Formulärets överkant

Formulärets nederkant

[EVENTS](http://fairfaxevents.co.nz/)

**onsdag, 03 april 2013**

Dirty smartphones: Devices keep traces of files sent to the cloud

When smartphone users upload files to cloud-based services, remnants of those files often remain on their handheld device, even if the data is meant to be stored only in the [cloud](http://www.networkworld.com/topics/cloud-computing.html), researchers have found.
The consequence is that hackers could potentially access files stored in the cloud, or get access to cloud accounts, using leftover data stored on your [Android](http://www.networkworld.com/slideshow/71827/android-turns-five-a-look-back.html) device, [iPhone](http://www.networkworld.com/slideshow/25506/5-years-of-iphone-evolution-of-a-game-changer.html) or other smartphone.
"That [smartphones](http://www.networkworld.com/slideshow/66430/the-top-17-smartphones-from-the-major-carriers.html) can essentially remember deleted information poses a huge risk to organizations that issue smartphones to employees and to organizations that don't explicitly disable the use of personal devices for work-related computing," says Pravin Kothari, founder and CEO of Cipher Cloud, a maker of cloud encryption software.
The tracing of leftover data on smartphones is not for the layperson, Kothari says, but could be looked at as the modern-day equivalent of Dumpster-diving for personal information.

Researchers at the University of Glasgow ran a variety of tests to come to their conclusions. Phones tested included the HTC Desire, running Android 2.1, and an [iPhone](http://www.networkworld.com/news/2013/031513-iphone6-rumors-267757.html) 3S running iOS 3, and cloud-based file storage systems tested included Box, Dropbox and SugarSync.
A hard reset of the phones being tested was done before 20 files were created on each of the devices, including images, documents, PDFs and music files. Researchers then "manipulated" the phones, by either powering them off, caching the [applications](http://www.networkworld.com/topics/applications.html) or both. As a control, some of the phones were left in active state without any caching. Researchers then did a "data dump" of the phones by copying the memory onto a flash drive, which they then analyzed.
Researchers found a variety of metadata leftover after the files had been uploaded to the cloud services. Email addresses of users and transaction logs of which files were uploaded to the cloud were visible, for example. Researchers said they were even able to piece together various metadata to get a URL address of where a file was located in Box's cloud. Researchers also found that all files marked for "offline access" were able to be recovered from both the Android and iOS devices. Even some deleted files were still traceable on the SD card of the Android device.

Files were recovered from both the Android smartphone and its SD card, while the recovered data from the iOS device was recovered from the phone's internal memory (the iPhone 3S does not use an SD card).

In most circumstances, the researchers found that if the applications had been cached, then recovering the files was more difficult, except for when using Box on the iOS device, in which case the same number of files was able to be recovered even after caching.

"Smartphone devices which access cloud storage services can potentially contain a proxy view of the data stored in a cloud storage service," the research concludes. Accessing the proxy data can lead to further data being exposed, they add. Files that were not viewed on the smartphone, but were in the user's cloud storage account, could not be recovered, although in some cases a thumbnail of a JPEG that had not been viewed on the phone was able to be seen.

Researchers say a variety of tools can be used to extract data from a smartphone, including products from private company Cellebrite, which makes the Universal Forensics Extraction Device (UFED). Micro Systemation's XRY makes another tool for forensic detection of data.

In response, a spokesperson for Box pointed out that the researchers were using outdated versions of the company's mobile application (Android Version 1.6.7 and iOS Version 2.7.1), which are both almost a year old. Since then, Box has begun encrypting all files that are saved for offline use. The current Android app has automatic encryption and the [Apple](http://www.networkworld.com/slideshow/72925/the-apple-family-tree-apple-platforms-through-the-years.html) version has a feature to enable encryption. Previews of files are always encrypted, Box added.
Researchers admit further testing would be needed to determine how widespread of a vulnerability this is on newer devices, operating systems and cloud platforms.

Kothari, from CipherCloud, says there are steps IT managers can take to prevent corporate data used on smartphones from being tracked by hackers. For one, encryption tools like CipherCloud's can be used in addition to or in replacement of whatever [security](http://www.networkworld.com/topics/security.html) measures cloud service providers offer. Data loss prevention (DLP) and audit monitoring services can also be used to ensure employees are not accessing sensitive information on their smartphones, ensuring that it never gets on the smartphone in the first place and therefore cannot be recovered by a hacker later.