

Re: DRMTICS 2005 Call for Papers

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-05/1126.html>

From: Francois GRIEU (*fgrieu_at_francenet.fr*)

Date: 05/27/05

Date: Fri, 27 May 2005 10:11:23 +0200

In article <1pfxtae9gtb9f.dlg@news.cis.dfn.de>, Sebastian Gottschalk <seppi@seppig.de> wrote:

- > *DRM works like this:*
- > a) *Encrypt the file.*
- > b) *Give the user the encrypted file, the decryption key,*
- > *the decryption algorithm and some software which obfuscates*
- > *the issues.*

Not quite all academic DRM proposals work like this. Some are

- embed identification of customer in the (say audio) file, in a manner that it is inaudible but hard to remove/detect without the proper key, or lowering the (audio) quality.
- explain to the customer that if the file leaks in breach of the contract, the embedded ID will allow tracing of the culprit.

Secure unremovable identification is not bound to be security thru obscurity. Consider this overly simplified scheme

- a secret key, known only to provider, is expanded using a good block cipher in CTR mode into a bitstream with as many bits as there are samples in the audio file.
- ID is encoded into a bitstream i , with one bit of the ID coded on many (say $n=2^{16}$) identical consecutive bits of i .
- audio is combined with bitstream: $s' = s + g * ((b^i) - 0.5)$ for some appropriate gain g .

Provably, the ID nor the bitstream can not be recovered without the key, or breaking the cipher. For some appropriate g , with knowledge of the key, the ID can be recovered (modulo synchronisation problems), even without knowledge of the original S , and even with lots of noise digitally added. Small variations of this scheme will survive a low pass-filter or analog recording. Much more complex variations may survive mp3 encoding.

Note: the above simple scheme is very vulnerable to a collusion of users buying the same music; this is meant as an illustration only.

François Grieu