veracode.com

AdiOS: Say Goodbye to Nosy iPhone Apps

By Mark Kriegsman

5-6 minutes

Over the past week there have been a few big stories on iOS apps transmitting users' address books as a convenience feature. Apple has even found themselves on the congressional hot seat this week about their device's address book privacy. AllThingsD reports that Apple, faced with growing criticism that they have given iOS developers far too much access to private data without requiring a user prompt, has pledged that apps dumping address book data will soon require explicit user permission to do so.

Dieter Bohn at The Verge states the problem best: "Any iOS app has complete access to a large amount of data stored on your iPhone, including your address book and calendar. Any iOS app can, without asking for your permission, upload all of the information stored in your address book to its servers. From there, the app developer can either use it to help find your friends, store it in perpetuity, or do any number of other things with it."

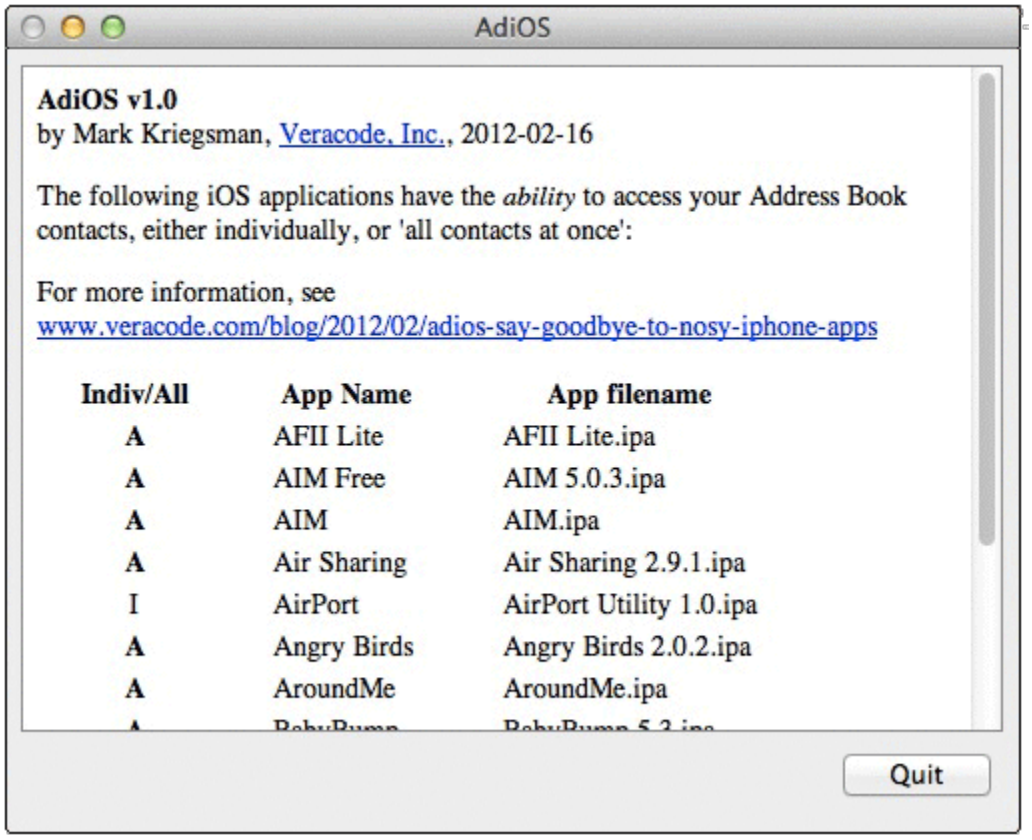
Introducing AdiOS

To find out how many of my iPhone apps were dumping the address book, I put together a utility called AdiOS (Addressbook Detector for iOS) that lets Mac users scan the iOS apps in your iTunes directory to see if they have the potential to dump your phone book externally. AdiOS detects apps that access your entire address book, by using a binary grep to look for use of the `ABAddressBookCopyArrayOfAllPeople` API call. AdiOS quickly and easily finds all the apps that have the potential to violate your privacy. It could also be used to see if your apps are complying with the new policies Apple is rolling out around protection of Address book information.

Using AdiOS to Audit Your Privacy

AdiOS allows Mac users to see what apps have potential privacy problems. Using AdiOS is easy. Just download AdiOS, unzip, double click on AdiOS.app, and let it run. If you have a few hundred apps, it'll take a couple minutes to complete.

Output will look something like this:



What We Discovered

A few of us in Veracode just tested AdiOS on our own machines. Of the roughly 450 iOS apps on my Mac, 50 of them appear to call `ABAddressBookCopyArrayOfAllPeople`. That by itself doesn't mean the app is transmitting any data, or doing so behind your back, but it does raise questions. Angry Birds does it. Citibank does it. Several Google apps do it. A number of lesser-known games do it, too. Why do all of these apps need to dump my entire address book? The quantity of apps with this ability really caught us off guard.

Most apps that have email functionality (e.g. "send this to a friend") wouldn't ever need to use `ABAddressBookCopyArrayOfAllPeople`. They could just use the standard view controller for contact info, the

`ABPeoplePickerNavigationController`. If they wanted a custom UI for the picker, then they have no choice but to dump the address book.

In order to check whether the app is actually transmitting the address book information, you'd need to perform a full static analysis, or a manual test using a tool such as mitmproxy.

Don't Panic!

Lots of apps access your whole contact list for legitimate reasons! Social networking apps do it so you can make connections. Maps/directions/GPS apps do it for convenient access to all of your friends' addresses. Many games do it so that you can "share your highscores", etc. But still, it's interesting to see which apps have the potential to do what with your personal address book data.

Should We Really Be Surprised?

Talking to the Veracode Research team about this iOS address book madness, the consensus was that none of this should come to a surprise to anyone who's been following mobile development or security research for mobile platforms.

At Veracode, we've already detected this issue in some of the mobile applications that we've scanned for our customers. More importantly, we can automatically determine if the app is actually transmitting the address book information once it has been retrieved. Obviously that requires much deeper analysis than this quick binary grep tool can provide! The deep static binary analysis service that we offer our customers uses data flow

graphs to connect the output of `ABAddressBookCopyArrayOfAllPeople` with downstream network APIs in order to confirm a privacy leak.

Along with running AdiOS, consumers of mobile apps should ask their providers to perform binary static analysis on the apps they offer.

Mark Kriegsman, Director of Engineering, is responsible for leading the development of Veracode's flagship static binary analysis system. In addition to providing direct technical leadership, he also works closely with Veracode's Research and Product Management teams to refine and improve Veracode's product offerings. Mark is a lifelong innovator and entrepreneur, with over twenty-five years experience in advanced software and systems development.