

EXADPrinter: Exhaustive Permission-less Device Fingerprinting in the Android Ecosystem*

Sihem Bouhenniche, Pierre Laperdrix, Walter Rudametkin

**Under submission at IEEE S&P 2026*

Pass the SALT - 2025

Android

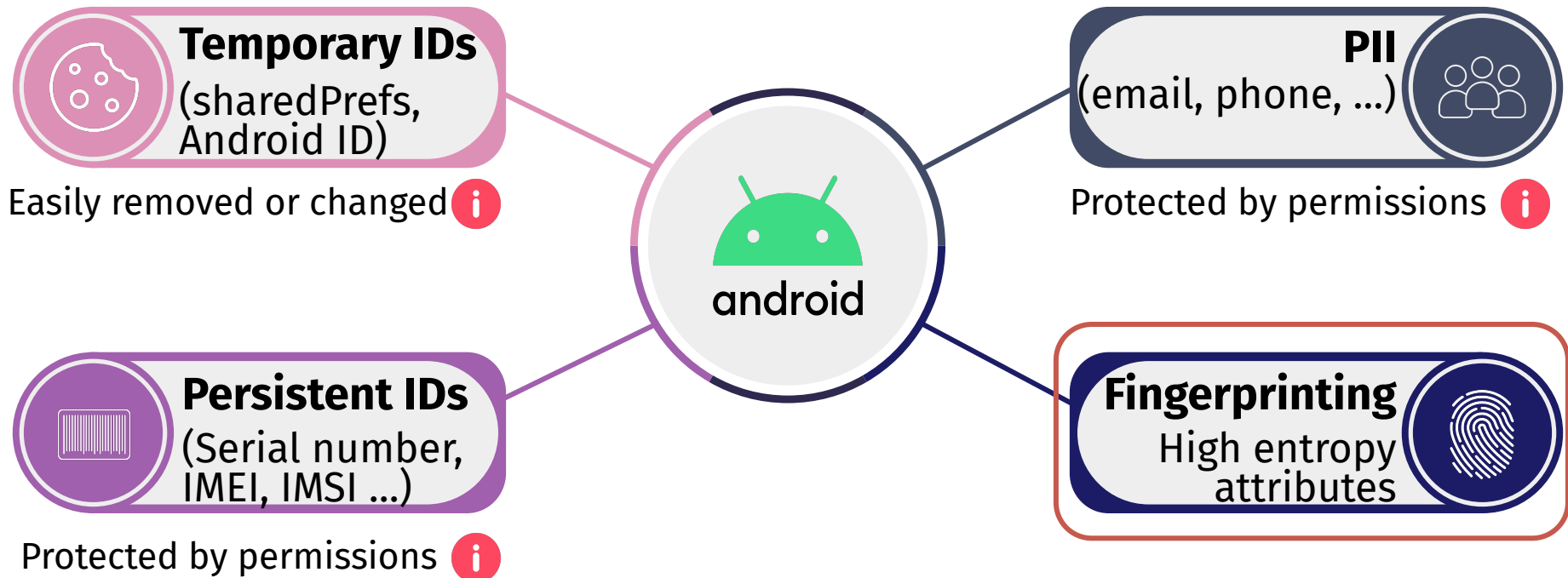


~4.69 billion People
Own a smartphone

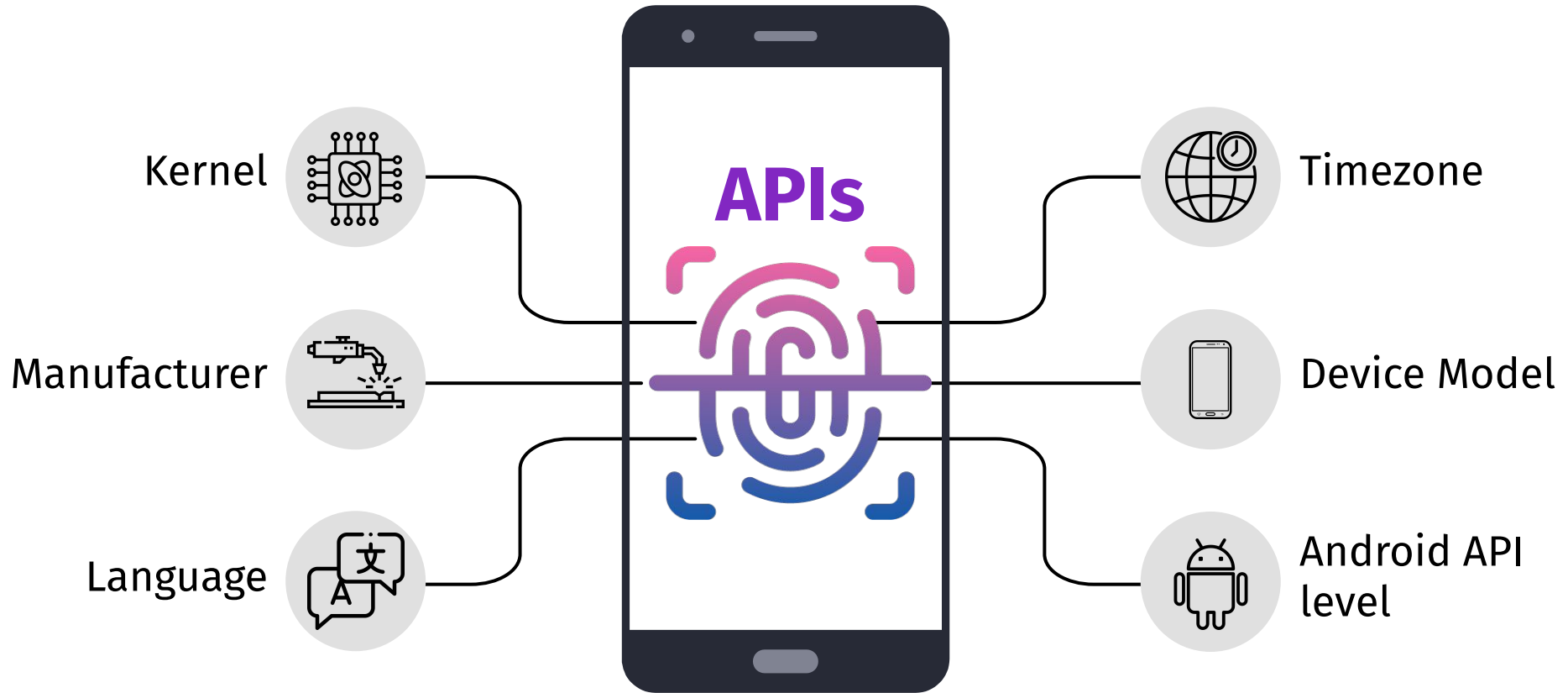
70% Mobile Market
Powered by Android OS

~1.54 Million Apps
Hosted in Google Play

Tracking in Android



Device Fingerprinting



Related Work

Efficient Fingerprinting-Based Android Device Identification With Zero-Permission Identifiers

WENJIA WU, JIANAN WU, YANHAO WANG, ZHEN LING, AND MING YANG

School of Computer Science and Engineering, Southeast University, Nanjing 211189, China

Corresponding author: W. Wu (wjwu@seu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61402104, Grant 61572000, Grant 61502100, Grant 61532013, Grant 61632008, and Grant 61320106007, in part by the Jiangsu Provincial Natural Science Foundation of China under Grant BK20140648 and Grant BK20150637, in part by the Jiangsu Provincial Key Technology Research and Development Program under Grant BE2014603, in part by the Jiangsu Provincial Key Laboratory of Network and Information Security, Grant BM2003201, and in part by the Key Laboratory of Computer Network and Information Integration of Ministry of Education of China under Grant 93K-9.

ABSTRACT Mobile device identification techniques can be applied to secure authentication. In particular, the importance for the security of mobile networks, such as avoiding spoofing attack devices, explicit identifiers, e.g., Android ID, are used to uniquely identify a device. However,

- **Manual** methodology
- **Identifier-based**
- Outdated due to Android ecosystem evolution (2016)

AndroPRINT: Analysing the Fingerprintability of the Android API

Gerald Palfinger

Secure Information Technology Center - Austria (A-SIT)

Graz, Austria

gerald.palfinger@iaik.tugraz.at

Bernd Prünster

Institute of Applied Information Processing and Communications (IAIK), Graz University of Technology

Graz, Austria

bernd.pruenster@iaik.tugraz.at

ABSTRACT

In recent Android versions, access to various (unique) identifiers has been restricted or completely removed for third-party applications. However, many information sources can still be combined to create a fingerprint, effectively substituting the need for these unique identifiers.

1 INTRODUCTION

Many mobile applications rely on personalised advertisement as a main stream of income [6]. To tailor these advertisements, they have to be recognised across applications. Many applications use fingerprinting to reidentify users [16]. However, with Android

- **Automatic** methodology
- Only **two manufacturers** and **single Android version**, limited generalizability, (2020)

Research questions

How to perform device fingerprinting **automatically** and **exhaustively** ?

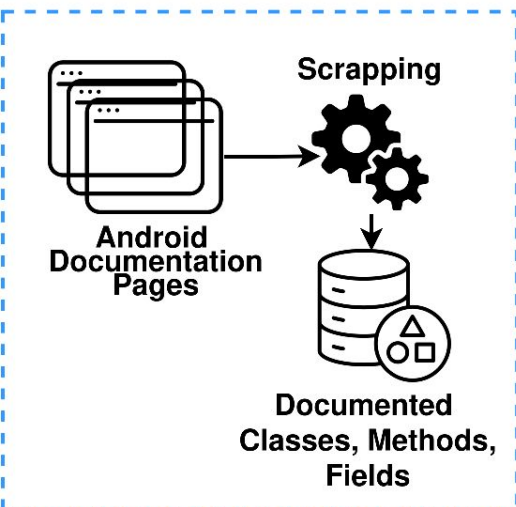
How does Android **diversity** impact the device fingerprints (uniqueness, stability) ?

What **sensitive** information is leaked **without permissions** on Android devices ?



Overview of EXADPrinter

Domain Exploration



Attribute Extraction

Shell attributes

```
String c = "uname -a";  
Process p = Runtime.getRuntime().exec(c);
```

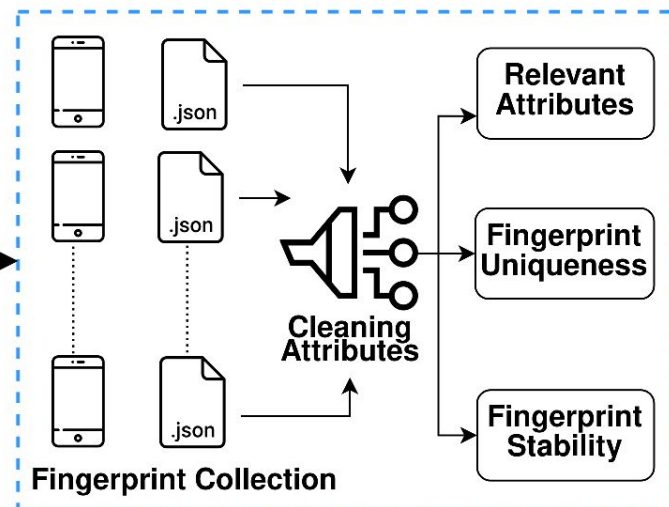
SDK attributes

```
Class<?> cls = Class.forName("android.os.Build");  
Field[] fields = cls.getFields();  
Method[] methods = cls.getMethods();  
// Get Fields values and Invoke methods ...
```

Content Providers attributes

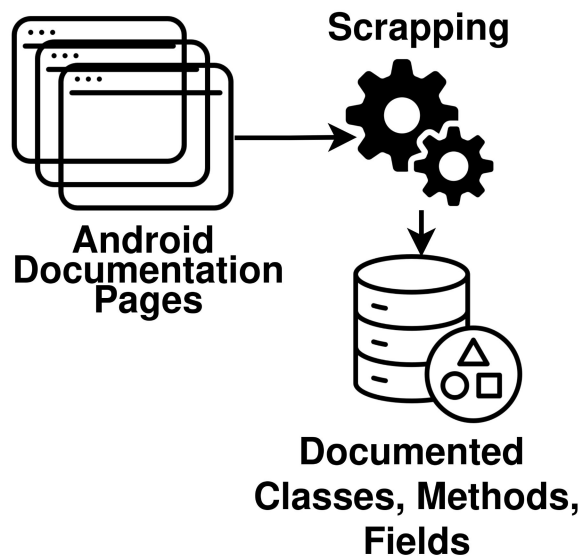
```
Uri<?> uri = Uri.parse("content://settings/global");  
ContentResolver cp = context.getContentResolver();  
Cursor cu = cp.query(uri, null, null, null, null);  
// Loop over the cursor ...
```

Device Identification



Approach

Scraping the API



- **6,022** documented classes*
- **65,259** documented fields
- **212,599** documented methods
- Idea : Java Reflection
 - Access **hidden** and **custom** APIs defined by vendors

```
// Samsung:  
android.widget.DigitalClock.SEM_DICTIONARY_ID  
android.os.UserManager.semHasBaseUserRestriction
```

*Scraping done in September 2024

Approach

Extracting attributes

Shell attributes

```
String c = "uname -a";  
Process p = Runtime.getRuntime().exec(c);
```

SDK attributes

```
Class<?> cls = Class.forName("android.os.Build");  
Field[] fields = cls.getFields();  
Method[] methods = cls.getMethods();  
// Get Fields values and Invoke methods ...
```

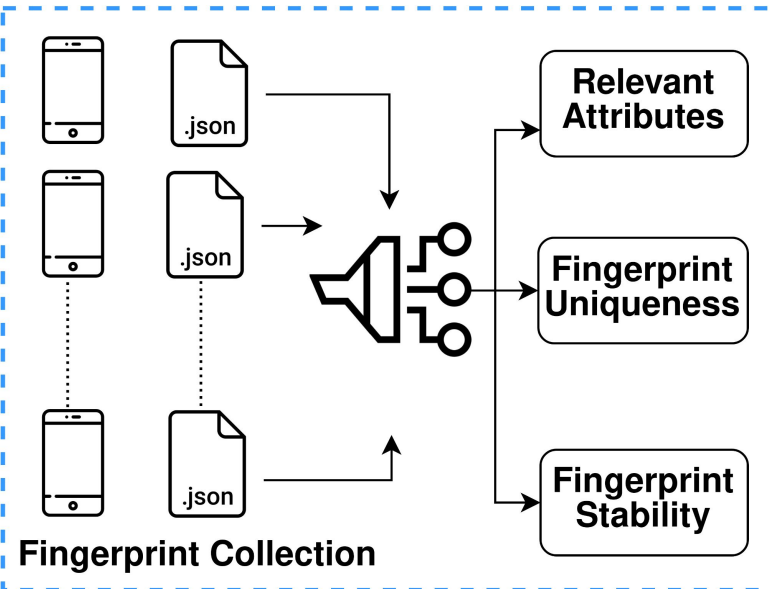
Content Providers attributes

```
Uri<?> uri = Uri.parse("content://settings/global");  
ContentResolver cp = context.getContentResolver();  
Cursor cu = cp.query(uri, null, null, null, null);  
// Loop over the cursor ...
```

- **6,022** Java classes to kickstart the Java Reflection process
- **43** Shell commands from **toybox**
- **3** content providers:
Settings.Global, **Settings.System**
and **Settings.Secure**

Approach

Attribute importance



- **Number of unique values of attribute A**

$$U(A) = |\{v \in V_A, |\{f \in F, A(f) = v\}| = 1\}|$$

- **Attribute Relevance by Shannon Entropy**

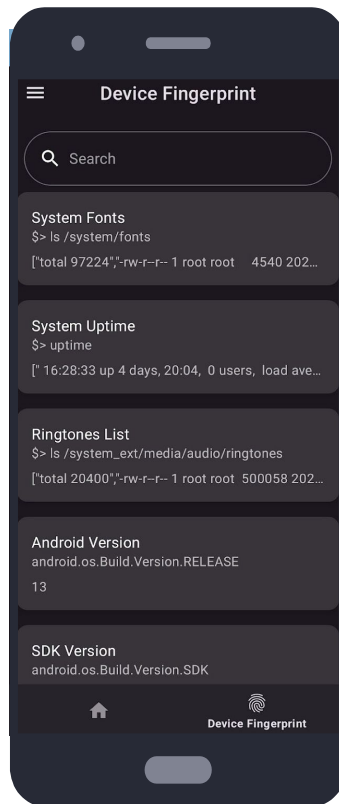
$$H(A) = - \sum_{i=1}^n P(a_i) \log_2 P(a_i)$$

- **Normalized Entropy**

$$H_{norm} = \frac{H(A)}{\log_2(n)}$$

Collecting our dataset

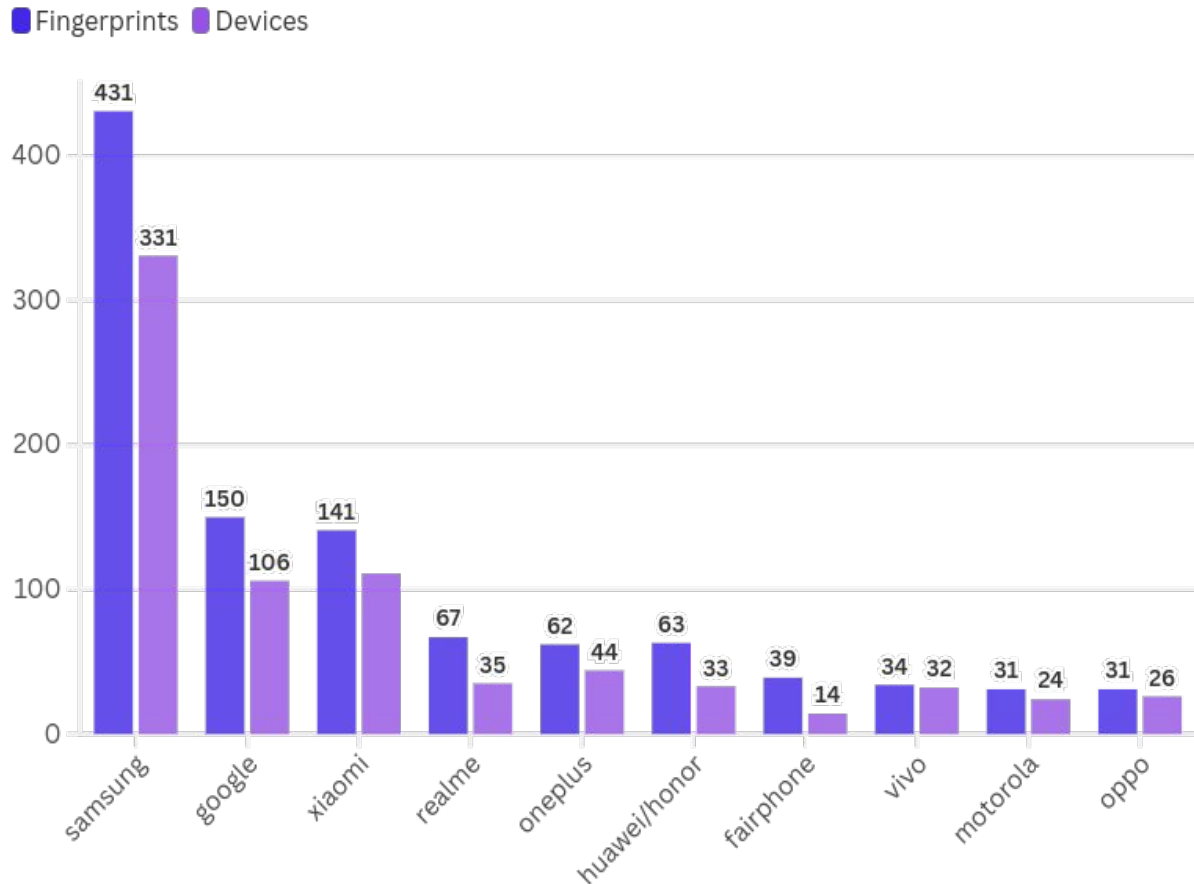
- Android application
- Real world devices
- (Almost) permission-less
- In Google's Play Store since October 2024
 - Please Install me 😊



Scan QR code
and install
AmlUnique

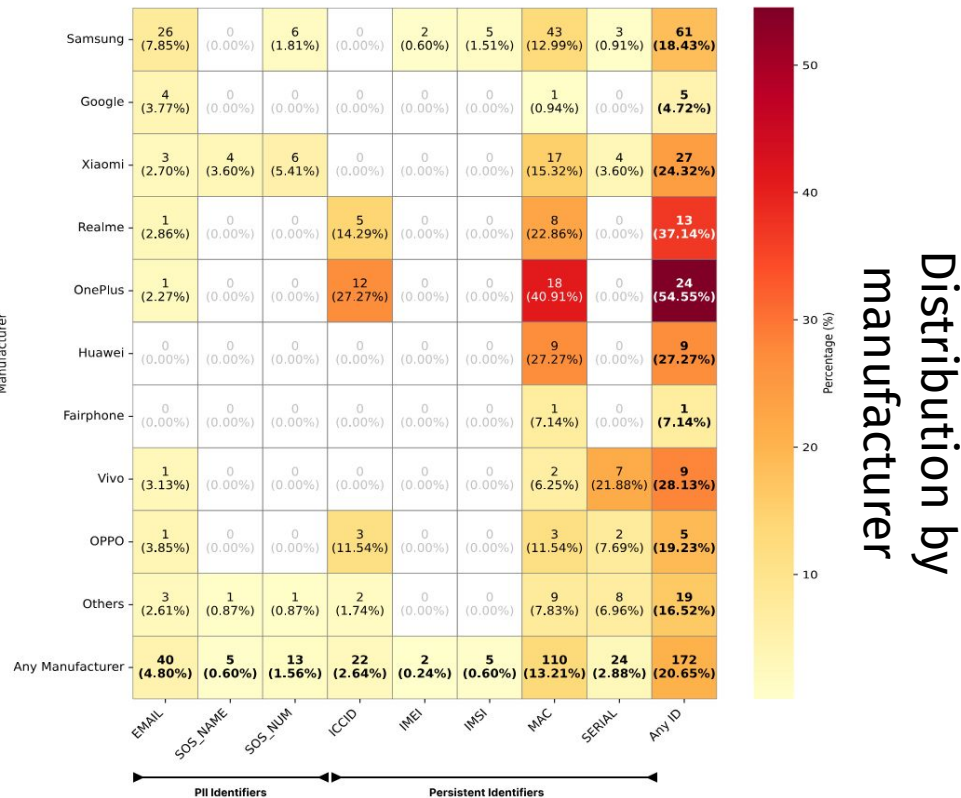
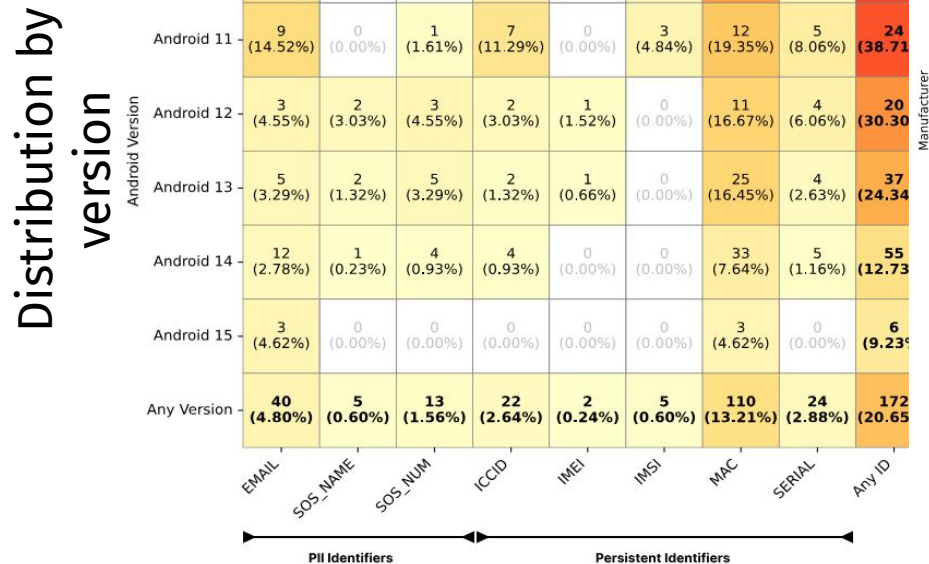
Dataset: 6 months

- **1151** fingerprints from **833** devices
- **7** versions of Android
 - versions 9 to 15
- **41** manufacturers
- **Large** fingerprints containing ~ **200.000** attributes



Results

Detected Unique Identifiers



***20,65% of devices identified by at least one unique identifier**

Detected Identifiers

Examples of unique identifiers

AOSP

MAC @

Vendor Customizations

Emergency contact

Email

*Settings.Global.bluetooth_headset_priority
_[MAC address]*



* 38 Affected devices

Settings.Secure.key_miui_sos_emergency_contacts



* 6 Affected devices

Settings.System.samsungaccount

SAMSUNG

* 8 Affected devices

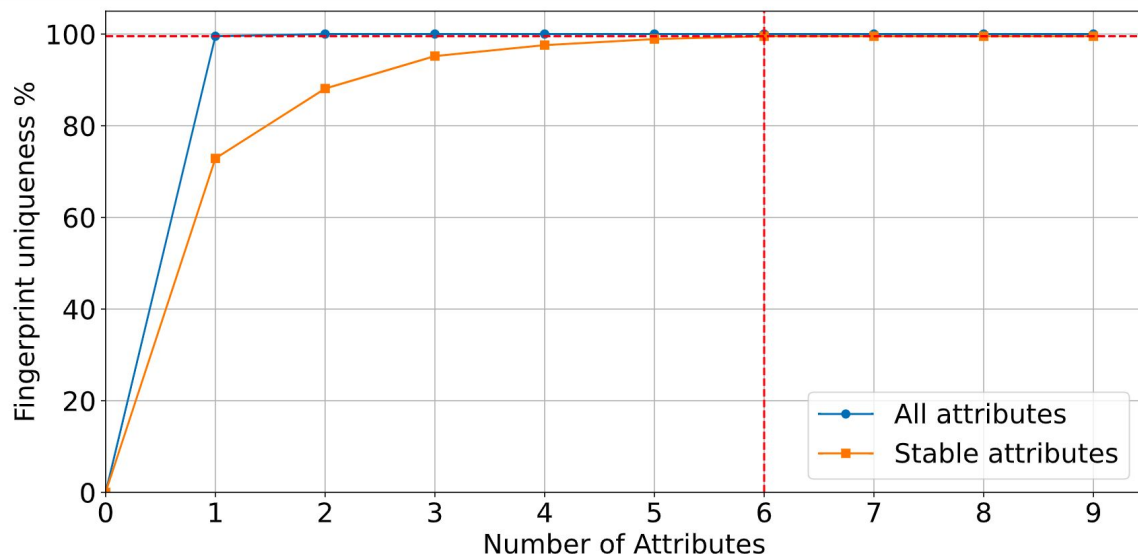
Results: Attribute examples

Attribute	Category	Examples	Distinct Values	Unique Values	Entropy
System Up Since	User-Related	"2024-10-28 09:35", "2025-01-10 17:54"	830	829	9.69
Web View Default User Agent	OS-Related & Hardware-Related	"Mozilla/5.0 (Linux; Android 13; PGT-AL00 Build/HUAWEIPGT-AL00; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/101.0.4951.61 Mobile Safari/537.36"	777	739	9.54
IMEI/MEID Type Allocation Code	Hardware-Related	86326005, 35950275	664	578	9.25
Device Name	User-Related & Hardware-Related	"Patrick's S24+", "Pixel 6a", "realme narzo 30 5G"	683	607	9.20
Available Displays	OS-Related & Hardware-Related	"Display id 0: DisplayInfo{\\\"Built-in Screen\\\", ..., real 1080x2400, largest app 2142x2142, smallest app 1080x1006}, DisplayMetrics{density=2.625, width=1080, height=2142,...}"	726	683	9.16
List of System Services	OS-Related	["HqmManagerService", "knoxcustom", "SEAMService", "SurfaceFlingerAIDL", ...]	656	565	9.12
Root Dir Total Space (Bytes)	OS-Related	1010438144, 982638592	628	527	9.02
Kernel Information	OS-Related	"Linux localhost 5.10.224-Kirisakura_Raviantah_2.5.1 #1 SMP PREEMPT Sat Oct 19 19:58:02 UTC 2024 aarch64 Toybox"	633	544	8.97
Memory Usable By Apps (MB) (Total*Swap)	OS-Related & Hardware-Related	"5601 x 3071", "7607 x 3071"	521	389	8.63
Device Ringtone	User-Related & OS-Related	content://media/external/audio/media/1000101?title=Mission%20Impossible%20(Ti%C3%ABsto%20Remix%20Radiocanonical=1")	617	560	8.78
Communication Device Name	User-Related	"LG HBS810", "WH-CH510", "JBL LIVE460NC"	418	304	8.23
Boot Count	User-Related	1664	316	166	7.77
Network and SIM Operators	User-Related	("PROMOBILE SN", "Orange"), ("AT&T", "AT&T"), ("NL KPN", "Lebara")	337	233	7.42
Next Alarm Time	User-Related	"Fri 16:27", "ven. 06:53", "tors 06:00"	402	370	5.92

Results

Fingerprintability of the Android ecosystem

- **100%** of uniqueness with **2** attributes
- Under stability constraints **100%** uniqueness with **6** attributes
- Example of unique attribute combinations:
 - (Device uptime, Boot count)
 - (Device name, TAC)



Contributions



EXADPrinter: an Exhaustive Fingerprinting Framework for Android



Dataset: **1,151** fingerprints coming from **833** devices



Highlighting the **impact** of **user** and **vendor** customizations



20.65% of devices identified by at least one **unique identifier**



Disclosed issues to concerned parties



100% Fingerprint Uniqueness with just 2 attributes



100% Stable Fingerprint Uniqueness with just 6 stable attributes

Limitations

- **Dataset size.** Small scale of our dataset
- **Stability analysis.** Limited number of fingerprints coming from same device

Future Work

- **Permissions Impact.** How do permissions influence fingerprinting?
- **Fingerprint Evolution.** How do fingerprints evolve over time ?

Conclusion

- **User preferences** make devices identifiable
- **Vendor customizations** enhance device fingerprinting
- Way too many attributes not protected by default

Thank you !

Questions?

Please Install Am I
Unique for Android



<https://github.com/ExadPrinter/>



sihem.bouhenniche@inria.fr