Tracking Mobile Trackers

A [Yale Privacy Lab](http://privacylab.yale.edu/tmt) Tech Primer

Share: [privacylab.yale.edu/tmt](http://privacylab.yale.edu/tmt)

[@YalePrivacyLab](https://twitter.com/YalePrivacyLab) | [privacylab@mastodon.social](https://privacylab@ mastodon.social)

Presented by Sean O'Brien
Are you worried that your phone is listening to you?
That it is tracking your movements?
You are being tracked by your phone in some way. This primer will help explain and offer some solutions.
Our phones are full of naughty apps.
At Yale Privacy Lab, we help identify mobile trackers, code that runs inside apps without your knowledge or consent.
What Are Trackers?

• We use the term **trackers** broadly, to encompass traditional advertisement surveillance, analytics, behavioral and location tracking, as well as *developer tools* such as crash reporters.

• We're talking about trackers bundled for app developers as **Software Development Kits** (SDKs) though there are also other ways to track users.
We also focus on **proximity** and **location tracking**.

Trackers that use Bluetooth and near-ultrasonic/ultrasonic signals are some of the worst offenders.
What About Apple?

We'll be talking about Android apps in Google Play.

Many of the same companies distributing Google Play apps also distribute apps via Apple, and tracker companies openly advertise SDKs compatible with multiple platforms.

Thus, advertising trackers may be concurrently packaged for Android and iOS, as well as more obscure mobile platforms.
Digging Deep

• To really understand a specific app and privacy or security concerns, it takes network analysis.

• App permissions are a big indicator something might be amiss (RECORDER_AUDIO etc.)

Be careful accepting permissions when you install an app!
We'll show you an easy way to detect tracker SDKs without needing to know anything about code, via the **Exodus Platform**.
reports.exodus-privacy.eu.org

εxodus scans Android apps in Google Play.
Anyone can scan an app via a slick Web UI
Detecting Tracker **SDKs**

- exodus scanner does **static analysis** of Android APKs to find signatures in embedded classes.

- Without exodus, you can make educated guesses by looking at the **Android manifest** XML and classes* **DEX** files.

- Remember, there are legal restrictions on static analysis of iOS apps, but many of these apps also have trackers (more on that later).
Cory Doctorow on the subject:

“iOS is DRM-locked and it's a felony – punishable by a 5-year prison sentence and a $500,000 fine for a first offense in the USA under DMCA 1201, and similar provisions of Article 6 of the EUCD in France where Exodus is located – to distribute tools that bypass this DRM, even for the essential work of discovering whether billions of people are at risk due to covert spying from the platform.

It's true that the US Copyright Office gave us a soon-to-expire exemption to this rule that started in 2016, but that exemption only allows Exodus to use that tool; it doesn't allow Exodus to make that tool, or to distribute it so independent researchers can investigate iOS.”
εxodus Static Analysis

APK file → unzip → dex files → dxdump

- trackers signatures
- Java classes

match

embedded trackers
```
dexdump classes*.dex | perl -n -e '^[A-Z]+(?::\w+//)+\w+)' & & print "$1\n"' | sort| uniq
com/amazon/device/ads/UserIdParameter
com/amazon/device/ads/Version
com/amazon/device/ads/VideoActionHandler
com/amazon/device/ads/ViewabilityChecker
com/amazon/device/ads/ViewabilityCheckerFactory
com/amazon/device/ads/ViewabilityInfo
com/amazon/device/ads/ViewabilityJavascriptFetcher
com/amazon/device/ads/ViewabilityJavascriptFetcherListener
com/amazon/device/ads/ViewabilityObserver
```

Amazon Ads is embedded
Quick exodus Stats

- 152 tracker signatures, 28,600 reports (Oct 1, 2018)
- 26,133 apps scanned, 400GB+ APK packages
Calling crash reporters like HockeyApp, Crashlytics "trackers" has been controversial, though they have advanced analytics features/options.
Adding & Improving Tracker Profiles

- We are updating profiles, adding new ones.
- We're correlating companies via OpenCorporates.
We're looking for more contributors, and you can help us by contacting Yale Privacy Lab directly or finding us on github.
Mozilla has been guiding us via the Open Leaders Program and our mentor Josefina Caro Magaña of Beyond Activismo.
Real-World Impact:
Working on tracker profiles with us means you're contributing to software projects that protect privacy such as εxodus, F-Droid, Yalp Store, and our ultrasonic jammer apps.
Our tracker profiles go **upstream** to these software projects. Here are some examples.
New Collaborations on Exposing Tracking

Since 2010, the F-Droid community has been working to provide only 100% verified Free Software, and to make apparent all forms of tracking, advertising, and “anti-features” commonly found in apps. F-Droid provides a complete app ecosystem where users are actively notified of tracking and advertising in the apps, and can make informed choices. We have achieved this through the work of many dedicated volunteers reviewing apps as they are submitted, and marking the things that they find.

Researchers at Exodus Privacy and Yale Privacy Lab are working on taking the next big step, by creating tools for automating the process of finding all the various forms of tracking that apps can include. F-Droid will work with them to merge efforts, increasing the effectiveness of volunteers, and exposing the inner workings of software in daily use worldwide.
F-Droid Package Scanning

- AI/machine learning in the future?
- **LibScout**

https://gitlab.com/fdroid/rfp/issues?label_name[]=trackers
Free Software Projects

- Utilize εxodus API:
  - εxodus CLI
  - εxodus Android app
  - εxodify browser addons

- PilferShush Android app

- PiRanhaLysis network interception/analysis (PiRogue, PiPrecious, Phorcys)
Now that we understand static analysis and tracker SDKs, let's talk about physical methods that companies use to track us.
Proximity Targeting

- Retailers are using **bluetooth** alongside **sonic** (near-ultrasonic/ultrasonic, 18kHz to 22kHz range) technology to track precise physical movements via **beacons**.

- The *de facto* bluetooth beacon standard is **Apple iBeacon**, one of the first to market.
Signatures of sonic tracker SDKs SilverPush, Alphonso, Lisnr, Shopkick, Fidzup, and Signal360 can be detected by εxodus. Their profiles are in our github repository.

We're detecting new trackers that utilize these creepy methods often. The latest is CopSonic.
Example Beacon Devices

Source: https://en.wikipedia.org/wiki/IBeacon
Important Caveats

- Beacons use a *combination* of technologies and **may not require an SDK** on a target person's phone.

- Special beacon devices are not required. Sonic tracking can occur via **stadium/arena** (Lisnr, Signal360), **retail** (Shopkick, Fidzup), **TV** (Alphonso, SilverPush) speakers.
Example Sonic Tracking Signals
Sonic Tracking Signal: Closer Look

Audio Sample, Macy's

Much More Info from Cityfreqs
Sonic Tracking Is Not Sci-Fi

- **Frequency Shift Keying** is the primary method.
- Some sonic trackers are very basic ([Fidzup](#)), others are complex ([Shopkick](#)).
- [FTC warnings](#) were issued for app devs who were using SilverPush in 2016.
- Many Alphonso apps were pulled in December 2017 after a [NYTimes](#) story.
Researchers and journalists have shared their app lists/checksums with us. We've got lists of sonic tracking apps still in the wild.

If you are interested in learning more, we can share these and other details (copies of ultrasonic recordings etc.)
Check out the following example of sonic tracking, via a demo video offered by a tracking company.
Sonic Proximity Targeting

- Demo w/ smartphone: [https://frama.link/fidvid01](https://frama.link/fidvid01)
- Video w/ signals: [https://frama.link/fidvid-tmt](https://frama.link/fidvid-tmt)
Forget The Duopoly (For Now). It’s The Little Guys Taking Heat On GDPR

by Allison Schiff // Tuesday, August 7th, 2018 - 1:45 pm

Bonjour, GDPR enforcement.

Google and Facebook may have bullseyes on their backs in Europe, but it’s two mid-sized French startups that received the first warning shots from the General Data Protection Regulation (GDPR) – and that shouldn’t be surprising.

“GDPR is not just there for the big guys,” said Ronan Tigner, an associate at Morrison & Foerster who’s focused on data privacy and security. “Small and medium companies can also fall under scrutiny, especially if they are very data-intensive.”

The companies in la chaise chaude are Teemo and Fidzup, both of which use an SDK to collect geolocation data for targeted advertising.
With the help of our PilferShush app, developed by Cityfreqs, we can successfully block these ultrasonic signals.
PilferShush

Detects & Blocks Sonic Tracking Signals

https://github.com/YalePrivacyLab/PilferShush_prod

• Android app by Cityfreqs.

• Two versions. PilferShush Jammer is the friendlier one for blocking signals.
Grab the **PilferShush Jammer**

- Available in [F-Droid](https://f-droid.org) & [Google Play](https://play.google.com)
Beacons are a pervasive adversary to privacy in our physical world.

We can hunt for beacons that may be sending sonic and bluetooth signals.
Beacon Hunting

On Android - Beacon Locator, iBeacon Detector

On iOS - Locate Beacon, DIY method

- Sonic tracking is useful in some cases, but bluetooth is more dynamic and widespread.
### iBeacon Detected!

<table>
<thead>
<tr>
<th>Address</th>
<th>Last Updated</th>
<th>RSSI</th>
</tr>
</thead>
</table>
Remember, you should turn off bluetooth on your devices by default, and be careful about both microphone and bluetooth settings, as well as app permissions.
Thank You!

- Mozilla Open Leaders and Josefina Caro Magaña
- Scott Shapiro, Laurin Weissinger, Jon Oronzo
- Rebecca Crootof, Jack Balkin, Mike Kwet, Yale ISP
- PiRanhaLysis and Exodus Privacy team
- City Frequencies
- Hans-Christoph Steiner and F-Droid team
- Eben Moglen and Danny Haidar, Freedombox Fndn
- Nathan Freitas, Guardian Project