Researchers successfully attack Android through device’s speaker

A group of researchers from the Chinese University of Hong Kong have demonstrated that even applications with zero permissions can be used to launch attacks that allow attackers to forge text and email messages, access private information, receive sensitive data, and even gain remote control of the targeted device.

Tested on a Samsung Galaxy S3, a Nokia N82 and a Motorola A953, their "DVS-Attack" was successful independently on whether the device was running the vendor’s official Android version or CyanogenMod OS.

"DVS-Attack utilizes an Android system built-in voice assistant module – Google Voice Search." They explain in a paper, and invokes the device’s speaker.

"Through Android’s internal mechanism, VoiceEmployer (their prototype attack app) triggers Google Voice Search to the foreground, and then plays prepared audio files like ‘Call number 1234 56798’ in the background. Google Voice Search can recognize this voice command and execute corresponding operations."

The researchers have also discovered a vulnerability of status checking in the Google Search app, which can be exploited by the DVS-Attack to make the device call arbitrary malicious numbers. This can be executed even when the device is locked and secured with a password, ideally in the early hours of the morning, when the device owner is more likely to be asleep.

In order to execute the attack, a malicious app – in this case the victim’s VoiceEmployer – has to be installed on the target’s phone and run.

Users who don’t block their phones are even in more danger, as the data contained on their device can be transmitted to the attacker, and he or she can gain control of the victim’s Android phone remotely.

The malicious app is able to do all this by bypassing a number of Android permissions (Read Contacts, Write SMS, Send SMS, Vibrate, Set Alarm, Get Accounts, and so on).

"DVS-Attack can trick a malicious number through playing a call. … when this call is answered by an auto call recorder module, actually the data transmission channel has been built. Any audio type of data can be transferred through this channel instead of commonly-used Internet connection," they explained.

It’s also interesting to note that a number of popular mobile apps weren’t able to detect VoiceEmployer as malicious.

"Through experiments, the feasibility of our attack schemes has been demonstrated in the real world," they concluded, adding that they hope that their research will "inspire application developers and researchers to rethink that zero permission doesn’t mean safety and the speaker can be treated as a new attack surface."

More about

Android variability

Share this article

Android Fake ID bug allows malware to impersonate trusted apps

Researchers successfully attack Android through device’s speaker

Continuous monitoring for enterprise incident response

Don’t miss

Endpoint breach prevention by reducing attack surfaces

Telecom services. Failed zeros for email-based attacks!

Rising the security myth: How can you protect your website?

New in tech products of the week: August 17, 2016

eBook: Windows PowerShell Scripting Tutorial

SUBSCRIBE TO OUR FREE MAGAZINE

Newsletters

Weekly newsletter Daily newsletter

Copyright ©2019 by Help Net Security. Need re-publication? About us Contact Advertising