PHYS ORG

Researchers show Android devices susceptible to eavesdropping

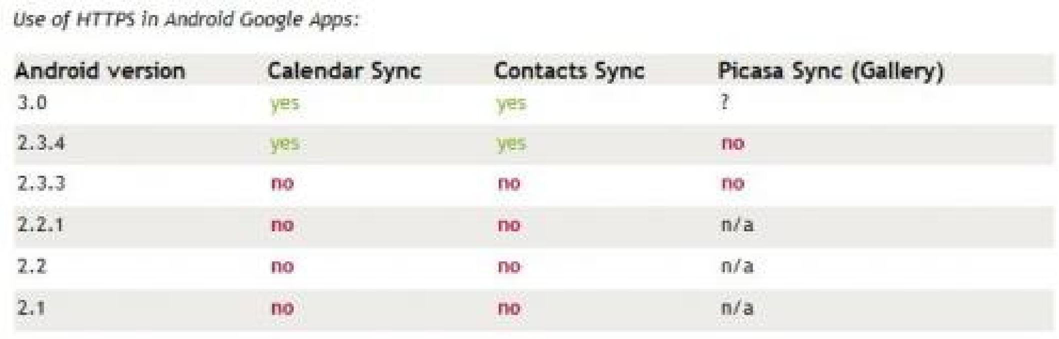
May 18 2011, by Bob Yirka

(PhysOrg.com) -- Following up on research done by Dan Wallach of Princeton University, that suggested Android devices were susceptible to an eavesdropping risk on open WiFi networks, German researchers Bastian Könings, Jens Nickels, and Florian Schaub have shown that by using commercially available software (Wireshark) they were able to listen in on an open WiFi network and gain sufficient information to impersonate a legitimate user. Posting their results on the University of Ulm website, they describe how they were able to obtain access to Google calendar and contact data as well as Picasa images via the capture of authentication tokens.

In a February 22nd University Center for Information Technology Policy, blog post, Wallach, remarked on how as part of a security class he was taking, he discovered that by sniffing data traffic coming to and from his Android smartphone using both Wireshark and Mallory, he was able to easily see Google calendar transactions and how easy it would be for someone to grab some of that information to impersonate him on Google applications.

The German research team, after seeing what Wallach had found, decided to look a little deeper; they found that because Android phones use tokens, called authTokens, that allow legitimate users to remain logged into certain Google applications for up to two weeks, that are unencrypted; nefarious characters listening in could capture those tokens and then use them for their own illegitimate purposes, such as scraping calendar information, contact email addresses or to view private images in Picasa.

In some respects, many might not see such a breach as all that big of a deal; it's not like Google is passing around bank account codes willy-nilly, but, that's beside the point. What's important is that Google, a huge company with vast resources and staffed with some of the best in the business, clearly knew and understood what it was doing when it chose to use plain text messaging as the means for transmitting it's authTokens; a move that demonstrates wanton disregard for the privacy of it's user community; something that the company is already in hot water over due to the recent discovery that it has been tracking users movements via GPS.



Use of HTTPS in Android Google Apps:

Android version	Calendar Sync	Contacts Sync	Picasa Sync (Gallery)
3.0	yes	yes	?
2.3.4	yes	yes	no
2.3.3	no	no	no
2.2.1	no	no	n/a
2.2	no	no	n/a
2.1	no	no	n/a

And while this issue will eventually go away as users upgrade the software on their phones, something else is rather important here, and that is the means by which this news has come to the fore, i.e. through a grad student taking an undergraduate course, basically just fooling around with sniffing software. This quite naturally begs the question of, what else is at risk? If there is no organization or agency testing the products that are sold by huge companies to users, how can we know that the things we do are safe from those who might wish to steal our data, impersonate us, or worse use the things they find against us, such as disseminating embarrassing pictures we thought were safely tucked away under password protection on [Picasa](https://phys.org)?

Citation: Researchers show Android devices susceptible to eavesdropping (2011, May 18) retrieved 27 April 2024 from https://phys.org/news/2011-05-android-devices-susceptible-eavesdropping.html