



## ¿ES POSIBLE LA IDENTIFICACIÓN Y AUTENTICACIÓN MEDIANTE «MARCAS DE AGUA»?

### El fenómeno Napster

Napster es uno de los ejemplos de lo que se ha dado en llamar sistemas basados en transferencias «peer-to-peer» o P2P. A partir del nacimiento de Napster han surgido y siguen surgiendo varias aplicaciones y protocolos<sup>1</sup> diseñados fundamentalmente para favorecer la colaboración e intercambio de todo

tipo de materiales entre los distintos agentes presentes en una red. Este tipo de cambio de planteamiento en la constitución y uso de Internet sin duda podría suponer una tercera revolución de Internet<sup>2</sup>. Estas iniciativas, aplicadas a redes públicas y abiertas como Internet, propugnan una Red más igualitaria, más horizontal, en la que no hay unos pocos grandes agentes polarizando las actividades y posibilidades de un montón de pequeños agentes, y esto puede dar lugar a modelos de comercio electrónico que no son los que se están considerando actualmente.

Pero no es en esto en lo que nos vamos a centrar en esta ocasión, sino en una cuestión que la prensa ha unido indisolublemente al fenómeno Napster: la protección de los derechos de autor. Es interesante ver si realmente es posible la protección del *copyright* sobre productos multimedia esencialmente digitales, si hay sistemas anti-copia eficaces, si es posible el control de uso de un objeto multimedia, etc.

### La SDMI

La iniciativa SDMI es un consorcio industrial cuyo objetivo es el desarrollo de una infraestructura de seguridad que permita la reproducción, almacenamiento y distribución controlada de música. El consorcio SDMI reúne a más de 200 compañías y organizaciones distintas<sup>3</sup> que van desde pequeñas empresas a grandes compañías multinacionales de todo el mundo y entre sus socios se encuentran los más importantes fabricantes de la electrónica de consumo, de las tecnologías de la información, de la música, y de las operadoras de comunicaciones móviles.

La tecnología de la SDMI sigue diferen-

**Durante los últimos años hemos visto cómo la distribución de registros musicales a través de Internet ha sido una de las actividades que más éxito ha tenido y que mejor ha enraizado en el día a día de La Red. Esto ha provocado la cólera de la industria discográfica y del entretenimiento en general, llevando a los titulares de los periódicos y revistas especializadas numerosos procesos judiciales en los EEUU. Uno de los elementos que se han propuesto para delatar a los culpables de la distribución ilegal es el uso de «marcas de agua» digitales que permitirían trazar e identificar los registros musicales que circulan por cualquier medio. Sin embargo, no está claro que esos sistemas sean realmente seguros o útiles para la defensa de los derechos de autor y eso es lo que nos planteamos en este artículo.**

tes enfoques para conseguir un mismo objetivo: no perder el control que hasta ahora ha tenido sobre los registros musicales. Así pues, ha puesto en pie una infraestructura física de seguridad, análoga a la de los sistemas anti-copia de los DVD, basada en el empleo de reproductores y expendedores con hardware específico de modo que los registros musicales no salen, en ningún momento, del control de los fabricantes de los equipos SDMI. El otro frente es la inclusión de «marcas de agua» de forma eficiente, robusta e inaudible que permita detectar la copia, intercambio e incluso uso no autorizado de cada registro musical.

Las marcas de agua son códigos que se incrustan en el registro musical para identificarlo y relacionarlo con su genuino dueño. Mientras que esos códigos son inaudibles para el oído humano, sí pueden detectarse automáticamente mediante monitores especialmente diseñados para ese fin<sup>4</sup>. Bajo las especificaciones SDMI, los suministradores de materiales multimedia tendrán el poder de marcar su producto con un conjunto de reglas de uso que establecerán qué puede hacer el propietario con ese producto. Estas reglas indicarán a los dispositivos con el sello SDMI, entre otras cosas, el número de veces que el contenido podría ser reproducido e incluso si está permitido reproducirlo.

Las marcas de agua son un ejemplo de la muy antigua técnica de escritura secreta, denominada «esteganografía» o «escritura oculta», que fue muy utilizada en tiempos pretéritos por griegos, hindúes, chinos y japoneses. El concepto actual equivalente es el de «canales subliminales», que son vías de comunicación secreta entre emisor y receptor a través de una

actividad que nada tiene que ver con la comunicación en sí y que, ante la observación de cualquier agente externo a ella, nada delata la existencia de tal comunicación. La posibilidad de montar canales subliminales en sistemas y protocolos criptográficos es bien conocida en el mundo de la Criptología civil desde hace ya casi una década.

La escritura oculta, al igual que los modernos canales subliminales, utiliza partes de la señal que transporta la información que son irrelevantes para ésta. Esas componentes, generalmente de «ruido», muy bien pueden ser sustituidas por mensajes en claro o incluso cifrados. Dado que no se ve afectada la información principal y mayoritaria —una atractiva fotografía, por ejemplo—, el observador no percibe su presencia y el mensaje permanece oculto. Aquellos que sí saben dónde buscar esos canales de comunicación pueden localizarlos fácilmente y desvelar la información que se transmite a través de ellos. Esta habilidad permite, entre otras cosas, el establecimiento de sistemas de «trazado» de los objetos de los que forman parte.

Para probar la solidez de sus sistemas de «marcado» el consorcio SMDI, a través de uno de sus directores ejecutivos, Leonardo Chiariglione, invitó a toda la comunidad Internet a romper sus sistemas de marcas de agua. Los resultados no se hicieron esperar, el 12 de octubre de 2000 en la revista digital Salon.com<sup>5</sup> y el 24 de octu-

<sup>1</sup> Scour, Gnutella, Frenet, etc.

<sup>2</sup> La primera fue la aparición del protocolo de conexión a través del transporte de paquetes de información (protocolo TCP/IP) y la segunda sería el nacimiento de la World Wide Web como tal gracias a la aparición del protocolo HTTP y del formato HTML.

<sup>3</sup> SDMI reúne al 90% de los propietarios de contenidos musicales

<sup>4</sup> La justificación del uso de estas técnicas de vigilancia radioeléctrica y de Internet es la protección de los derechos de autor y su dudosa aceptabilidad es una cuestión que se escapa a los objetivos de este artículo.

<sup>5</sup> 12 de octubre [www.salon.com](http://www.salon.com) ver el artículo [http://www.salon.com/tech/log/2000/10/12/sdmi\\_hacked/index.html](http://www.salon.com/tech/log/2000/10/12/sdmi_hacked/index.html)

bre a través de la agencia Reuters<sup>6</sup> se informó de que se habían roto todos los sistemas de marcas de agua de la SDMI. Un poco más tarde, unos investigadores de las universidades de Princeton y Rice, y del centro de investigación de Xerox en Palo Alto, anunciaron, a través de una página *web*<sup>7</sup> haber «crackeado» la tecnología de protección de los derechos de autor desarrollada por SDMI. Inicialmente, SDMI negó dichos éxitos.

Según esos investigadores, habían logrado hacer indetectables las marcas de agua que se habían incluido en los registros, sin degradar significativamente la calidad sonora de las muestras y, según ellos, el éxito de estos resultados lo pusieron de manifiesto los propios servidores de SDMI que no pudieron encontrar las marcas de agua sobre los ficheros previamente modificados por los atacantes.

### Lecciones del pasado

La industria de los ordenadores personales experimentó hace ya diez años que pretender proteger de copia el software no era algo técnicamente alcanzable y, desde luego, no cuenta con el beneplácito de los consumidores. La industria del software ha tenido que migrar hacia modelos más abiertos para la creación y distribución de software<sup>8</sup>.

Los adeptos al ocio digital, y en particular los consumidores de música y materiales multimedia, ya han puesto claramente de manifiesto su deseo de poseer, sin restricciones, copias de lo que han comprado. En lo que se refiere a la música, primero fueron las cintas magnéticas, después los cassettes, y por último el CD-R (tanto en formato cda como mp3) o el Minidisk. Uno podría pensar que la industria de la música podría tomar nota de lo aprendido por los empresarios del software y adoptar nuevos modelos de producción y distribución de música; sin embargo, no es así, los grandes de ese sector industrial prefieren defender el antiguo modelo de mercado frente a muchos de sus clientes, a los que no dudan en llamar «piratas» en el sentido más estricto y clásico de la palabra. Hasta cierto punto puede ser fácil justificar esta actitud tan básica en que los beneficios obtenidos durante la

última mitad del siglo que ha terminado, han sido abundantes y fáciles de conseguir.

### La situación española

La Sociedad General de Autores y Editores (SGAE) es una entidad muy activa en lo que a campañas para la detección del fraude contra los derechos de autor se refiere. De hecho son varios los proyectos en los que se ha lanzado al uso de las tecnologías más recientes para conseguir sus fines y en todos ellos parece utilizar «marcas de agua». Ejemplo de ello lo tenemos en el Proyecto Argos que es un «registro de uso» de los derechos de autor de obras distribuidas por medios electrónicos; todas ellas tendrán una «marca de agua» de forma que cuando la obra se difunda, su uso quedará registrado en el correspondiente centro Argos.

Hace ya más de un año, la SGAE y Verance Corp., fabricante de sistemas basados en marcas de agua, firmaron un acuerdo por el cual la SGAE utilizará la tecnología MusiCode® de Verance para «marcar» todas las piezas musicales y poder hacer un seguimiento en directo de su uso en radios, televisiones y emisoras de radio digital en Internet<sup>9</sup>. Para la decodificación la SGAE dijo en su momento que iba a instalar un sistema de monitorización capaz de analizar un 1% de las emisiones de radio y televisión en España. En el caso de Internet, desde hace tiempo la SGAE se dedica, mediante su «Araña», a localizar sitios *Web* que ofrezcan música «a la carta» de su jurisdicción, y les ofrece las correspondientes licencias para que regulen su posición.

Así pues, la industria discográfica española parece confiar plenamente en los sistemas basados en marcas de agua para la identificación automática de sus registros musicales y, a fecha de hoy, ya se ha demostrado públicamente la debilidad de tales planteamientos.

### Conclusiones

Las técnicas esteganográficas basan su eficiencia en no ser descubiertas por el atacante ya que su secreto es su esencia; si el atacante sabe dónde ir a buscarlas, siempre puede eliminarlas o alterarlas irreversiblemente. Utilizar «marcas de agua» en sistemas para la «detección de traidores» es algo clásico pero su correcto funcionamiento sólo se consigue en circunstancias específicas muy controladas. Estos sistemas no pueden funcionar en entornos tan abiertos y extensos como lo son la distribución de productos musicales o multimedia. De nada sirve intentar ponerle un

número de serie único a cada registro musical del mismo modo que se hace con las armas de fuego o los bastidores de los coches ya que, en aquel caso como en éstos, siempre es posible «borrar» o alterar dichos números haciendo no identificable al objeto. Intentar etiquetar a todas y cada una de las copias de registros musicales que hay en el planeta y, además, pretender que no existan y circulen versiones «incontroladas» de los mismos es algo realmente ingenuo que se ha demostrado del todo inútil en ocasiones anteriores.

El problema del control de copias es uno de los clásicos en los entornos de la seguridad informática y la Criptología moderna, y se han hecho algunas propuestas en esa dirección, pero eso no significa que sean soluciones reales para cualesquiera situaciones; incluso algunas, en sus mejores casos, presentan limitaciones importantes e insalvables. Por todo ello, es necesario tener mucho cuidado al elegir una tecnología criptográfica o de seguridad y, antes de nada, es preciso conocer y apreciar sus debilidades y limitaciones ya que «no es oro todo lo que reluce» en el mercado tecnológico moderno. La actualidad del problema de la protección de los derechos de autor hace florecer un montón de pretendidas soluciones de seguridad que realmente no lo son y se sabe.

Dado este panorama, la solución para las compañías discográficas o del entretenimiento no es probable que se encuentre en la persecución desesperada y desmesurada de la «piratería», ya que no cuenta con un arsenal técnico realmente eficiente para tal fin. Quizá sea hora de cambiar su enfoque del problema y encontrar otras soluciones para la defensa de los intereses de los autores y nuevas estructuras de distribución y tipos de negocio que hagan poco atractiva la piratería, sin intentar impedirlo por medio de sanciones de cualquier tipo.

No es tan difícil aceptar que Internet pueda estar cambiando el mercado de la distribución musical y que para sobrevivir las empresas del sector deban adaptarse a los nuevos aires. Nadie pudo haber realmente pensado que esto de las «Nuevas Tecnologías» y la «Nueva Economía» iba a ser una historia «de vino y rosas» para todos los sectores, por lo que la Industria del Arte debe encontrar su nuevo puesto en la sociedad que se nos avecina. ●

JORGE DÁVILA MUÑOZ

Laboratorio de Criptografía  
LSIIS - Facultad de Informática - UPM  
jdavila@fi.upm.es

<sup>6</sup> «They Did Too Hack SDMI Code». Reuters. 10:55 a.m. Oct. 24, 2000 PDT

<sup>7</sup> Ver <http://www.cs.princeton.edu/sip/sdmi>

<sup>8</sup> Por ejemplo, podemos encontrar el movimiento «open source».

<sup>9</sup> El primer uso de esa tecnología en nuestro país aparece en septiembre de 1998 cuando se publica el CD «Poeta en Nueva York» de Manolo Tena, cuyos registros contienen marcas de agua de Verance.