**Submitted as a poster to EuroSys'17**

# A Preliminary Look into Unsolicited Mobile App Traffic

Tomasz Lyko * and Yehia Elkhatib
School of Computing and Communications, Lancaster University, UK
{i.lastname}@lancaster.ac.uk

## 1. Background

As of May 2016, Google Play hosted 2.6 million apps and had an accumulative total of 65 billion app downloads.[1] Any developer can publish apps through Play, and it is quite prevalent to granting apps permission use the phone's network interfaces at will and under very limited supervision (beyond overall traffic volume and bitwise access to an interface) [1]. But should we trust mobile developers to "do no evil" in terms of the volume and type of traffic their apps generate? We are motivated to identify whether there is a need for more scrutiny on the connections apps make, especially when not in use.

## 2. Methods

We installed 16 of the free apps most downloaded from Play UK as of December 2016, covering 4 main types: shopping, multimedia, utility, and gaming. They were installed on a Motorola Moto X handset operating Android 6.0. Each app is monitored for a continuous period of 24 hours with 4 brief usage times (≈10 minutes each) and no other user app running. A usage period involves starting the app and lightly using it (*e.g.,* searching for a product) without signing in to the app where available. After every usage period, the app is exited to prevent it from actively running in the background, although many continue to despite explicit user exit. Application-specific traffic traces are passively collected as pcap files, then analysed using Java (for timeseries and destination-based analysis) and Wireshark (for flow-level and packet-level investigation).

* Student

[1] `https://www.statista.com/statistics/281106/number-of-android-app-downloads-from-google-play/`



## 3. Results

Aside from the anticipated traffic recipients such as CDNs and cloud servers, we have found a number of unexpected ones. For instance, eBay communicates constantly with PayPal (a previous subsidiary) and Threat Metrix (a fraud detection company in the Netherlands). This is perhaps to be expected if it were not for the fact that no purchases or bids were made. More interestingly, the eBay app terms and conditions do not mention such information sharing.

A number of apps (*e.g.,* Crazy Kitchen, Auto Trader) kept sending data to Facebook even when the app is not being used nor the user signed in. Moreover, a Google server opened an HTTPS connection to Crazy Kitchen whilst the app was not being used. The worst culprit here is the 100 Pics Quiz game that constantly downloaded mp4 ads of other games, which were subsequently not showed to the user!

Some apps also showed systemic miscommunications. For instance, Fruit Ninja Free made repeated DNS lookups for `bn.tl`, a CDN domain in East Timor that does not exist. The app might have been forwarding sensitive user information to a place where it is illegal to store. Moreover, such behaviour could easily be misconstrued as being malware. This is surprising to see in an extremely popular app which is regularly updated by a multinational (Halfbrick).

## 4. Conclusion

We experienced a number of highly popular apps sending traffic when not being used to multiple servers without informing the user. The user is not just unaware of how much data an app sends, but also of whom it goes to. As the number of apps keeps growing, it is increasingly difficult to make sure that an app is using the network reasonably. Therefore, there is a need for automated mechanisms to scrutinise the network behaviour of apps, and for having more expressive user controls to allow fine-grained control over access to the network. Furthermore, app terms and conditions need to be more forthright about which third parties they share information with in order to allow users to make informed decisions.

## References

[1] X. Wei, L. Gomez, I. Neamtiu, and M. Faloutsos. Profiledroid: Multi-layer profiling of android applications. In *Mobicom*, pages 137–148. ACM, 2012. .

# A Preliminary Look into Unsolicited Mobile App Traffic


## Tomasz Lyko and Yehia Elkhatib

School of Computing and Communications, Lancaster University, UK

{i.lastname}@lancaster.ac.uk


## Background

Any developer can publish apps through Play, and most apps require users to allow use of the phone's network interfaces under very limited supervision. Should we trust mobile developers to "do no evil" in terms of the volume and type of traffic their apps generate, especially when not in use?

## Research Questions

1. What traffic do mobile apps create?
2. How does traffic type and volume vary over on and off use periods?
3. Are there any recognisable patterns across apps?

## Methods

We investigated 16 free apps most downloaded from Play UK as of Dec 2016, covering 4 types: shopping, multimedia, utility, and gaming. Each app is:

- Installed on a Motorola Moto X operating Android 6.0
- Monitored for 24 hours with no other user app running
- Used 4 times: open app and lightly use (≈10 minutes) without signing in, bidding/purchasing, or streaming media
- App is exited to avoid actively running in the background, although many continue to despite explicit user exit
- Application-specific traffic traces are collected and analysed

## Recipients

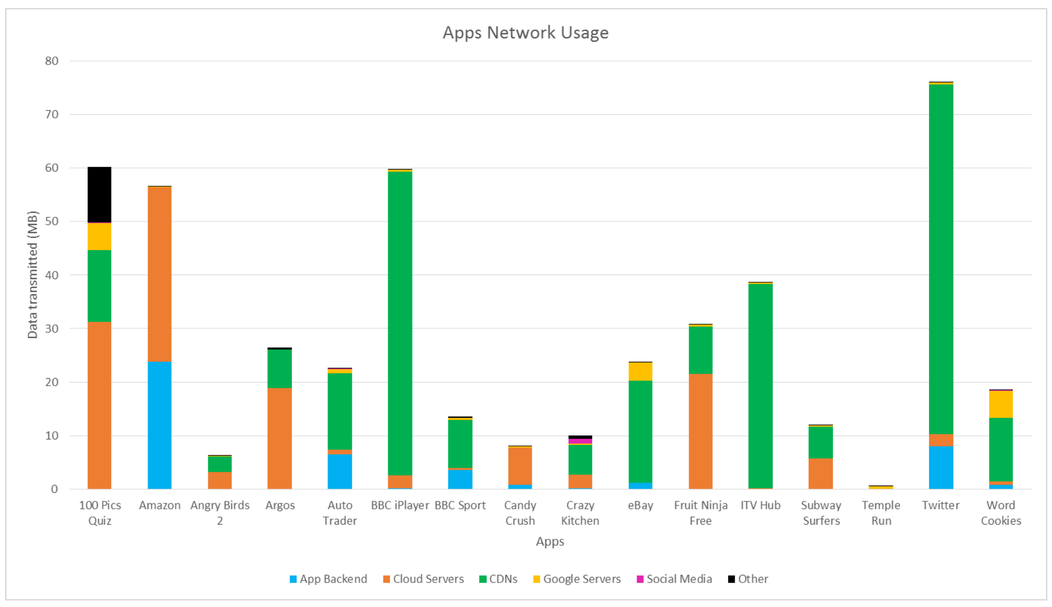


**Figure 1:** Overall breakdown of traffic recipients per app.

## Unexpected Third Parties

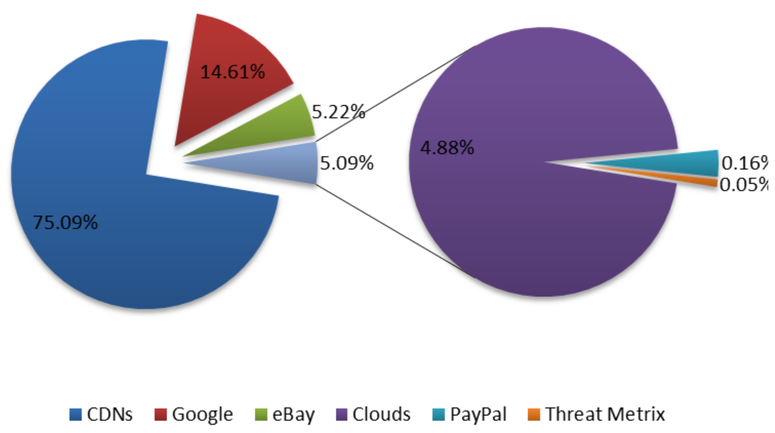


**Figure 2:** eBay - communicates constantly with PayPal (a previous subsidiary) and Threat Metrix (a fraud detection company in the Netherlands) even though no purchases or bids were made. Terms and conditions do not mention such information sharing.

Also, a number of apps (*e.g.*, Crazy Kitchen, Auto Trader) kept sending data to Facebook even when the app is not being used nor the user signed in.

## Out of Use Traffic

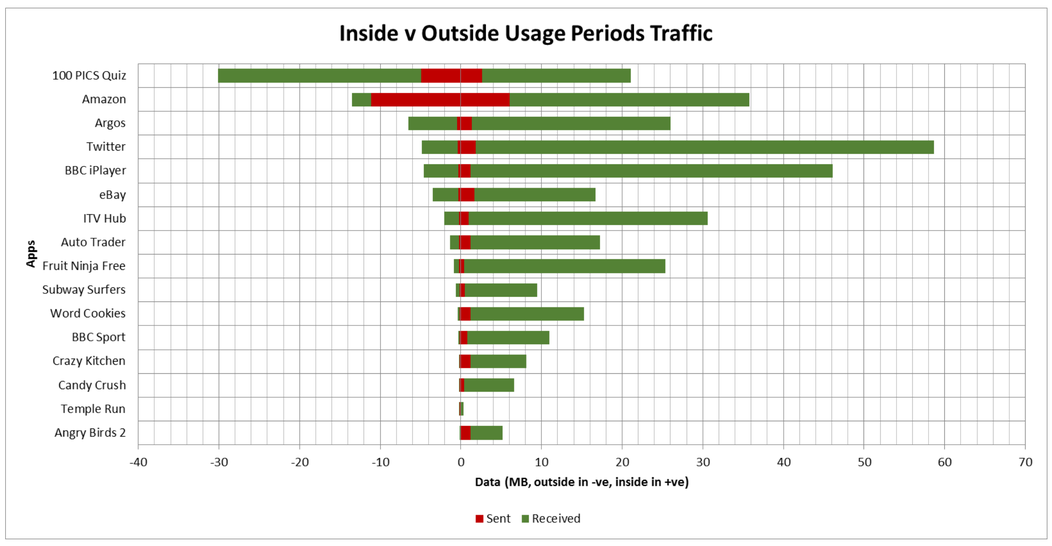


**Figure 3:** Some apps have significant network usage when not being used.

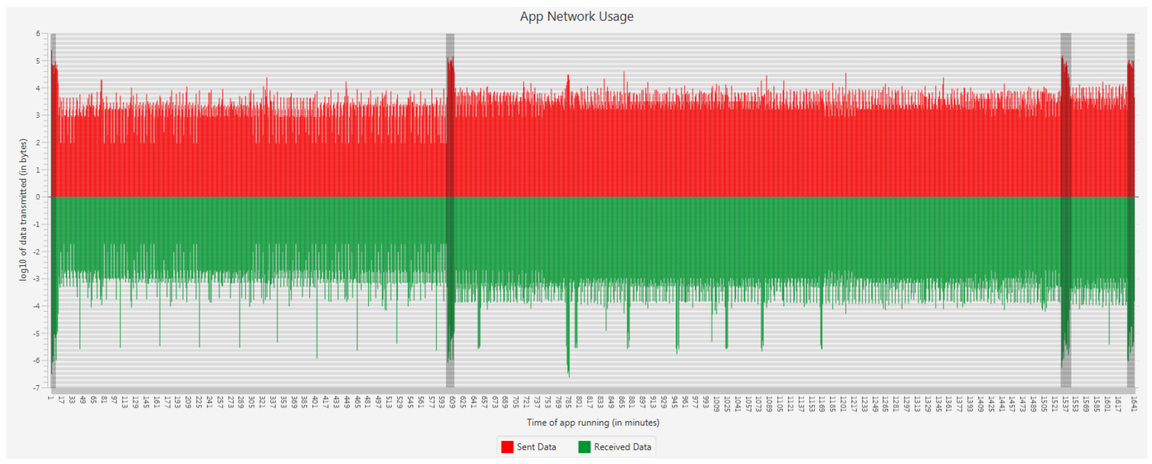


**Figure 4:** 100 Pics Quiz - the worst offender when out of use, mostly downloading (and not showing!) mp4 ads of other games.

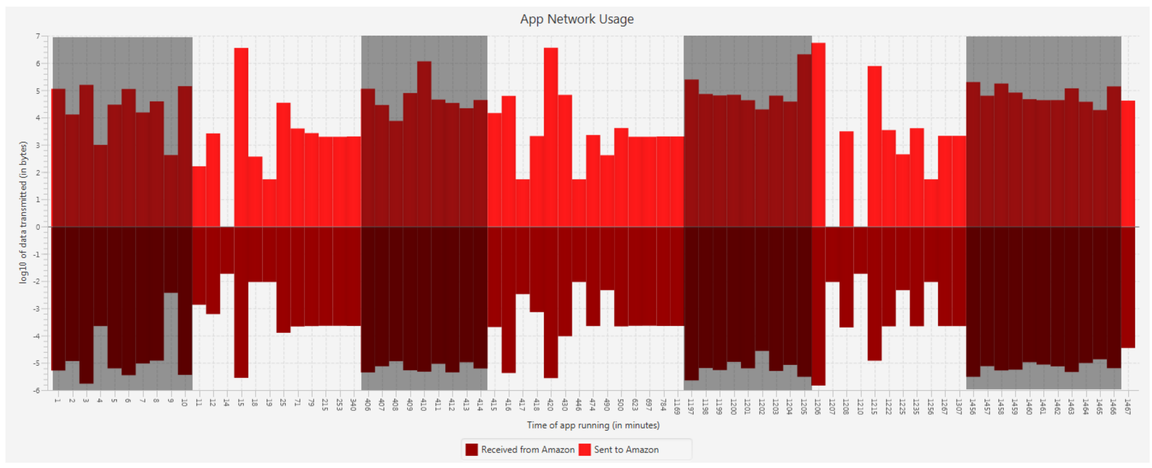


**Figure 5:** Amazon - constant communication with Amazon backend servers in and out of use, although user was not signed in.

## Bad Domains

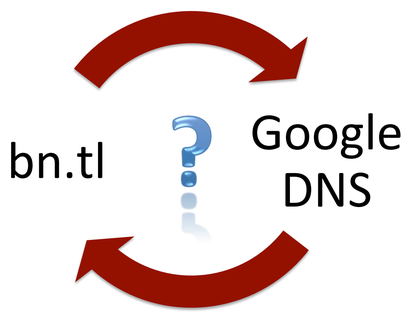


**Figure 6:** Fruit Ninja Free - made 2 DNS lookups every hour for a non-existent CDN domain in East Timor.

## References


[1] Falaki, H., Mahajan, R., Kandula, S., Lymberopoulos, D., Govindan, R., and Estrin, D. Diversity in smartphone usage. In *MobiSys* (2010), ACM, pp. 179–194.

[2] Qian, F., Wang, Z., Gao, Y., Huang, J., Gerber, A., Mao, Z., Sen, S., and Spatscheck, O. Periodic transfers in mobile applications: Network-wide origin, impact, and optimization. In *WWW* (2012), ACM, pp. 51–60.

[3] Shafiq, M. Z., Ji, L., Liu, A. X., Pang, J., and Wang, J. A first look at cellular machine-to-machine traffic: Large scale measurement and characterization. *SIGMETRICS Perform. Eval. Rev. 40*, 1 (June 2012), 65–76.

[4] Taylor, V. F., Spolaor, R., Conti, M., and Martinovic, I. AppScanner: Automatic fingerprinting of smartphone apps from encrypted network traffic. In *EuroS&P* (March 2016), pp. 439–454.

[5] Vallina-Rodriguez, N., Shah, J., Finamore, A., Grunenberger, Y., Papagiannaki, K., Haddadi, H., and Crowcroft, J. Breaking for commercials: Characterizing mobile advertising. In *IMC* (2012), ACM, pp. 343–356.

[6] Vixie, P. A. It's time for an internet-wide recommitment to measurement: And here's how we should do it. In *Workshop on Traffic Measurements for Cybersecurity* (2016), ACM, pp. 1–2.

[7] Wei, X., Gomez, L., Neamtiu, I., and Faloutsos, M. Profiledroid: Multi-layer profiling of android applications. In *Mobicom* (2012), ACM, pp. 137–148.