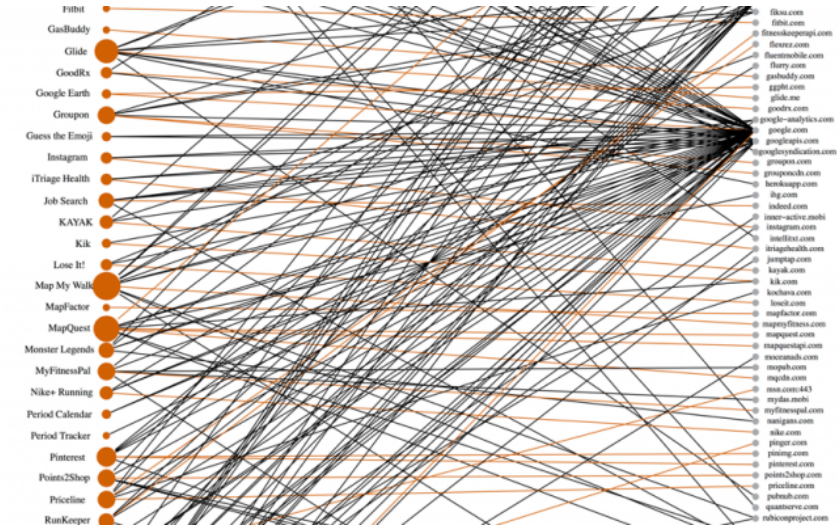
RISK ASSESSMENT / SECURITY & HACKTIVISM

User data plundering by Android and iOS apps is as rampant as you suspected

Most commonly shared data for Android is e-mail addresses; for iOS, it's GPS data.

by **Dan Goodin** - Nov 4, 2015 8:40am PST

113



Enlarge / A sampling of third-party data sharing by Android apps. Images for iOS apps looked similar.

Technology Science

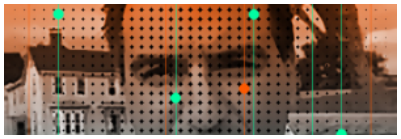
Apps in both Google Play and the Apple App Store frequently send users' highly personal information to third parties, often with little or no notice, according to recently published research that studied 110 apps.

The researchers analyzed 55 of the most popular apps from each market and found that a significant percentage of them regularly provided Google, Apple, and other third parties with user e-mail addresses, names, and physical locations. On average, Android apps sent potentially sensitive data to 3.1 third-party domains while the average iOS app sent it to 2.6 third-party domains. In some cases, health apps sent searches including words such as "herpes" and "interferon" to no fewer than five domains with no notification that it was happening.

"The results of this study point out that the current permissions systems on iOS and Android are limited in how comprehensively they inform users about the degree of data sharing that occurs," the authors of the study, titled *Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps*, wrote. "Apps on Android and iOS today do not need to have permission request notifications for user inputs like PII and behavioral data."

The personal information most commonly transmitted by Android apps was a user's e-mail address, with 73 percent of the apps studied sending that data. In total, 49 percent of Android apps sent users' names, 33 percent transmitted users' current GPS coordinates, 25 percent sent addresses, and 24 percent sent a phone's IMEI or other details. An app from Drugs.com, meanwhile, sent the medical search terms "herpes" and "interferon" to five domains, including doubleclick.net, googlesyndication.com, intellitxt.com, quantserve.com, and scorecardresearch.com, although those domains didn't receive other personal information.

LATEST FEATURE STORY



FEATURE STORY (3 PAGES)

"Bribes," gay porn, and copyright trolls: The rise and fall of lawyer Marc Randazza

Arbiter says Randazza took bribes, lied to employer, and must pay $600k.

WATCH ARS VIDEO

How a group of neighbors created their own Internet service

Powered by radios in trees, homegrown network serves 50 houses on Orcas Island.

STAY IN THE KNOW WITH

LATEST NEWS

DEPT. OF SPECTACULAR EXPLOSIONS

As Orbital seeks to fly again, new photos of its dramatic crash last year

DOJ indicts man who blasted false stock info on Twitter then traded on it

CANDY CRUSH FILM NOT YET ANNOUNCED

Further expanding beyond consoles,

Also concerning were Android apps that sent third parties potentially sensitive combinations of data. Facebook, for example, received users' names and locations from seven of the apps analyzed in the study—American Well, Groupon, Pinterest, RunKeeper, Tango, Text Free, and Timehop. The domain Appboy.com received the data from an app called Glide.

The researchers also noticed that 51 of the 55 Android apps tested connected to the domain safemovedm.com. The researchers wrote:

> The purpose of this domain connection is unclear at this time; however, its ubiquity is curious. When we used the phone without running any app, connections to this domain continued. It may be a background connection being made by the Android operating system; thus we excluded it from the tables and figures in order to avoid mis-attributing this connection to the apps we tested. The relative emptiness of the information flows sent to safemovedm.com indicate the possibility of communication via other ports outside of HTTP not captured by mitmproxy.

```
---START REQUEST-----------------
('_flow_', 79)
('_scheme_', 'http')
('_host_', '54.230.38.136')
('_port_', 80)
('_path_', '/webping-s.html?unused=1405960213165')
('_method_', 'GET')
_assemble_
GET /webping-s.html?unused=1405960213165 HTTP/1.1
Cache-Control: no-cache
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.4.2; SPH-L710
Build/KOT49H)
Host: hla2.safemovedm.com
Accept-Encoding: gzip


----END REQUEST--------------------
```

Enlarge / A Web request made by an Android phone to the little-known safemovedm.com domain.

Technology Science

A Google spokeswoman contacted for this post didn't provide any information about safemovedm.com or say why the Android operating system would connect to it. Web searches provided a variety of theories about the purpose of Android connections to the domain.

iOS apps, meanwhile, most often sent third parties a user's current location, with 47 percent of apps analyzed in the study transmitting such data. In total, 18 percent of apps sent names, and 16 percent of apps sent e-mail addresses. The Pinterest app sent names to four third-party domains, including yoz.io.facebook.com, crittercism.com, and flurry.com.

Several of the apps in the study sent other sensitive information. For instance, Period Tracker Lite, an app that tracks menstrual cycles, transmitted symptom inputs such as "insomnia" with apsalar.com, while job-search apps from Indeed.com and Snagajob shared employment-related inputs such as "nurse" and "car mechanic" with four domains, including 207.net, healthcareresource.com, google-analytics.com, and scorecardresearch.com.

One thing app users can do to safeguard their personal information, the researchers suggest, is to supply false data when possible to app requests. The researchers also said that apps can be redesigned to allow users to opt out of data collection and that app stores could more prominently inform users about third parties who may receive their data.

PROMOTED COMMENTS

coachmark2 | Ars Centurion — jump to post

I did an experiment like this about six months ago.

It's getting to the point where running all traffic through a VPN with traffic inspection and intelligent scanning is required. I started using a VPN on my phone to avoid AT&T's analytics dickery. Then in packet captures, I started noticing this sort of nonsense being leaked out everywhere. My intrusion protection system notes literally thousands of blocked connections per day.

And the contents of those blocked packets are downright frightening. Email addresses, GPS data, screen power-on hours per day, quantity of data passed in a day, a full manifest of all apps installed,

Activision announces a film division


Weight loss apps no better at helping shed pounds than pamphlets

WATCHING YOU
Websites can keep ignoring “Do Not Track” requests after FCC ruling

THE POWER OF THE CLOUD
Microsoft considers blocking SHA-1 certificates after cost of collisions slashed

names of numerous confidential documents stored on my (encrypted) phone....

It was apalling. Marshmallow's granular permissions settings can't come soon enough.

202 posts | registered Nov 25, 2013

robertchin | **Wise, Aged Ars Veteran** | **et Subscriptor** **jump to post**

> peaceminded wrote:
> There is no good way to solve this problem though. The only thing I can think of is some trusted 3rd party like EFF starting a App Privacy Rating System - essentially do what this research did only on an ongoing basis and publish results - people can then consult it and decide whether to install an app or not.

If this ever became a thing, apps would just collect the data and route everything through their own domain name before sending it off to third party servers. If it's encrypted it would be even harder to tell what they are sending.

But I wonder if maybe some app developers don't even know what is being sent to third party servers. If you blindly use a thir party library, especially one provided as just a binary blob with no source code, it's going to be hard to tell what kind of nefarious things that library does.

112 posts | registered Jun 6, 2003

coachmark2 | **Ars Centurion** **jump to post**

> dio82 wrote:
> show nested quotes
>
> Would you care to elaborate a bit more on your VPN setup? Especially any pointers to traffic inspection, intelligent scanning and intrusion protection system?

Certainly.

I run a pfSense box at my home which is running an OpenVPN server, Snort Intrustion Protection System, and SquidGuard w/ HTTPS inpsection.. My family and I all dial into this VPN when we're on the road.

First, OpenVPN stops AT&T from being AT&T and snooping on our browsing habits. All data sent over their LTE network looks like encrypted UDP gibberish to them and it's all bound for a single IP. Not much analytics you can really do on that.

Once the traffic hits the pfSense box, it is decrypted and Snort gets a crack at it. Snort looks at your traffic and matches patterns against certain rules to stop anything sketchy going on. And you can get REALLY granular. (Like, don't allow an Excel file inside a ZIP file in an email from a server in XX IP space between the hours of 4pm and 9pm).

After Snort has inspected the traffic, it hits SquidGuard. Squidguard intercepts any HTTP or HTTPS traffic and proxies it on my behalf. If it's plain-text, it can read what's going on. If it's encrypted, it decrypts it on the fly and then re-encrypts it when it's done with it. Essentially, I am performing a man-in-the-middle attack against myself to inspect the traffic on the fly. My devices all trust the certificate that SquidGuard uses to sign off on this "attack." SquidGuard blocks advertising and tracking domains based on Shalla's Blacklists.

Finally, the traffic is sent out the firewall's WAN interface to the wide open Internet. All that just to maintain privacy while using my phone.

203 posts | registered Nov 25, 2013

READER COMMENTS 113

Dan Goodin / Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.
@dangoodin001 on Twitter

← OLDER STORY NEWER STORY →