# The Logic of Open DRM

February 7, 2007

Original link

---

In his recent essay, Thoughts on Music, Apple CEO Steve Jobs has called for the labels to stop requiring him to sell their music with DRM. Most of his argument is that the labels already sell the vast majority of their music perfect digital copies without DRM — namely, CDs — but he also argues that the alternative of having an "open" DRM system is impossible.

Jobs is less than clear here. He writes: "There is no theory of protecting content other than keeping secrets. In other words, even if one uses the most sophisticated cryptographic locks to protect the actual music, one must still 'hide' the keys which unlock the music on the user's computer or portable music player. No one has ever implemented a DRM system that does not depend on such secrets for its operation."

Since this is a fairly important point and no one else is explaining what he means, I thought I'd give it a try.

DRM works by encrypting songs. Encryption works by performing a mathematical scrambling operation that can only be reversed with the right "key". As a very simple example, imagine you have the message "hello" and the key "5". One simple encryption system is to simply move each letter five letters forward (so "a" becomes "f") and you get "mjqqt". To decode it, you just need to know the number 5 and move each letter back that far. (This is a very bad encryption system, for a lot of reasons, but it works the same basic way as the good ones.)

The way DRM works, essentially, is that when you buy a song from the iTunes store it's encrypted with a certain secret key (presumably one a lot bigger than the number 5). To play the music, you need the key to decrypt it. But the only software that has the key is iTunes and iTunes will only decrypt it if you're following their rules — only playing it on 5 separate machines, for example.

For "Open DRM" to work, Apple would need to give the key to other people who made music players. But as soon as Apple gives the key to someone, they can do whatever they want with the music. If the key gets out on the Internet, anyone can decrypt the songs. DRM only works because the key is secret. Open DRM is an oxymoron.