Appthority discovers app developers hard coding credentials into mobile applications using Twilio, putting users at risk

November 10 2017, by Bob Yirka

Credit: CC0 Public Domain

(Tech Xplore)—A team at Appthority, a threat protection company, has found that many app developers have been hard-coding credentials into products that use Twilio communications services. Doing so, they note makes it relatively easy for hackers to gain access to communication services such as calling and texting. The company has published its findings on its website.

One of the basic ideas in computer science is to use code that has been written for more than one purpose—a simple procedure or function that does one simple thing, such as adding two numbers together, gives other programmers the same functionality without rewriting code. All they have to do is invoke the procedure using unique parameters. Over the past several years, this concept has been expanded to work between companies—one company can write procedure code that another can use if it licenses the software.

Twilio is one such company. It writes code that accesses and makes use of the communications abilities of mobile devices—other companies than license that software and use it in their own applications. The means by which the new apps interact with the software from Twilio is through APIs, which send credentials (information identifying the app as a lawful user). But, as Twilio notes on its website, app developers are expected to use a non-hard-coded means of storing those credentials (such as storing them in a separate encrypted file). As it turns out, however, many app developers have taken a shortcut and coded the credentials right into their app code. That means that a hacker breaking the app code can very easily access the credentials and use them to gain access to user communication services.

Appthority reports that they have found over 700 apps with the security risk, including 170 of which are currently in official app stores. This, they note, means that millions of users around the globe are currently at risk. Communication services at risk, they further report, include records that keep track of calls, such as the duration of saved recordings—and more importantly, the contents of SMA and MMS text messages.

Citation: Appthority discovers app developers hard coding credentials into mobile applications using Twilio, putting users at risk (2017, November 10) retrieved 20 March 2024 from https://techxplore.com/news/2017-11-appthority-app-hard-coding-credentials.html