"Do Androids Dream of Electric Sheep?"

On Privacy in the Android Supply Chain

Julien Gamba

PhD thesis defense — 15th of September, 2022

institute IMDEA networks

3 billion users

and counting!

The supply chain can be *very* large

The supply chain can be *very* large

truecaller
McAfee
skype
Baidu 百度
LinkedIn
ironSource

Customizations can impact users' privacy and security

PRIVACY INTERNATIONAL

WHERE WE WORK | WHAT WE DO | TOPICS

Home

"Betrayed by an app she had never h
How TrueCaller is endangering journ

The New York Times

Facebook Gave Device Makers Deep Access to Data on Users and Friends

The company formed data-sharing partnerships with Apple, Samsung and dozens of other device makers, raising new concerns about its privacy protections.

By GABRIEL J.X. DANCE, NICHOLAS CONFESSORE and MICHAEL LaFORGIA JUNE 3, 2018

TECHNICA

SUBSCRIBE

TRIADA —

Google confirms that advanced backd
came preinstalled on Android devices

After Google successfully beat back Triada in 2017, its developers found a

DAN GOODIN - 6/6/2019, 10:47 PM

THE WALL STREET JOU

U.S. Edition | June 10, 2019 | Print Edition | Video

TECH

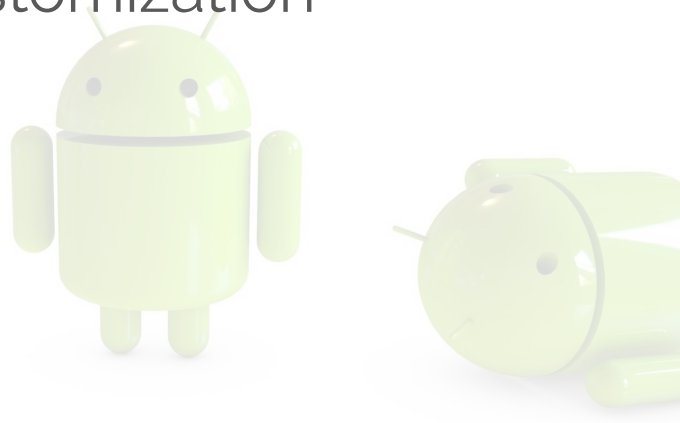
App Traps: How Cheap Smartphones Siphon User Data in Developing Countries

Tension between privacy and sharing of user data stokes a debate in West, but much less so in developing economies

Research questions

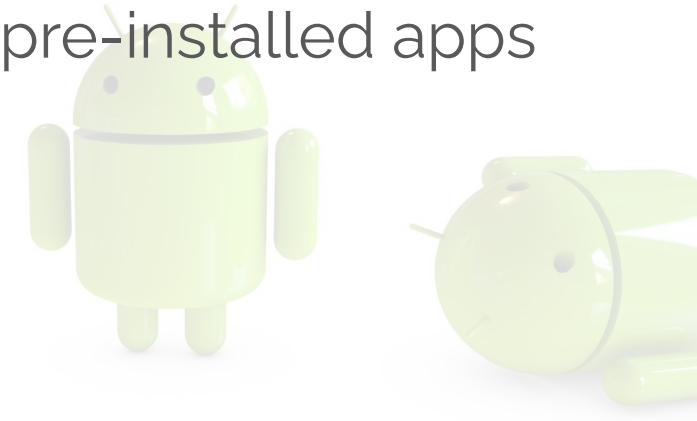
1. Exploring the Android system apps ecosystem

2. Measuring the consequences of customization on users' privacy and security



Contributions of this thesis

1. first large-scale study of pre-installed apps ecosystem
2. temporal evolution of Android's permission system
3. in-depth analysis of privacy risks of pre-installed apps




Data collection

Collecting pre-installed apps at scale

5:17

Firmware Scanner

The openness of the Android OS makes it possible for any handset manufacturer to ship a custom version of the system, along with proprietary pre-installed apps. These apps can be useful to users but can also be unwanted and cause harm to users' privacy. Some Android vendors have recently come under scrutiny by the media for collecting personal data from users and engaging in deceptive practices.

Unfortunately, this software is not available on Android app stores for study. This app will extract pre-installed software from your phone and send it to our server for further analysis. **No personal and sensitive data is collected**. Given the data size of pre-installed software, we will only upload the APKs over WiFi. If you wish, we will also report to you our findings about the privacy risks of your phone.

This app is part of an academic research project run by IMDEA Networks (Spain) and sponsored by Consumer Reports (USA), in partnership with University Carlos III of Madrid (Spain), and ICSI (USA).

If you have any questions of if you would like to know more about the project, you can contact us by email at iag.networks@imdea.org

☐ **I have read and understand the purpose of the project. I give consent to collect pre-installed software from my device.**

LET'S START!

Project sponsored by

institute imdea networks

CR Consumer Reports

5:17

Firmware Scanner

Progress:

Computing apps hashes... (1063 out of 3279 apps hashed)

If you have any questions of if you would like to know more about the project, you can contact us by email at iag.networks@imdea.org

PAUSE

Project sponsored by

institute imdea networks

CR Consumer Reports

Copyright: IMDEA Networks, 2018.

5:18

Scan complete

Thank you for you contribution! We have been able to

A few questions about this phone

Where did you buy this phone?

Why did you buy it?

Is it rooted? (if you do not know, click "No")

◯ Yes ◯ No

Anything more to add?

If you would like us to contact you about any concerning pre-installed app in your phone, you can enter your email below. We will not use your email for any other purpose.

CANCEL OK

com.android.bluetoothmidiservice
com.android.bookmarkprovider
com.android.calllogbackup
com.android.camera2

5:19

Scan complete

Thank you for you contribution! We have been able to scan your device and detect 3279 pre-installed binaries, including:

Applications	293
Certificates	200
Libraries	1199

If you would like to know more about the project, visit our website at http://androidobservatory.com/

If you would like us to contact you about any concerning pre-installed app in your phone, you can enter your email below. We will not use your email for any other purpose.

me@email.com SEND

We are currently analyzing your applications on our servers. You will be notified when the results are ready.

Here is the list of the applications pre-installed on your device:

android
com.android.apps.tag
com.android.backupconfirm
com.android.bips
com.android.bluetooth
com.android.bluetoothmidiservice
com.android.bookmarkprovider
com.android.calllogbackup
com.android.camera2

5:19

Scan complete

Certificate Installer
com.android.certinstaller

Signing certificate details

Issued to
Common name (CN): Android
/emailAddress=android@android.com
Organization (O): Android
Organizational unit (OU): Android

Issued by
Common name (CN): Android
/emailAddress=android@android.com
Organization (O): Android
Organizational unit (OU): Android

Validity period
Not Before: Sep 19 18:41:40 2011 GMT
Not After : Feb 4 18:41:40 2039 GMT

Serial number
a3:82:3f:b2:7f:62:89:b8

Requested permissions

Declared permissions

OK

com.android.carrierdefaultapp
com.android.cellbroadcastreceiver
com.android.certinstaller

Collecting pre-installed apps at scale

(12/09/2022)

32,576 package names

1,380,805 apps

127,881 users

35,774 devices

1,068 vendors


Supply chain analysis

How to identify app developers?

```
==========================================================================
Package name: com.google.uid.shared
SHA-2 (APK): 49572bd409287faf62e4049033283da580d849825180e43761619f53affaf6db
--------------------------------------------------------------------------
Certificate:
     Data:
          Version: 3 (0x2)
          Serial Number:
               c2:e0:87:46:64:4a:30:8d
     Signature Algorithm: md5WithRSAEncryption
          Issuer: C=US, ST=California, L=Mountain View, O=Google Inc.,
                  OU=Android, CN=Android
          Validity
               Not Before: Aug 21 23:13:34 2008 GMT
               Not After : Jan 7 23:13:34 2036 GMT
          Subject: C=US, ST=California, L=Mountain View, O=Google Inc.,
                   OU=Android, CN=Android
```

How to identify app developers?

```
==========================================================================
Package name: com.ppswipe.blurewards
SHA-2 (APK): 31623c4a5d08262018409851e00c71fb18422b4b9364eabeb344686d5fcb1b85
--------------------------------------------------------------------------
Certificate:
     Data:
          Version: 3 (0x2)
          Serial Number:
               6f:81:bf:fd:bd:a8:cb:08:d5:c2:3a:2f:05:8b:77:76:34:88:c9:88
     Signature Algorithm: sha256WithRSAEncryption
          Issuer: C=US, ST=California, L=Mountain View, O=Google Inc.,
                  OU=Android, CN=Android
          Validity
               Not Before: Sep 1 21:10:53 2017 GMT
               Not After : Sep 1 21:10:53 2047 GMT
          Subject: C=US, ST=California, L=Mountain View, O=Google Inc.,
                   OU=Android, CN=Android
```

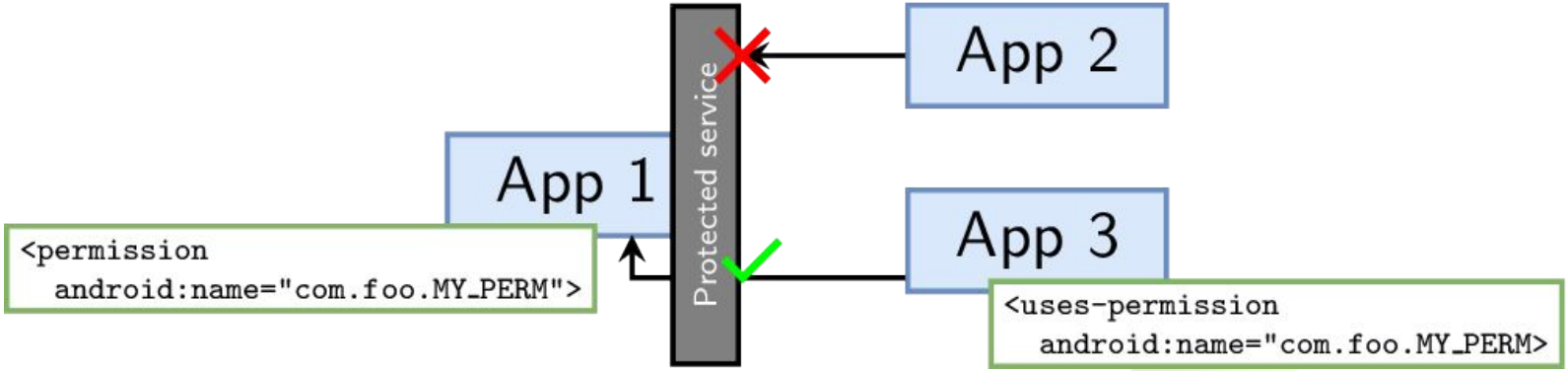
System apps developer ecosystem

Company name	Country	# of certificates	Certified partner?
Google	United States	92	—
Motorola	US/China	65	Yes
Asus	Taiwan	60	Yes
Samsung	South Korea	38	Yes
Huawei	China	29	Yes

System apps developer ecosystem

Company name	Country	# of certificates	# of vendors
MediaTek	China	19	17
Aeon	China	12	3
Tinno Mobile	China	11	6
Verizon Wireless	United States	10	5
Unknown company	—	7	1

Android custom permissions — an example



Custom permissions in system apps

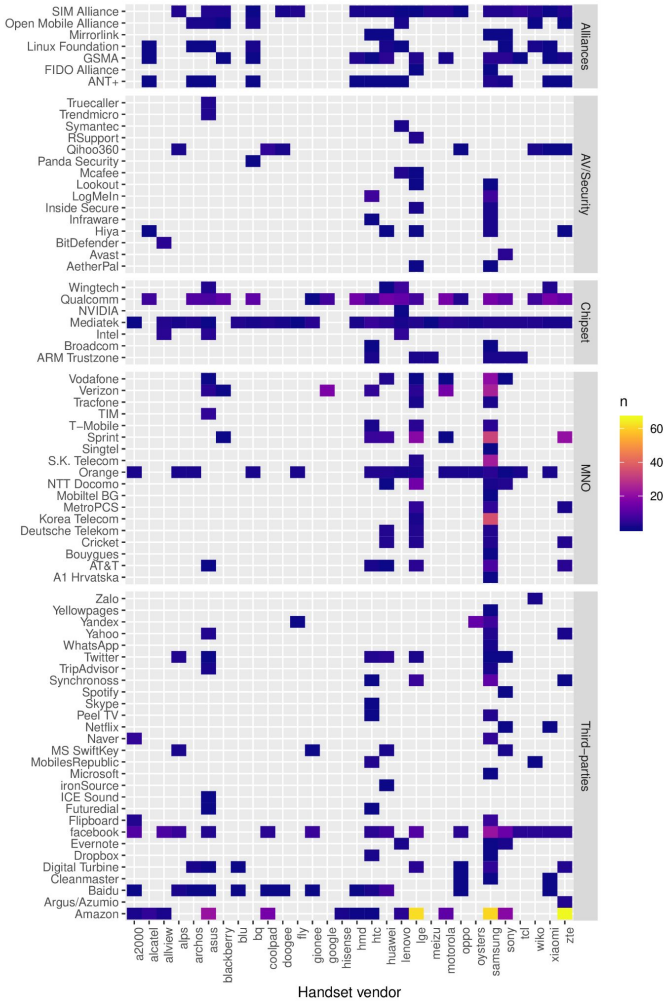
- ➔ `android.permission.BAIDU_LOCATION_SERVICE`
- ➔ `com.digitalturbine.ignite.ACCESS_LOG`
- ➔ …

All custom permissions	Providers							
	Vendor	3rd party	MNO	Chipset	Security	Alliance	Browser	Other
4,845 (108)	3,760 (37)	192 (34)	195 (15)	67 (63)	46 (13)	29(44)	7 (6)	549 (75)

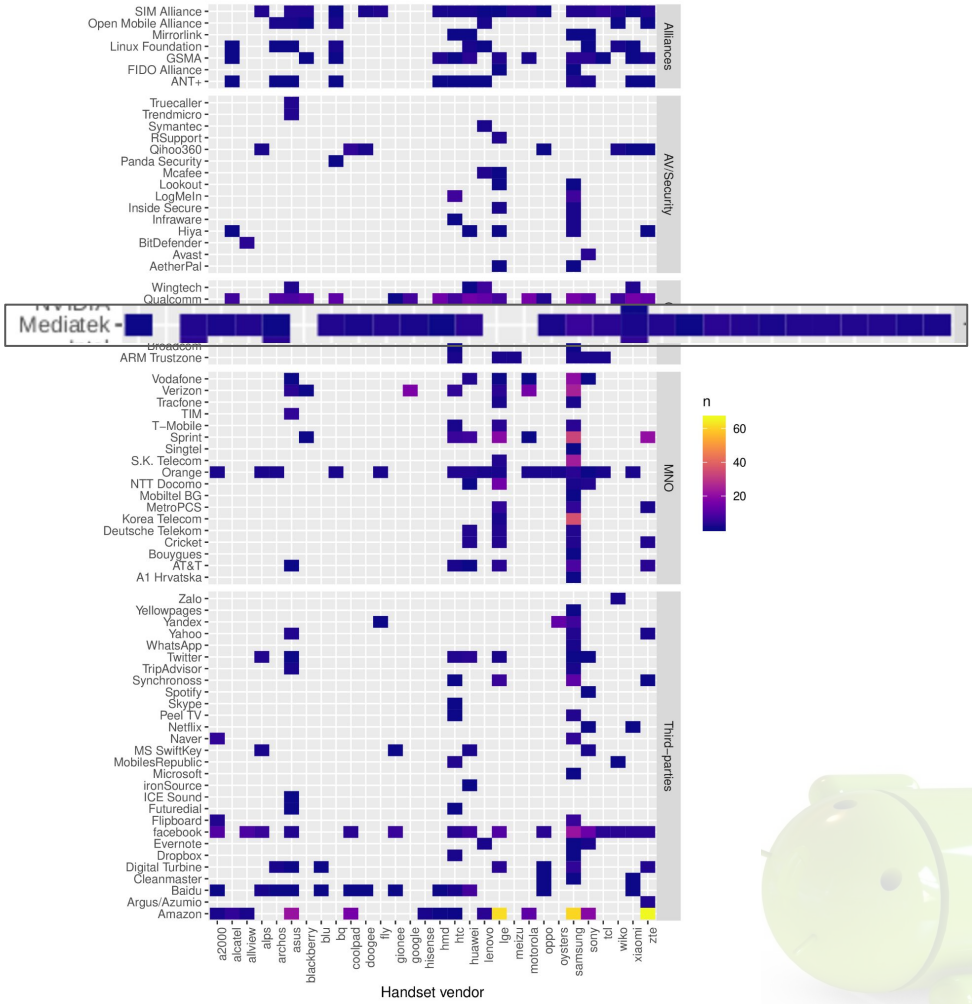
Custom permissions in core Android apps

	All custom permissions	Providers							
		Vendor	3rd party	MNO	Chipset	Security	Alliance	Browser	Other
`android`	494 (21)	410 (9)	—	12 (2)	4 (13)	—	6 (7)	—	62 (17)
`com.android.systemui`	90 (15)	67 (11)	1 (2)	—	—	—	—	—	22 (8)
`com.android.settings`	87 (16)	63 (12)	—	1 (1)	—	—	—	—	23 (8)
`com.android.phone`	84 (14)	56 (9)	—	5 (2)	3 (5)	—	—	—	20 (10)
`com.android.mms`	59 (11)	35 (10)	—	1 (2)	—	—	1 (1)	—	22 (8)
`com.android.contacts`	40 (7)	32 (3)	—	—	—	—	—	—	8 (5)
`com.android.email`	33 (10)	18 (4)	—	—	—	—	—	—	15 (17)

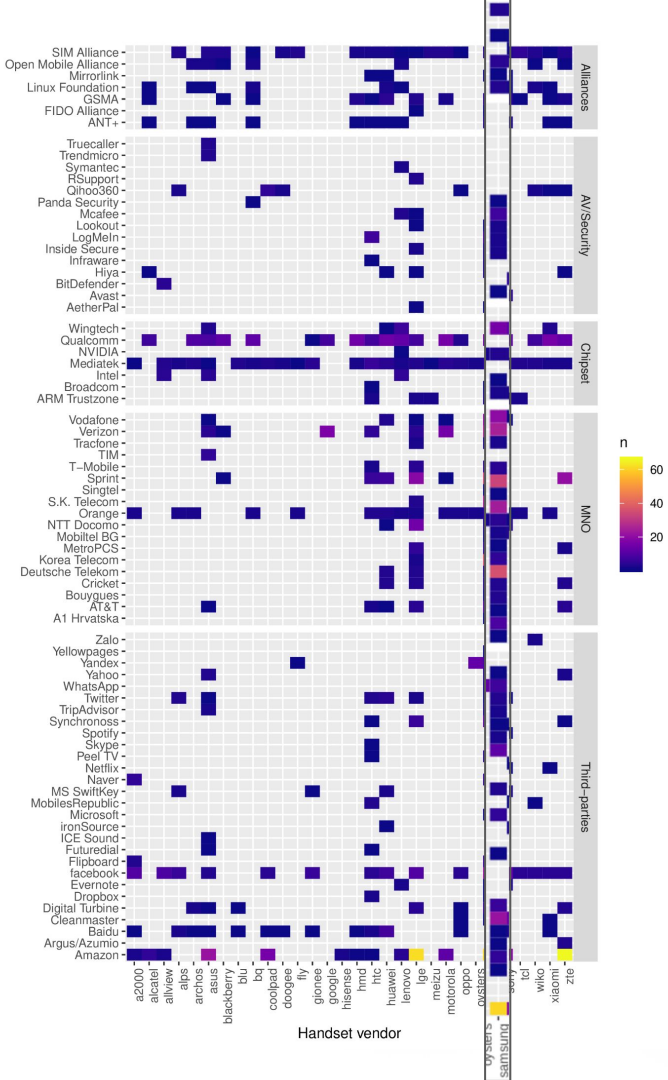
Revealing partnerships through custom permissions



Revealing partnerships through custom permissions



Revealing partnerships through custom permissions



Access to sensitive information

Accessed PII	Apps (#)	Apps (%)
IMEI	687	22%
IMSI	379	12%
MCC/MNC	552	18%
Operator name	315	10%
SIM state	383	12%
Installed apps	1,286	41%
Phone type	375	12%

Accessed PII	Apps (#)	Apps (%)
Logs	2,568	84%
Current network	1,373	44%
Data plan	699	22%
Contacts	164	11%
Phone calls	339	11%
Native code	775	25%
Shell commands	563	18%

Dangerous behaviors

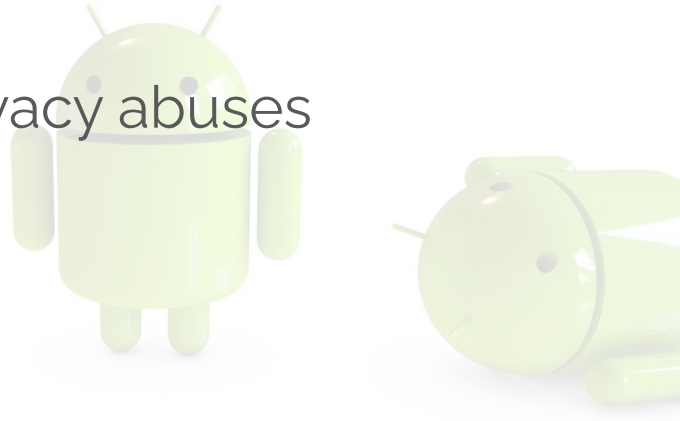
- Known malware
  - Triada
  - Rootnik
  - Gmobi
- But also
  - Rooting apps
  - Engineering mode apps
  - Blockers
  - …

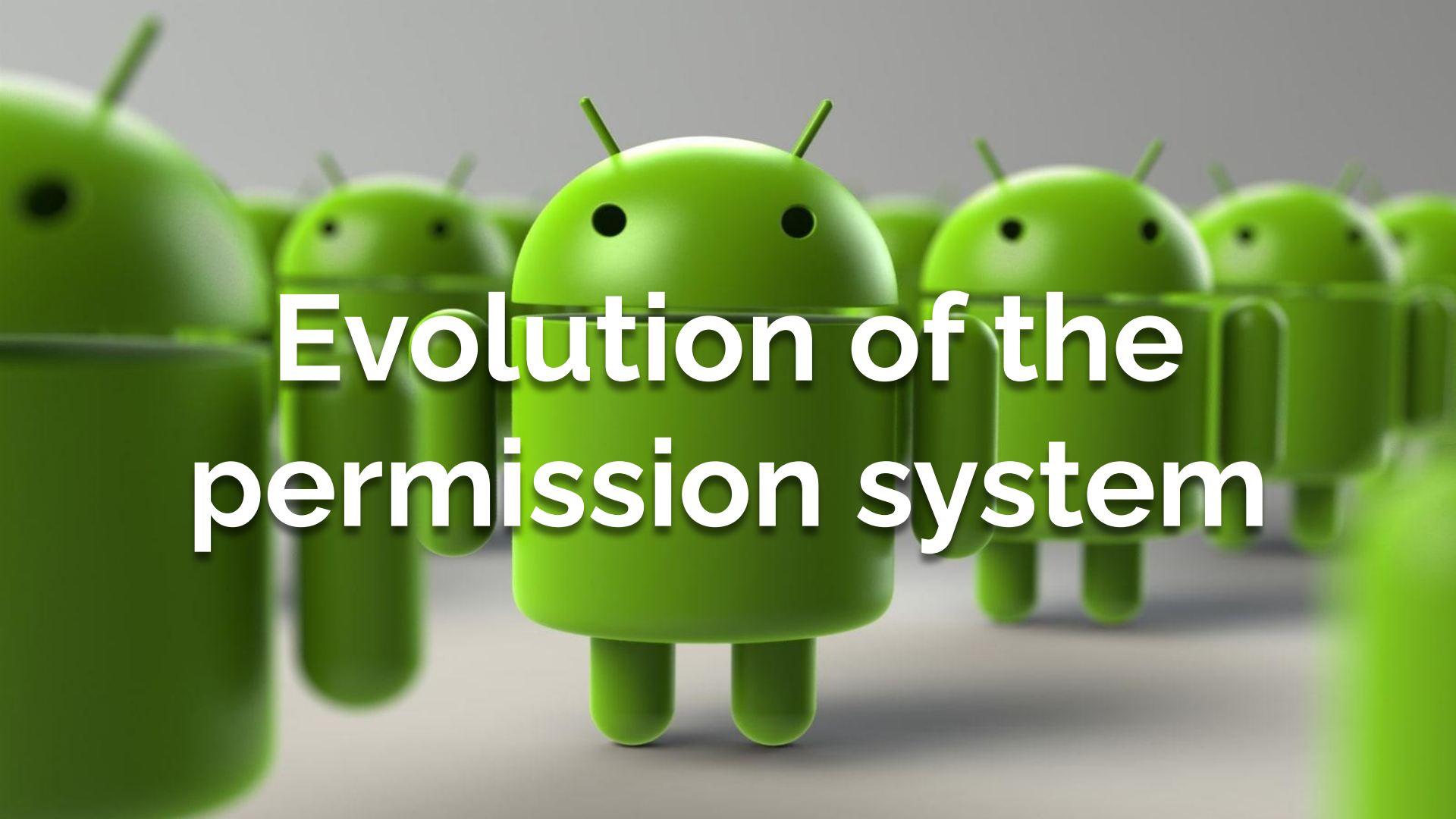
A case study: apps accessing system logs

- ➔ System logs can contain private information and are protected by the `READ_LOGS` permission
- ➔ Listed as "*Not for use by third-party applications*"
- ➔ We find system apps with capabilities to access those logs
- ➔ Some apps have capability to send full system logs to cloud services

Takeaways

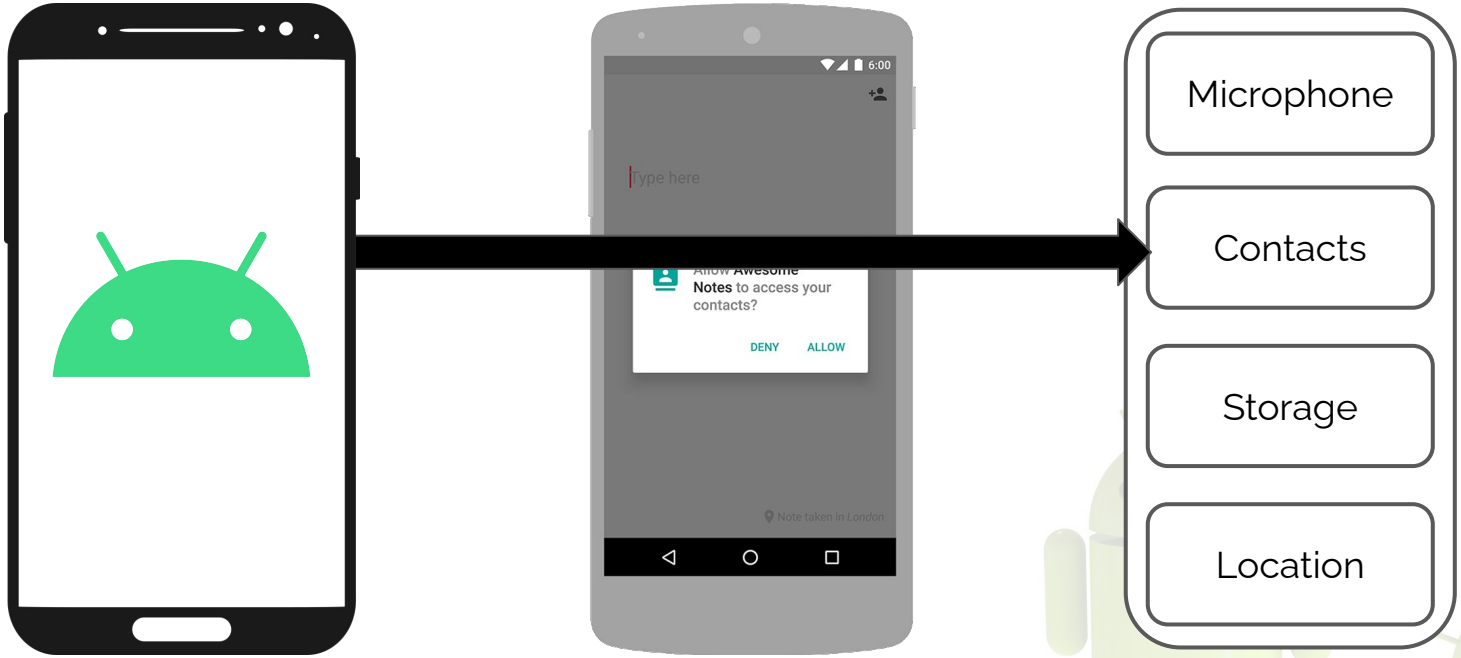
- ➔ There is a vast and unexplored ecosystem of pre-installed Android apps
- ➔ A large number of organizations have access to privileged partitions on users devices
- ➔ Anecdotal evidence of security and privacy abuses



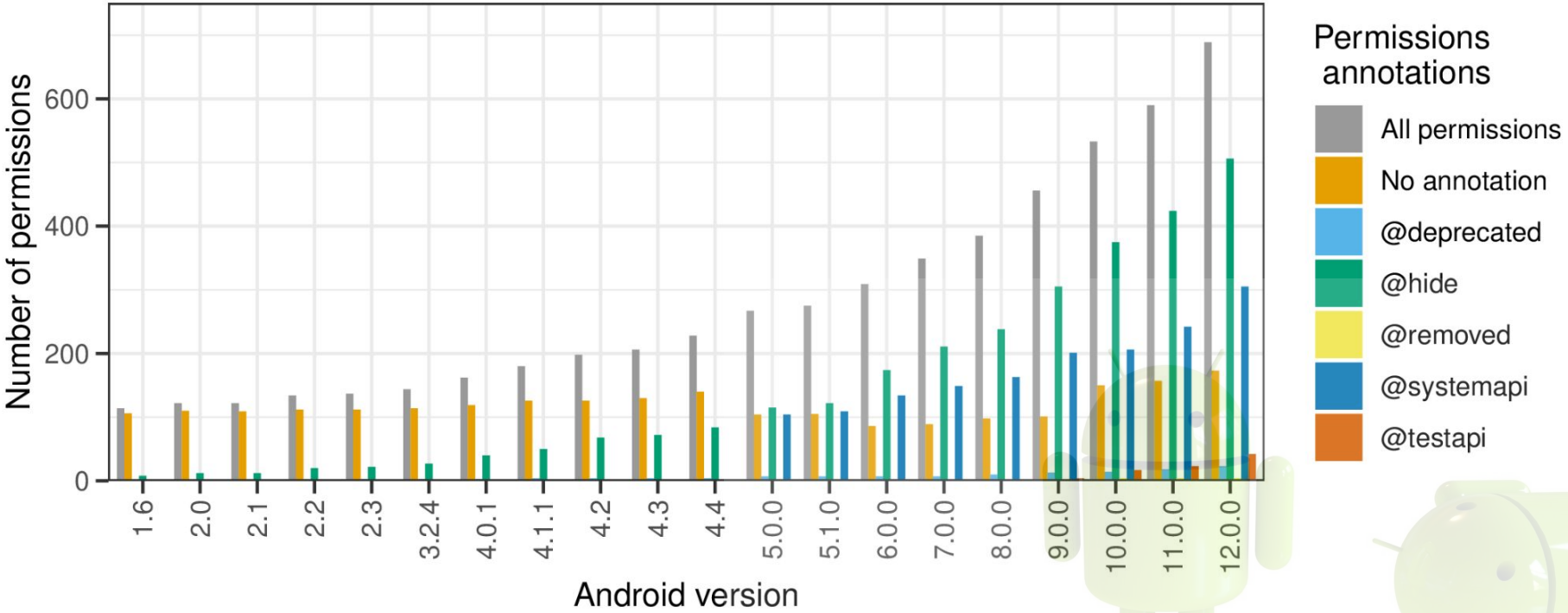


Evolution of the permission system

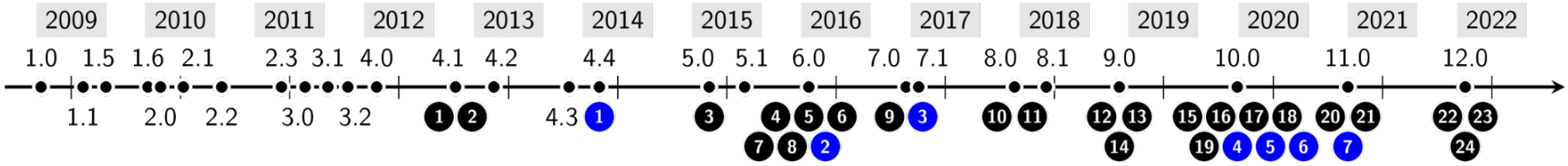
Android permission model



Temporal evolution of the permission system



Temporal evolution of the permission system



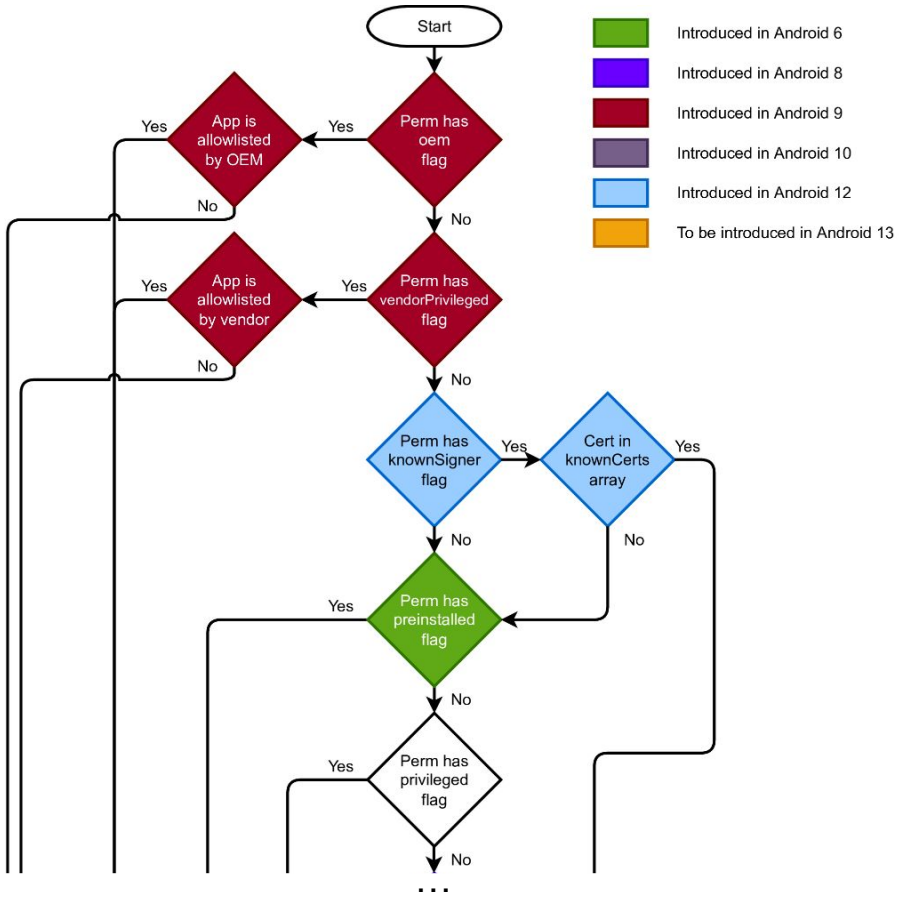
7. **`preinstalled`**: grant the permission to any system app that requests it

8. **`privileged`**: grant the permission to any privileged app that requests it

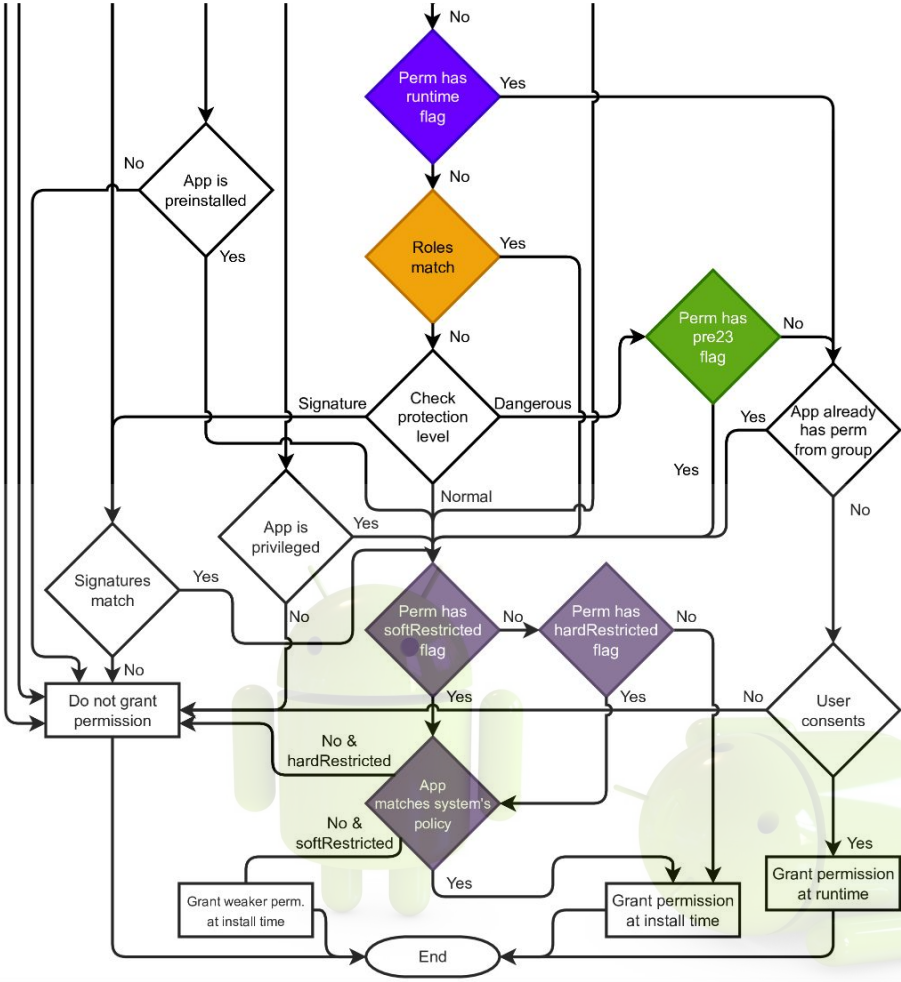
12. **`oem`**: pre-grant OEM permissions to OEM applications

13. **`vendorPrivileged`**: pre-grant vendor permissions to vendor applications

Temporal evolution of the permission system

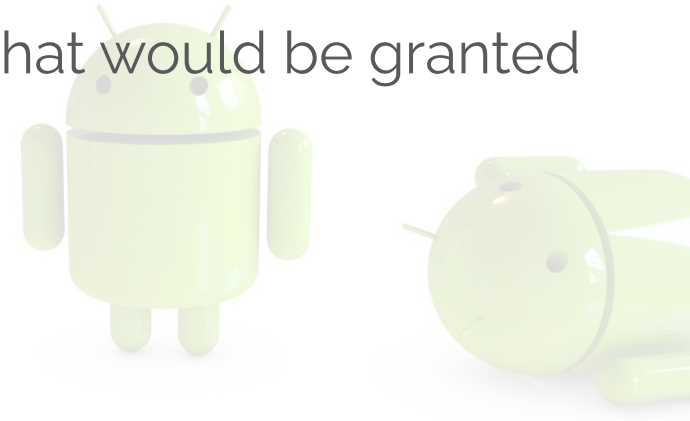


...



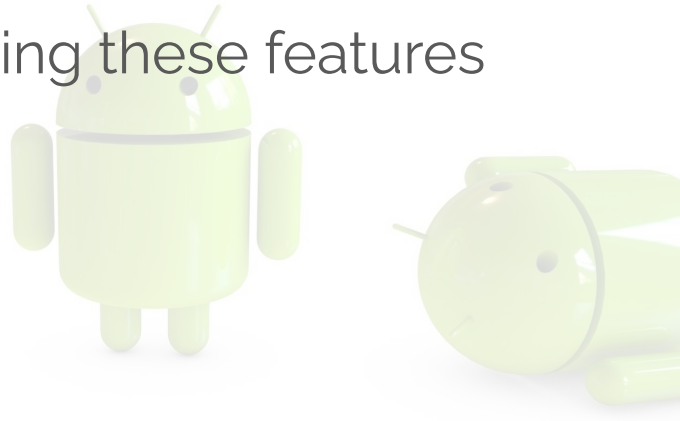
Flags usage in the wild

- ➔ Half of the flags are never used in our dataset
- ➔ 150K+ permissions defined by pre-installed apps with the `privileged` flag
- ➔ We find third-party pre-installed apps that would be granted these permissions



Takeaways

- ➔ The permission system is becoming significantly larger and more complex
- ➔ Some features could enable privacy and security abuses
- ➔ Evidence of third-party apps already using these features



Custom permission behavior analysis

Data sources

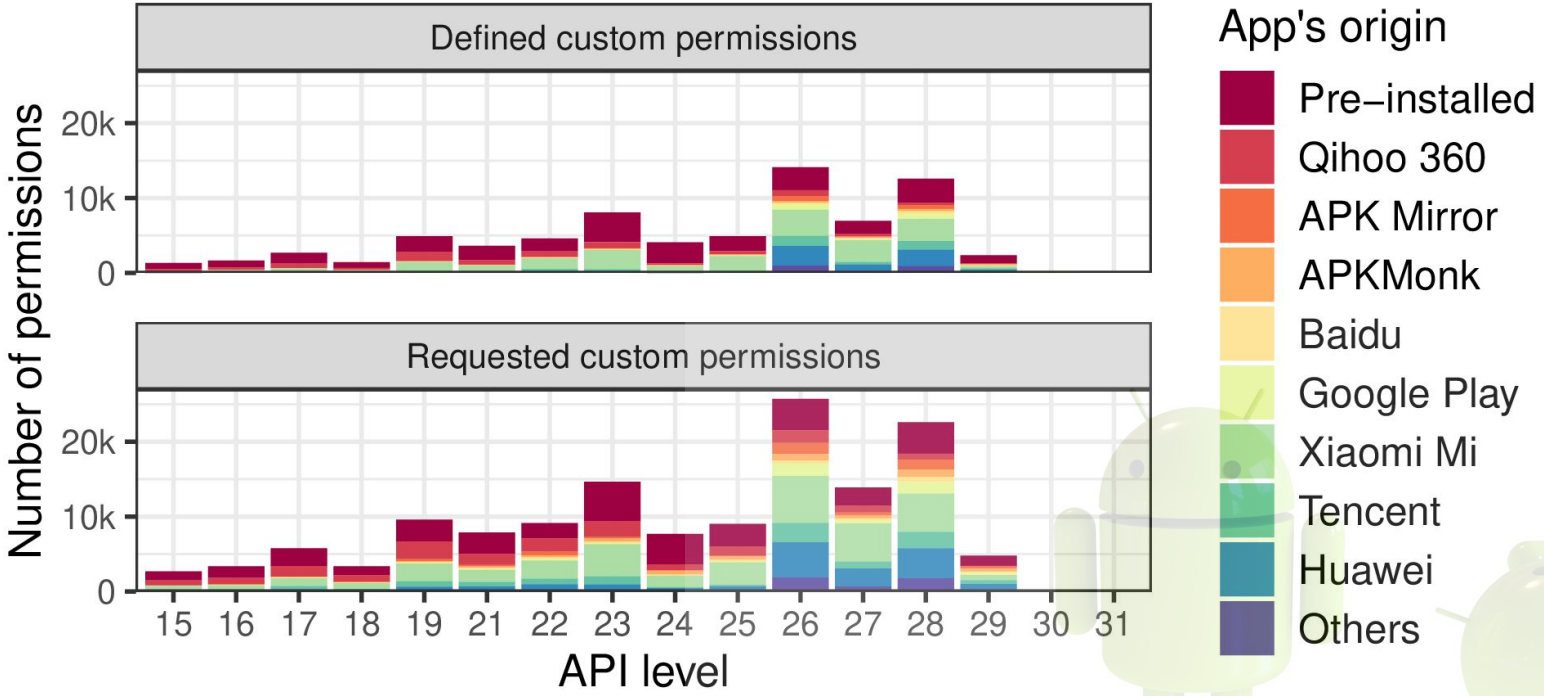
Androzoo apps

Pre-installed apps

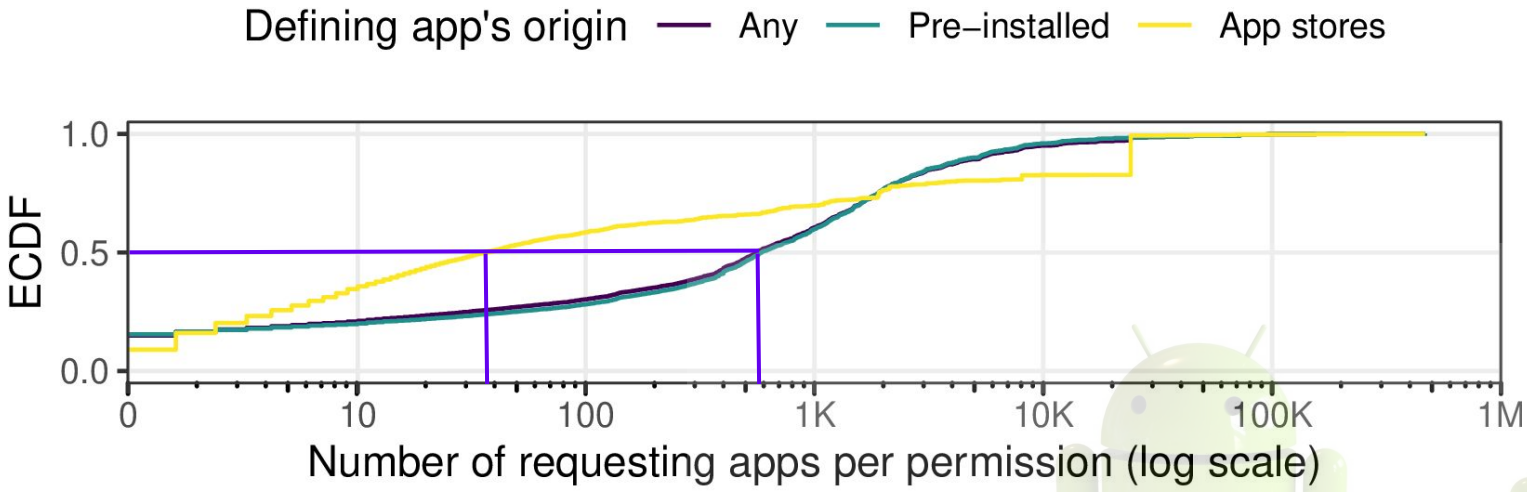
2,234,506 apps

52,468 custom perms

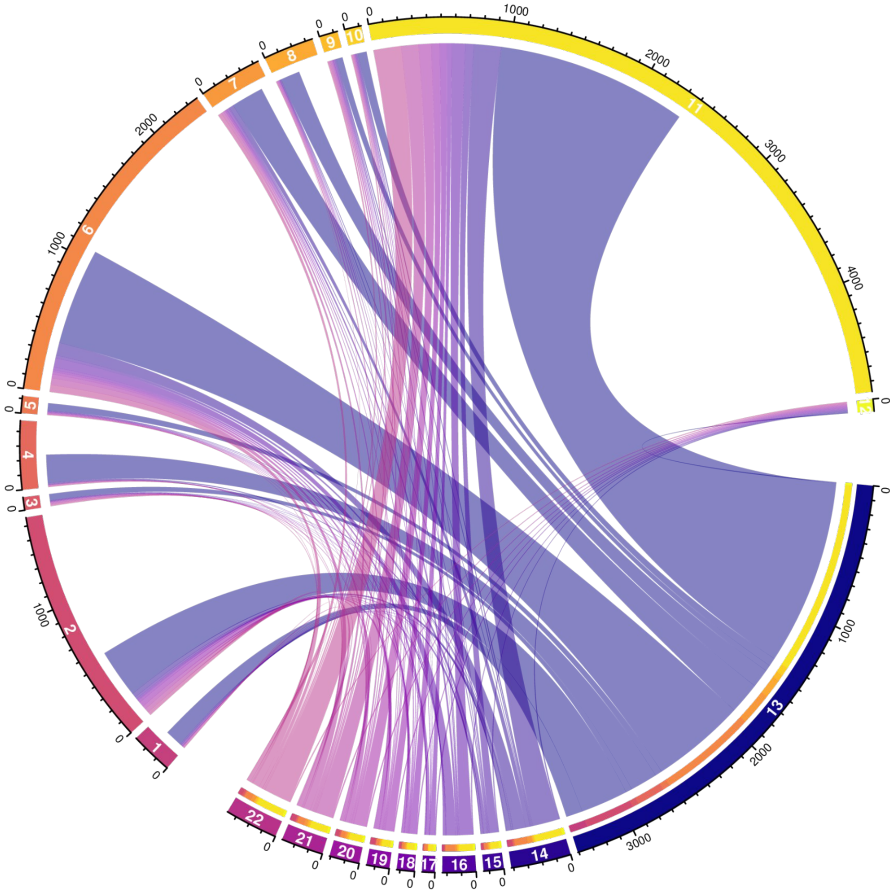
Prevalence of custom permissions



Prevalence of custom permissions



Prevalence of custom permissions



Origin of defining apps

- Asus
- Huawei
- Lenovo
- Motorola
- Oppo
- Samsung
- Sony
- Vivo
- Xiaomi
- ZTE
- Others
- GMS

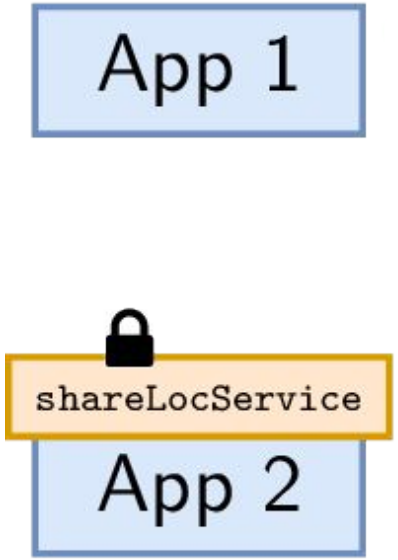
Origin of requesting apps

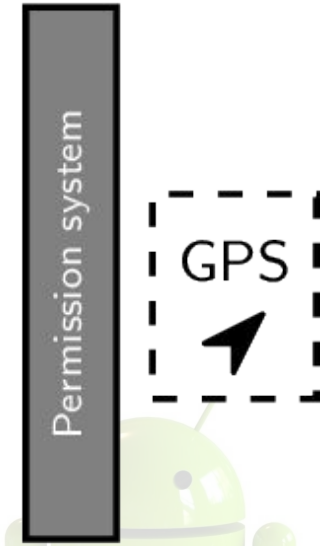
- Pre–installed
- Google Play
- Qihoo 360
- APK Mirror
- APKMonk
- Baidu
- Huawei store
- Xiaomi Mi
- Tencent
- Other stores

Attribution — naming and definition conventions

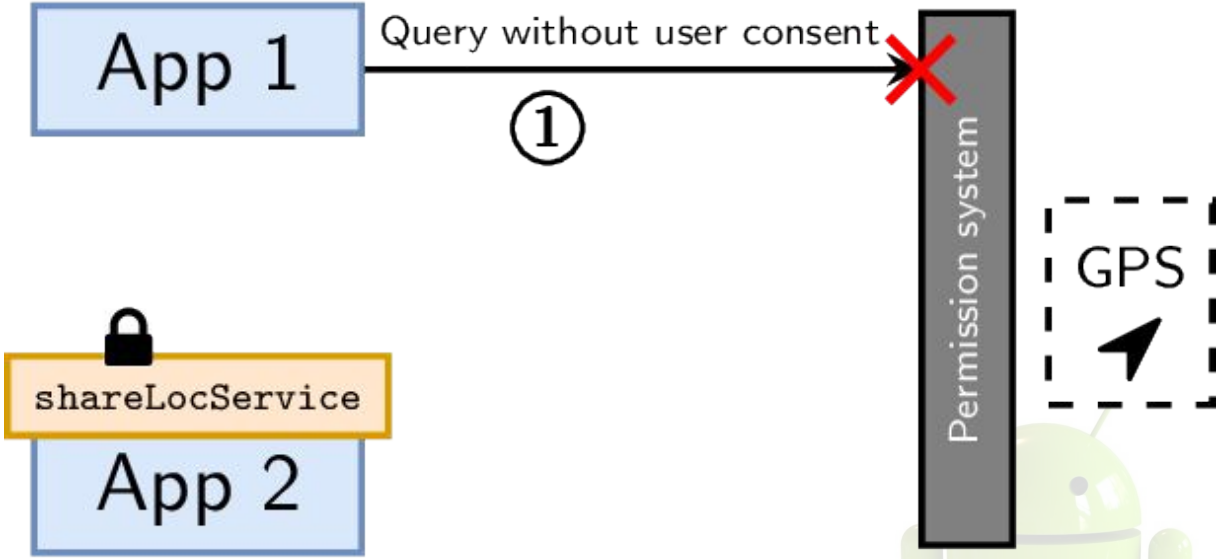
- com.samsung
- com.sec
- com.google
- com.huawei

Detecting leaky custom permissions

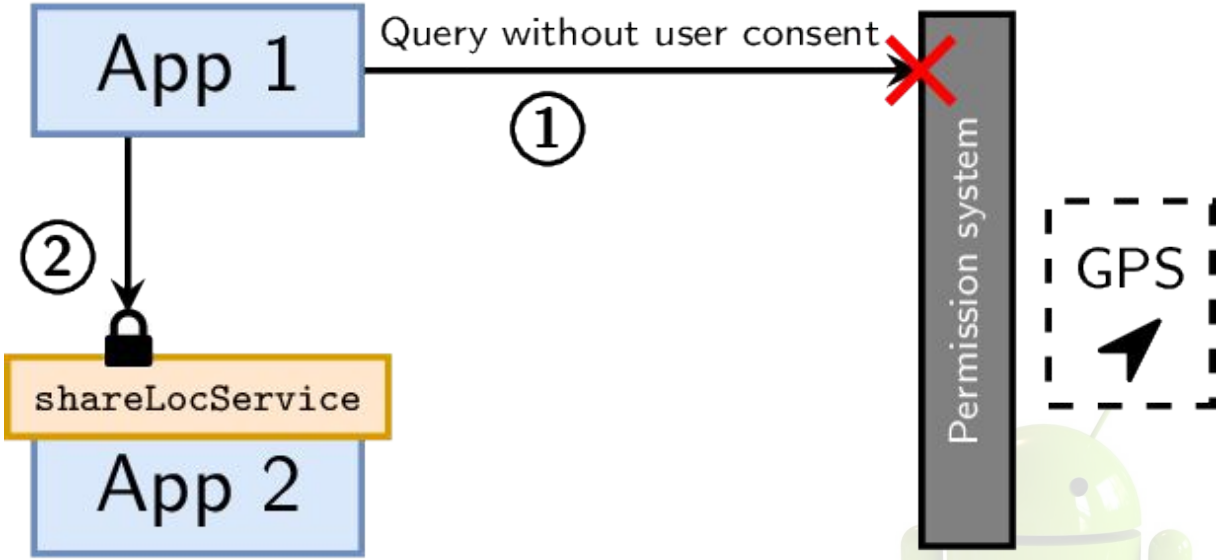




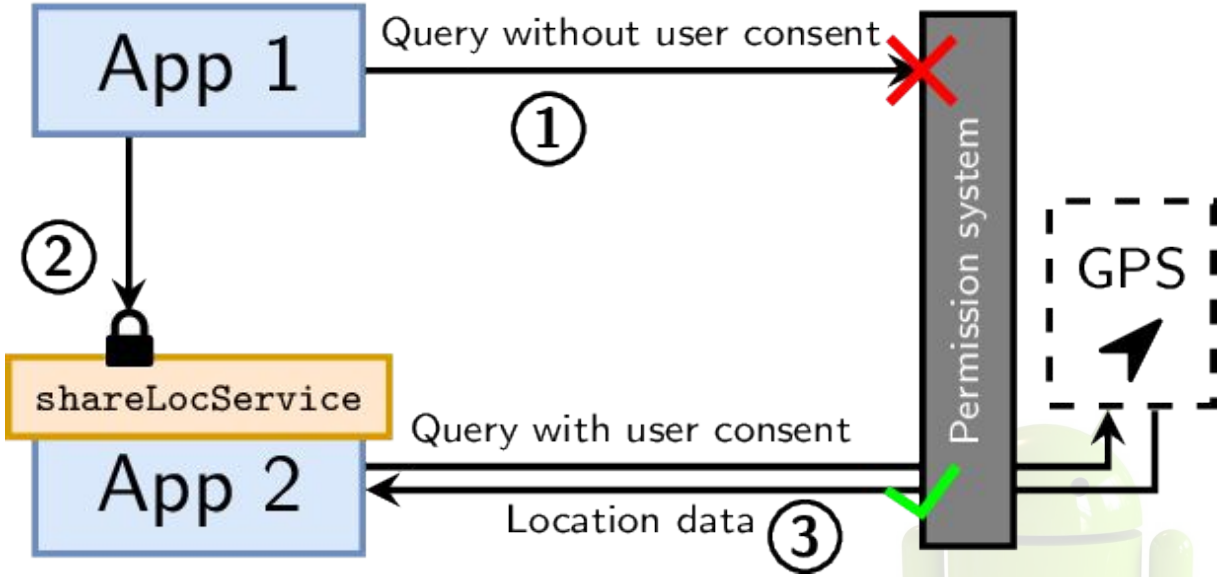
Detecting leaky custom permissions



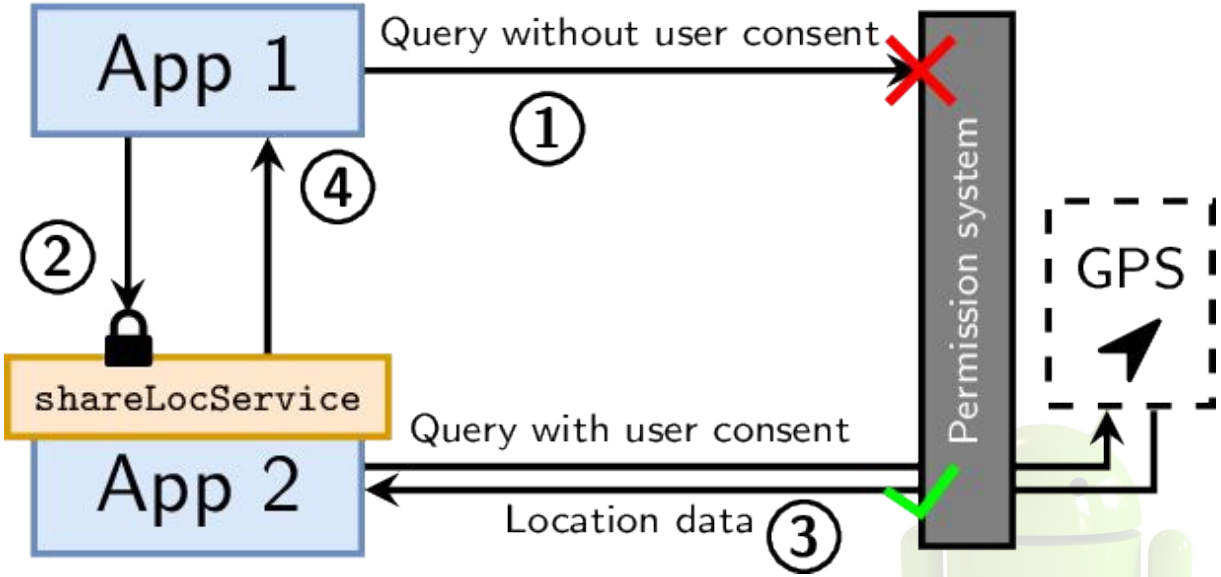
Detecting leaky custom permissions



Detecting leaky custom permissions

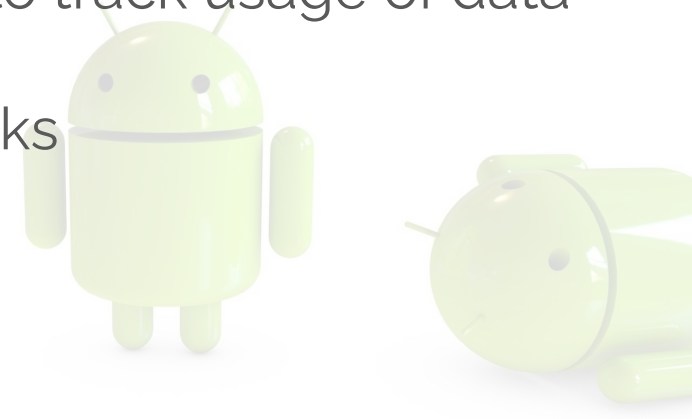


Detecting leaky custom permissions



Detecting leaky custom permissions

- We develop two tools:
  - `permissionTracer`: triage apps based on accessed data
  - `permissionTainter`: taint analysis to track usage of data
- We rely on lists of data sources and sinks



Detecting leaky custom permissions

- Ran tools on 96,748 unique apps exposing to 214,943 protected components
- 11% (24,648 components) access are least one protected API
  - 1,209 protected by `normal` permissions
- 5 potential PII leaks triggerable by simply sending intent

- 212,277 apps do not use their custom permissions

Takeaways

- ➔ Custom permissions are prevalent both in pre-installed and publicly available apps
- ➔ Despite this, users are kept in the dark and custom permissions remain completely opaque
- ➔ We create and publicly release new tools to audit apps using such permissions

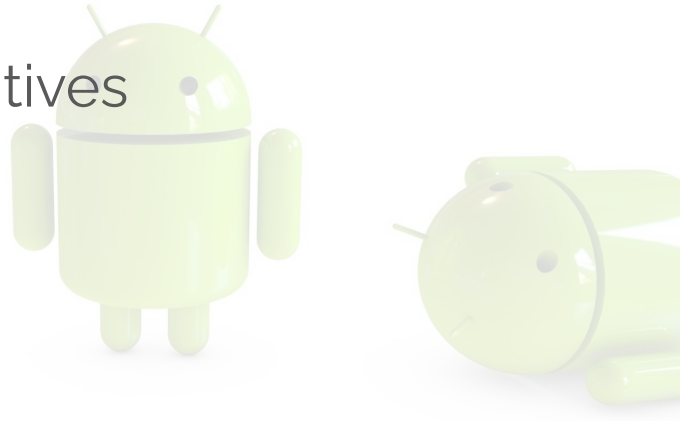
Discussion and recommendations

Attribution and accountability

- ➔ No reliable way to attribute pre-installed apps or custom permissions to developers
- ➔ App certificates could be signed by a global authority
- ➔ Certificates details could be listed on a central repository
- ➔ Developers should document custom permissions

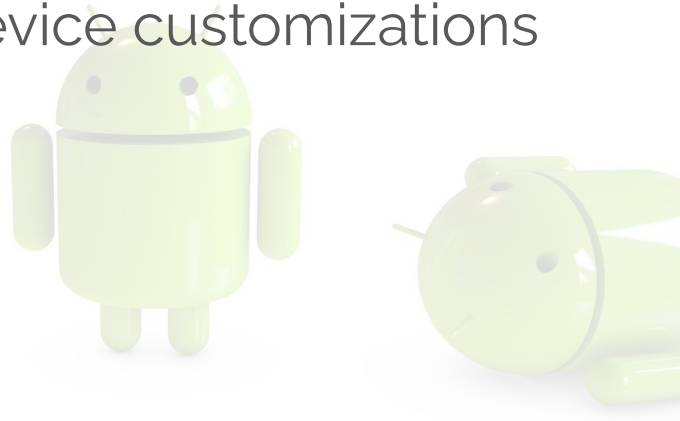
Privilege escalation due to custom permissions

- ➔ Difficult to prevent, if possible at all
- ➔ Two steps approach to spot true positives
  - ◆ Static triage to find potential cases
  - ◆ Taint analysis to weed out false positives



Transparency and user control

- ➔ Users are kept in the dark
- ➔ Virtually no user consent to data collection
- ➔ Details about pre-installed apps and device customizations should be publicly available



Impact of our studies

ifex

What We Do | Our Network | Resources | Articles | Contact

Articles ▸ Android pre-installed apps must follow normal privacy-respecting Play Store rules

International | Digital Rights

Android pre-installed apps must follow normal privacy-respecting Play Store rules

PRIVACY INTERNATIONAL

People shouldn't have to privacy and security for smartphone.

Also available in: Es

Do you think someone who buys a cheap smartp someone who can afford the latest iPhone? No? to ensure every Android phone protects their use

Dear Google,

People shouldn't have to trade their privacy and secu changes we believe are needed most urgently are as

- Individuals should be able to permanently uninstall pre-installed apps on their phones. This should include any related background services that continue to run even if the apps are disabled.

aepd agencia española protección datos

BUSCAR | MENU

Prensa y comunicación > Últimas noticias

> Análisis del software preinstalado en dispositivos Android y riesgos para la privacidad de los usuarios

14 DE MAYO DE 2019

Análisis del software preinstalado en dispositivos Android y riesgos para la privacidad de los usuarios

Maddie Stone
@maddiestone
Follow

✨Come join me THURSDAY at 14:30 at @BlackHatEvents! 1st I'll discuss the differences in reversing Android pre-installed apps vs user apps. Then I'll share 4 case studies of security issues we discovered in OEM devices. 3 of which have never been discussed publicly. #BHUSA ✨

Securing the System: A Deep Dive into Reversing Android Pre-Installed Apps

Łukasz
@maldr0id
Follow

My talk about the #Android supply chain got accepted to @RSAConference 2020 in San Francisco! See you there!

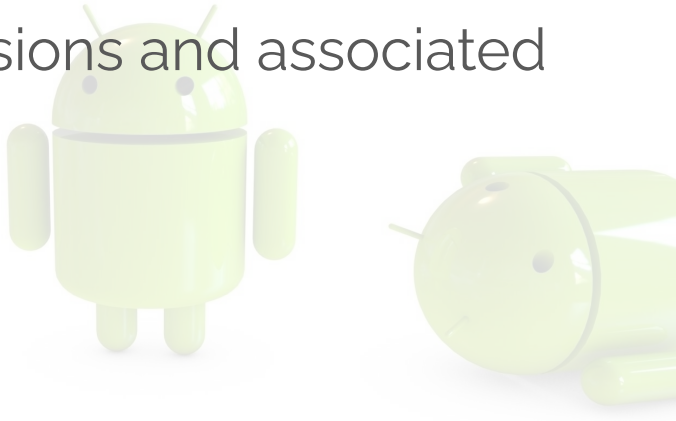
7:25 AM - 20 Nov 2019

1 Retweet 33 Likes

2 1 33

In conclusion

- ➔ First large-scale study of pre-installed apps ecosystem
- ➔ Show large amount of stakeholders and their relationships
- ➔ Demonstrate increasing complexity of permission system
- ➔ Highlight prevalence of custom permissions and associated privacy and security risks for end-users



Open issues and future work

- ➔ Android framework customization
- ➔ Privacy and security risks due to native libraries
- ➔ Dynamic analysis at scale of pre-installed apps

"Do Androids Dream of Electric Sheep?"

On Privacy in the Android Supply Chain

Thank you for your attention!

institute IMDEA networks