Google to boost Android encryption, joining Apple (Update)

September 18 2014, by Glenn Chapman

The Google Nexus 7 Android tablet, made by Asus is displayed during an event on July 24, 2013 in San Francisco, California

Google and Apple on Thursday said they are hardening encryption tactics on devices powered by their mobile operating systems and tossing away the keys.

The move should mean that even the government with its court-issued warrants will be blocked from getting hold of pictures, messages and

other personal data stored on forthcoming Android or Apple smartphones and tablets.

Google and Apple are among Internet titans intent on firming up trust shaken by revelations of massive online spying by US officials and by the recent hacking of celebrity iCloud accounts that exposed nude photos.

A Google spokesman told AFP that encryption is already offered for the Android system on smartphones and tablets, but will be turned on automatically in the upcoming version of software.

"For over three years Android has offered encryption, and keys are not stored off of the device, so they cannot be shared with law enforcement," the spokesman said in a statement.

"As part of our next Android release, encryption will be enabled by default out of the box, so you won't even have to think about turning it on."

Google has not said when the next update of Android is due for release.

Apple announced that its new encryption is built into the iOS 8 operating system available on the iPhone 6, which goes on sale Friday. It also can be installed on many existing iPhones and iPads.

Apple is essentially allowing people to lock iPhones, iPads or iPods using encrypted passwords without giving itself any keys.

"Your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders, is placed under the protection of your passcode," says the new policy on Apple's website.

"Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8."

Internet spying scandal

Leaked documents from former National Security Agency contractor Edward Snowden have highlighted concerns about the role of major tech firms in government spying programs.

Internet titans including Facebook, Microsoft, Apple, Yahoo and Google have been campaigning for the freedom to let people know more about requests made under the auspices of anti-terrorism law that mandates such queries be kept secret.

Apple's chief executive Tim Cook said the company is dedicated to protection of personal data and that security at iCloud was beefed up after photos stored online were pilfered from celebrity accounts.

The Cupertino, California-based company insisted there was no breach of its cloud storage system, but that hackers used "targeted attacks" aimed at celebrities.

An Apple statement suggested that the celebrities had their accounts hacked by using easy-to-guess passwords, or by giving up their personal data to cybercriminals posing as Apple, a technique known as "phishing."

Companies say they are required to comply as best they can with legitimate court orders and other legal requests, but fight for people's privacy along the way.

"We have never worked with any government agency from any country to create a backdoor in any of our products or services. We have also never allowed access to our servers. And we never will," Cook said.

Privacy activists praise the effort and hope more Internet firms will follow suit.

"This is very awesome for privacy," Joseph Hall, chief technologist at the Washington-based Center for Democracy and Technology, said of Apple encrypting passwords.

"This is an important assurance for people. It's not security just some of the time, it's security all of the time."

Hall added that the move is "good for the industry because there is a real deficit of trust" after the celebrity photo hacking.

Outstanding issues

Marc Rotenberg, president of the Electronic Privacy Information Center, said it was "good news for Internet users."

But Rotenberg said other privacy issues still need to be addressed, notably how Apple handles personal data for its HealthKit system for fitness monitoring.

"The issue is the flow of user data to the app developers," Rotenberg told AFP. "Apple has created a platform that can allow for the transfer of sensitive medical data."

Jeffrey Chester at the Center for Digital Democracy also expressed caution.

"Apple at the moment is serving as a data collection 'middleman,' as it builds a new business as a financial and health data supplier," Chester said.

© 2014 AFP

Citation: Google to boost Android encryption, joining Apple (Update) (2014, September 18) retrieved 5 May 2024 from
https://phys.org/news/2014-09-google-boost-android-encryption-apple.html