>> Jorge Dávila

¿A la seguridad a través de la ignorancia?

La legislación norteamericana parece estar en contra de los análisis independientes de seguridad y la difusión de sus resultados, ya que aplica literalmente el Digital Millennium Copyright Act (DMCA) de 1998. Se detienen y se llevan ante los tribunales a aquellos que encuentran un fallo en los sistemas de seguridad de grandes grupos de interés y, sobre todo, si lo cuentan públicamente. Microsoft llama al "*sigilo sacramental*" como mecanismo de cooperación de los expertos en seguridad, para combatir a los diseñadores y codificadores de virus y gusanos informáticos. Éstos y otros ejemplos aparecen desde hace cierto tiempo en los noticiarios de todo tipo y pueden indicar que el miedo provocado y la amenaza son parte nada infrecuente del escenario informático actual.

En 1998 la administración Clinton y el Congreso de los EEUU actuaron en representación de las compañías mediáticas presentando, defendiendo y aprobando algunas medidas legales que convierten en delito federal, entre otras cosas, la publicación de cualesquiera informaciones que pudiesen poner en riesgo la seguridad de cualquier software. A ese conjunto de normas se las conoce como el **D**igital **M**illennium **C**opyright **A**ct (DMCA)[1] y se justifica como un conjunto de medidas dirigidas a defender los derechos de las industrias editoras, cinematográficas y discográficas, principalmente.

Lo que en principio podría parecer bien a todos aquellos que acepten la existencia de la propiedad privada, quizá ya no sea tan bueno cuando esa misma normativa se refiere a lo que denominan "tecnologías para burlar límites o restricciones" o *"circumvention technologies"* si queremos referirnos a las fuentes. Por tales se entienden todos aquellos elementos, técnicas, códigos ejecutables, informaciones, y un largo etcétera de cosas que permitan, o que incluso pudiesen llegar a dar pistas de cómo poner en jaque un sistema de protección.

Ejemplos recientes de la debilidad de esas mal llamadas "medidas de seguridad" los encontramos en la protección anticopia de los DVD's, en el sistema WEP[2] de cifrado utilizado en redes inalámbricas[3], en el sistema de marcas de agua SDMI[4] para la protección de registros musicales, etc.

En todos estos casos, el análisis público[5] e independiente de cada uno de los sistemas ha llevado al desarrollo de herramientas, muy sencillas en la mayoría de los casos, que han echado por tierra la presunta seguridad declarada por sus promotores y fabricantes.

Eliminar el análisis independiente y público de la seguridad y resistencia real de cualquier producto es lo mismo que abrirle paso a productos defectuosos, mediocres e imprevisibles.

En el caso del SDMI, y dentro del reto público organizado por dicha fundación, a los participantes no se les aplicaría el contenido del DMCA ya que aquellos autorizan explícitamente el estudio de sus tecnologías. Sin embargo, el pasado mes de abril, el profesor Edward Felten y su equipo de investigación de la Universidad de Princeton, recibieron una carta[6] de Matthew J. Oppenheim, Vicepresidente de la RIAA[7], en la que se le recordaba que la publicación de sus descubrimientos sobre las debilidades de las tecnologías SDMI *"facilitaría y animaría"* al ataque de materiales con contenidos de *copyright* protegido, con lo que, de hacerlo, se pondría "a tiro" de la aplicación del DMCA.

Bien es cierto que se han publicado diferentes interpretaciones de la ley y que se han lanzado serias dudas sobre la constitucionalidad de la DMCA y su mismo significado, pero sigue vigente y no es sorprendente que algunos investigadores en este tipo de temas estén confundidos y hayan decidido no publicar ciertos resultados de sus investigaciones, por temor a ser perseguidos con el DMCA en la mano.

Un ejemplo para ello lo podemos encontrar en el caso de Dimitry Sklyarov, programador ruso de 26 años, que fue arrestado el 17 de julio del pasado año en Las Vegas, a la salida de una conferencia internacional; su delito era haber escrito un programa que rompía una protección de Adobe en su sistema de publicación electrónica (*e-books*). El Departamento de Justicia americano

1 La revisión en 1998 de las leyes americanas de protección de los derechos de autor, dio lugar a la norma que se conoce como *Digital Millennium Copyright Act*, y convierte en delitos federales ciertas acciones como burlar mecanismos de protección.
2 **W**ired **E**quivalent **P**rivacy algorithm
3 http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
4 **S**ecure **D**igital **M**usic **I**nitiative ver http://www.sdmi.org/
5 por ejemplo, en el caso del SDMI ver http://www.cs.princeton.edu/sip/sdmi/faq.html o http://www.theregister.co.uk/content/archive/14211.html
6 http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010409_riaa_sdmi_letter.html
7 **R**ecording **I**ndustry **A**ssociation of **A**merica,

acusó a Sklyarov de diseñar –aunque lo hizo en su calidad de empleado de la empresa rusa Elcomsoft– un producto para saltarse las medidas de protección del *copyright* diseñadas por Adobe.

El DMCA llama a las "cazas de brujas" y termina con doscientos años de tradición democrática americana en lo que a la defensa de los derechos de autor se refiere, y prohíbe taxativamente la ingeniería inversa y el "*cracking* de los sistemas electrónicos de protección".

Con el apoyo legal a las medidas hardware y/o software para la protección del *copyright*, esta ley pone la defensa de los derechos de autor en manos de los ingenieros informáticos y de las compañías que los contratan, y no en las cortes de justicia como sería de esperar en el ordenamiento institucional habitual de los países democráticos.

Con este tipo de leyes sólo se consigue criminalizar, que no impedir, algunos tipos de estudios básicos en unas tecnologías que pueden llegar a ser muy importantes, y esta actitud representa un buen ejemplo de la ingenua y funesta aproximación de "***a la seguridad a través de la ignorancia***", que mil veces se ha demostrado y se demostrará, ineficaz con el paso del tiempo.

El análisis "**independiente**" es un componente esencial en el diseño de los sistemas de seguridad, y el problema que representa el DMCA es que oculta dicho análisis y lo restringe a una *élite* discreta, en aras a proporcionar una cobertura legal suplementaria para los precarios sistemas de protección del *copyright* existentes.

El llamamiento de Microsoft

Por otra parte, Microsoft ha publicado un llamamiento[8] a la comunidad profesional dedicada a la seguridad para que no se divulguen los errores detectados en sus productos para, así, no proporcionar información gratuita a los *hackers* que después les permita explotar las debilidades del sistema. En ese llamamiento su autor razona la conveniencia de «no dar demasiados detalles sobre los fallos» que se detectan, y limitar al máximo la información que se proporciona a los administradores para que estos puedan «parchear» sus sistemas y poco más. Lo curioso es que este planteamiento se justifica en cuanto a la responsabilidad del fabricante de software frente a sus clientes y no frente a la denominada «*security community*».

Al mismo tiempo, Microsoft llama a la colaboración a esos mismos estudiosos que antes negaba, invocando a su madurez profesional para no causar el pánico en el sector informático. El escrito de Microsoft incluso reconoce que eliminar la, por ellos denominada, "*anarquía informativa*" no sería suficiente para evitar que surjan nuevos virus, gusanos, caballos de troya, etc., ya que "*la gente que escribe gusanos es bastante lista*".

La seguridad, en lugar de ser una característica deseable del software, de los servidores, de los datos y de los procesos a los que se someten, se está convirtiendo en la fuente de temores que pueden llegar a permitir cambiar cosas que no deben cambiarse.

El "culto al miedo"

Ambos ejemplos, el de las leyes DMCA y la iniciativa de Microsoft, son ejemplos de un curioso fenómeno que afecta actualmente a todas las actividades de nuestra sociedad y que, podríamos llamarlo, el "culto al miedo". La seguridad, en lugar de ser una característica deseable del software, de los servidores, de los datos y de los procesos a los que se someten, etc., se está convirtiendo en la fuente de temores que pueden llegar a permitir cambiar cosas que no deben cambiarse.

Eliminar el análisis independiente y público de la seguridad y resistencia real de cualquier producto es lo mismo que abrirle paso a productos defectuosos, mediocres e imprevisibles. Amenazar con el peso de la ley a aquellos que hagan público lo que cualquier otro también ha podido haber descubierto, limita lo que uno puede llagar a saber y fomenta el secretismo de élites "bien informadas" que se erigen inmediatamente en las que deciden lo que debe ser y no ser.

Ninguna medida que limite a los ciudadanos el acceso a información veraz, sea tanto en su calidad de clientes o usuarios, no puede ser buena para ellos y, por tanto, para los sistemas realmente democráticos.

Sólo tienen miedo al ojo público aquellos que tienen algo que esconder y quizá detrás de la campaña de Microsoft o en la misma esencia del **D**igital **M**illennium **C**opyright **A**ct lo único que haya sea un reconocimiento implícito de la incapacidad de la industria para producir sistemas operativos y aplicaciones suficientemente buenos y seguros como para no poner en riesgo a todo el sistema informático o de servicios que opte por utilizar dichos productos. Si los mecanismos para la protección de los derechos de autor no son buenos, mejor será reconocer este hecho que aceptar la pantomima de oscuros y secretos sistemas de protección que para nada sirven.

Ayer por la tarde, paseando por Madrid, me paré en un puesto de CD's cuyos bajos precios indicaban, sin lugar a dudas, que no podían ser "legales". Allí encontré, y en curiosa consonancia con su título, el último disco de Estopa, lo cogí para ver más de cerca lo cuidado de la reproducción de sus carátula y allí me encontré con un sello que decía "protegido contra copia" "no puede reproducirse en un PC"; no pude evitarlo, aquel descubrimiento se merecía una sonrisa. n

Jorge Dávila Muro
Director
Laboratorio de Criptografía
LSIIS - Facultad de Informática - UPM
jdavila@fi.upm.es

8 *It's Time to End Information Anarchy* por Scott Culp; octubre de 2001 http://www.microsoft.com/technet/columns/security/noarch.asp