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

Runtime Permissions >= Android 6.0

lack of context
Install-time Permissions
< Android 6.0

Runtime Permissions
>= Android 6.0

lack of context

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
Start chatting today!
Allow this app to record audio?

DENY  ALLOW
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?

False transparency attacks on runtime permissions

Affects Android 6-11
Breaking the security guarantees of runtime permissions
Contextual Guarantee
• Users will always be provided with context
• Users will *always* be provided with context

- Allow permission requests to be made only from the foreground
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
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()`
• 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**

**APIs to move within the task stack!**

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

**transparency**
• 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
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

Start chatting today!

Allow this app to record audio?

[Deny] [Allow]
Would you grant this permission?
Would you grant this permission?

Susceptibility

No 26%
Yes 74%
Susceptibility

Would you grant this permission?

1 user mentioned request looking fishy
Who’s requesting this permission?
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 an app requests irrelevant permissions.
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!
Acarlar Mahallesi, Ephesus...
Defense and Countermeasures

Existing defenses 😅
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-trivial 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-trivial solution

Recommendations:
Defense and Countermeasures

Existing defenses 😅

- Background app starts on Android 10
- Attacks still work on Android 10 and 11
- Non-trivial 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-trivial solution

Recommendations:

- ✔️ Mandatory app transition effects
- ✔️ App name checks in:

Viber Messenger - Messages, Group Chats & Calls
Viber Media S.à r.l.

Communication #1 Top Grossing Editors' Choice

UNINSTALL OPEN

Contains ads • In-app purchases

What's new
Last updated Jun 2, 2019
Spring is always a good time for cleaning and refreshing!
So that's what we've done. We've cleared up some bugs and
made improvements to keep chatting on Viber as sparkling.

READ MORE

Rate this app
Tell others what you think

WRITE A REVIEW

Google Play

Android
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
  - Android
- 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-trivial solution

Recommendations:

- Mandatory app transition effects
- App name checks in:
  - Google Play
  - Android
- 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