Understanding the Mobile Ecosystem with the Lumen Privacy Monitor

Narseo Vallina-Rodriguez

Project sponsors:

DISCLAIMER: The opinions expressed in this presentation are solely those of the presenter
1st parties (Direct)

Web-specific!

3rd parties (Indirect)
Project Goals

- Identify 3rd-party tracking services on mobile apps
- Evaluate their impact on user privacy
- Promote mobile transparency and enable user control
How?
Lumen Privacy Monitor
Preliminary research results
Dataset

- Accurate traffic fingerprints
  - 1000+ users (containing real user-stimuli)
  - 2,900+ apps
  - 3,200+ second-level domains
1st party vs. 3rd party services

Basic heuristic: \( \text{deg} \ (n) > 1 \)
How to distinguish ad networks and trackers (ATS) from CDNs and other online services?
Challenges in classifying domains

1. Domain blacklists (e.g., Easylist) are web-oriented
2. URL classification services are inaccurate and incomplete

<table>
<thead>
<tr>
<th>URL</th>
<th>Status</th>
<th>Categorization</th>
<th>Reputation</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://flurry.com">http://flurry.com</a></td>
<td>Categorized URL</td>
<td>- Internet Services</td>
<td>Minimal Risk</td>
</tr>
</tbody>
</table>
Custom classifier

- Identify unique identifiers in data flows
  - IMEI, IMSI, Android ID, MAC Address, Serial Number, …
- Analyse the content of their landing pages with a web scraper and NLP
## Results

<table>
<thead>
<tr>
<th>Set</th>
<th>Total</th>
<th>Previously reported ATS (%)</th>
<th>Third Parties (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>All domains</td>
<td>3261</td>
<td>11</td>
<td>31</td>
</tr>
<tr>
<td>UID Harvesters</td>
<td>336</td>
<td>9</td>
<td>41</td>
</tr>
</tbody>
</table>
Ad and Tracking Services (ATS) in mobile apps
Over 68% of tracking services are cross-platform
Trackers by app category

Are games and educational apps COPPA compliant?
Abusive practices (I)

- `getprop` command contains unique IDs
- Unprotected by Android permissions
  - Enables tracking without user consent

```
[dhcp.wlan0.domain]: [networks.imdea.org]
[net.hostname]: [android-db216281e95dfab1]
[persist.service.bdroid.bdaddr]: [40:B0:FA:5C:D0:80]
[ro.boot.serialno]: [04efb34e55e22fcc]
[ro.build.fingerprint]: [google/occam/mako:5.1.1/LMY48T/2237560:user/release-keys]
```
Abusive practices (II)

Host: track.XXXX.com
Accept-Encoding: gzip

device=angler&installDate=2016-11-02_0126-0700&firstLaunchDate=2016-11-02_0126-0700&sdk=23&carrier=&
date1=2016-11-02_0126-0700&af_preinstalled=false&advertiseIdEnabled=false&TRACKERKey=yZnL9BNtUz
ZLva6evLpUg5&lang=English&app_version_name=2.2.0&dkh=yZnL9BNt&android_id=84f942c74fffbdef&adve
rtiserId=fff3ca7e-61d7-4298ab14-256033002de9&deviceType=userdebug&af_v=da33e2cb0879238eb1dc9d93
e0ce38b4564fbd9d&app_version_code=3&network=WIFI&operator=&brand=Android&date2=2016-11-02_0126-
0700&af_timestamp=1478118372355&uid=1478118365655-1389078544330603868&isFirstCall=true&counter=1
&product=aosp_angler&model=AOSP+on+angler
A tool for users
Enabling system-wide user control
The Haystack Project

Install the Lumen Privacy Monitor for Android!

[ About The ICSI Haystack Project ]

Your phone hosts a rich array of information about you and your activities. This includes a range of identifiers, location data and even your contacts list. Often time, apps collect such privacy-sensitive information and share it with third parties such as ad networks and analytics services without your consent for advertising and tracking purposes.

The Haystack Project is an academic initiative led by independent academic researchers at ICSI—UC Berkeley and IMDA Networks in collaboration with UMass and Storrs Brock University. At the core of the project is the Lumen app, an Android app that analyses your mobile traffic and helps you to identify privacy leaks inflicted by your apps and the organizations collecting this information.

Project sponsors:

The Haystack project is sponsored by the National Science Foundation (NSF) and the DataTransparencyLab (DTL).