

Re: DRMTICS 2005 Call for Papers

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-05/1135.html>

From: Francois GRIEU (fgrieu_at_francenet.fr)

Date: 05/27/05

Date: Fri, 27 May 2005 13:31:33 +0200

In article <1ojdnrwe31sbj\$.dlg@news.cis.dfn.de>, Sebastian Gottschalk <seppi@seppig.de> wrote:

> > *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 (modulus*
> > *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.*
> >
> *It will not survive applying the same scheme some additional times*
> *to the audio.*

I believe it survives applying the same scheme many times by someone ****without**** the key. It all works because the receiver is able to use its knowledge of the key to cancel-out undesired signal (such as noise, re-inscriptions, and s if it is unknown). BTW, the decoder computes

$$i' = \text{sign}(\text{sum}((s' - s) * (b - 0.5)))$$
with 'sum' over the n samples coding the same bit of ID.

[If s is unknown, make $s = 0$, or some approximation of s by appropriate processing of s']
The process is reminiscent of the correlation in a DPA attack.

The process I outlined does not survive a collusion of a few users to merge their tagged version of the same bitstream to reconstruct an un-tagged (or worse, miss-tagged) version. Also, I skipped many details (for example, the coding used for ID must survive a polarity change; and the decoder not knowing s in advance will have a hard time achieving synchronisation).

> *As far as we know there can't be any such scheme that would*
> *survive both psychoacoustical encoding and re-embedding.*

Any pointer to recent authoritative literature on this ? I stopped looking at watermarking after 1999 (I then briefly worked on a demo of a music distribution system with plans to use watermarking when it would work).

François Grieu