Characterizing Indirect Privacy Leaks in Mobile Apps with the Lumen Privacy Monitor

Narseo Vallina-Rodriguez
Protecting access to sensitive data

Odd Socks
Version 2.7.0 can access

$ In-app purchases
  • Google Play billing service

Identity
  • find accounts on the device

Photos/Media/Files
  • modify or delete the contents of your USB storage
  • read the contents of your USB storage

Wi-Fi connection information
  • view Wi-Fi connections

Device ID & call information
  • read phone status and identity

Other

You can disable access for these permissions in Settings. Updates to Odd Socks may automatically add additional capabilities within each group. Learn more
1st parties (Direct)          3rd parties (Indirect)

Web-specific!
Project goals:

Identify 3rd-party advertising and tracking services on mobile apps

Evaluate their impact on user privacy

Promote mobile transparency and enable user control
How?
Lumen Privacy Monitor

Int. Computer Science Institute-UC Berkeley  Tools

Everyone

This app is compatible with all of your devices.

Installed
Lumen monitoring state:

On
Research Efforts

900+ users
2500+ apps (paid and pre-installed ones)
1st-party vs. 3rd party services

How to distinguish ad networks and trackers (ATS) from CDNs?
ATS classifier (beta)

**Goal**: Automatically classify domains by their offered service:
1) Analytic services
2) Ad networks

**Problem**: Existing URL classification services may be incomplete:

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

**Solution**: Analyse their behaviour and the content of the domain’s landing page using NLP
Results

- 280 domains (N=446) ATS domains:
  - 4% FPR
  - 58 domains remained unreported by MalwareBytes and Easylist

- 15% of apps connect to more than 5 trackers
ATS Penetration

68.5% of identified ATS domains are cross-platform
Tracking users without consent

Unique identifiers are highly sensitive data

Examples:

- IMEI
- Google ID

Android permissions control access to sensitive resources

```java
Runtime.getRuntime().exec("getprop")
```

```
[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

11-02 13:26:14.077  9756 10171 I Haystack.Flow:
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&advertiserIdEnabled=false&adpsflyerKey=yZnL9BNtUzZLva6evLpUg5&lang=English&app_version_name=2.2.0&dkh=yZnL9BNt&android_id=84f942c74fffbdef&advertiserId=fff3ca7e-61d7-4298-ab14-256033002de9&deviceType=userdebug&af_v=da33e2cb0879238eb1dc9d93e0ce38b4564fbd9d&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
Tracking the Trackers: Towards Understanding the Mobile Advertising and Tracking Ecosystem

Narseo Vallina-Rodriguez, Srikanth Sundaresan, Abbas Razaghpanah, Rishab Nithyanand, Mark Allman, Christian Kreibich, Phillipa Gill

(Submitted on 22 Sep 2016 (v1), last revised 26 Oct 2016 (this version, v2))

Third-party services form an integral part of the mobile ecosystem: they allow app developers to add features such as performance analytics and social network integration, and to monetize their apps by enabling user tracking and targeted ad delivery. At present users, researchers, and regulators all have at best limited understanding of this third-party ecosystem. In this paper we seek to shrink this gap. Using data from users of our ICSI Haystack app we gain a rich view of the mobile ecosystem: we identify and characterize domains associated with mobile advertising and user tracking, thereby taking an important step towards greater transparency. We furthermore outline our steps towards a public catalog and census of analytics services, their behavior, their personal data collection processes, and their use across mobile apps.
Method to identify and classify third-party tracking services
Anonymised data gathered with the **Lumen Privacy Monitor**
Promote user awareness and mobile transparency
Enable user control