App Reputation Report – February 2013

Appthority

The Authority in App Security™

contact@appthority.com | 1-855-346-SAFE | @GetAppthority | www.appthority.com

Introduction

The Appthority® App Report for February 2013 provides an overview of the security risks behind 100 free iOS and Android apps. Appthority examined the differences between the Android and iOS app ecosystems; compared app behaviors across five popular app categories (business, education, entertainment, finance, games); and looked at the developers behind these apps.

This report focuses on free mobile apps rather than paid apps. Free apps are more inclined to collect data on the user and share it with outside parties, such as ad networks or analytics companies, as a method of generating revenue. With no initial fee to download, free apps are also widely popular with consumers, who in turn bring those apps into the workplace. For this reason, Appthority analyzed the top 10 free apps across five common categories from the Apple App Store and Google Play.

Appthority believes that the user should be armed with the knowledge of what apps actually do and have the choice to opt in to app permissions. Enterprises must also be aware of the risks posed by employee mobile devices when they're used for work purposes. As employees bring new apps into the workplace, they're putting company data, and the networks these devices access, at risk.

Testing Methodology

Appthority's research team used the cloud-based Appthority Platform™ to perform static and dynamic app analysis on the 100 most popular apps. The company analyzed each app for particular behaviors within a test environment. These behaviors include sending and receiving data without encryption, location tracking, sharing data with advertising or analytics networks, accessing the user's contact list or address book, and accessing the user's calendar. From this internal data, the company identified the top security risks behind these mobile apps.

Report Highlights

- The vast majority of free apps send and receive data to outside parties without encryption.
- 96% of total apps share data with advertising networks and/or analytics companies.
- 79% of the top 50 free iOS and Android apps are associated with risky behaviors or privacy issues. Overall, iOS apps exhibited more risky behaviors than Android apps.
- Entertainment apps were the worst offenders out of the top five categories, with the highest number of apps that track for location and share data with advertising networks and/or analytics companies.
- While 14% of iOS apps had access to a user's calendar, none of the Android apps had similar access.
- More than half of the total apps track for location by accessing the device GPS or using other location tracking methods.
- More than 80% of apps across categories come from different unique, individual developers.

iOS and Android App Statistics

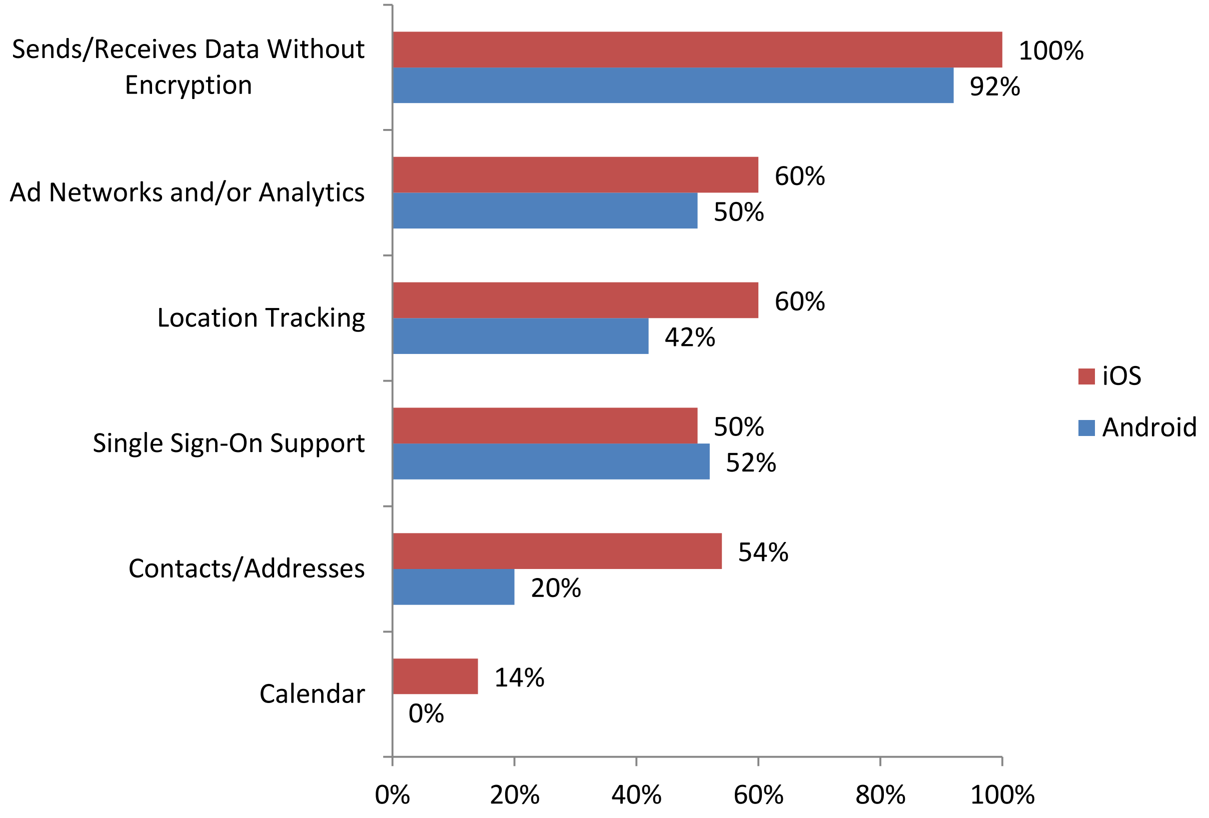
Risky App Behaviors: iOS vs. Android

Of the 100 free apps – 50 Android apps and 50 iOS apps in five equivalent categories – iOS apps exhibited more risky behaviors. In fact, all 50 iOS apps (100%) and 46 of the Android apps (92%) send and receive data without encryption. This potentially includes user data collected by the app and delivered back to the developer.

The results show that iOS apps have more access to user data. The majority of iOS apps track for location (60%), share data with advertising or analytics networks (60%) and have access to the user's contact list (54%). A small percentage of iOS apps also had access to the user's calendar (14%).

Android apps were not too far behind. Half of the Android apps shared data with ad networks and/or analytics companies, and 42% tracked for location. However, substantially fewer Android apps had access to contacts (20%) and none of them accessed the user's calendar.

An interesting emerging trend is the popularity of single sign-on (SSO) support on both iOS and Android. SSO can be great for users from a functionality perspective, allowing them to leverage Facebook, Twitter, or other popular social networking authentication methods (username and password). However, common security vulnerabilities in SSO methods can also be detrimental to any app that incorporates the faulty SSO feature.

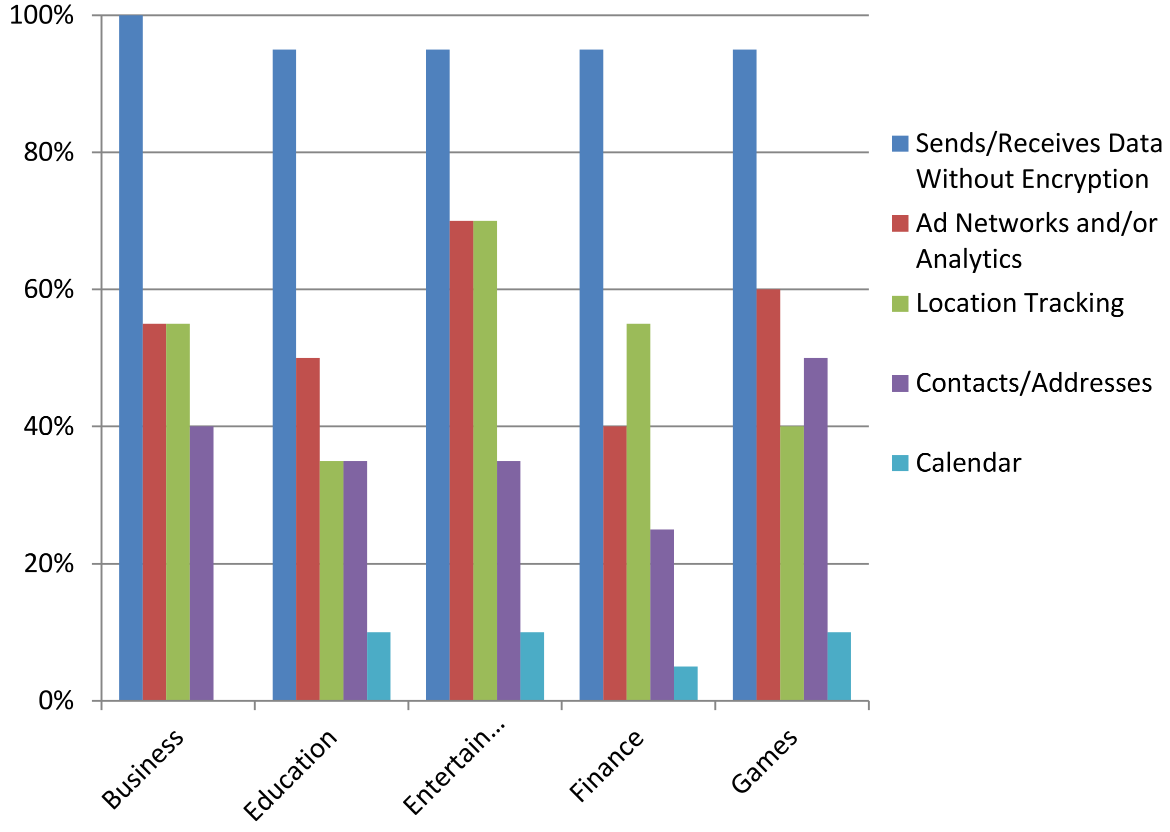


App Categories: Which Apps Put Data At Risk?

With a wide variety of apps available in the Apple App Store and Google Play, Appthority set out to examine the top 10 free mobile apps on both platforms across five categories: business, education, entertainment, finance and games. The entertainment category included a variety of apps, including movie and photo apps, while the gaming category strictly included mobile games. The chart below shows how each app category ranked in terms of risky behaviors.

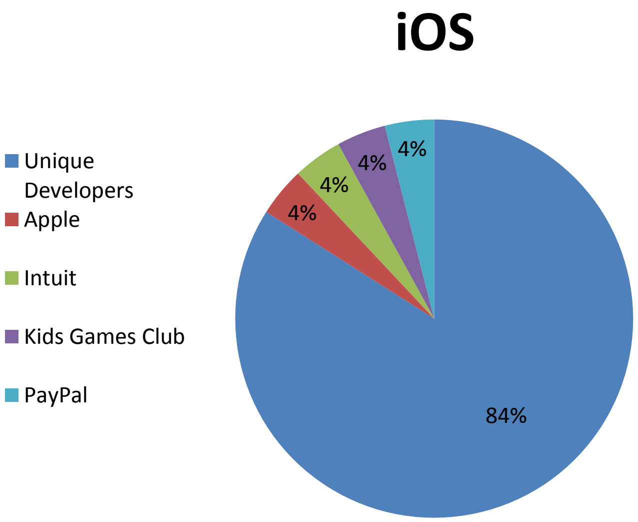
The majority of apps showed evidence of at least one risky app behavior. For example, almost all of the apps send or receive data without using encryption. More than 50 percent of the apps did some form of location tracking. More than half of the apps also shared data with ad networks or analytics companies. Also, over a third of these apps had access to contact lists (37%), but very few had access to the user's calendar (14%).

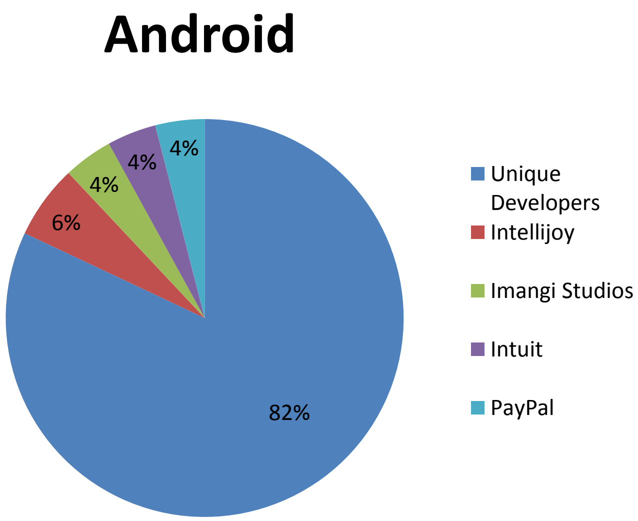
Overall, entertainment apps exhibited the highest number of risky behaviors, particularly in terms of tracking the user's location and sharing data with ad networks and analytics companies. Games and business apps scored similarly, with the exception of access to the user's calendar. Surprisingly, none of the top business apps accessed the user's calendar. Education and finance apps showed the fewest risky behaviors.



Developer Breakdown

In examining the companies behind these popular apps, more than 80% of these apps came from individual developers. Apple, Intuit, Kids Games Club and PayPal had more than one app in the top 50 for iOS, while Intellijoy, Imangi Studios, Intuit and PayPal had multiple Android apps. Intellijoy developed the largest number of apps that were tested, with three different Android apps in the education category.





Summary and Analysis

The results show that the majority of the top free mobile apps are associated with substantial security risks and privacy issues. While none of the apps showed any signs of mobile malware, most of them share unencrypted data and exhibit other risky behaviors.

Compared to the last report in July 2012, risky behaviors slightly decreased, but developer fragmentation increased. Last year, Appthority analyzed the top 50 free apps for both platforms regardless of category, and measured the top business and gaming apps separately. In this report, the company selected 10 popular apps from five different categories on each platform to see which apps put the most data at risk. As stated earlier, entertainment apps are most likely to track for user location and share data with third parties.

Similar to last year's report, iOS apps had more access to user data than Android. In fact, this year's iOS apps had even more access to data than the iOS apps from last year. Appthority anticipates that this trend will increase for both iOS and Android apps moving forward. As developers seek ways to monetize free mobile apps, users will be asked to approve of more app permissions that have less to do with these apps, but collect their personal data and share it with outside parties.

It's generally perceived that Android devices are more "dangerous" due to the increasing amount of Android malware. But in actuality, mobile malware infects less than one percent of apps. The real concern should be over how mobile apps are handling personal info and company data. In that respect, iPhones should not be considered any safer than Android devices. Any Internet-connected device can be put data at risk.

With the rise of the BYOD ("bring your own device") trend, personal mobile devices are being introduced into the workplace and used for company purposes. But doing so introduces a new problem: the mixing of personal and company data on the same device. So how can organizations protect their company data on an employee's cell phone? Mobile App Risk Management must be built into our policies.

Users should take simple steps to protect themselves by reviewing app permissions before downloading an app. But even so, developers have found numerous loopholes around the permission-based model to obtain user data. Organizations must build new policies to address BYOD, set employee risk profiles according to job role and educate employees on these risks. By building Mobile App Risk Management into new policies, companies can empower their employees to use the mobile tools they need to get their work done while ensuring that corporate data stays within the organization.

About Appthority

Appthority® – The Authority in App Security™ helps the enterprise identify and manage the risks hidden in mobile apps. The cloud-based Appthority Platform™ automatically identifies and grades risky security and privacy behavior in mobile apps including known and unknown malware, and corporate data exfiltration. The Appthority Platform integrates with the enterprise's existing mobile solutions, adding app reputation and risk analysis capabilities to Enterprise Mobility Management (EMM), Mobile Device Management (MDM), Mobile App Management (MAM) Enterprise App Catalogs/Stores, and the Enterprise Mobile App Developers' Software Development Lifecycle (SDLC). For more information, and to learn more about Mobile App Risk Management, please visit www.appthority.com.