Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de ATI (Asociación de Técnicos de Informática). _Novática_ edita también _Upgrade_, revista digital de CEPIS (_Council of European Professional Informatics Societies_), en lengua inglesa.

<http://www.ati.es/novatica/>
<http://www.upgrade-cepis.org/>

ATI es miembro de CEPIS (*Council of European Professional Informatics Societies*) y tiene un acuerdo de colaboración con ACM (*Association for Computing Machinery*). Tiene asimismo acuerdos de vinculación o colaboración con AdaSpain, AI2 y ASTIC

Coordinación Editorial y Redacción Central (ATI Madrid)
Padilla 66, 3º, dcha., 28006 Madrid
Tlf.914029391; fax.913093685 <*novatica@ati.es*>
Composición, Edición y Redacción ATI Valencia
Reino de Valencia 23, 46005 Valencia
Tlf./fax 963330392 <*secreval@ati.es*>
Administración y Redacción ATI Cataluña
Via Laietana 41, 1º, 1ª, 08003 Barcelona
Tlf.934125235; fax 934127713 <*secregen@ati.es*>
Redacción ATI Andalucía
Isaac Newton, s/n, Ed. Sadiel, Isla Cartuja 41092 Sevilla
Tlf./fax 954460779 <*secreand@ati.es*>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza
Tlf./fax 976235181 <*secreara@ati.es*>
Redacción ATI Asturias-Cantabria <*gp-astucant@ati.es*>
Redacción ATI Castilla-La Mancha <*gp-clmancha@ati.es*>
Redacción ATI Galicia
Recinto Ferial s/n, 36540 Silleda (Pontevedra)
Tlf.986581413; fax 986580162 <*secregal@ati.es*>
Suscripción y Ventas: <*http://www.ati.es/novatica/interes.html*>, o en ATI Cataluña y ATI Madrid
Publicidad: Padilla 66, 3º, dcha., 28006 Madrid
Tlf.914029391; fax.913093685 <*novatica.publicidad@ati.es*>

Imprenta: 9·Impressió S.A., Juan de Austria 66, 08005 Barcelona.
Depósito Legal: B 15.154-1975
ISSN: 0211-2124; CODEN NOVAEC

Portada: Antonio Crespo Foix / © ATI 2003

novática
UPGRADE
Revista de la Asociación de Técnicos de Informática

MAYO · JUNIO 2003
163

SUMARIO

Monografía del próximo número:
«Ingeniería del Software: estado de un arte»

Conocimiento abierto / *Open Knowlegde*

'Informática de confianza' y política sobre competencia: temas a debate para profesionales informáticos

Ross Anderson
Universidad de Cambridge

<Ross.Anderson@cl.cam.ac.uk>

Traducción: Alicia Díaz Migoyo

Este artículo se publica bajo la licencia *GNU Free Documentation License*y es una versión abreviada, especial para *Novática* y *Upgrade*, de un artículo titulado *«Cryptography and Competition Policy - Issues with 'Trusted Computing'»* que se puede encontrar en <http://www.ross-anderson.com/>.

Resumen: *el desarrollo estratégico más significativo que se ha producido en el último año ha sido 'informática de confianza' --en inglés* Trusted Computing *(o TC). En este artículo se describe a grandes rasgos qué es TC y se esbozan los efectos que pudiese tener en el sector informático y en las personas que trabajan en él.*

Palabras clave: *antimonopolio, atado de producto, control de accessorios,* copyright*, DMCA, EUCD, Intel, Microsoft, monopolio, Palladium, política sobre competencia, TCPA, TCG,* Trusted Computing.

1. Introducción

Uno de los problemas más complejos que tienen los profesionales informáticos es hacer frente a las estrategias de precios que los proveedores utilizan para sacarle hasta el último céntimo a su base de clientes. Los proveedores dominantes --como Microsoft hoy e IBM en la generación anterior-- intentan atar a los clientes a sus arquitecturas para ir extendiendo el control de un producto a otro. Muchos productos funcionan en ciclos que van «de ganga a timo»: una vez que has comprometido a tu organización con una determinada tarjeta inteligente, o paquete contable, los precios suben misteriosamente. Otra estrategia es la de atar productos, y un buen ejemplo son los cartuchos de tinta para impresoras. Son los cartuchos los que hacen rentables a estas impresoras: esta fórmula permite a los fabricantes utilizar el mismo producto para los grandes usuarios de las empresas y para los usuarios domésticos que miran más el precio. A esta subvención cruzada le ponían un cierto límite los cartuchos reciclados y los de otras marcas. Por eso ahora muchos cartuchos vienen con chips para que las impresoras los autentifiquen, una práctica que empezó en 1996 con la Xerox N24 (ver en [5] la historia de los chips de cartucho). En un sistema cualquiera, si la impresora detecta un cartucho de otra marca o un cartucho reciclado, puede bajar el rendimiento de 1.200 p.p.p. a 300 p.p.p., o incluso dejar de funcionar.

Más reciente es la introducción de la fecha de caducidad: los cartuchos de la HP BusinessJet 2200C caducan cuando están en la impresora más de 30 meses, o a los 4,5 años de la fecha de fabricación - provocando la indignación de los consumidores, por supuesto.

Esta práctica con los cartuchos de impresora nos lleva a un conflicto comercial entre EE.UU. y la Unión Europea. En EE.UU., el fabricante de impresoras Lexmark ha conseguido un mandamiento judicial que impide la venta de cartuchos de terceros con chips que permitan su utilización en impresoras Lexmark. Al mismo tiempo, el Parlamento Europeo ha aprobado una «Directiva sobre material eléctrico y electrónico de desecho» que en 2006 forzará a los Estados miembro a impedir que las compañías incumplan la normativa sobre reciclado de la UE mediante la fabricación de productos con chips que impiden su reciclado [8].

El control postventa y el atado de un producto son prácticas que están creciendo con rapidez y utilizando todo tipo de mecanismos técnicos. Los fabricantes de teléfonos móviles, por ejemplo, suelen ganar más con las baterías de los teléfonos que con los teléfonos en sí, así que han introducido chips de autentificación que dificultan la utilización de baterías de la competencia [10]. Los fabricantes de coches están utilizando el bloqueo del formato de datos para impedir que mecánicos independientes reparen los vehículos de sus clientes [12]. Y las compañías de juegos de ordenador llevan años cobrando *royalties* a los desarrolladores de software, para subvencionar con esos ingresos la venta de consolas [11].

¿Esto es bueno o malo para el mercado? Según los economistas, «depende». Hal Varian argumenta que, desde el punto de vista de la política de ventas, unir las impresoras a los cartuchos puede no ser demasiado cuestionable, porque en el mercado de las impresoras todavía hay competencia y esa práctica hace que los fabricantes de impresoras compitan más para vender más unidades y, por lo tanto, bajen los precios [9].

Pero cuando esta técnica se utiliza para unir dos mercados en los que la competencia es relativamente escasa, el mercado de sistemas operativos o de servidores de Internet, por ejemplo puede limitar las opciones de los clientes y hacer subir los precios. Ésta fue una de las objeciones que se le pusieron a la iniciativa Passport de Microsoft en términos de política de competencia: los comerciantes que querían utilizar Passport estaban obligados a utilizar también servidores de Microsoft.

Autor

Ross Anderson dirige el grupo de seguridad del laboratorio de Informática de la Universidad de Cambridge (Reino Unido). Pertenece a la Institution of Electrical Engineers y al Institute of Mathematics and its Applications. Ha publicado artículos bien conocidos sobre temas de políticas de seguridad, desde privacidad médica a sistemas bancarios, así como sobre tecnologías subyacentes como criptografía y protección contra falsificaciones. Es autor del libro «*Security Engineering - A Guide to Building Dependable Distributed Systems*». Preside la Foundation for Information Policy Research.

Los fabricantes tendrán más facilidades aún para implementar una compleja política de precios y un mayor control postventa gracias a la introducción de *Trusted Computing* (TC), o «informática de confianza» [2].

2. Informática de confianza

En junio 2002, Microsoft anunció el lanzamiento para el 2004 de Palladium, una versión de Windows para implementar la 'Informática de confianza'. En este contexto, «de confianza» significa que terceros pueden confiar en el software de un PC con el que están en comunicación y que el propietario de la máquina no ha modificado ese software. Los programas también se podrán comunicar unos con otros --y con sus autores-- con total confianza. Esto abre toda una serie de nuevas e interesantes posibilidades.

La aplicación más obvia sería la gestión de los derechos digitales (*Digital Rights Management* o DRM, en inglés): Disney podría vendernos DVD que se descriptarían y funcionarían en una plataforma Palladium, pero que no se podrían copiar. La industria discográfica podría vendernos descargas de música que no se podrían intercambiar, o CDs que sólo se podrían escuchar tres veces o el día de nuestro cumpleaños. Esta aplicación será polémica, mientras que otras quizá no lo serán tanto. Un ejemplo: las plataformas con TC pueden albergar juegos en los que sea más difícil hacer trampas.

Palladium surgió gracias al trabajo de la Alianza para una Plataforma con Informática de Confianza (*Trusted Computing Platform Alliance* o TCPA, en inglés), fundada por Microsoft, Intel, IBM y HP. A ella se ha unido ahora ADM y se ha rebautizado como el Grupo de Informática de Confianza (*Trusted Computing Group*, o TCG en inglés) [13]. El TCG propone rediseñar el hardware de PC para darle a la unidad central de proceso (CPU) más privilegios (que permite a los procesos acceder a zonas de memoria inaccesibles incluso para los superusuarios normales) y un componente de seguridad del hardware --el chip Fritz-- que comprueba el software y el hardware que está utilizando una máquina. Los chips Fritz de diferentes máquinas se pueden comunicar entre sí. El papel de Fritz en el entorno 'de confianza' es asegurar a terceros que nuestra máquina es realmente la que nosotros decimos que es y que realmente utiliza el software que decimos que utiliza.

No todo el mundo está de acuerdo con el calificativo 'de confianza' para describir a esta tecnología. Microsoft prefiere hablar de 'Informática fiable' (*Trustworthy Computing* en inglés), porque confiar en un sistema no significa necesariamente que el sistema sea fiable. Si vemos a un empleado de la Agencia de Seguridad Nacional (NSA) norteamericana en los servicios de un aeropuerto internacional vendiéndole material clave a un diplomático chino, y siempre que esa operación no estuviese autorizada, diríamos que ese empleado es 'de confianza pero no fiable' (de hecho, la definición de la NSA de un sistema de confianza es «*un sistema que puede romper la política de seguridad*»).

En el lado opuesto del debate, Richard Stallman, de la Fundación para el Software Libre (FSF), prefiere hablar de 'Informática traicionera' (*Treacherous Computing* en inglés), porque el objetivo real de la tecnología del TCG es que el propietario del PC deje de tener el control efectivo del mismo [15]. Yo utilizaré TC y así el lector puede convertirlo en las siglas inglesas de 'Informática de Confianza', 'Informática Fiable' o 'Informática Traicionera', lo que prefiera.

2.1. Control y gobernación

Si el dueño de un ordenador ya no va a poder controlarlo, la gran pregunta es ¿quién ejercerá ese control? Las compañías relacionadas con TC han expresado diferentes opiniones dependiendo del momento. La especificación 1.0 de la TCPA original sugería una jerarquía en los organismos que pudiesen certificar los diferentes componentes de hardware y de software que fuesen a componer un sistema TC. De esta forma habría un control centralizado ejercido por un consorcio de empresas del sector.

La opinión actual de la industria es que los fabricantes de aplicaciones TC o del contenido de las mismas son los que deciden qué combinaciones de software y de software del sistema operativo son las aceptables. En el caso de DMR, por ejemplo, sería Disney --o quizá Microsoft como vendedor de Media Player-- el encargado de certificar una plataforma concreta como apta para reproducir Blancanieves. Un servidor mantenido por el fabricante de la aplicación suministraría lo necesario para cumplir las reglas que una aplicación concreta tiene que aplicar, como etiquetas para CD comerciales que digan «Prohibida su copia» o «Sólo copia de seguridad», o para películas que digan «Grabación permitida para visionado posterior; prohibida su copia».

3. Valor para usuarios corporativos y gubernamentales

Las aplicaciones de seguridad podrán especificar una amplia gama de políticas. Un sistema TC que, por ejemplo, se utilice para hacer cumplir una normativa gubernamental de protección de datos podría establecer que la información sólo puede enviarse hacia un nivel superior, de forma que un archivo 'confidencial' sólo se podría cortar y pegar en otro 'secreto', y no al revés. Pero resulta difícil que funcionen bien los mecanismos para controlar el flujo unidireccional de la información [1], así que es poco probable que estos mecanismos sean la aplicación rompedora (*killer app*) en lo que se refiere a la TC.

Utilizar sistemas TC para proteger secretos corporativos es la aplicación que se está utilizando para promocionar la TC. «*Tiene gracia*», comenta Bill Gates, «*esto se nos ocurrió para la música, pero luego nos dimos cuenta de que el correo electrónico y los documentos son terrenos mucho más interesantes*» [19]. En el Servidor Windows 2003 [16] se acaba de comercializar una implementación de los mecanismos de control de derechos de autor que se puede aplicar para controlar información confidencial en vez de música y vídeos.

El Servidor Windows 2003 permite al creador de un documento o de un archivo ejercer cierto control sobre el mismo, independientemente de donde se pueda enviar. Se podrá mandar un mensaje de e-correo con restricciones, como que el destinatario no lo pueda reenviar, o no lo pueda imprimir, o que sólo lo pueda leer si tiene una acreditación 'secreta', o que el documento sólo se pueda leer hasta finales de mes. Los usuarios de Windows que quieran utilizar esta función de TC pueden apuntarse a ella y entonces parece que será un servicio en línea el que decida si entrega una clave de descriptación para la aplicación (esto se acababa de hacer público en el momento de redactar este artículo y no se habían decidido todavía los detalles de su funcionamiento).

Uno de los argumentos clave para la venta de esta tecnología es que la empresa puede hacer que, a los 90 días, los

mensajes de e-correo ya no se puedan leer. En Microsoft ya funciona esta norma interna. Dadas las tácticas cada vez más agresivas que se utilizan en los litigios legales, a algunas firmas les podría gustar la idea de que dichos mensajes sean tratados como llamadas telefónicas en vez de como cartas. Pero incluso una aplicación tan sencilla como ésta puede ser difícil de desplegar en el mundo real. Algunos bufetes de abogados podrían poner pegas a recibir instrucciones de un cliente a través de un e-correo que sólo puede leer uno de los socios, o que no se pueda imprimir, o que sea ilegible a los 90 días. ¿Cómo se podría defender el bufete de acusaciones de mala práctica profesional, o qué garantías tendrían los otros socios?

Pero hay más: en muchos países, las leyes de exportación exigen a las compañías que conserven copias de las comunicaciones sobre software, documentación o *know-how* que se exporte y que estén comprendidas en la lista de doble uso. Esto puede suponer conservar los e-correos pertinentes durante tres años. Las normas contables pueden exigir la conservación de los e-correos pertinentes durante seis años. Se pueden prever innumerables escaramuzas entre políticas que exijan la destrucción y políticas que exijan la conservación. Como bien sabe cualquier director de Sistemas de Informacióngestor de Seguridad Interna, automatizar procedimientos que antes, dejando que fuese el raciocinio humano el encargado de dilucidar las cuestiones espinosas, habían evitado conflictos, es sinónimo de crear un campo de minas.

4. Valor para propietarios de contenidos

Las industrias discográfica y cinematográfica han presionado mucho para implantar mecanismos de tipo TC, buscando reforzar los sistemas de gestión de derechos digitales. Ya han conseguido una mayor protección legal para los sistemas existentes. Su argumento es que las copias digitales destruirán su negocio, pero el argumento está perdiendo fuerza porque hace ya varios años que resulta muy fácil copiar CD y no parece que eso haya afectado mucho a las ventas.

Analizando detenidamente la cuestión, no está claro que un mecanismo de DRM mucho más fuerte --como el prometido por TC-- supusiese una mejora importante en el status quo de los propietarios de contenidos [20]. Además, existe otro riesgo: si las máquinas TC se generalizan, los otros las pueden usar con la misma facilidad. Los usuarios pueden establecer 'redes negras' para intercambiar material prohibido de todo tipo y sería más fácil crear sistemas entre iguales (*peer-to-peer*), como Gnutella o Mojonation, pero que resisten mucho mejor los ataques de la industria discográfica, porque sólo podrán participar los verdaderos clientes. Ya no funcionarán los métodos actuales para atacar estos sistemas que consisten en denegaciones de servicio realizadas por clientes introducidos por un troyano [21]. Así que la implementación de TC podría tener como consecuencia no deseada que la industria discográfica fuese la víctima en lugar de la beneficiada.

5. Valor para fabricantes de hardware

La experiencia nos dice que los mecanismos de seguridad suelen favorecer los intereses de quien los paga y no los intereses de los clientes, para los que supuestamente se desarrollaron [1]. La publicidad nos contó que la autentificación y encriptación en los móviles GSM era para ofrecer una mayor seguridad a los usuarios, porque con los teléfonos analógicos eran más fáciles la clonación y las escuchas.

Pero la experiencia nos demuestra que los principales beneficiarios han sido las compañías telefónicas que financiaron esa mejora de seguridad.

Con los teléfonos analógicos, los usuarios que querían llamar gratis o defraudar al sistema llamando a números 900 controlados por asociados, podían clonar los teléfonos, y eso solía costarles dinero a las compañías telefónicas. Con el sistema GSM, los delincuentes pueden comprar teléfonos con tarjetas de crédito robadas (pasándoles el coste a los bancos) o, lo que es cada vez más frecuente, utilizan teléfonos robados en la calle (y el que paga el pato es el cliente). En cuanto a la confidencialidad, las agencias de espionaje de todo el mundo ya tienen acceso a las redes principales para conseguir datos claros de voz.

Por eso deberíamos examinar el posible efecto que TC tendría sobre la actividad empresarial de sus promotores.

En el caso de Intel, sus motivos para unirse a la TCPA fueron estratégicos. Intel copa la mayoría del mercado de microprocesadores para PC, de donde consigue la mayoría de sus beneficios, y la empresa crecería si crece el mercado de PC. Intel, por lo tanto, ha desarrollado un programa de investigación para apoyar una estrategia de «liderazgo en la plataforma», por la cual la empresa se pone a la cabeza de la industria para desarrollar tecnologías que amplíen la utilidad del PC, como el bus PCI y USB [23].

La parte positiva de esta estrategia es que Intel hizo crecer el mercado global de PC. La parte negativa es que utilizaron cárteles para la explotación de patentes y acuerdos obligatorios de licencias cruzadas para evitar que nadie de la competencia consiguiera una posición dominante en cualquier tecnología que pudiese poner en peligro su control sobre el hardware de PC. Los más descreídos señalan que Intel no podía permitirse que prevaleciera el bus de microcanal de IBM: no era sólo la competencia en la plataforma de hardware, era también que IBM no tenía interés alguno en ofrecer el ancho de banda necesario para que el PC compita con los sistemas superiores. En términos estratégicos, el efecto es parecido al que conseguían los antiguos romanos cuando destruían todos las edificaciones y todos los árboles que estaban cerca de sus carreteras y sus fortificaciones. La estrategia de Intel ha ido evolucionado hasta convertirse en una forma muy eficaz de sortear la ley antimonopolio.

6. Valor para fabricantes de software

El caso de Microsoft es aún más interesante. En su formato original, TC tenía potencial para eliminar el uso de software sin licencia: una plataforma 'de confianza' conectada con un servicio central de autorizaciones podría sencillamente impedir el uso de ese software ilegal. Los mecanismos para registrar el software se podrían hacer mucho más difíciles de sortear: el chip Fritz mantiene una lista de hardware y de componentes de software del sistema de una máquina TC, y se instala una comprobación online de los mismos.

Tras algunas protestas públicas, Microsoft afirma ahora que no habrá mecanismos de listas negras --por lo menos al nivel del sistema operativo [17]. El sistema Windows 2003 parece basarse en mecanismos más sutiles. El control no se ejercerá ahora de abajo a arriba por medio del hardware con TC, sino de arriba hacia abajo por medio de las aplicaciones. Disney

podrá decidir libremente en qué condiciones quiere ofrecer contenidos a sistemas con un determinado hardware y software. Si Disney decide cobrar 12,99 E por la versión en DVD de 'Blancanieves', 9,99 E por una descarga para TC/Windows utilizando Media Player, pero se niega a ofrecer contenidos para cualquier otra plataforma de ordenadores, Microsoft puede argumentar --frente a los medios y frente a las autoridades antimonopolio-- que quien niega los contenidos no es Microsoft sino Disney.

Los incentivos resultantes favorecen mucho a Microsoft: si TC/Windows se convierte en la plataforma dominante, los que desarrollan contenidos se lo ofrecerán a esa plataforma en primer lugar, y a los otros después (y no siempre) --igual que los productos se comercializaban primero para Windows y después para Mac (y no siempre), una vez que estaba claro que el mercado del PC se estaba decantando por Wintel. No puede sorprender que Apple esté tratando de desenfundar antes que Microsoft lanzando su propio servicio de descarga de medios.

6.1. Importancia de las aplicaciones

Microsoft parece estar invirtiendo en equipar la plataforma de sistemas operativos con mecanismos de TC para conseguir mayores ingresos con sus aplicaciones. Puede ser directamente (cobrando el doble por Office, por ejemplo), o indirectamente (cobrando un porcentaje de todos los contenidos comprados a través de Media Player, por ejemplo). Para las empresas de la competencia, todo dependerá de lo difícil que les resulte que sus contenidos interactúen con las aplicaciones y los contenidos de Microsoft. Y, por supuesto, a Microsoft le interesa que sea lo más difícil posible.

Supongamos que hay un servicio de suscripción a música popular que utiliza Media Player, y que Media Player ahora requiere una plataforma TC: el resultado es que los suscriptores tendrán que pasarse a una plataforma TC si quieren seguir accediendo a la música que ya han almacenado. Una vez que se haya extendido la utilización de una aplicación TC, con muchos usuarios cautivos en ella, se pueden implementar mecanismos para exigir una licencia, que pueden ser tan difíciles de evadir como difícil es sortear la tecnología. A continuación puede ponerse en práctica el modelo empresarial, que introdujo Nintendo y después siguieron otros fabricantes de consolas, en el que un software caro subvenciona a un hardware barato. El sistema operativo TC se convertiría entonces en un componente necesario y subvencionado cuya función real es maximizar los ingresos con productos de alto precio como Office, juegos y alquiler de contenidos. Si muchas empresas imponen controles obligatorios de acceso para e-correo con Windows 2003, y estos controles de acceso antes o después exigen una plataforma TC, los usuarios no tendrán más remedio que pasarse a ella. De hecho probablemente tengan menos opciones que los suscriptores a música, porque éstos siempre tendrán la alternativa de comprar nuevos CD, como hicieron cuando el CD sustituyó al vinilo. Pero si muchos archivos corporativos y oficiales están protegidos por claves criptográficas, las empresas no tendrán más opción que seguir los mecanismos que protegen y controlan estas claves.

6.2. Costes del cambio y clientes cautivos

En los últimos años las empresas han tenido en cuenta los costes de cambiar de operador a la hora de valorar los productos y servicios de información. En industrias que necesitan tener cautivos a sus clientes --como la industria del software-- el valor neto de la base de clientes de una compañía es igual al monto total de los costes que sus clientes tendrían que pagar para cambiar a otra empresa de la competencia [22]. Si fuese mayor, a la competencia le compensaría sobornar a esos clientes para conseguirlos. Si fuese menor, la empresa podría sencillamente subir los precios.

Un efecto de TC es aumentar enormemente la posibilidad de tener clientes cautivos. Supongamos, por ejemplo, que el Director de Informática de una empresa quiere dejar de comprar Office y pasar a OpenOffice, con una plataforma GNU/Linux. En la actualidad tiene que afrontar los costes de volver a formar al personal, los costes de instalar el nuevo software y el coste de convertir los archivos o documentos ya existentes. También habrá costes permanentes por incompatibilidades ocasionales. En la actualidad, la teoría económica indica que los costes serían muy parecidos a los que hay que pagar por Office.

Sin embargo, TC dificultaría la conversión de archivos desde formato Office a cualquier otro, y los costes se dispararían [24]. Quizá ni siquiera exista el procedimiento o el mecanismo para exportar contenido TC a una plataforma que no sea de TC, incluso aunque el propietario del contenido lo permita. Y aunque existan los medios para esa exportación, lo más probable es que no sean suficientes por sí mismos si se generalizan los mecanismos obligatorios de control de acceso impuestos por TC. La razón es que muchos de los datos almacenados en los archivos de la compañía aparecerían como propiedad de terceros. Un bufete de abogados, por ejemplo, puede recibir documentos confidenciales de un cliente, dirigidos a la atención de un número especificado de personas.

El bufete puede exigir el derecho a acceder a esos documentos durante seis años, por si tienen que defenderse de acusaciones de malas prácticas profesionales. Todo eso constaría codificado en los atributos de gestión de derechos del documento y se cumpliría gracias a los mecanismos TC. Las reglas de acceso sólo las podría contravenir el propietario del documento, es decir, su creador. Si el bufete de abogados quiere migrar de Office y Windows a OpenOffice y una futura plataforma TC/Linux, tendrían que obtener el permiso de sus clientes para exportar todos los documentos protegidos. Con el tiempo cualquier bufete puede llegar a tener miles de relaciones profesionales y algunas seguro que se tuercen; incluso dando por hecho que fuesen aceptables la logística y la política de pedir permiso a todos los clientes para exportar los documentos, algunos seguro que negaban ese permiso, por diferentes razones. El resultado es que el bufete se vería obligado a mantener un entorno TC/Windows, además del nuevo.

Hay otros efectos suaves, además de los duros. Por ejemplo, la controversia que se genere alrededor de TC puede aumentar la incertidumbre, que a su vez puede llevar a empresas y consumidores a pensar que «*más vale malo conocido que bueno por conocer*». El resultado puede ser un aumento en los costes de cambio que pueden superar incluso los derivados de la tecnología. (Los lectores de más edad recordarán la controversia que se creó con el elemento de «miedo, incertidumbre y duda», FUD en inglés, que IBM introducía en su

marketing, cuando era IBM --y no Microsoft-- la que se llevaba el gato al agua).

6.3. Temas antimonopolio

Existen, por lo tanto, muchas posibilidades de que TC se extienda utilizando el efecto red, y de que las principales aplicaciones de TC --una vez que dominen en un determinado sector-- estén, en la práctica, completamente a salvo de los competidores. Esto arrojará nueva luz sobre los conocidos argumentos esgrimidos en los casos antimonopolio de la industria de la información. Muchos economistas de las industrias de la información han aceptado la competencia 'por el mercado' diciendo que es igual de justa que la competencia 'dentro del mercado', especialmente por el carácter volátil de la industria y porque cada pocos años todos tienen posibilidades dado que el progreso socava las normas establecidas y se reinventan sectores completos de la industria. Pero este argumento habrá que revisarlo si las enormes --y crecientes-- cantidades de datos de aplicaciones que las compañías y los particulares almacenan pueden quedar cautivos de unas compañías que, en la práctica, están a salvo de los competidores. En cualquier caso, el incentivo para Microsoft está claro: el valor de la compañía es equivalente a los costes directos e indirectos que a las empresas les suponga cambiar a la competencia; si ese cambio es el doble de difícil, el valor del software de Microsoft será también doble.

Hay también otros temas. Varian ya ha apuntado que TC puede reducir la innovación porque limita las posibilidades técnicas de modificar los productos existentes [9], y las cosas irán a peor cuando los datos estén cautivos. En la actualidad, muchas empresas recien creadas consiguen introducirse porque ofrecen formas adicionales de utilizar las grandes cantidades de datos de las aplicaciones existentes en los formatos más utilizados. Una vez que los propietarios de la aplicación principal se adhieran a TC, tendrán todos los incentivos para cobrar por acceder a esos datos. Esto parece pensado para favorecer a las grandes marcas y perjudicar a las pequeñas y a la competencia, además de dificultar la innovación.

Otros fabricantes de aplicaciones de software se enfrentarán a la amenaza de no poder acceder a los datos de las aplicaciones de otros fabricantes, pero también a la perspectiva de que, si consiguen que su producto arraigue y que muchos clientes lo utilicen para sus datos, podrán utilizar los mecanismos de TC para tener a esos clientes cautivos de una forma más eficaz que la que les permitían los anticuados mecanismos de formatos propietarios o los restrictivos contratos firmados a golpe de clic de ratón. Esto posibilitará una valoración mucho más alta de las compañías, así que muchos vendedores de software se verán muy presionados para que adopten TC y si pierden el tren será difícil cogerlo más adelante.

Algunos sectores concretos de la industria pueden sufrir más las consecuencias. Los vendedores de tarjetas inteligentes, por ejemplo, pueden enfrentarse a la perspectiva de que muchas de las aplicaciones que ellos querían colonizar con sus productos utilizan en su lugar las plataformas TC en PC, PDA y teléfonos móviles. En general, la industria de la seguridad en la información se enfrentará a cambios importantes cuando muchos productos migren a TC o se abandonen.

Es difícil encontrar analogías en otras situaciones históricas, quizá la más parecida se dio hacia 1830, cuando el ferrocarril sustituyó a los canales en el transporte. Todo el que tuviera un barco podía transportar mercancías por el canal, pero el ferrocarril es un monopolio natural y suscitó ese tipo de críticas en su momento. El ferrocarril, por supuesto, no era en sí un desastre económico, pero sí contribuyó a crear concentraciones de poder económico y casos de competencia desleal que, a su vez, contribuyeron a que ciertos países se dotaran de leyes antimonopolio y a que en otros el ferrocarril pasase a manos públicas.

Es difícil hacer predicciones a largo plazo, pero a corto plazo parece razonable que la implantación de TC produzca efectos económicos: las compañías pequeñas saldrán perjudicadas y las grandes favorecidas; el mercado favorecerá a las empresas ya establecidas y penalizará a las nuevas; y se incrementarán los costes y los riesgos de montar nuevas empresas. Las industrias de informática y de comunicaciones se parecerán más a las de sectores tradicionales, como la automovilística o farmacéutica. Y eso no está muy claro si es bueno o malo.

7. ¿Qué consecuencias tiene la TC para los profesionales informáticos?

Durante muchos años, los ingenieros de seguridad se han quejado de que ni los fabricantes de hardware ni los de software se han preocupado de incorporar mecanismos de seguridad en sus productos. Las primeras investigaciones realizadas sobre economía de la seguridad nos permiten ahora saber el por qué [25]. Muchas empresas informáticas tuvieron que hacer frente a costes fijos altos, costes marginales bajos, altos costes para cambiar y efectos de red, y todo ello se tradujo en industrias con firmas dominantes y con claras ventajas para los que llegaron antes. Resulta vital reducir el plazo entre la creación de un producto y su comercialización y por eso era perfectamente racional la filosofía que adoptó Microsoft en los años 90 de «*lo sacamos el martes, y en la 3ª versión ya habremos corregido los fallos*».

Además, cuando se compite para dominar un mercado en red, las empresas tienen que contar con fabricantes de bienes y servicios complementarios. Los fabricantes de sistemas operativos tienen pocos incentivos para ofrecer complejos mecanismos de control de acceso porque éstos estorban a los que desarrollan las aplicaciones. La relativa poca importancia del usuario final, comparada con la de los fabricantes complementarios, llevó a las empresas a adoptar tecnologías (como PIK) que hacen que los fabricantes pasen a los usuarios finales los costes de seguridad y de administración.

El control de la interfaz de programación de la aplicación es vital para el propietario de la plataforma, así que intenta hacerlo propietario, complicado, extensible y, por lo tanto, sujeto a fallos. Es mucho más importante hacer posible la discriminación por precios que hacer posible la privacidad. Y por último, ante la falta de un amplio conocimiento sobre seguridad, los malos productos echaron del mercado a los buenos. ¿Qué le hizo cambiar tan súbitamente de opinión a Microsoft?

Un cínico diría que el reciente acuerdo antimonopolio al que Microsoft ha llegado con el Departamento de Justicia de los EE.UU. le obliga a compartir información sobre interfaces y sobre protocolos, excepto cuando afecte a la seguridad. Así que la solución es decir que todo lo que hace la compañía tiene

que ver con la seguridad. Microsoft también ha argumentado que la publicidad que se le ha dado a los ataques de varios tipos que ha sufrido la Red actúa como un incentivo para que se produzcan más ataques. Pero parece difícil que un gusano o dos al año justifique un cambio tan brusco de política y de dirección.

Este artículo sostiene que otro factor importante que ha decidido a Microsoft a gastar cifras de nueve dígitos en la seguridad de la información --después de haber desdeñado el tema durante décadas-- es la posibilidad de aumentar el número de clientes cautivos. (Es curioso comprobar que Intel, AMD, IBM y HP también están invirtiendo sumas considerables en TC, aunque no hay a la vista ninguna amenaza antimonopolio).

TC plantea otros muchos temas, desde censura hasta soberanía nacional, pasando por el futuro del movimiento por un software libre y de fuente abierta [2]. Pero para el hombre de negocios con el colmillo retorcido, TC será competencia pura y dura. La pregunta clave es: «*¿Cómo podrá Microsoft sacarme dinero con esto*?». La respuesta es muy sencilla: «*Teniéndote cada vez más cautivo con plataformas Microsoft como Office*».

¿Qué podrían hacer los legisladores y los reguladores? En las leyes de patentes podemos encontrar precedentes muy útiles. Durante años, un contrato que ataba de forma ilegal podía invalidar una patente en el Reino Unido: si el dueño de una patente de un proceso para fabricar harina le permite a otro utilizar ese proceso a condición de que le compre a él el grano, el dueño de la patente de hecho la está invalidando. Como poco, se podría sugerir que se invalidara la protección legal que la DMCA (Digital Millennium Copyright Act de los EE.UU) y la EUCD (Directiva europea sobre *copyright* 2001/29/EC) ofrecen a los mecanismos de TC, que se suponen que están a su vez protegiendo los derechos de autor, siempre que se utilizasen para dificultar la competencia --con controles adicionales o teniendo más cautivos a sus clientes.

La sugerencia es que los legisladores vean si la aplicación de TC aumenta o disminuye el saldo positivo de los consumidores. Es la prueba que propondría la jurisprudencia sobre patentes abusivas [26]. Ya que se afirma que TC creará más valor para los clientes y que, evidentemente, creará más valor para los fabricantes, y dada toda la polémica generada sobre los puntos positivos y negativos de la gestión de derechos digitales, quizá la forma más sencilla y más práctica de llegar a una política coherente y sólida sea ver si los clientes han salido favorecidos o perjudicados.

Referencias

[1] R.J. Anderson, *Security Engineering - a Guide to Building Dependable Distributed Systems*, Wiley (2001) ISBN 0-471-38922-6.

[2] R.J. Anderson, «TCPA/Palladium FAQ», en <http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html>.

[3] M. Magee, «HP inkjet cartridges have built-in expiry dates - Carly's cunning consumable plan, *The Inquirer*, 29 abril 2003, en <http://www.theinquirer.net/?article=9220>.

[4] «Ink Cartridges with Built-In Self-Destruct Dates», Slashdot, en <http://slashdot.org/articles/03/04/30/1155250.shtml>.

[5] «Computer Chip Usage in Toner Cartridges and Impact on the Aftermarket: Past, Current and Future», Static Control, Inc., en <http://www.scc-inc.com/special/oemwarfare/whitepaper/default.htm>.

[6] «Lexmark invokes DMCA in Toner Suit», Slashdot, en <http://slashdot.org/article.pl?sid=03/01/09/1228217 &mode =thread& tid=123>.

[7] «Prepared Statements and Press Releases», Static Control, Inc., en <http://www.scc-inc.com/special/oemwarfare/lexmark_vs_scc.htm>.

[8] M. Broersma, «Printer makers rapped over refill restrictions», ZDnet 20 diciembre 2002, at <http://news.zdnet.co.uk/story/0,,t269-s2127877,00.html>.

[9] H.R. Varian, «New Chips Can Keep a Tight Rein on Customers», *New York Times,* July 4 2002, en <http://www.nytimes.com/2002/07/04/business/04SCEN.html>.

[10] «Motorola Announces Availability of New Wireless Phone Batteries for Increased Performance and Safety, Featuring New Hologram Design», nota de prensa de Motorola, 23 julio 1998, sacada tras ser mencionada en [2]; ahora archivada en <http://www.ftp. cl.cam.ac.uk/ftp/users/rja14/mototola_battery_auth.html>.

[11] D. Becker, «Sony loses Australian copyright case», on CNN.com, 26 julio 2002, en <http://rss.com.com/2100-1040-946640.html?tag=rn>.

[12] N. Pickler, «Mechanics Struggle With Diagnostics», AP, 24 junio 2002; antes en radicus.net; sacada tras ser mencionada en [2]; ahora archivada en <http://www.ftp. cl.cam.ac.uk/ftp/users/rja14/car-diagnostics.html>.

[13] Trusted Computing Group, <http://www.trustedcomputinggroup.org/>.

[14] J. Lettice, «Bad publicity, clashes trigger MS Palladium name change», *The Register*, 27 enero 2003, en <http://www.theregister.co.uk/content/4/29039.html>.

[15] R. Stallman, «Can you trust your computer?», en <http://newsforge.com/newsforge/02/10/21/1449250.shtml?tid=19>.

[16] Microsoft Corp., «Windows Server 2003», 20 feb 2003, en <http://www.microsoft.com/windowsserver2003/rm>.

[17] J. Manferdelli, «An Open and Interoperable Foundation for Secure Computing», en *Hoja informativa* de Windows Trusted Platform Technologies, marzo 2003.

[18] A. Huang, «Keeping Secrets in Hardware: the Microsoft Xbox Case Study», 26 may 2002, en <http://web.mit.edu/bunnie/www/proj/anatak/AIM-2002-008.pdf>.

[19] P. Thurrott, «Microsoft's Secret Plan to Secure the PC», WinInfo, 23 junio 2002, en <http://www.wininformant.com/Articles/Index.cfm?ArticleID=25681>.

[20] S. Lewis, «How Much is Stronger DRM Worth?» en *Second International Workshop on Economics and Information Security*, en <http://www.cpppe.umd.edu/rhsmith3/index.html>.

[21] S.E. Schechter, R.A. Greenstadt, M.D. Smith, «Trusted Computing, Peer-To-Peer Distribution, and the Economics of Pirated Entertainment», en *Second International Workshop on Economics and Information Security*, en <http://www.cpppe.umd.edu/rhsmith3/index.html>.

[22] C. Shapiro, H. Varian, «Information Rules», Harvard Business School Press (1998), ISBN 0-87584-863-X.

[23] A. Gawer, M.A. Cusumano, «Platform Leadership: How Intel, Microsoft, and Cisco Drive Industry Innovation», Harvard Business School Press (2002), ISBN 1-57851-514-9.

[24] J. Brockmeier, «The Ultimate Lock-In», Yahoo News. 12 mar 2003, en <http://story.news.yahoo.com/news?tmpl= story2&cid=75&ncid=738&e=9&u=/nf/20030312/tc_nf/20982>.

[25] R.J. Anderson, «Why Information Security is Hard - An Economic Perspective», en *Proceedings of the Seventeenth Computer Security Applications Conference* IEEE Computer Society Press (2001), ISBN 0-7695-1405-7, pp 358-365, en <http://www.cl.cam.ac.uk/ftp/users/rja14/econ.pdf >.

[26] C. Shapiro, «Antitrust Limits to Patent Settlements», preprint, en <http://faculty.haas.berkeley.edu/shapiro/settle.pdf>