Hacker Lexicon: What Is Full Disk Encryption?

Author: Kim Zetter.Kim Zetter Security
WIRED | 2016-07-02

There's been a lot of talk in recent years about encryption and what the FBI terms its "Going Dark" problem—its inability to read the communications of surveillance targets because more and more data is being encrypted. And while the end-to-end messaging encryption that protects data in transit in apps like WhatsApp get a lot of press, it's a problem that applies equally a data at rest. The kind that full-disk encryption is designed to protect.

That type of protection did get significant attention during the recent FBI-Apple battle over protected data on the San Bernardino shooter's iPhone. In fact, it turned out to be an unintentional marketing coup for the tech giant, highlighting the strength of the company's encryption scheme for data stored on its mobile devices. Neither the FBI nor Apple could bypass the password lock on the iPhone without undoing the disk encryption Apple employs on the latest versions of its devices.

That's apparently not the case with Android devices. A story this week reveals that the full disk encryption in the Android operating system can be broken with brute-force attacks—which involves using a script to send thousands of password guesses to a device to determine the correct one that unlocks the encryption.

Full disk encryption, also known as whole disk encryption, protects data that's at rest on a computer or phone, as opposed to email and instant messaging data that's in transit across a network. When done effectively, it prevents any unauthorized person, including phone and computer makers themselves, from accessing data stored on a disk. This means that if you leave your laptop or phone behind in that Uber driver's car, or some shifty government agent tries to access your computer at an airport or other border crossing, they won't be able to get at your data without your help—even if they remove the hard drive and place it in another machine.

Full disk encryption comes built into all major commercial operating systems; a user simply has to opt to use it and choose a strong password or phrase. To access a system locked with full disk encryption, the user is prompted, after turning on the device but before it boots up fully, to enter that password or phrase. When entered, that password unlocks an encryption key in the system, which in turn unlocks the system, and gives you access to it and your files. Some full disk encryption systems require two-factor authentication, prompting the user to enter not only a password but to slip a smart card into a reader connected to the computer, or enter a number generated randomly by a security token.

Full disk encryption differs from file encryption in that the latter only encrypts individual files you specify for encrypting. Full disk encryption protects all data on a system, including the operating system. But it only protects the system while it's turned off. Once an authorized user logs in to the computer, this unlocks the full disk encryption, leaving data and system files exposed to anyone able to access the computer while the user is logged in, unless the user manually encrypts individual files as well. It also doesn't protect systems from being attacked by hackers over the internet. It only protects against someone who gains physical access to your device.

Even then, it's not necessarily ironclad. An encryption system only works as well as its design. A system that uses weak encryption or that contains vulnerabilities in how it encrypts the disk provides a false sense of security. The recent Android vulnerability illustrates this

problem. Flaws in the kernel of the Android operating system—and in the Qualcomm processor used in millions of Android devices—undermine the Android disk encryption system.

Still, occasional vulnerabilities aside, full disk encryption is one of the most important tools in securing the data on your devices.

Go Back to Top. Skip To: Start of Article.

read:https://www.wired.com/2016/07/hacker-lexicon-full-disk-encryption/