The Prevalence and Privacy Risks of Leaky Apps

Reema Al-Marzoog

Mentor: Ming Chow

December 15, 2015

Abstract

With the proliferation of mobile applications comes concern about the security and privacy issues they pose. Mobile apps often collect analytics about their users that can be used to collect detailed personal information about a user, which may violate a user's privacy, especially when the data is not properly secured and the user is unaware that the information is being collected. Even when users technically grant their consent for the application to collect these analytics, they may not have a clear understanding of what they are agreeing to, or the clause may be hidden in a Terms of Service agreement. Using this information, an attacker or a governmental agency may be able to reconstruct a detailed profile of the user. We analyze the major privacy risks related to data leakage and data storage that are present in an alarming number of mobile apps.

Table of Contents

Introduction

Most people are aware that the applications on their mobile devices access information about them. They may have differing degrees of concern about the amount and type of data being accessed, but generally understand that, for instance, a photo editing app probably has a good reason it needs to permission to use their photos. Privacy problems arise, however, when these apps expose the data to third parties, insecurely handle the data they are collecting, or are collecting more data than the user is aware of. Applications that expose users' personal information to third parties -- which range from advertisers to attackers to the NSA ("What To Do") -- are said to be *leaky*.

There are two main kinds of leaky apps. The first kind of leaky apps are apps that actually leak your data: personal information that the app accesses is exposed to third parties ("What To Do"). This category includes apps like Angry Birds, whose massive collection of data about their users was reported to have been accessed by the NSA (Fairchild). The report, based off information leaked by Edward Snowden, also "described how, since 2012, British intelligence analysts have been able to intercept Angry Birds players' profiles, as well as advertising data, which might include information about everything from their location and marital status to political affiliations and income" (Schwartz).

The second kind of leaky apps are ones in which a third party steals your data. These apps are usually downloaded not from official app stores, but from third party sources. Malicious third party apps are often trying to steal login credentials, sometimes to try to access a user's finances. Apps from official sources undergo more regulation than do third party apps, so they tend to be a little safer, though still not without risks ("What To Do").

To the community

The importance of the problem with leaky apps lies in their prevalence and in their inconspicuousness. One of the reasons leaky apps are so dangerous is that they often seem reliable or innocuous ("A Data Spill"). Among Android apps that have been shown to be leaky are Outlook and The Weather Channel ("A Data Spill"), both of which a user might assume are trustworthy. One of the most commonly used examples of leaky apps, after all, is the aforementioned Angry Birds. Users may be unlikely to think about a gaming app's security, or, even if they do, may not think that a gaming app could possibly have access to sensitive personal information about them.

Even when an app comes from official stores and therefore has passed inspection by Apple or Google or some other company, it is not necessarily free from data leakage. Andrew Hoog, CEO of NowSecure, writes that his "internal audit shows that 60% of the 100 most popular apps, for business and/or recreational purposes, have a **High-Risk** rating in one or more security areas. All of these apps are available through Google Play and iTunes – and none of them would alert users that a cyber criminal is in their midst" ("A Data Spill"). Thus, even applications that have undergone some form of review should not be assumed to be free from the risk of data leakage.

While users may not have a problem with an app accessing some information about them to allow the app to function as expected, it is extremely common for apps to collect data beyond that which their functionality requisites. According to Matthew Schwartz, "One 2012 study … found that nearly half of all mobile apps collect more data than they require, while one-third ask for many more permissions than they require. In many cases, this data grab has to do with feeding mobile advertising networks, while the excess permissions trace to lazy developers not taking the time to give their app only the permissions it requires."

With this information, third parties can reconstruct detailed information about a user. A telling illustration of the problem is proposed by Charlie Fairchild: "Consider a healthcare app this

[sic] is used to track how often a patient experiences a particular symptom of a disease. If the app also contained analytics that reported how often that same section of the application was viewed, it would be possible for someone with analytics access to determine the medical condition of a specific user -- and place the provider in violation of HIPAA compliance." Not only would a very personal detail about a user's life be exposed, but the creators of the application would also be violating the law.

Data leakage is a problem in both consumer and business sectors, and personal apps that a user has on their phone can cause business risks if they also use that phone for work ("A Data Spill"). As Hoog writes, "The danger is that one unsecured app or 'leaky' app on a single employee's phone can act as a gateway to loss of your company's financial information and customer data" ("Leaky Apps"). A user's privacy might be violated and their financial data might be stolen, a business's trade secrets, confidential data, and finances may be at risk, and software developers may jeopardize their users' information and therefore their trust, all because of leaky applications. Thus, data leakage is a problem that affects anyone with any connection to mobile applications.

Recommendations

Defenses for users

While an application user can almost never be certain that their data is always being handled securely, there are a number of precautions users who are worried about data leakage can take. When you are deciding whether or not to use an app, try to find as much information as possible about what data is being collected. This means everything from being very conscious of what permissions the app is explicitly asking for -- your contacts list, for example -- to data you might be accidentally giving them permission to access through Terms of Service agreements, which you

should at the very least skim. Be suspicious of the permissions an app is asking for especially if there is no clear reason why an app with its purported functionality would need that information. If you'd like to check what permissions apps you currently have installed have been granted, most smartphones allow you to see a list of them in their Settings menu.

Of course, sometimes you do need to give an application access to your data for it to function properly. If you decide that you are not willing to give up that functionality, just be aware that you usually cannot know everything the app is doing with your data, including whether or not it is storing and transferring that data securely. For more harmless information, you may not mind taking this risk, but if the information is very private or confidential, you might want to think twice about whether you're willing to accept the possibility that the data may be leaked.

As previously mentioned, official app stores have vetting processes and do not allow apps that do not pass inspection to be listed in the store. While these review processes are very far from perfect and many instances of potential data leakage escape notice during these examinations, they are better than nothing. So, avoid installing apps from untrusted sources and from third parties. For businesses, giving employees devices for work-related purposes only is the best option because it allows for more control over settings and installed apps. Whether or not this option is possible, employees should be instructed in mobile security policies, including which apps are allowed to be installed on their devices ("What To Do") and when and how they are allowed to transmit confidential information and work credentials ("A Data Spill"). There are also several services that can be used to compare the list of apps on an employee's phone to a list of apps that have been deemed trustworthy, another option for employers ("What To Do").

Action items for developers

Developers without malicious intents may accidentally create leaky apps due to lack of consideration or knowledge about security and privacy issues. Developers should make a conscious effort to avoid data leakage. Companies and individuals releasing software should have a security review system, but it is also crucial to incorporate security and privacy into the actual process of creating an application. There are several ways to hold code to high security and privacy standards in terms of data leakage during the development process.

Perhaps the most basic way to prevent data leakage is to transfer and store data in secure ways. This entails making sure that the information is encrypted and that when transferred, it is sent over secure SSL connections, such as over HTTPS (Schwartz). Caution must be paid to ensure that these techniques are being used everywhere. David Katz, quoting Vinny Sakore, writes about an app that stores users' insurance cards for convenient access, saying that "[a]lthough the app itself was encrypted, 'when it first downloaded the insurance card, it stored it in an area of the phone that was not encrypted … So [their researchers] found people's insurance cards — all the information, Social Security number, group I.D. number, member I.D. number, all that stuff.'" As the previous example illustrates, haphazard application of these techniques will not succeed in securing data.

Another basic and relatively easy way to at least minimize data leakage is to only collect data that your app actually needs. Do not ask for any permissions that are not necessary to your application's functionality, and don't abuse the ones that are necessary. It is also important to test your app for common security vulnerabilities, such as man-in-the-middle attacks ("Leaky Apps"), since these attacks may be used to steal the data your app is transferring.

When adding advertising to your application or using an analytics service for telemetry, carefully review how the service's security and privacy practices (Fairchild). The company behind Angry Birds, for instance, alleges that the aforementioned leaks to the NSA might have been the

fault of advertising networks (Schwartz). Needless to say, analytics services inherently often handle a large amount of users' data and data about the application itself. Thus, they can be a center of vulnerability with potentially devastating risk should they be compromised. It is also important not only to consider how the analytics service you use might be handling your data, but also to be mindful of the data you provide it with.

Even if the analytics service is relatively secure, collecting unnecessary information about users is a huge privacy violation. To continue with an earlier example, imagine you are building a photo-editing application. As someone who cares about how your users are using your app, you might want to collect statistics about how often they edit photos with your product. Privacy concerns might arise if, for example, you did this by keeping a log of the titles of the image files. You do not need the image titles to determine how often your app is being used. Rather, you just need a simple count of the number of images being edited, not any information about the images themselves. While collecting this extra information is in itself a privacy violation even if the data does not get leaked, collecting extraneous information also heightens the potential damage that could be caused should any data be leaked.

Conclusion

Data leakage is a pervasive problem in mobile applications and, given the widespread use of smartphones, poses enormous privacy risks for both consumers and enterprises. While there are steps app users can take to reduce the likelihood that their data is leaked and should be aware that any information an application has access to may become compromised, ultimately the responsibility for reducing data leakage lies with developers. Any time data is being stored, accessed, collected, or transferred, deliberate and thorough care must be paid to ensure that the data is being handled as securely as possible. Furthermore, thought must given to whether that data needs to be handled at

all. After all, the only way to be completely confident that a piece of information will not be leaked while being transferred is not to transfer it. Attention to security and privacy issues must be paid during the development process, not merely as an afterthought. Data leakage is a problem that affects everyone who uses or creates mobile apps and has the potential to cause significant damage to users, enterprises, and developers.

Works cited

Fairchild, Charlie. "Mobile App Development: 5 Worst Security Dangers." *InformationWeek*. 18 Apr. 2014. Web. 7 Dec. 2015.

Hoog, Andrew. "A Data Spill from an Oil Rig: Protecting Mobile Devices from 'Leaky' Apps." *Breaking Energy*. 23 Apr. 2015. Web. 7 Dec. 2015.

Hoog, Andrew. "Leaky Apps Are the Gateway to Risk Flood." *Mobile Enterprise*. 23 Nov. 2014. Web. 7 Dec. 2015.

Katz, David. "Beware of Leaky Apps." *CFO*. 6 May 2015. Web. 13 Dec. 2015.

Schwartz, Matthew. "Angry Birds Site Toppled After Surveillance Report." *Dark Reading*. 29 Jan. 2014. Web. 13 Dec. 2015.

"What To Do About Leaky Apps." *CyberTrend*. 8 Sept. 2015. Web. 7 Dec. 2015.