

Re: A Media Distribution Problem

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-05/5468.html>

From: Simon Johnson (ckwop_at_hotmail.com)

Date: 05/30/04

Date: Sun, 30 May 2004 21:44:13 +0000 (UTC)

"Andrew Swallow" <am.swallow@eatspam.btinternet.com> wrote in message
news:c932m8\$duf\$1@titan.btinternet.com...

> *Here is a theoretical problem that is likely to become real in
> a few months time.*

>

> *A supplier wishes to sell his goods by realtime downloading
> over the internet. The goods could be a TV channel or "radio"
> broadcast or constantly changing data like stock market prices.*

>

> *Real time TV over internet becomes technically viable at
> about 1.5 Mbps when compressed using MPEG4. Many of
> the readers of this newsgroup already own modems that
> fast, the phone companies have simply chosen to limit the
> line's speed.*

>

> *The supplier wants to get paid so he wishes to encrypt
> his signal. To minimise bandwidth he wants to multi-drop
> the signal; that is a common broadcast which everyone
> listens to. He suspects that a second server will be
> needed to handle the payment of subscription fees and
> automatic distribution of daily/hourly key variables.*

>

> *The supplier is willing to download a player to his
> subscribers. One file of which can be unique to each
> subscriber.*

>

> *Threats*

> *1. People may try and watch his shows without paying.*

> *2. Groups of people may take a single subscription and
> send copies of the key variable to the rest of the group.*

> *3. People may try and logon using someone else's identity.*

> *4. Payment is to be via PayPal, credit card and phone
> type cards purchased at shops. These need transferring
> over the internet from the subscriber to the supplier in
> a secure manner.*

> *5. Interference and lost packets may require the subscribers
> to individually resynchronise the signal.*

>
> *Andrew Swallow*
>

In general there is no way to do this. It's copy protection and it's fundamentally impossible to protect against.
At the end of the day, regardless of the protections on that data during in transit that protection is stripped off so that you can actually view the video. There will always be a way to obtain that unprotected data..

The most we can do is make it non-trivial to copy the data but with computers this is even harder. A very difficult and highly technical attack can be packaged into a small 133tware program that any script-kiddie could use.

I propose that rather than trying to defend against copying itself a better approach is to forget about protecting against copying but be sure you can catch the copiers when they copy. This is a much easier problem. If you can run some code on the video stream before you send it to the client you can imbed a watermark that's provably undetectable and robust [1]. The system would be configured such that each of your users will have a watermark imbedded on the fly. Each user's watermark would be different and the media would be streamed to them using an encrypted channel.

The next phase is to use the copyright law in conjunction with the set-up. While computer science is generally bad at defending copyrights the law (rightly or wrongly) is very good at defending copyrights. Ensure that in your Terms of Service you make the registered user liable for damages for any copies of the data streamed to them should they become available on the internet or by other forms.

Life is now a lot tougher if you decide to copy that data. Getting that watermark out is going to be tough. Robust steganography (as defined in [1]) means that you accept that an attacker may change the data in your communications channel to try an obfuscate any hidden message. It is designed repulse these kinds of attacks.

I'm fairly confident that even with quite drastic changes the watermark could survive. Remember that our watermark isn't war and peace. A 34-bit serial number would be able to uniquely identify every person on earth for the foreseeable future. We could embedded this 34-bit serial number over and over in the media stream. I recon that even if a clever attacker managed to re-encoded the video stream with a totally different codec enough artefacts of the original watermark would remain for you to convince a jury [2] of the original source of the file.

I believe copyrights can be vigorously defended on digitised media but it requires a blend of computer science and legal techniques.

Cheers,

Simon.

[1] –

<http://citeseer.ist.psu.edu/cache/papers/cs/26481/http:zSzzSzprint.iacr.orgzSz2002zSz137.pdf/hopper02provably.pdf>

[2] – Remember, civil cases don't have the same standard of evidence as criminal cases. In civil cases you only have to show the person is guilty on the balance of probabilities in criminal it's beyond reasonable doubt. I think this difference is crucial to the legal success of the scheme.