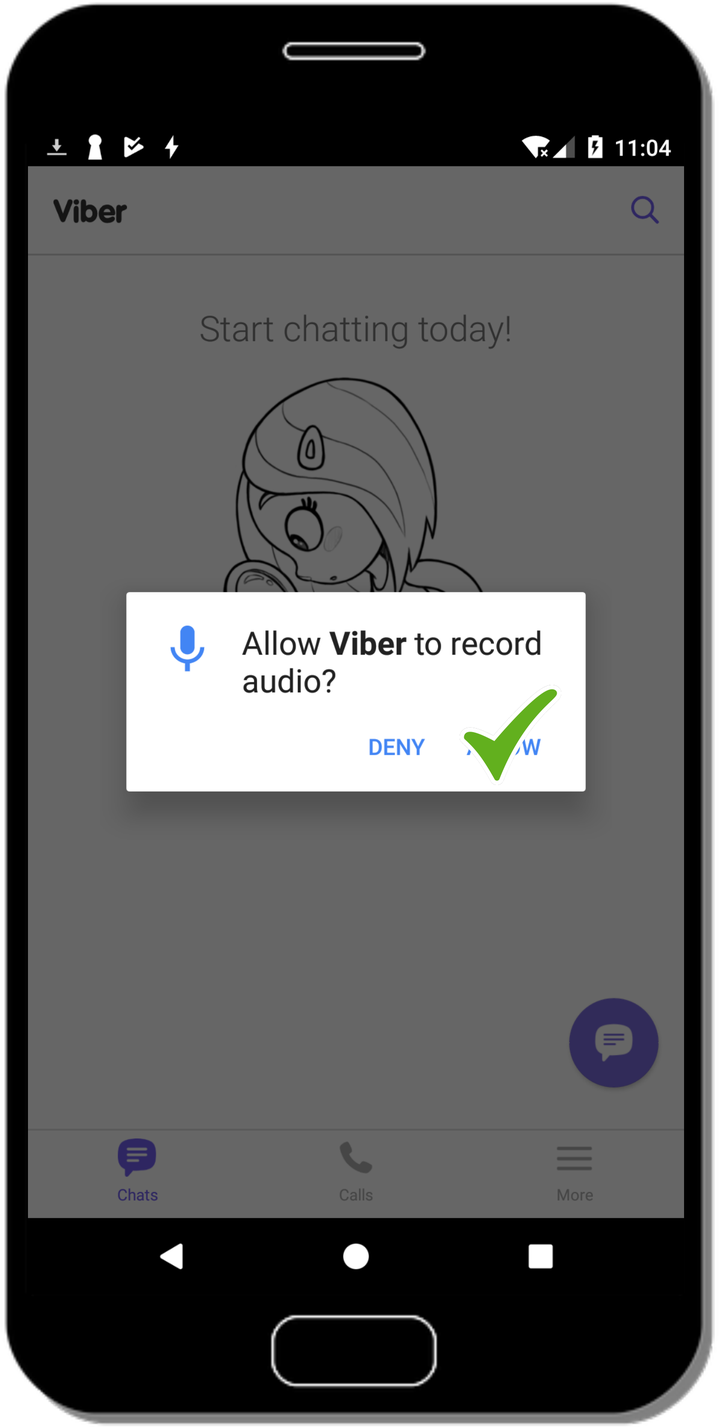
Request only when there's an app in the foreground



Users are more likely to deny permission requests with NO app in the foreground

Yeah okay.

Realistic Attacks (1)



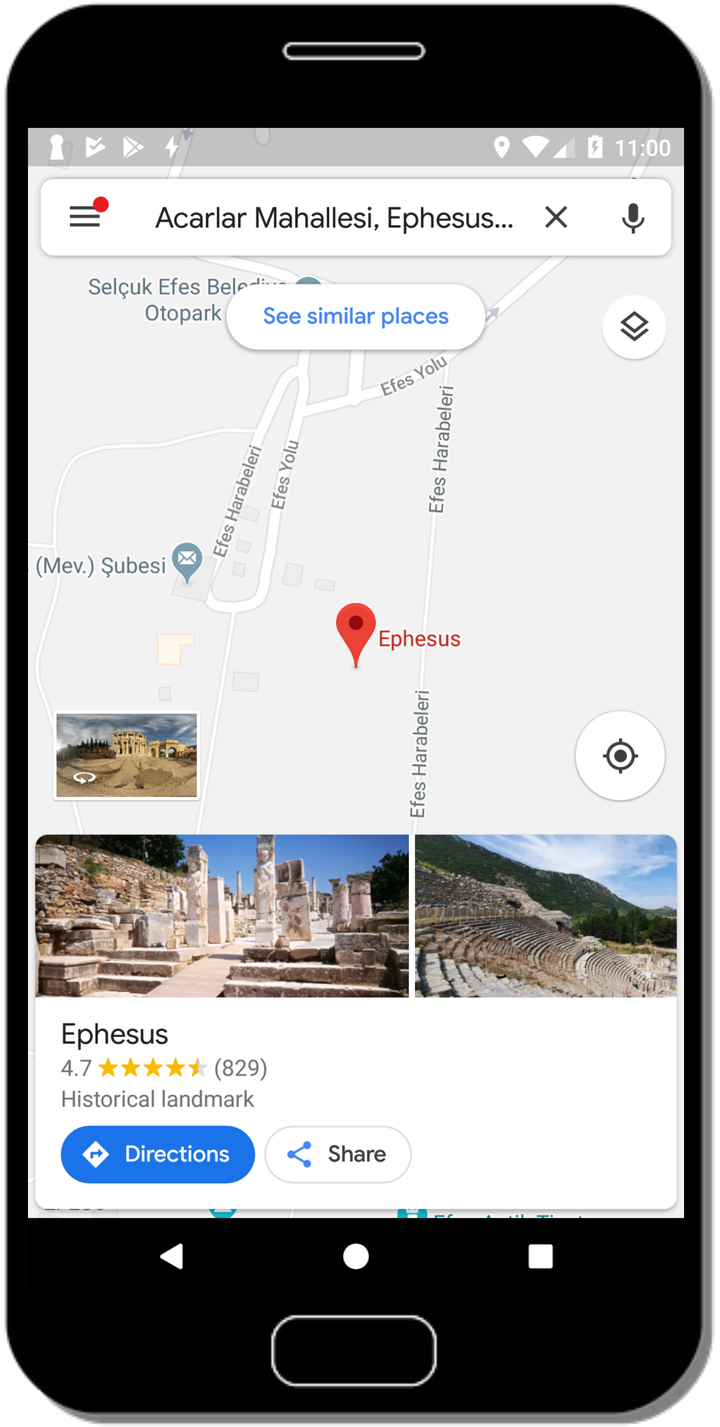
Request only when there's an app in the foreground

How:
getRunningTasks()

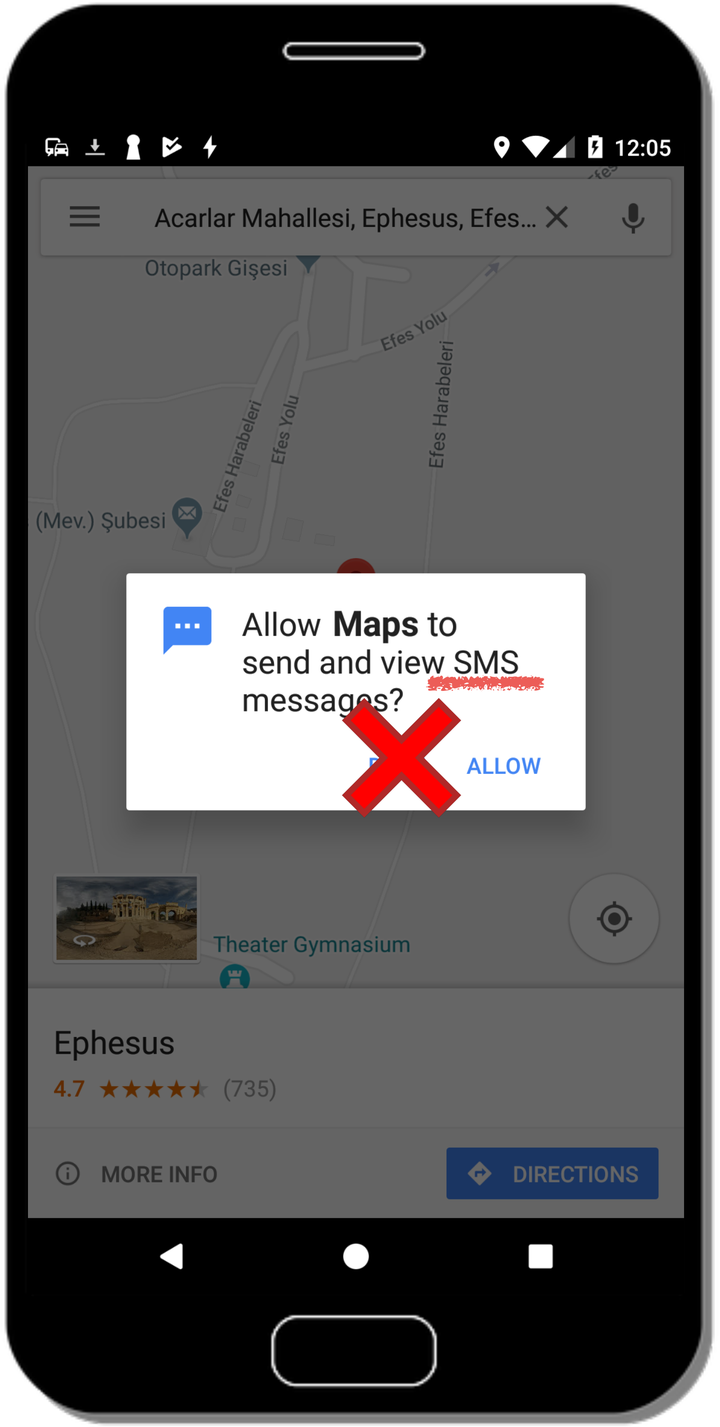
Users are more likely to deny permission requests with NO app in the foreground

Yeah okay.

Realistic Attacks (2)



Realistic Attacks (2)

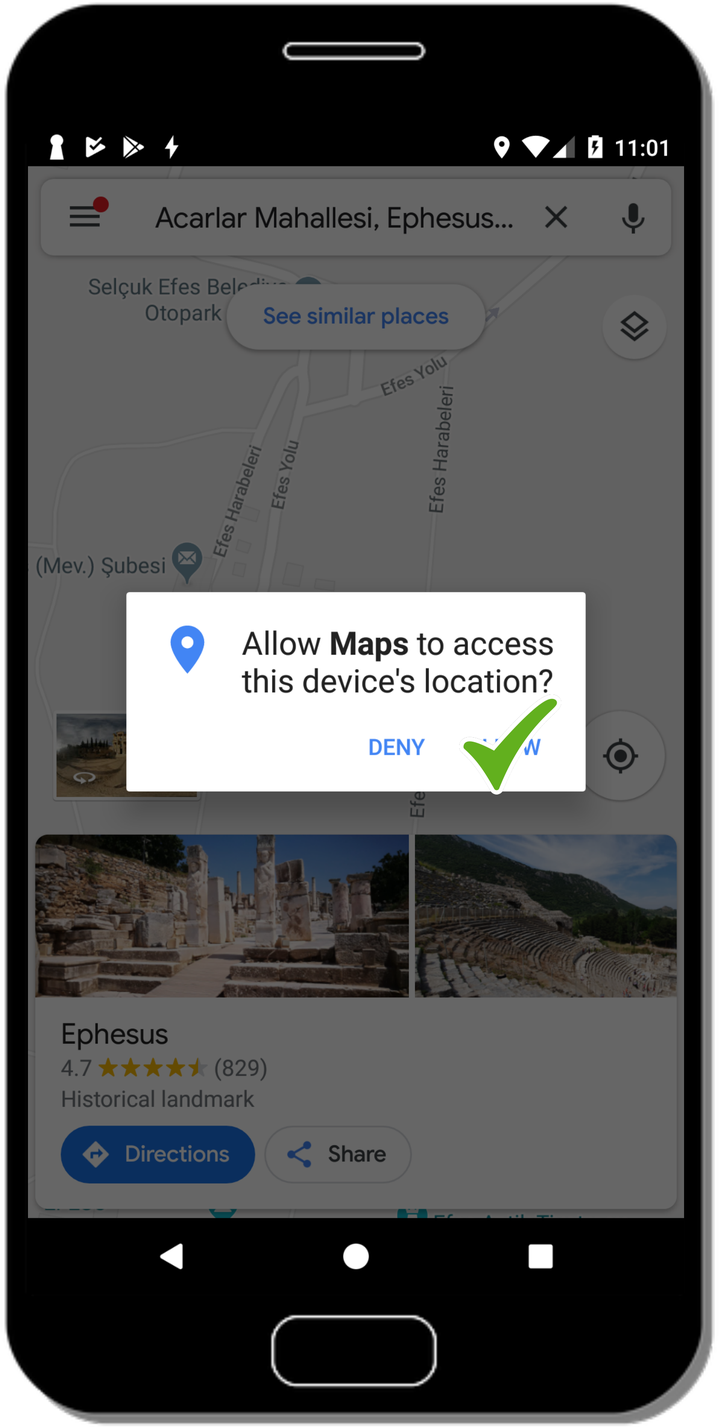


Users are more likely to deny if app requests irrelevant permissions

WTH?

Realistic Attacks (2)

Request only the relevant permissions



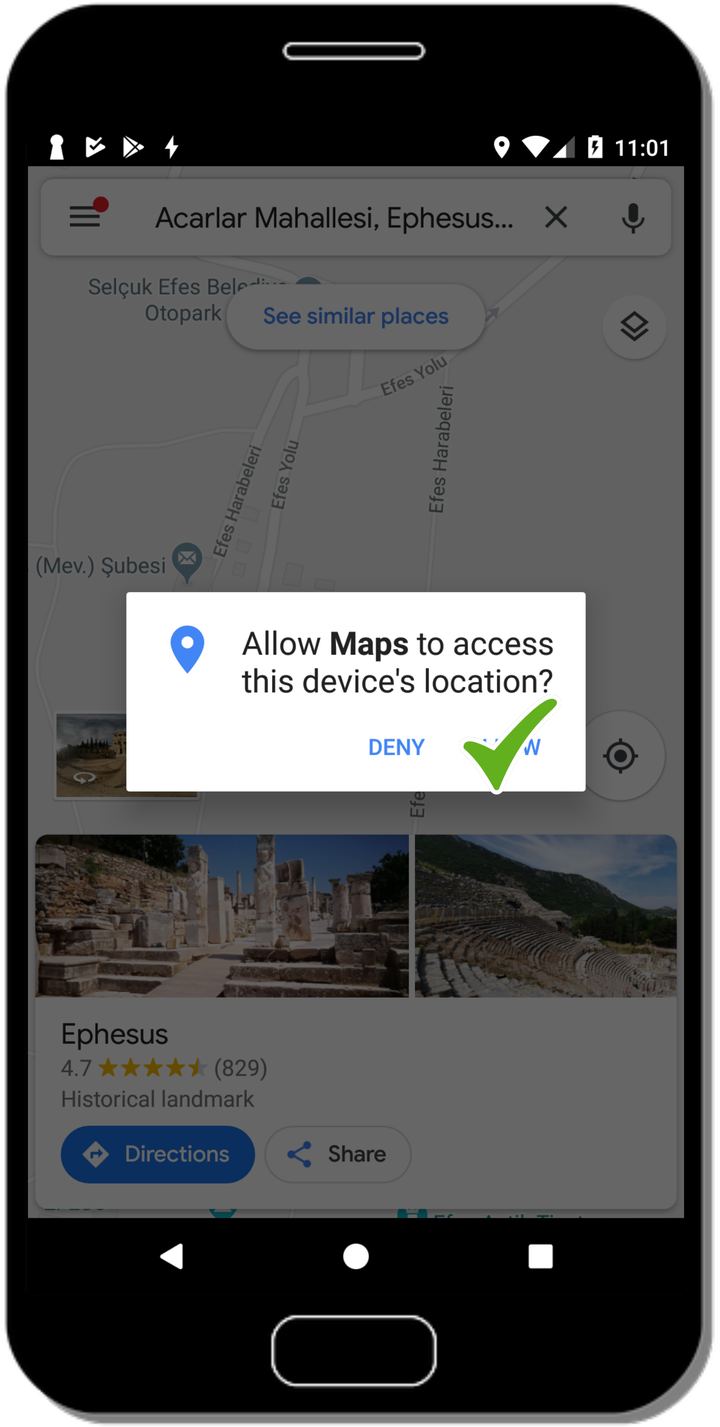
Users are more likely to deny if app requests irrelevant permissions

Yeah okay.

Realistic Attacks (2)

Request only the relevant permissions

- Infer the foreground app



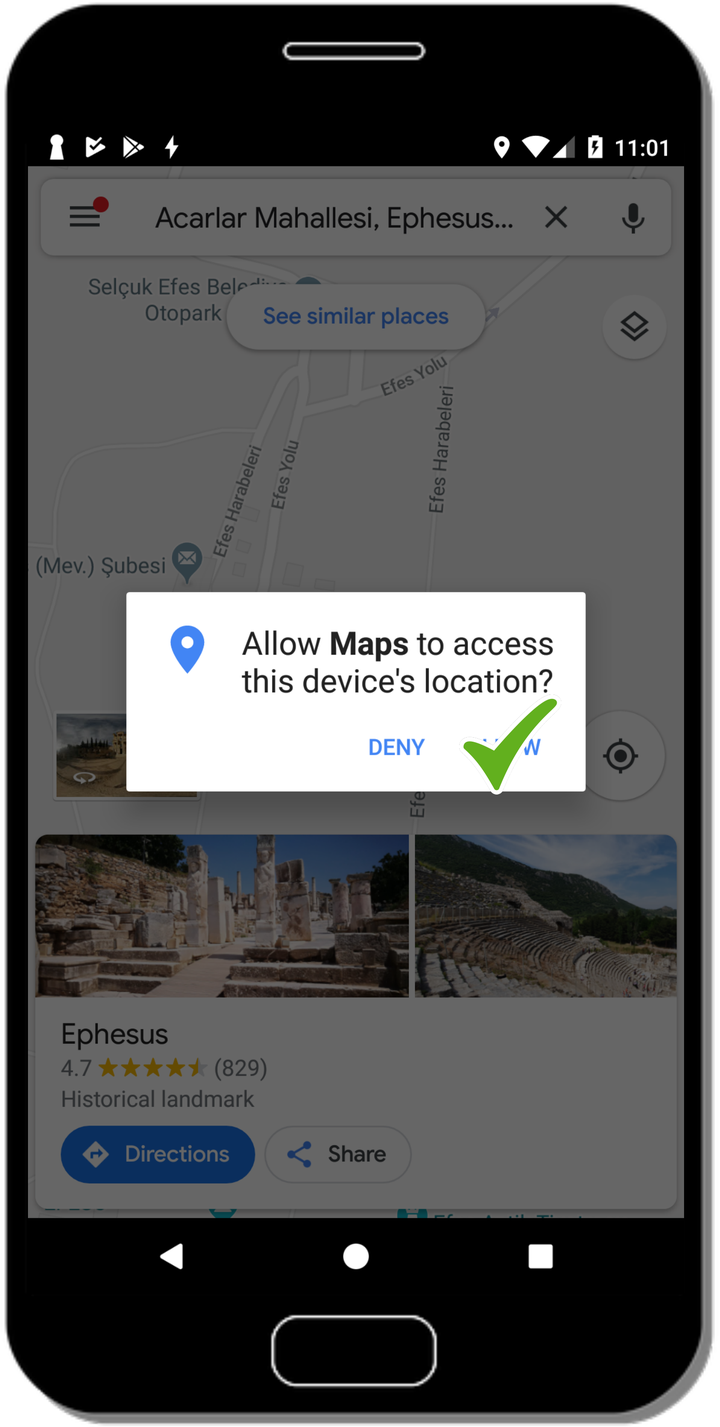
Users are more likely to deny if app requests irrelevant permissions

Yeah okay.

Realistic Attacks (2)

Request only the relevant permissions

- Infer the foreground app
- Only request permissions required by this app



Users are more likely to deny if app requests irrelevant permissions

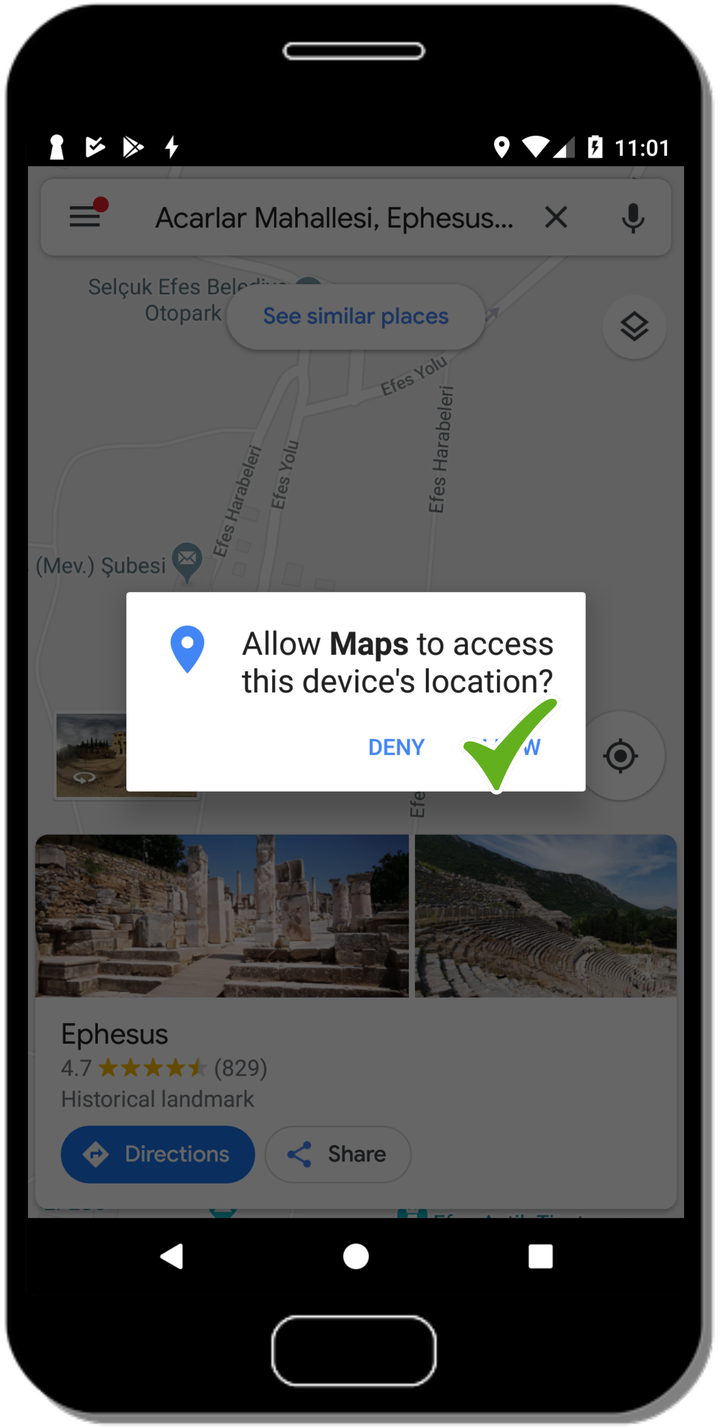
Yeah okay.

Realistic Attacks (2)

Request only the relevant permissions

- Infer the foreground app
- Only request permissions required by this app

How: ProcHarvester



Users are more likely to deny if app requests irrelevant permissions

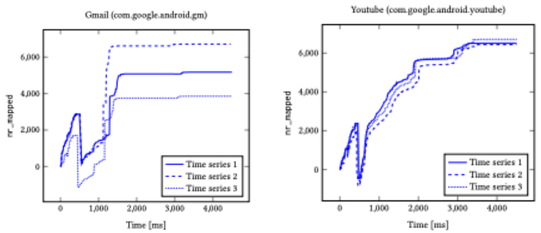
Yeah okay.

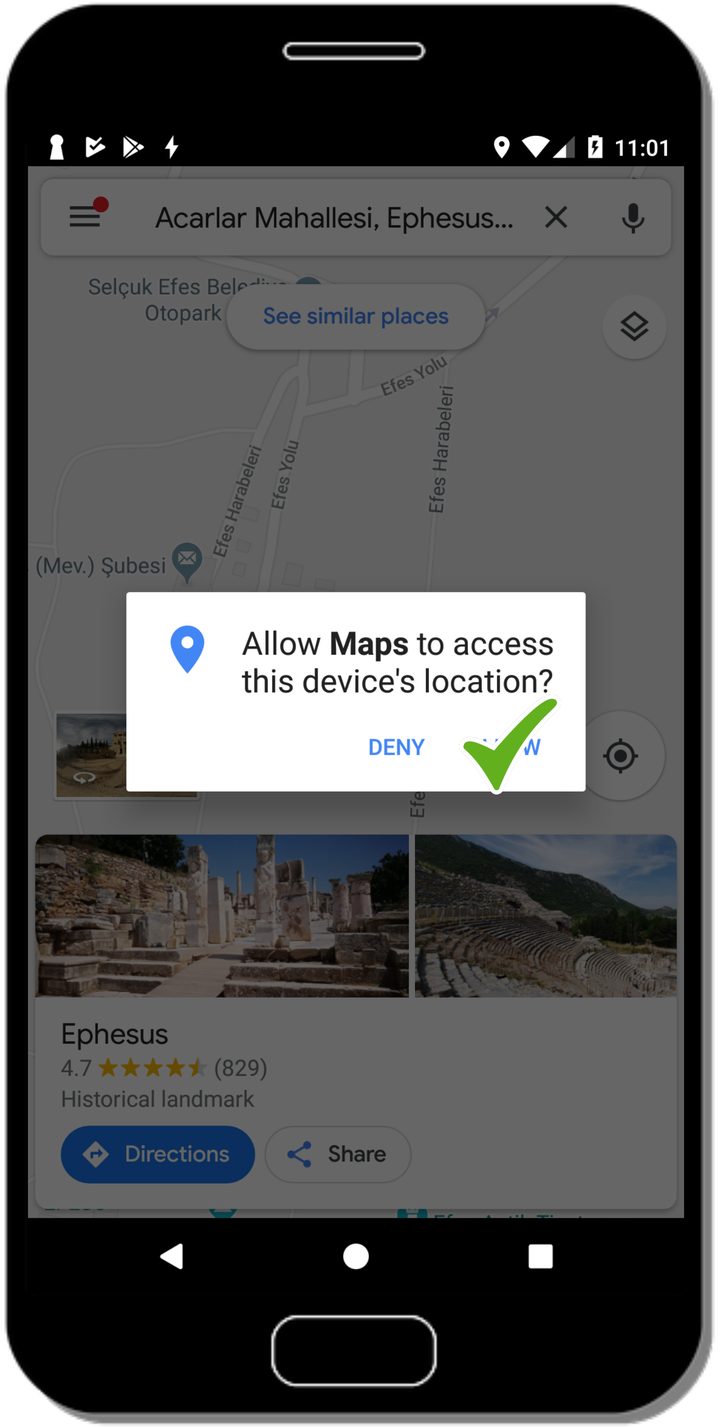
Realistic Attacks (2)

Request only the relevant permissions

- Infer the foreground app
- Only request permissions required by this app

How: ProcHarvester





Users are more likely to deny if app requests irrelevant permissions

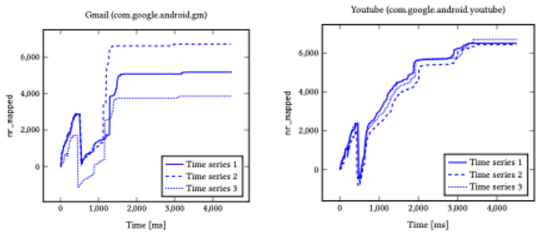
Yeah okay.

Realistic Attacks (2)

Request only the relevant permissions

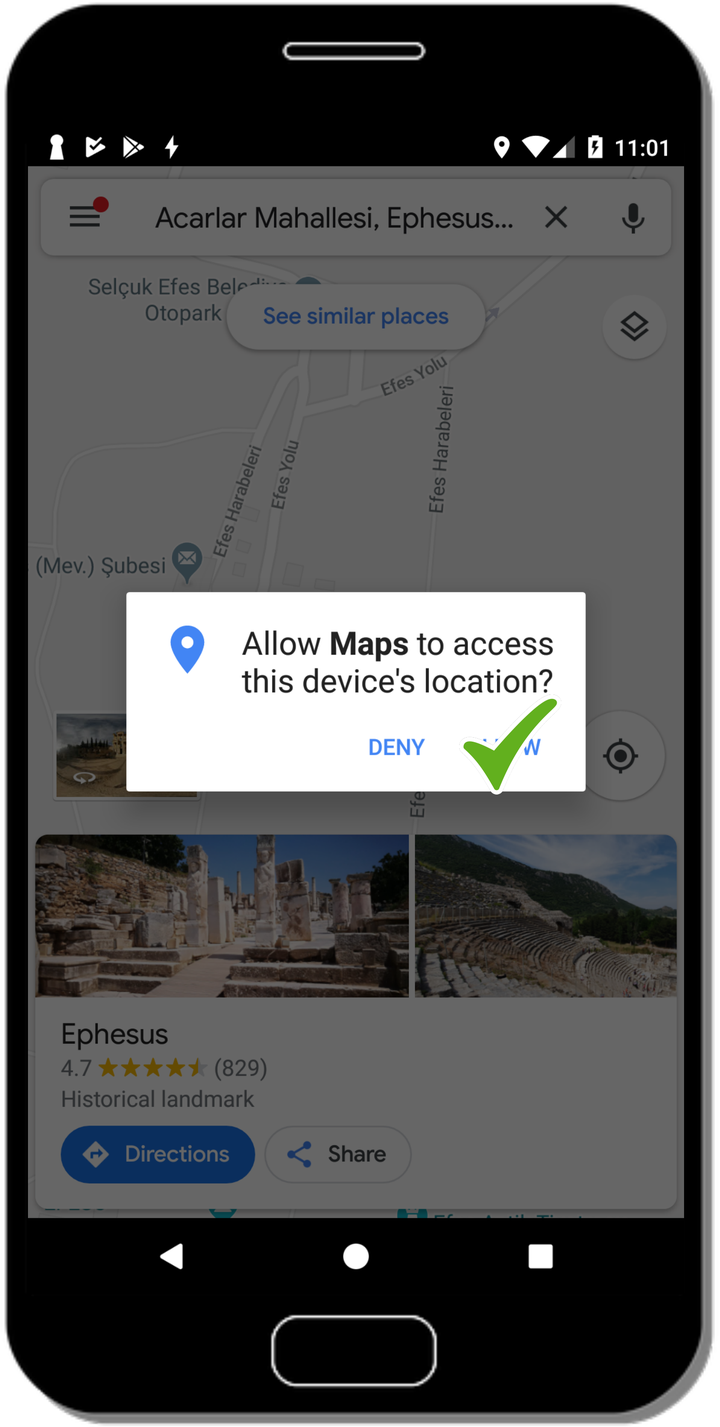
- Infer the foreground app
- Only request permissions required by this app

How: ProcHarvester



- Adapted ProcHarvester to realistic attack scenarios

- 90% accuracy



Users are more likely to deny if app requests irrelevant permissions

Yeah okay.

Feasibility

Feasibility

20 lab participants

Feasibility

20 lab participants

Realistic setting with everyday tasks and popular apps:

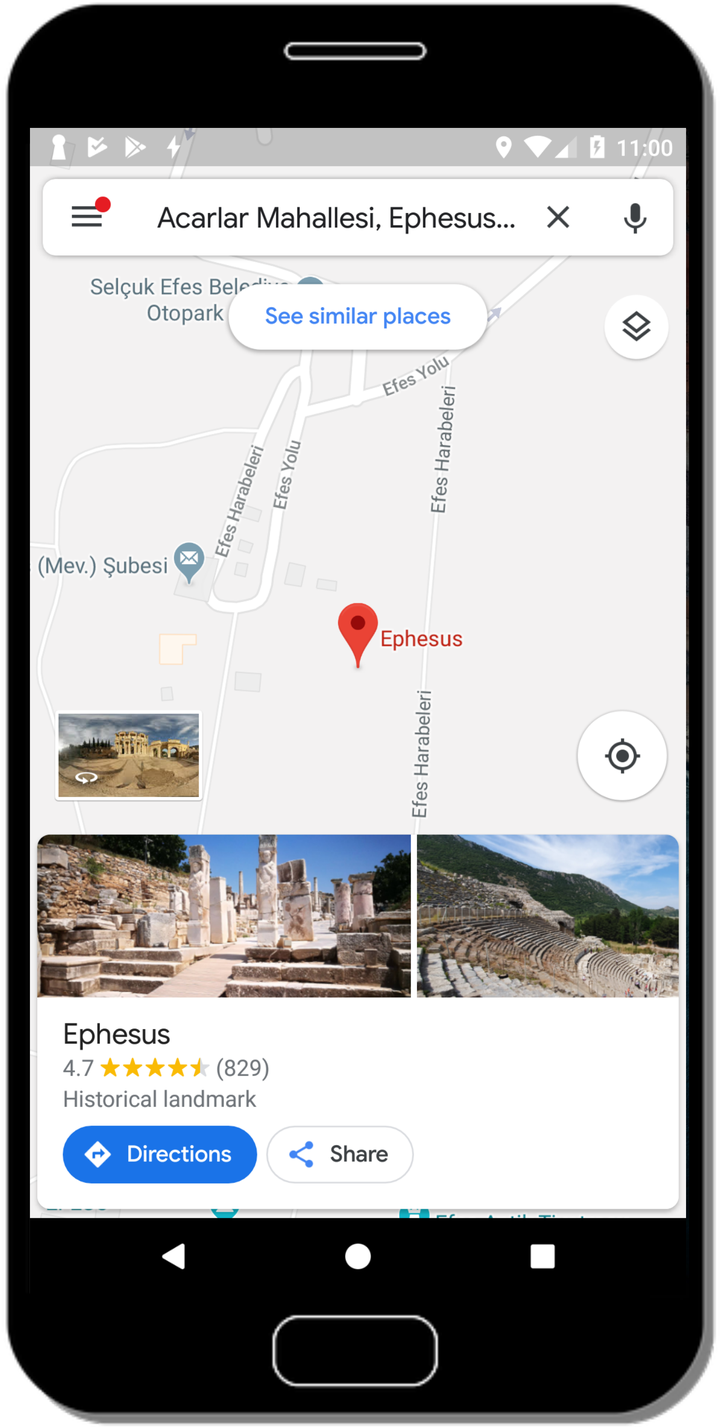
Feasibility

20 lab participants

Realistic setting with everyday tasks and popular apps:

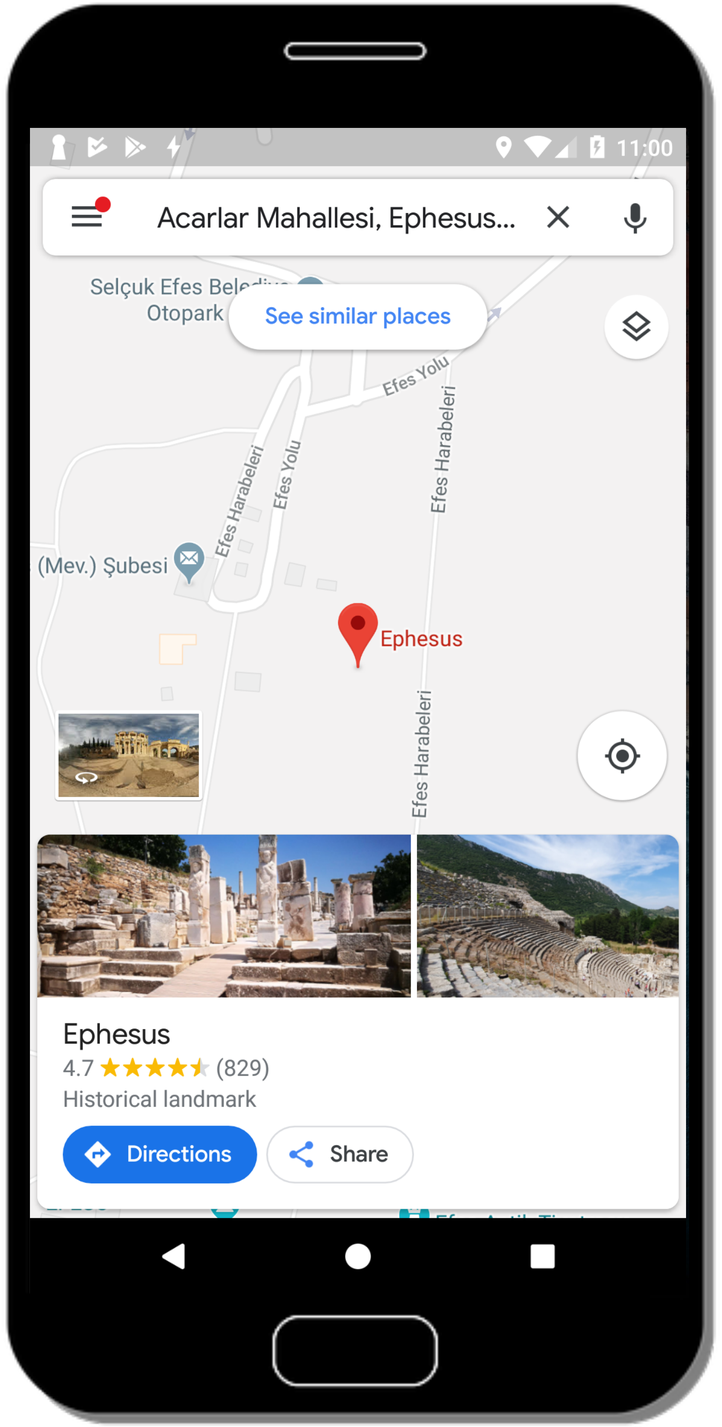
None of the participants noticed the attack!

Defense and Countermeasures



Defense and Countermeasures

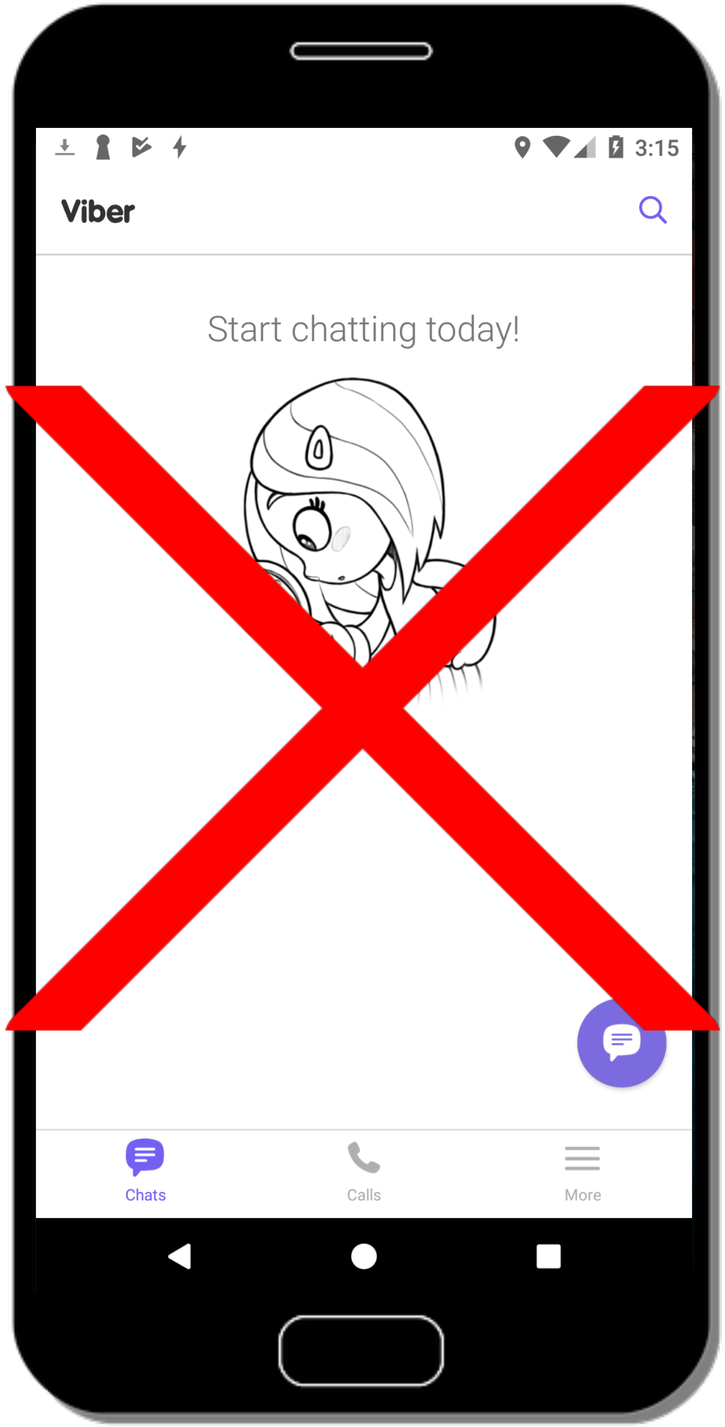
Existing defenses 😅



Defense and Countermeasures

Existing defenses 😅

Background app starts on Android 10

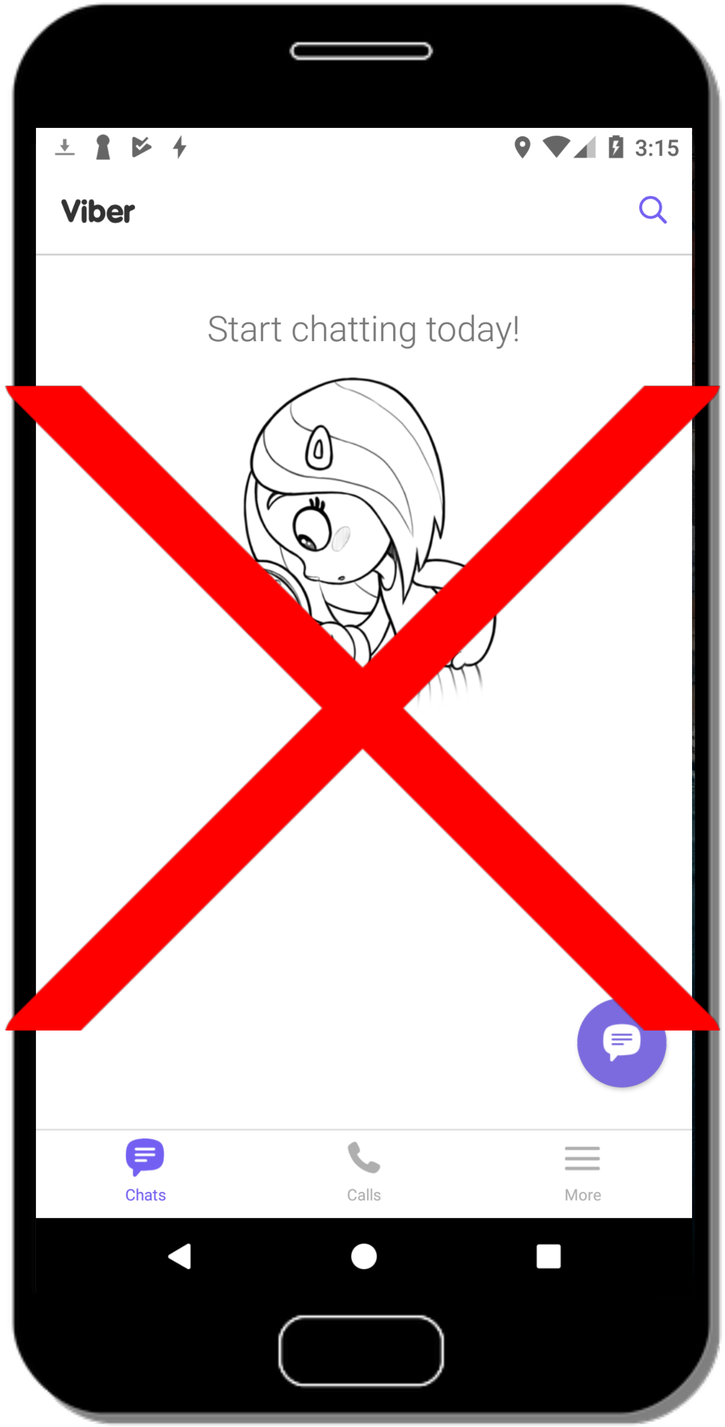


Defense and Countermeasures

Existing defenses 😅

Background app starts on Android 10

Attacks still work on Android 10 and 11



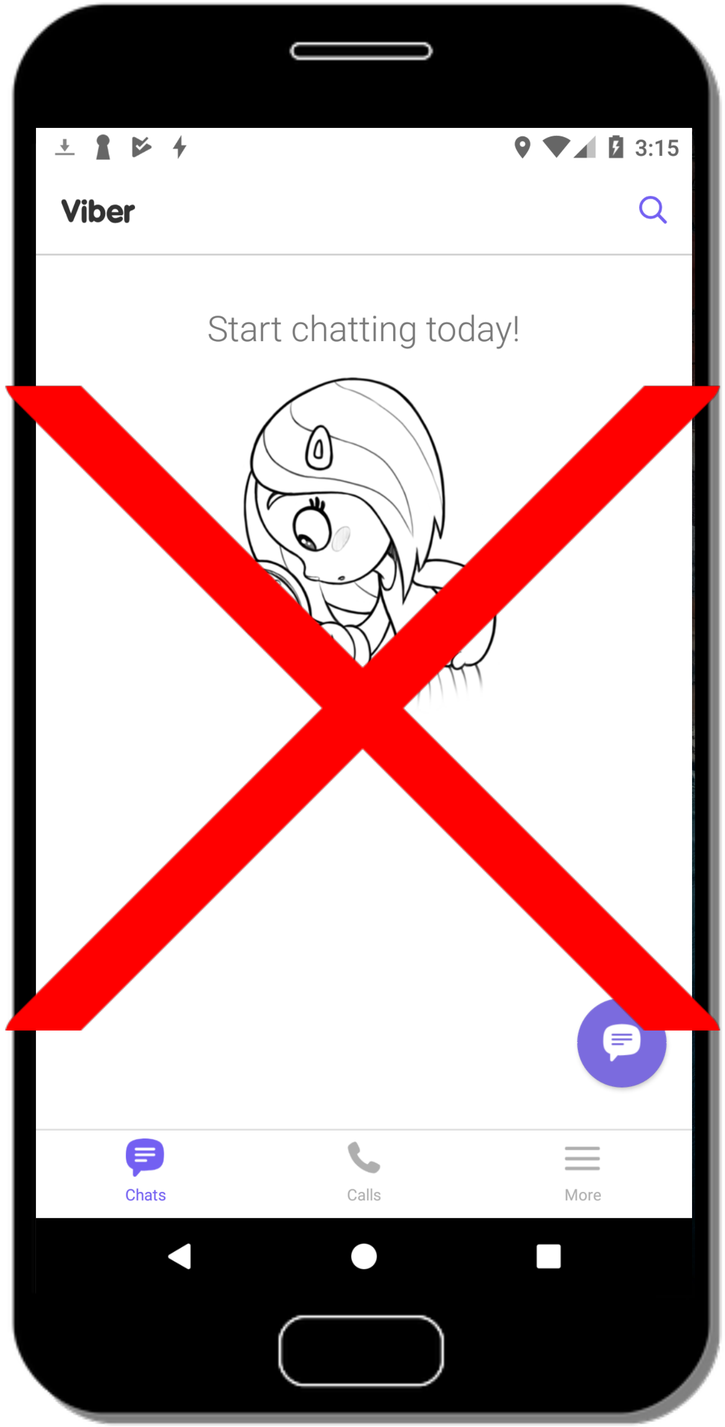
Defense and Countermeasures

Existing defenses 😅

Background app starts on Android 10

Attacks still work on Android 10 and 11

Non-trival solution



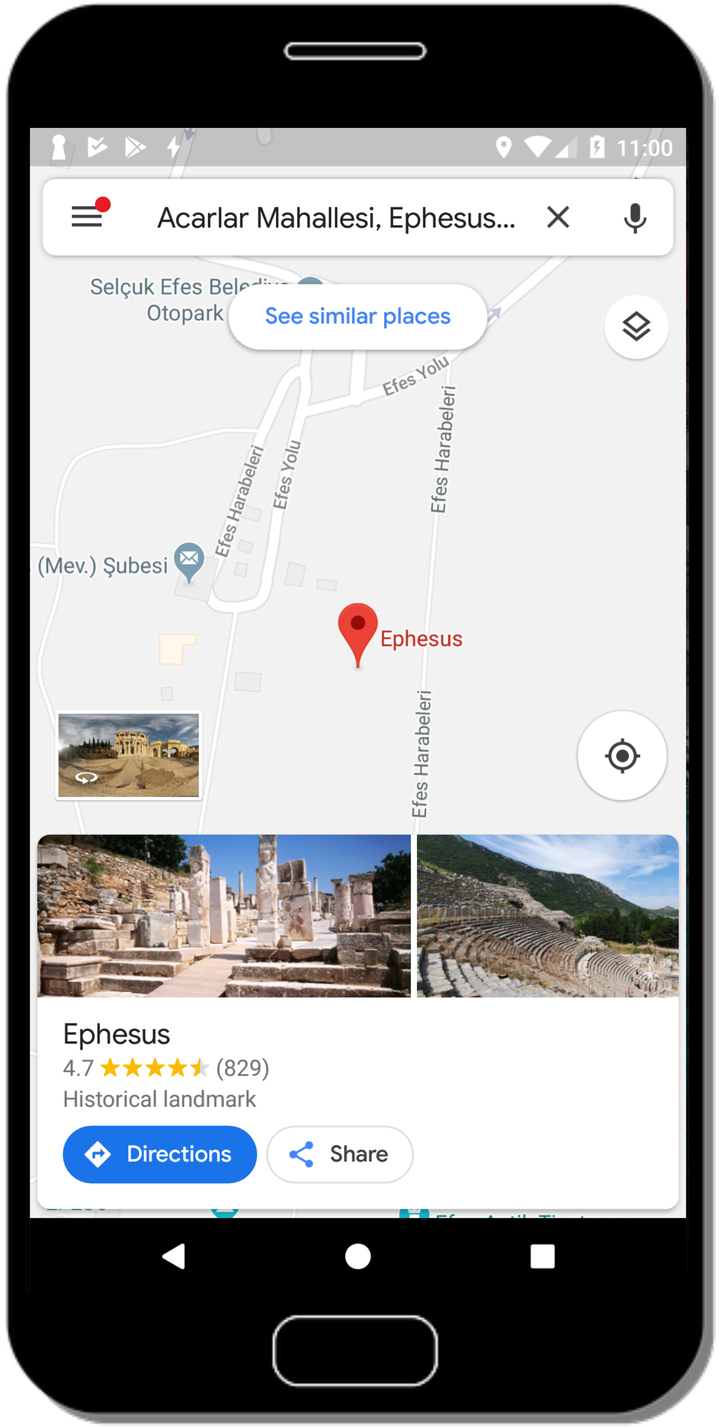
Defense and Countermeasures

Existing defenses 

Background app starts on Android 10

Attacks still work on Android 10 and 11

Non-trival solution



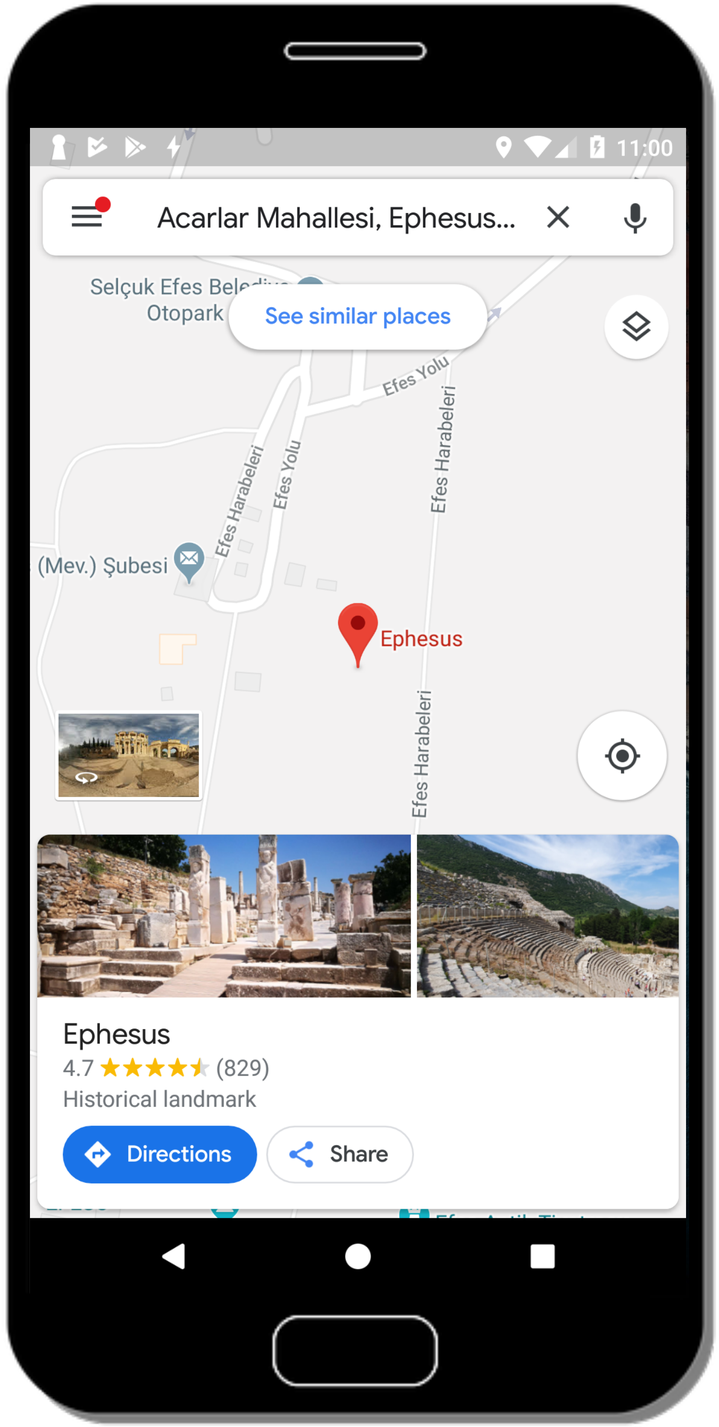
Defense and Countermeasures

Existing defenses

Background app starts on Android 10

Attacks still work on Android 10 and 11

Non-trival solution



Recommendations:

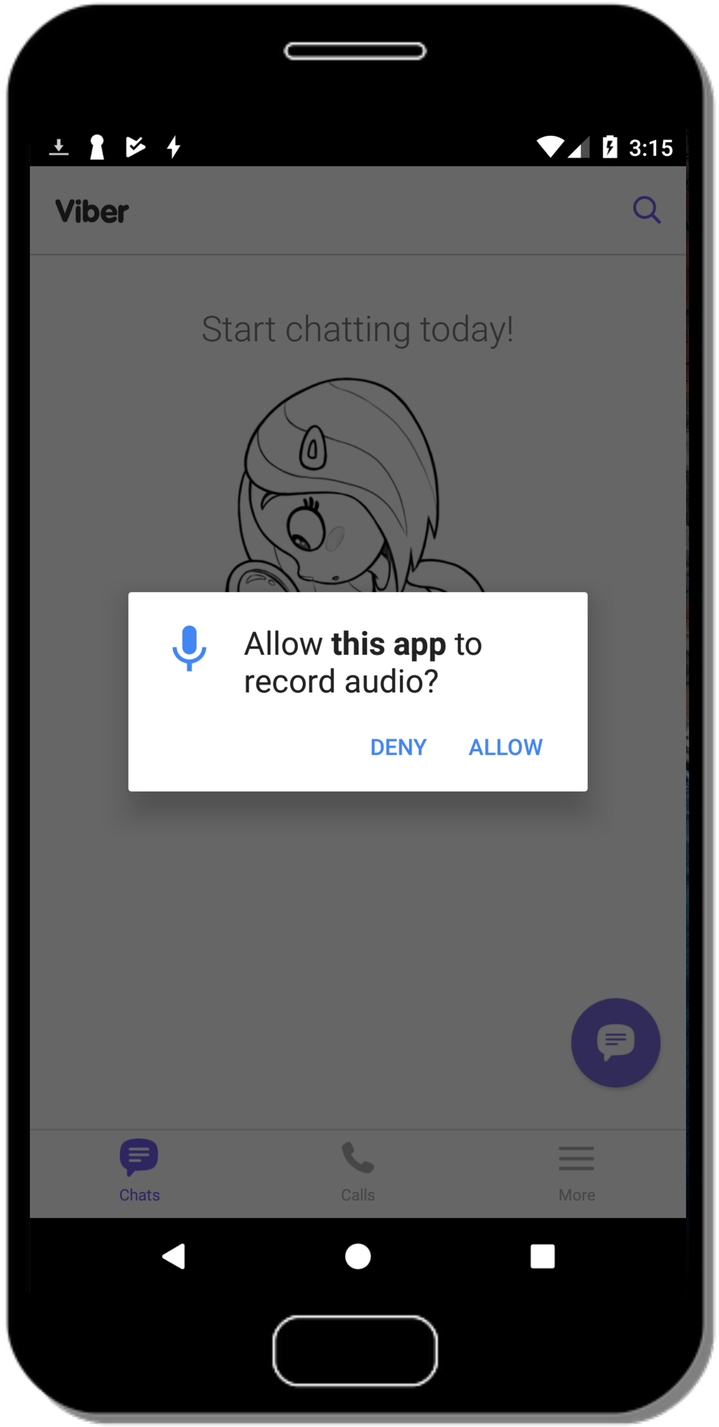
Defense and Countermeasures

Existing defenses

Background app starts on Android 10

Attacks still work on Android 10 and 11

Non-trival solution



Recommendations:

✓ Mandatory app transition effects

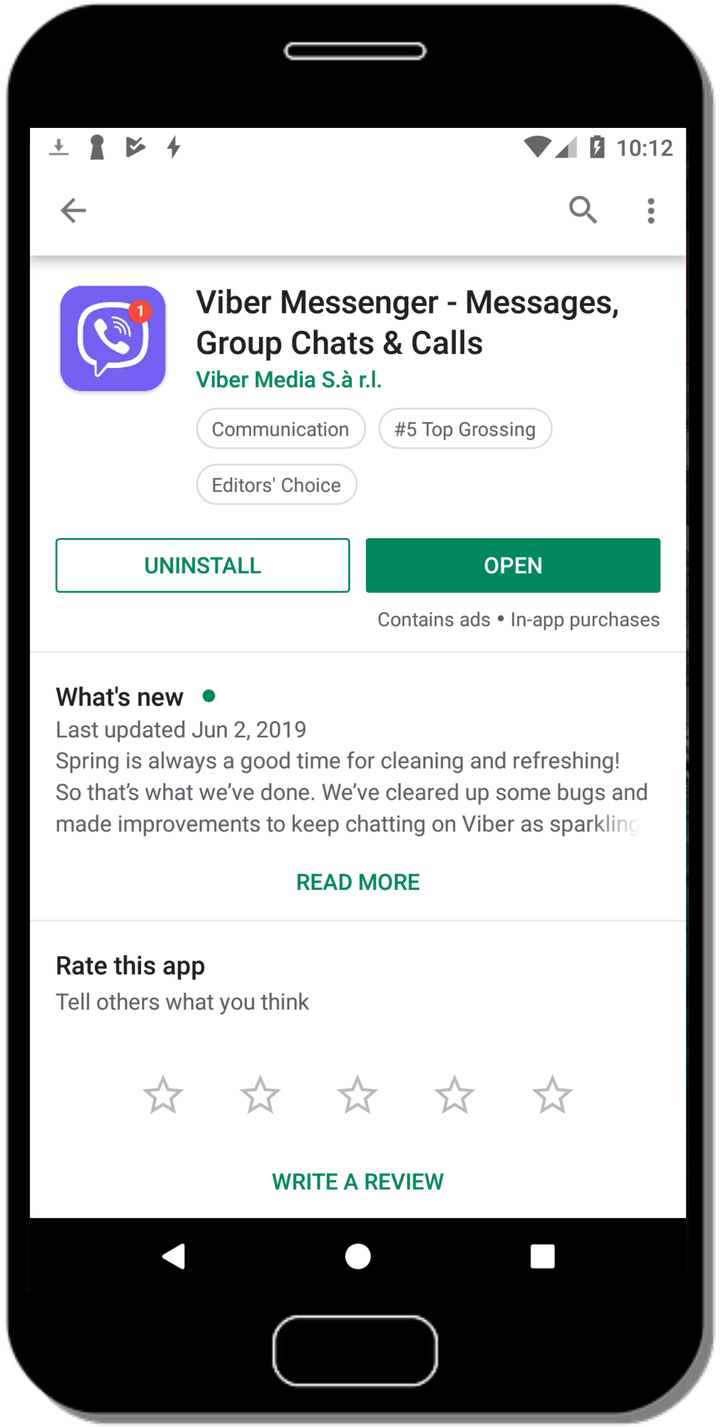
Defense and Countermeasures

Existing defenses

Background app starts on Android 10

Attacks still work on Android 10 and 11

Non-trival solution



Recommendations:

✓ Mandatory app transition effects

✓ App name checks in:

Google Play

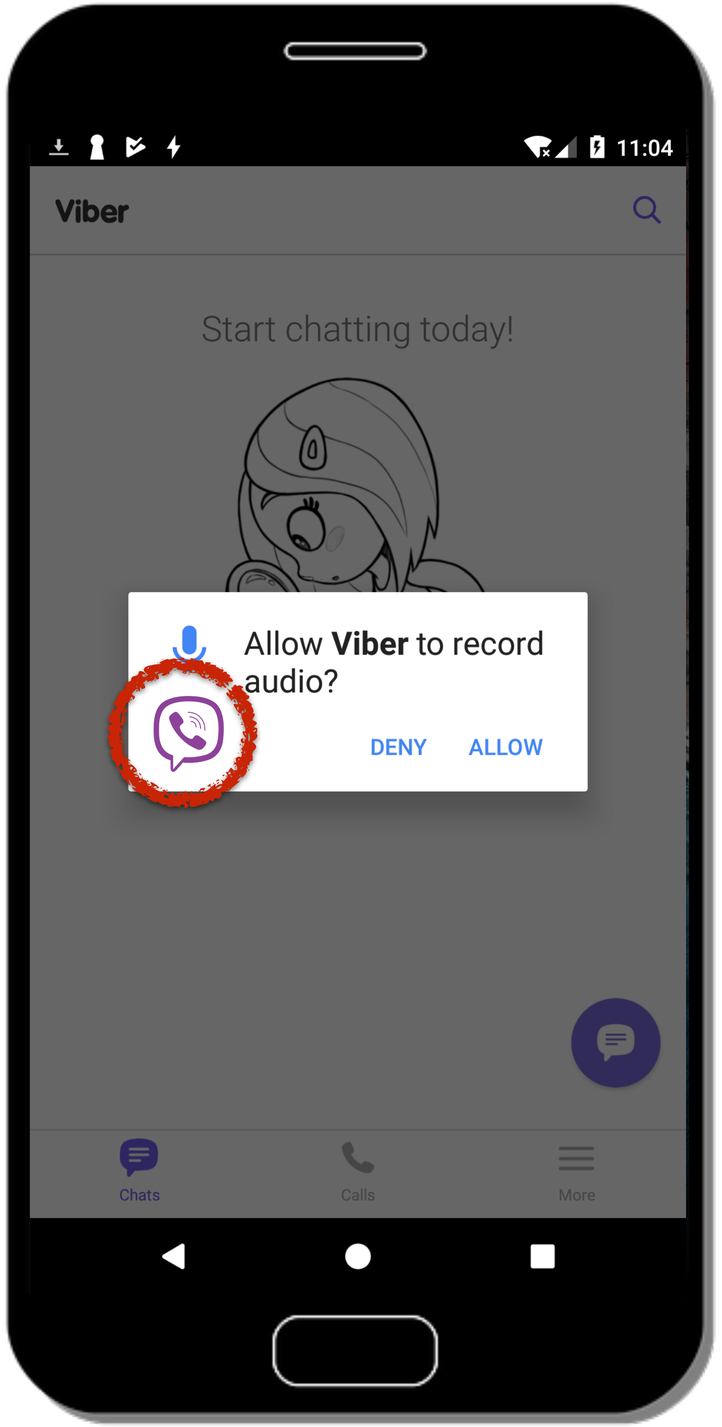
Defense and Countermeasures

Existing defenses

Background app starts on Android 10

Attacks still work on Android 10 and 11

Non-trival solution



Recommendations:

- Mandatory app transition effects
- App name checks in:

Google Play

- Additional app identifiers in permission dialogs

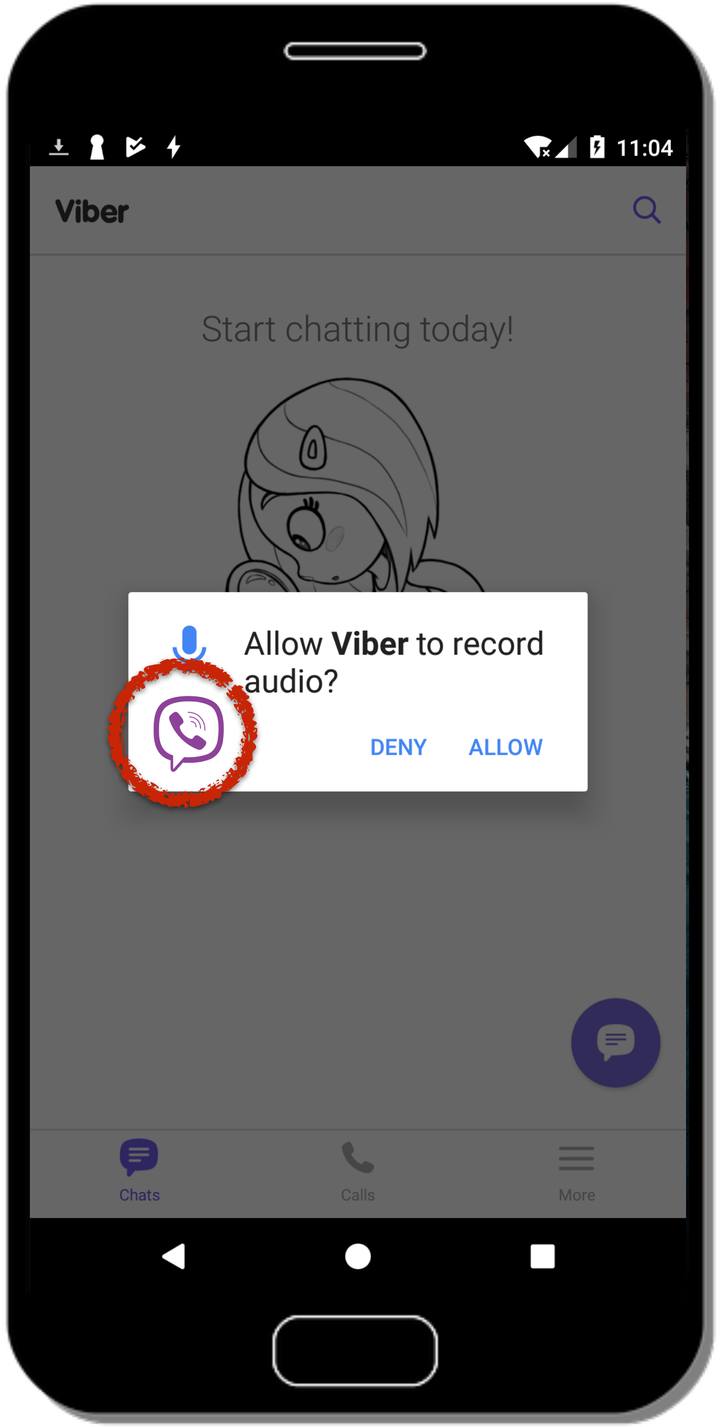
Defense and Countermeasures

Existing defenses

Background app starts on Android 10

Attacks still work on Android 10 and 11

Non-trival solution



Recommendations:

- Mandatory app transition effects
- App name checks in:

Google Play

- Additional app identifiers in permission dialogs
- No more transparent UI

Thank you!

See No Evil: Phishing for Permissions with False Transparency

Güliz Seray Tuncay*†, Jingyu Qian†, Carl A. Gunter†

*Google, †University of Illinois at Urbana-Champaign