



Bisoños Usuarios de Linux de Mallorca y Alrededores | Bergantells Usuaris de Linux de Mallorca i Afegitons

Preguntas Frecuentes sobre TCPA y Palladium

Por [kyle kyle](http://linuca.org) (<http://linuca.org>)

Creado el 30/06/2002 20:04 y modificado por última vez el 14/07/2002 23:14

Este artículo es la traducción del texto de Ross Anderson [TCPA / Palladium Frequently Asked Questions](#)⁽⁵³⁾, en el que explica cómo Intel y Microsoft se han aliado para implementar tecnología para el Control de Derechos Digitales. Hemos actualizado la traducción a la version 1.0 recientemente publicada por el autor.

Version 1.0 – 9 Julio 2002

[Ross Anderson](#)⁽¹⁾

Traducción : [Francisco García](#)⁽²⁾

1. ¿Qué son TCPA y Palladium?

TCPA significa [Trusted Computing Platform Alliance](#)⁽³⁾ (algo como "Alianza para una Plataforma Informática Fiable"), una iniciativa liderada por Intel. Su meta es "una nueva Plataforma Informática para el nuevo siglo que aporte seguridad mejorada dentro de la plataforma PC". [Palladium](#)⁽⁴⁾ es el software que Microsoft dice que planea incorporar a versiones futuras de Windows; y se ejecutará sobre hardware TCPA, que añadirá algunas [características extra](#)⁽⁵⁾.

¿Qué harán TCPA / Palladium, en castizo?

Aporta una plataforma informática donde las aplicaciones no pueden ser alteradas o modificadas, y donde éstas se pueden comunicar de forma segura con su fabricante. Su aplicación más obvia es [el Control de Derechos Digitales \(digital rights management – DRM\)](#)⁽⁶⁾ : Disney podrá venderte DVDs que sólo se descodifiquen y ejecuten en plataformas Palladium, pero que no podrás copiar. La industria discográfica podrá venderte descargas de música que no podrás intercambiar. Podrán venderte CDs que sólo podrás oír 3 veces, o sólomente el día de tu cumpleaños. Toda una nueva gama de posibilidades en marketing a su alcance.

TCPA / Palladium hará también muy difícil ejecutar Software sin licencia. El Software 'pirateado' se podrá detectar y borrar de forma remota. También hará más fácil el alquiler de Software, en lugar de su compra. Si dejas de pagar su alquiler, el Software no sólomente dejará de funcionar, si no que dejarás de poder acceder a tus propios documentos. Durante años, Bill Gates ha soñado con encontrar la forma de [hacer pagar a China por el Software que usa](#)⁽⁷⁾: Palladium podría ser la respuesta a su plegaria.

Hay muchas otras posibilidades. Los Gobiernos serán capaces de ajustar las cosas de tal forma que todos los documentos de Microsoft Word creados en PCs de funcionarios civiles sean 'clasificados' y no se puedan filtrar electrónicamente a la Prensa. Los sitios Web de subastas pueden hacer obligatorio el uso de TCPA/Palladium para pujar. Hacer trampas en juegos en línea también puede ser más difícil.

También hay desventajas. Puede que haya censura remota: los mecanismos diseñados para borrar música 'pirateada' bajo control remoto se pueden usar para borrar documentos que un Juez (o una compañía de Software) dedidan que son ofensivos – cualquier cosa desde pornografía a escritos que critiquen a determinados líderes políticos. Las compañías de Software también pueden hacer más difícil el cambio hacia productos de otros competidores: por ejemplo, Word podría encriptar todos sus documentos con claves a las que solo tendrían acceso otros productos de Microsoft; de tal forma que solo tendrías acceso usando programas de esa compañía, y no con ningún otro procesador de textos de la competencia.



3. Entonces, ¿ya no podré usar mis MP3s nunca más?

Con los MP3s existentes, quizá no pase nada durante algún tiempo. Microsoft dice que Palladium no hará que nada deje de funcionar de repente. Pero una reciente actualización del Windows Media Player ha causado [gran controversia](#)⁽⁸⁾ insistiendo en que los usuarios están de acuerdo en futuras medidas anti-piratería, que pueden incluir el borrado de contenido 'pirateado' encontrado en el ordenador. Del mismo modo, es poco probable que programas que dan a las personas más control sobre sus PCs, como [VMware](#)⁽⁹⁾ y [Total Recorder](#)⁽¹⁰⁾, funcionen bajo TCPA. Así que tendrás que usar un reproductor diferente – y si éste reproduce MP3s pirateados, parece difícil que esté autorizado a reproducir los nuevos títulos, ya protegidos.

Establecer las políticas de seguridad de sus ficheros es problema de cada una de las aplicaciones, usando un Servidor de Políticas. De esta forma Windows Media Player puede averiguar bajo qué condiciones se debe reproducir un determinado título protegido. De esta forma, yo espero que Microsoft haga acuerdos con los Proveedores de Contenidos, pudiendo éstos experimentar con nuevos modelos de negocios: quizá puedas comprar CDs a un tercio de su precio, pero que solo se reproduzcan 3 veces; si pagas lo restante, obtienes derecho a oírlo cuantas veces quieras. Quizá se te permita dejar tu copia digital de un disco a un amigo, pero entonces tu propia copia no funcionaría hasta que tu amigo te la devuelva. Con más probabilidad, no podrás dejar música a tu amigo en absoluto. Estas políticas harán la vida más incómoda a determinadas personas; por ejemplo, la codificación regional te puede prohibir ver una película en polaco si tu PC fue comprado fuera de Europa.

Esto se podría hacer hoy en día – Microsoft simplemente tendría que poner un parche en el WMP – pero una vez que TCPA / Palladium impida a la gente alterar los programas reproductores, y haga más fácil a Microsoft controlar los parches y actualizaciones, será imposible escapar; pero también será una forma más atractiva de hacer negocios.

4. ¿Cómo funciona?

TCPA provee métodos para monitorizar los componentes de los PCs ensamblados en el futuro. La implementación elegida en la primera fase de TCPA es un chip 'Fritz' – una tarjeta inteligente soldada a la placa madre.

Cuando arranques tu PC, Fritz toma el control. Revisará que la ROM de arranque está como se espera, la ejecutará, examinará el estado de la máquina; y después analizará la primera parte del sistema operativo, lo cargará y ejecutará, revisará el estado de la máquina, y así sucesivamente. El límite de confianza, de hardware y software considerados conocidos y fiables, será firmemente aumentada. Se guarda una tabla del hardware (tarjeta de sonido, video, etc) y del software (sistema operativo, drivers); si hay cambios significativos, la máquina debe ser certificada nuevamente. El resultado es un PC arrancado en un estado conocido con una combinación aprobada de hardware y software. El control es cedido al software de Verificación de Cumplimiento del sistema operativo – presumiblemente Palladium, si su sistema operativo es Windows.

Una vez que la máquina esté en este estado, Fritz lo puede certificar ante terceras partes: por ejemplo, puede autenticarse ante Disney para probar que la máquina es un receptor adecuado de "Blancanieves". Esto significa certificar que el PC está ejecutando en ese momento un programa autorizado – MediaPlayer, DisneyPlayer, lo que sea. El servidor de Disney entonces manda datos encriptados, con una clave que usará Fritz para desencriptarlo. Fritz solamente pondrá la clave a disposición de la aplicación mientras el entorno permanezca 'fiable' (trustworthy). En este caso, fiable significa de acuerdo a lo que la Política de Seguridad bajada del servidor de políticas diga. Esto significa que Disney puede decidir poner a disposición su contenido a una determinada aplicación, contando en que ésta no haga copias no autorizadas. También se ha pensado en pagos: Disney puede insistir, por ejemplo, en que la aplicación pida un dólar cada vez que ves una película. De hecho, la aplicación en sí misma puede ser alquilada, siendo esto de gran interés para las compañías de Software. Parece que las posibilidades están solamente limitadas por la imaginación de los vendedores...

5. ¿Para qué mas se pueden usar TCPA y Palladium?

Se puede usar TCPA para implementar controles de acceso mucho más fuertes para documentos confidenciales. Por ejemplo, un ejército puede decidir que sus soldados solamente pueden crear documentos Word marcados como 'Confidenciales' o superior, y que sólo un PC TCPA con un certificado expedido por su propia agencia de seguridad, puedan leer un documento como este. Esto se llama 'Control de Acceso Obligatorio' y esto le gusta a los gobiernos. El anuncio de Palladium implica que los productos Microsoft soportarán esto: se podrá configurar Word de tal forma que encriptará todos los documentos generados en el compartimento de tu máquina, y compartirlos solo con otros usuarios en un grupo definido.



Las corporaciones podrán hacer esto también, para hacer la vida más difícil a los empleados desleales. Se podrá configurar que los documentos de la empresa solamente se puedan leer en los ordenadores de la misma, a no ser que una persona autorizada los marque para que se puedan leer fuera. También podrán poner límites de tiempo: pueden hacer que todos los correos electrónicos se evaporen después de 90 días, salvo que alguien haga un esfuerzo por preservarlos. (Piensa qué útil sería esto para Enron, o Arthur Andersen, o la propia Microsoft en el juicio antimonopolio). La Mafia podría usar las mismas características: pueden hacer que una hoja de cálculo con los últimos embarques de droga solamente pueda ser leída en PCs fiables, y que ésta se desvanezca a final de mes. Esto hará la vida más complicada para el FBI – aunque Microsoft está en conversaciones con determinados gobiernos para que los policías y espías obtengan algún tipo de acceso a las claves maestras. Pero, en cualquier caso, un empleado desleal que envíe por correo electrónico un documento a un periodista, conseguirá muy poco, dado que el chip Fritz del ordenador del periodista no le dará la clave para descifrarlo.

T CPA / Palladium también parece destinado a ser usado en sistemas de pago electrónico. Parece ser que una de las visiones de Microsoft es mover la funcionalidad de las tarjetas de los bancos hacia software, una vez que las aplicaciones sean resistentes a alteraciones. Esto es necesario si queremos tener un futuro donde tengamos que pagar por los libros que leamos, y la música que escuchemos, según una tarifa por las hojas que leamos o los minutos que escuchemos. Incluso si esto no funciona como modelo de negocio – y hay [buenos motivos](#)⁽¹¹⁾ para que no sea así – es claramente un asunto de competencia para un número de sistemas de pago online. Si, en un plazo de 10 años, no es cómodo comprar en línea con una tarjeta de crédito si no tienes T CPA o Palladium, eso podría mover a mucha gente al sistema.

6. Bien, aquí habrá vencedores y vencidos – Puede que Disney haga una gran fortuna, y los fabricantes de tarjetas inteligentes se vayan al garete. Pero seguramente Intel y Microsoft no estarán invirtiendo un dineral solamente por caridad? ¿Cómo pretenden sacar dinero de todo esto?

Mis espías de Intel me dicen que esto es una jugada defensiva. Dado que hacen la mayor parte de su dinero a través de los microprocesadores para PC, y ya tienen la mayor parte del mercado, solo pueden hacer crecer la compañía agrandando el mercado. Están decididos a que el PC sea el centro de las futuras redes domésticas. Si el entretenimiento será la aplicación principal, y el DRM será una tecnología crítica para ello, los PCs tienen que proveer DRM o corren el riesgo de verse desplazados del mercado.

Las motivaciones de Microsoft también vienen del deseo unir el mercado del entretenimiento a su imperio. Pero por otra parte creen que si T CPA o Palladium se convierten populares, los podrán usar para evitar la copia ilegal de Software. 'Hacer que los chinos paguen por su Software' es una de las grandes metas de Bill; con Palladium, puede ligar a cada PC una única copia registrada de Office, y con T CPA puede ligar a cada placa madre su propia licencia de Windows individual. T CPA también tendrá una lista negra de las copias de Office que se pirateen.

Finalmente, Microsoft querría encarecer el proceso de cambio de sus productos (como Office) hacia productos rivales (como [OpenOffice](#)⁽¹²⁾). Esto les permitiría poder cobrar más dinero por sus actualizaciones sin que sus clientes abandonen el barco.

7. ¿De dónde viene la idea?

Apareció por primera vez en un ensayo escrito por Bill Arbaugh, Dave Farber y Jonathan Smith, ['Una Arquitectura Segura y Fiable para Secuencias de Arranque \(Bootstraps\)'](#)⁽¹³⁾, en los procesos del Simposio IEEE sobre Seguridad y Privacidad (1997) pp 65–71. Esto llevó a la patente US 'Arquitectura Segura y Fiable para Secuencias de Arranque', U.S. Patent No. 6,185,678, February 6th, 2001. Las ideas de Bill se desarrollaron a partir del trabajo sobre firmado de código que hizo mientras estaba en la NSA en 1994. Este chico de Microsoft también solicitó una [protección por patente](#)⁽⁶⁾ en los [aspectos del sistema operativo](#)⁽¹⁴⁾. (Los textos de las patentes están [aquí](#)⁽¹⁵⁾ y [aquí](#)⁽¹⁶⁾.)

Puede que existan bastantes desarrollos anteriores (prior art). Markus Kuhn escribió hace años sobre el [Procesador TrustNo1](#)⁽¹⁷⁾ y la idea sobre la que subyace – un 'Monitor de Referencia' fiable que supervisa las funciones de control de acceso de un ordenador – se remontan al menos a [un escrito de James Anderson para la USAF en 1972](#)⁽¹⁸⁾. Esta ha sido una característica que deseaba en los sistemas militares seguros de USA desde ese momento.

8. ¿Cómo se relaciona todo esto con el número de serie de los Pentium 3?

Intel inició un programa previo entorno a 1997 que hubiera añadido la funcionalidad de los chips Fritz dentro del procesador principal del PC, o dentro del controlador de caché, en el 2000. El número de serie del Pentium 3 fue un



paso previo en esta dirección. La adversa respuesta pública parece haber causado una pausa, de tal forma que se creó un consorcio junto a Microsoft y otros.

¿9. Por qué se le llama un chip 'Fritz'?

En honor al senador Fritz Hollings, de Carolina del Sur, que trabaja incansablemente en el congreso para hacer TCPA una parte obligatoria en todos los productos electrónicos de consumo.

10. OK, entonces el TCPA impide que los críos intercambien música, y ayuda también a que las compañías mantengan sus datos confidenciales. También puede ayudar a la Mafia, a no ser que el FBI tenga una puerta trasera; yo asumo que la tendrá. Pero a parte de piratas, espías industriales y activistas, quien estará en desacuerdo?

Muchas compañías tienen mucho que perder. Por ejemplo, la industria europea de tarjetas inteligentes puede ser dañada, puesto que las funciones que ahora aportan sus productos, se implementarán dentro de chips Fritz en los portátiles, PDAs, móviles y móviles de tercera generación. De hecho, gran parte de la industria de la Seguridad estará muy molesta si el TCPA se lleva a cabo. Microsoft afirma que Palladium detendrá el spam, los virus y prácticamente cualquier otra cosa en el ciberespacio – si esto es así, las compañías de software antivirus, los spammers, los vendedores de filtros anti-spam, las firmas que desarrollan firewalls y los detectores de intrusiones ya no tendrán nada que comer.

Hay graves preocupaciones sobre los efectos en la Industria de Bienes y Servicios de la Información, y en particular en la innovación, en la tasa de formación de nuevas empresas y en la posibilidad en que empresas relacionadas puedan expandir sus monopolios. Los problemas sobre la innovación están bien explicados en una [reciente columna del NY Times](#)⁽¹⁹⁾ del distinguido economista Hal Varian.

Pero hay problemas mucho más profundos. El tema fundamental es que quien controle los chips Fritz obtendrá una inmensa cantidad de poder. Hay gran cantidad de formas en que se puede abusar de este poder, e Intel ha rechazado responder preguntas sobre la dirección del consorcio TCPA.

11. ¿Cómo se puede abusar del TCPA?

Una de las preocupaciones es la censura. Se diseñó TCPA desde el principio para permitir la revocación centralizada de bits 'pirateados'. Se notificará y desactivará el Software 'pirateado' cuando se intente ejecutar, pero ¿qué pasa con las canciones y videos 'pirateados'? Y cómo puedes transferir una canción o un video que tú posees de un PC a otro, a no ser que puedas revocarlo en la primera máquina? La solución propuesta es que una aplicación TCPA, como un reproductor de archivos o un procesador de textos, tenga su política de seguridad administrada remotamente por un servidor, que tendrá una lista de ficheros malos. Esta será actualizada de vez en cuando y usada para monitorizar todos los ficheros que la aplicación abra. Los ficheros se pueden revocar por su contenido, por el número de serie de la aplicación que los creó y por otros criterios. El uso propuesto para esto es que si todo el mundo en China usa la misma copia de Office, no paras todas las copias que se ejecuten en máquinas TCPA; esto simplemente motivaría a los chinos para usar PCs normales en lugar de PCs TCPA, para escapar de la revocación. Así que haces que cada PC TCPA en el mundo se niegue a leer ficheros que han sido creados usando un programa 'pirateado'.

Esto es suficientemente malo, pero el potencial de abuso se extiende mucho más allá de la coacción comercial o el conflicto económico, hasta llegar a la censura política. Yo espero que esto se lleve a cabo paso a paso. En un primer lugar, algún policía bien-intencionado obtendrá una orden en contra una foto pornográfica de un niño, o un manual de cómo sabotear señalizaciones de trenes. Todos los PCs TCPA borrarán o notificarán estos documentos malos. Entonces, un litigante en un libelo o en un juicio sobre derechos de autor (copyright) obtendrá una orden en contra de un documento ofensivo; quizá los Cienciologistas intenten meter en la lista negra el famoso Fishman Affidavit. Una vez que los abogados y los censores del gobierno se den cuenta del potencial, el goteo se convertirá en una inundación.

La edad moderna empezó cuando Gutenberg inventó la imprenta móvil en Europa, que permitió que la información se preservara y diseminara incluso si los príncipes y obispos querían prohibirla. Por ejemplo, cuando Wycliffe tradujo la Biblia al inglés en 1380–1, el movimiento Lollard que el inició fue reducido fácilmente; pero cuando Tyndale tradujo el nuevo testamento en 1524–5, fue capaz de imprimir más de 50000 copias antes que le cogieran y quemaran en la hoguera. El viejo orden en Europa se vino abajo, y la nueva era comenzó. Las sociedades que han intentado controlar la información se convirtieron en poco competitivas, y con la caída de la Unión Soviética parecía que el capitalismo democrático liberal había ganado. Pero ahora, TCPA y Palladium ponen en riesgo la herencia invaluable que Gutenberg nos dejó. Los libros electrónicos, una vez publicados, serán vulnerables; los juzgados pueden prohibir su



publicación, y la infraestructura TCPA les hará el trabajo sucio.

Así que después de los intentos de la Unión Soviética de registrar y controlar todas las máquinas de escribir y faxes, TCPA intenta registrar y controlar todos los ordenadores. Las implicaciones para la libertad, democracia y justicia son preocupantes.

12. Esto asusta. ¿No se podría simplemente desconectar?

Seguro – a no ser que su administrador configure la máquina de tal forma que TCPA sea obligatorio, siempre lo podrás desactivar. Entonces puedes usar tu PC con privilegios de administrador, y usar aplicaciones inseguras.

Sin embargo, hay un aspecto en el que no puedes desactivar a Fritz. No puedes hacer que ignore el software pirateado. Incluso si está informado que el PC arranca en modo inseguro, todavía chequeará que el número de serie del sistema operativo no esté en una lista negra. Esto tiene implicaciones de cara a la soberanía nacional. Si Saddam es suficientemente tonto para actualizar sus PCs de tal forma que usen TCPA, entonces el Gobierno americano podrá averiguar sus licencias de Windows y apagar todos sus PCs la próxima vez que haya guerra. Arrancar en modo no seguro, no servirá de mucho. Tendría que desenterrar viejas copias de Windows 2000, cambiarse a GNU/Linux o encontrar una forma de aislar a Fritz de sus placas madre sin romperlo.

Si no eres alguien al que el presidente de los USA odie personalmente, eso puede no ser un problema. Pero si desactivas TCPA, tus aplicaciones TCPA no funcionarán, o no funcionarán de la misma forma. Sería como cambiarse de Windows a Linux estos días; tienes más libertad, pero acabas teniendo menos elección. Si las aplicaciones que usan TCPA/Palladium son más atractivas para la mayoría de la gente, puedes acabar simplemente teniendo que usarlas – de la misma forma que mucha gente tienen que usar Microsoft Word porque todos sus amigos y colegas les envían documentos en formato Microsoft Word. Microsoft dice que Palladium, al contrario que TCPA estándar, permitirá ejecutar aplicaciones fiables y no fiables al mismo tiempo en diferentes ventanas; esto presumiblemente hará más fácil el cambio para la gente.

13. Así que el aspecto económico va a ser fundamental en todo esto?

Exactamente. Los mayores beneficios en los mercados de bienes y servicios tecnológicos van a compañías que pueden establecer plataformas (como Windows o Word) y controlan la compatibilidad con ellas, para conducir a los mercados a productos complementarios. Por ejemplo, [algunos fabricantes de móviles usan una autenticación 'desafío-respuesta'](#)⁽²⁰⁾ para verificar que la batería del teléfono es genuina y no de otra marca – pudiendo negarse a recargarla, o intentar gastarla lo más rápidamente posible. Algunas impresoras autentican sus cartuchos de tinta de forma electrónica; si se usa un sustituto barato, la impresora silenciosamente cambia su calidad de 1200dpi a 300dpi. La consola Sony Playstation 2 usa una autenticación similar para asegurarse de que sus cartuchos de memoria han sido hechos por Sony en lugar de por un competidor de precios más bajos.

El TCPA parece diseñado para maximizar el efecto, y de esta manera el poder económico, de semejantes artimañas. Teniendo en cuenta el record de Microsoft en jugarretas anti-competitividad, espero que Palladium las soporte. Así que si tú controlas una aplicación que usa TCPA, tu servidor de políticas puede asegurarse de que tu elección de qué aplicaciones manejan los ficheros que tú creas, se cumpla. Se pueden proteger estos ficheros usando criptografía fuerte, con claves controladas por los chips Fritz en las máquinas de todas las personas. Esto significa que una aplicación TCPA exitosa valdrá mucho más dinero para la empresa de software que la controla, dado que pueden alquilar el acceso a sus interfaces para cualquier cosa que el mercado demande. De este modo, habrá grandes presiones para que los desarrolladores de software hagan aplicaciones TCPA; y si Palladium es el primer sistema operativo que soporte TCPA, esto le dará una ventaja competitiva sobre GNU/Linux y MacOS para la comunidad de desarrolladores.

14. Espera un segundo, la ley no da derecho para hacer ingeniería inversa con fines de compatibilidad?

Sí, y eso es muy importante para el funcionamiento del mercado de bienes y servicios tecnológicos; ver Samuelson y Scotchmer, [Aspectos Económicos y Jurídicos de la Ingeniería Inversa](#)⁽²¹⁾, Yale Law Journal, May 2002, 1575–1663. Pero la ley, en la mayoría de los casos, sólo te da la oportunidad de probar, no de tener éxito. Antes, cuando la compatibilidad significaba tener que jugarretar con los formatos de ficheros, había una disputa real – Cuando Word y Word Perfect luchaban por dominar el mercado, cada uno de ellos intentaba leer los ficheros del otro e impedir que que leyera los propios. Sin embargo, con TCPA se acabó el juego; sin acceso a las claves, o algún modo de irrumpir en el funcionamiento del chip, no se puede hacer.



Bloquear el acceso de los competidores a los formatos de fichero fue una de las motivaciones principales para TCPA: ver un [post](#)⁽²²⁾ de Lucky Green, y una charla suya en el [Def Con](#)⁽²³⁾ para oír más. Es una táctica que va más allá del mundo informático. El congreso está [molesto](#)⁽²⁴⁾ por que los fabricantes de coches usan un formato de datos cerrado para evitar que sus clientes reparen sus coches en talleres independientes. Y el chico de Microsoft dice que quieren Palladium en todas partes, incluso en tu reloj. Las consecuencias económicas para los negocios independientes pueden ser significativas.

15. ¿Así que no se puede burlar el TCPA?

Las primeras versiones serán vulnerables a cualquiera con las herramientas y paciencia suficiente para crackear el hardware (p.e., obtener datos en claro en el bus entre la CPU y Fritz). Sin embargo, a partir de la fase 2, Fritz simplemente desaparecerá dentro del microprocesador – llamémosle 'Hexium' – y las cosas se pondrán mucho más difíciles. Algún oponente serio todavía será capaz de crackearlo. Por el contrario, esto irá siendo cada vez más difícil y caro.

Además, en muchos países crackear a Fritz será ilegal. En los Estados Unidos, la Digital Millennium Copyright Act (DMCA) ya lo impide, mientras que la situación en la Unión Europea varía entre cada país, dependiendo de cómo las leyes nacionales les implementen la Directiva Europea sobre Copyright.

Por otra parte, en muchos productos el control sobre compatibilidad se mezcla deliberadamente con el control sobre copia. Los chips de autenticación de la Sony Playstation también contienen el algoritmo de encriptación de los DVD, por lo que los que hagan ingeniería inversa pueden ser acusados de burlar un mecanismo de protección de copia y ser juzgados bajo la DMCA. La situación legal es poco clara – y esto favorecerá a las grandes compañías con buenos bufetes de abogados.

16. ¿Cómo será el efecto económico en general?

Las industrias del contenido pueden ganar un poco más cortando la copia ilegal de música – Espere que Michael Jagger sea un poco más rico. Pero yo espero que el efecto económico más significativo sea el fortalecimiento de los poseedores de derechos en los mercados de bienes y servicios de la información, a expensas de nuevos competidores. Esto puede significar un aumento en el tope del mercado para firmas como Intel, Microsoft e IBM – pero a costa del crecimiento y la innovación general. La mayoría de las innovaciones que generan crecimiento económico no son anticipadas por los fabricantes en las plataformas en que se basan; y los cambios tecnológicos en los mercados de bienes y servicios tecnológicos son generalmente acumulativos. Provistos los poseedores de derechos nuevas formas para hacer la vida más difícil a aquellos que quieran desarrollar nuevos usos para sus productos, crearán todo tipo de trampas y perversos incentivos (N.T.: para que no lo hagan).

La inmensa centralización de poder económico que TCPA y Palladium representan favorecerá a las empresas grandes sobre las pequeñas; habrá efectos similares dado que Palladium permitirá a las grandes compañías obtener más de sus actividades económicas, como con las empresas de coches forzando a los dueños a hacer sus revisiones en establecimientos autorizados. Como el mayor crecimiento en el empleo tiene lugar en el sector pequeño o mediano, esto podría tener consecuencias para los puestos de trabajo.

También puede que haya distintos efectos regionales. Por ejemplo, el patrocinio durante muchos años por parte de los Gobiernos Europeos han hecho a la industria de tarjetas inteligentes muy fuerte, a costa de impedir otras innovaciones. Según los veteranos de la industria a los que he consultado predicen que una vez que la segunda fase de TCPA inserte las funcionalidades de Fritz en el procesador principal, esto destruirá las ventas de tarjetas inteligentes. Muchas de las funciones que los fabricantes de tarjetas inteligentes quieren que éstas hagan se podrán hacer con los Fritz de tu portátil, tu PDA o tu teléfono móvil. Si esta industria es eliminada debido a TCPA, Europa podría perder mucho. Además, gran parte de la industria en seguridad de la información desaparecerá.

17. ¿Quién más perderá?

Hay muchos sitios donde los actuales procesos de negocios se alteran para permitir que los poseedores del copyright obtengan nuevos beneficios. Por ejemplo, recientemente solicité permisos para convertir un campo que tenemos en un jardín; para hacer esto, necesitaba aportar seis copias de un mapa 1:1250 del terreno. Antiguamente, todo el mundo podía obtener un mapa de la biblioteca local y fotocopiarla. Ahora los mapas están en un servidor en la biblioteca, con control de copias, pudiendo solamente hacer 4 copias de cualquier hoja. Para un particular, eso es fácil de burlar: compro hoy 4 copias y mañana mando a un amigo a por las dos restantes. Pero los negocios que usen mapas



habitualmente acabarán pagando mucho más a las compañías de mapas. Eso puede parecer un pequeño problema; multiplícalo para tener una idea sobre los efectos de la economía en general. Parece ser que las transferencias de beneficios, una vez más, serán desde las pequeñas empresas a las grandes, y de las nuevas firmas a las viejas.

Con un poco de esperanza, esto causará resistencia política. Un muy conocido abogado británico ha dicho que las leyes de copyright solamente se toleran por que no se asegura su cumplimiento para la amplia mayoría de pequeños infractores. Y puede que haya algunos casos particularmente resaltables. Entiendo que las regulaciones de copyright en Gran Bretaña a finales de este año eliminarán el derecho de uso—justo a los invidentes para usar sus programas de interpretación para leer libros electrónicos. Normalmente, una estupidez burocrática como esta puede que no importe mucho, dado que mucha gente simplemente la ignoraría y la policía no sería tan idiota como para perseguir a nadie. Pero si se asegura el cumplimiento de las regulaciones sobre copyright a través de una protección hardware que son difícilmente rompibles, entonces los invidentes pueden perder derechos gravemente. (Hay otros grupos menores en situación similar)

18. Uhh! ¿Qué más?

La TCPA puede minar la General Public License (GPL), la licencia bajo la cual se distribuyen muchos productos libres y de código abierto. La GPL ha sido diseñada para impedir que los frutos del trabajo voluntario y en común sean secuestrados por compañías privadas para su beneficio. Cualquiera puede usar y modificar software distribuido bajo esta licencia, pero si distribuyes una copia modificada, tienes que ponerla disponible al mundo junto con el código fuente para que otros usuarios puedan hacer modificaciones por sí mismos.

Al menos dos compañías ya han iniciado un programa de desarrollo de una versión de GNU/Linux que soporte TCPA. Como sacarán dinero de esto? Bueno, hacer una versión TCPA del producto supondrá limpiar el código y eliminar una serie de características. El patrocinador enviará el código recortado a un laboratorio de evaluación, junto con una cantidad de documentación describiendo el trabajo hecho, incluyendo un número de análisis probando por qué varios ataques ya conocidos contra el código no funcionarían. El truco es éste. Aunque el programa modificado esté cubierto por la GPL, y sea libre para todo el mundo, no hará uso de las características TCPA a no ser que sea firmado, y tenga un certificado que le permita usar la infraestructura de clave pública (PKI) de TCPA. Eso es lo que costará dinero (si no en un principio, sí en algún momento)

Se podrán hacer modificaciones al código modificado, pero no se podrá firmar el código resultante (al menos, no con una clave que haga que terceras partes confíen en el código). Algo similar sucede con el [linux distribuido por Sony](#)⁽²⁵⁾ para su Playstation 2; los mecanismos de protección anticopia de la consola impiden la ejecución de binarios alterados, y de usar una serie de características del hardware. Incluso si un filántropo hiciera un linux seguro y sin buscar beneficios, el producto resultante no sería una versión GPL de un sistema operativo TCPA, si no un sistema operativo propietario que el filántropo podría dar libremente. (Hay todavía aspectos sobre quién podría pagar para usar la PKI que expide certificados para los usuarios.)

La gente pensaba que la GPL haría imposible que ninguna compañía se aprovechara y robara el código producto del esfuerzo de la comunidad. Esto animaba a que la gente estuviera deseosa de emplear su tiempo libre escribiendo Software Libre para el beneficio de la comunidad. Pero la TCPA cambia eso. Una vez que la mayoría de PCs del mercado sean compatibles TCPA, la GPL no funcionará como se preveía. El beneficio para microsoft no es que esto destruirá el software libre directamente. Por el contrario, el propósito es este: una vez que incluso el código GPL pueda ser secuestrado para propósitos comerciales, los programadores estarán mucho menos motivados para escribir software libre.

19. Mucha gente se molestará con esto.

Y hay muchos otros aspectos políticos — la transparencia del procesamiento de datos personales que la directiva Europea sobre protección de datos regula; el problema sobre la soberanía, sobre qué regulaciones sobre copyright promulgará cada país, como en el presente; o si Microsoft utilizará TCPA para impedir que rivales le hagan la competencia, como por ejemplo Apache; y si la gente estará de acuerdo con que sus PCs, en realidad, estén efectivamente, bajo control remoto — un control que se podría ser usurpado por jueces o agencias gubernamentales sin su conocimiento.

20. Espera un segundo, la TCPA no es ilegal bajo la ley antimonopolio?

Intel ha empleado una 'plataforma de liderazgo', en la cual ellos conducen los esfuerzos de la industria para desarrollar nuevas tecnologías que hagan a los PCs más útiles, como el bus PCI y el USB. Su modus operandi se describe en un



[libro de Gawer y Cusumano](#)⁽²⁶⁾. Intel establece establecer un consorcio para compartir el desarrollo de la tecnología, hacer que los miembros fundadores ponga algo de Propiedad Intelectual (PI) en ello, publicar un estándar, esperar algunos momentos, y licenciarlo a la industria bajo la condición de que los licenciarios, en retorno, licencien cualquier propiedad intelectual suya que interfiera, bajo coste cero para todos los miembros del consorcio.

El aspecto positivo de esta estrategia es que Intel hará crecer el mercado de los PCs; lo más oscuro es que impedirán que ningún competidor llegue a alcanzar una posición dominante en ninguna tecnología pueda amenazar la dominancia de Intel en la plataforma PC. Así, del mismo modo que Intel no pudo adquirir el bus microchannel de IBM, no sólo como un nexo competitivo en la plataforma PC, si no por que IBM no tenía ningún interés en dar el ancho de banda necesario para que los PCs compitieran con sistemas de gama alta. El efecto en términos estratégicos es similar a la antigua práctica romana de demoler todas las casas y cortar todos los árboles cercanos a sus carreteras o castillos. Ninguna estructura rival será permitida cerca de la plataforma de Intel; todas deben ser niveladas en comunes. Pero comunes ordenados y bien regulados: los interfaces deberían ser "abiertos pero no libres".

La idea del consorcio ha evolucionado en una forma altamente efectiva de burlar la ley antimonopolio. Hasta ahora, las autoridades no parecen preocuparse de semejante consorcio – mientras que los estándares sean abiertos y accesibles a todas las compañías. Quizás necesiten llegar a ser un poco más sofisticados.

Por supuesto, si Fritz Hollings consigue llevar su ley hasta el Congreso, TCPA será obligatorio y el problema del antimonopolio caerá, al menos en Estados Unidos. Esperemos que los legisladores Europeos tengan más fundamento.

21. ¿Cuándo llegará a la calle todo esto?

Ya lo ha hecho. La primera [especificación](#)⁽²⁷⁾ se publicó en 2000. Atmel ya está vendiendo un [chip Fritz](#)⁽²⁸⁾, y aunque hace falta firmar un acuerdo de no divulgación (Non Disclosure Agreement – NDA) para obtener una hoja de especificaciones, puedes comprarlo instalado en [la serie Thinkpad de IBM](#)⁽²⁹⁾ desde mayo de 2002. Algunas de las características en Windows XP y en la X-Box son características de TCPA: por ejemplo, si tu cambias la configuración hardware de tu PC, tienes que volver a registrar tu PC con la empresa de Redmod. Desde Windows 2000, Microsoft ha estado trabajando en certificar todos los controladores (drivers): si intentas cargar un driver no firmado, XP se quejará. Hay también un creciente [interés del gobierno de los Estados Unidos](#)⁽³⁰⁾ en el proceso de estandarización técnica. El tren está en marcha.

Las fechas de implantación no están tan seguras. Parece ser que hay algo de desacuerdo entre Microsoft e Intel; Palladium también correrá en hardware de la competencia como [Wave Systems](#)⁽³¹⁾, y aplicaciones escritas para ser ejecutadas con TCPA estándar han sido reescritas para soportar Palladium también. Esto parece una jugada para asegurar que la plataforma informática segura del futuro sea controlada exclusivamente por Microsoft. También puede ser una táctica para desanimar a otras compañías que intenten desarrollar plataformas de software basadas en TCPA. Intel y AMD parece que planean para la segunda generación que las funcionalidades de Fritz estén integradas en el procesador principal. Esto podría aportar más seguridad, pero les permitiría controlar los desarrollos, en lugar de Microsoft.

Sé, efectivamente, que el anuncio Palladium fue hecho más de un mes antes de que yo presentara [un documento](#)⁽³²⁾ en una conferencia sobre [Economía del Software de Código Abierto](#)⁽³³⁾ el 20 de Junio. Este trabajo criticaba TCPA como anticompetitivo, como ampliamente ha sido confirmado por revelaciones desde entonces.

22. ¿Qué es TORA BORA?

Parece que es un chiste interno de Microsoft: mira la [presentación de Palladium](#)⁽³⁴⁾. La idea es que 'Trusted Operating Root Architecture' (Palladium) impedirá los ataques 'Break Once Run Anywhere' que significa que un contenido 'pirateado', una vez desprotegido, puede ser enviado a la red y usado por cualquiera.

Parece sers que se han dado cuenta desde entonces que este chiste puede ser de mal gusto. En una charla a la que atendí el 10 de Julio en el centro de Investigación de Microsoft, el eslogan había cambiado a 'BORE-resistance', donde BORE significa 'Break Once Run Everywhere'. (Por cierto, el ponente describió el marcado de agua como 'monitorización de contenidos' (content screening), un término que usó para referirse a impedir que los menores vean pornografía: la maquinaria de relaciones públicas está claramente cambiando! También nos contó que no funcionaría si no todo el mundo usase un sistema operativo 'fiable'. Cuando le pregunté si esto significaría eliminar Linux, me contestó que los usuarios de Linux deberían acostumbrarse a la monitorización de contenidos.



23. *¿Pero la seguridad del PC no es algo bueno?*

La pregunta es: ¿seguridad para quién? El usuario medio preferirá no preocuparse por virus, pero TCPA no solucionará eso: los virus explotan la forma en que las aplicaciones (como Microsoft Office y Outlook) utilizan el scripting. Puede que le moleste el SPAM, pero eso no será arreglado tampoco. (Microsoft afirma que eso se arreglará filtrando todos los mensajes no firmados – pero los spammers simplemente comprarán PCs TCPA. Acabas antes configurando tu cliente de correo actual para que filtre el correo de la gente que no conoces y ponerlo en una carpeta a la que echas un vistazo todos los días). Puede que se preocupe sobre la privacidad, pero TCPA no solucionará eso: casi todas las violaciones de privacidad resultan del abuso de acceso autorizado, generalmente obtenido mediante aceptación por la fuerza. La compañía de seguros médicos requerirá tu consentimiento para compartir sus datos con tu jefe, y con cualquiera a la que quiera venderse los, no va a parar simplemente por que sus PCs sean ahora oficialmente 'seguros'. Al contrario, es probable que los vendan más ampliamente, por que los ordenadores son ahora 'fiables'.

Los economistas se han dado cuenta de que cuando un fabricante hace un producto 'verde', habitualmente incrementa la contaminación, debido a que la gente compra 'verde', en lugar de comprar menos. Podemos ver un equivalente en esta 'trampa social de elección'. Además expandiendo los monopolios, la TCPA aumentará los incentivos para premiar la discriminación y de esta forma recolectar datos personales para realizar perfiles.

El aspecto más caritativo de la TCPA nos es mostrado por un investigador de Microsoft: hay algunas aplicaciones en las que tú quieres restringir las acciones del usuario. Por ejemplo, tú quieres impedir que la gente manosee el cuentakilómetros de un coche antes de venderlo. De forma análoga, si tú quieres hacer Control de Derechos Digitales (DRM) en un PC, tienes que tratar al usuario como el enemigo.

Visto en éstos términos, TCPA y Palladium no dan tanta seguridad al usuario, si no que lo hacen al fabricante del PC, al proveedor de Software y a la industria del contenido. No añaden valor para el usuario. Más bien lo destruyen por que restringen lo que se puede hacer con un PC – para permitir obtener más dinero de los usuarios a los proveedores de aplicaciones y servicios. Esto es la definición clásica de un cártel explotador – un acuerdo de la industria que cambia los términos del mercado para disminuir el beneficio del consumidor.

Sin duda, Palladium estará lleno de nuevas características de tal forma que en suma, parezca añadir valor a corto plazo, pero en la economía a largo plazo, las implicaciones legales y sociales requieren una reflexión seria. No doubt Palladium will be bundled with new features so that the

24. *Entonces, ¿por qué se le llama a todo esto 'Informática Fiable'? No veo por ningún sitio por qué debería fiarme en absoluto!*

Es prácticamente un chiste interno. En el Departamento de Defensa de los Estados Unidos, un 'sistema o componente fiable' es aquel que 'puede romper la política de seguridad'. Esto puede parecer anti-intuitivo en un principio, pero simplemente párate a pensarlo. Un guardian de correo o un firewall que están entre un sistema Secreto y otro Top Secret pueden – si fallan – romper la política de seguridad que dice que el correo solamente puede ir de Secreto a Top Secret, pero nunca al revés. Así, es fiable si asegura el cumplimiento de la política de flujo de información.

Un ejemplo civil: imagina que confías en que tu doctor guarde sus archivos médicos de forma privada. Esto significa que tiene acceso a tus informes, pudiendolos filtrar a la prensa si fuera poco cuidadoso o malicioso. Tu no te fías de mí para mantener tus informes médicos, por que no los tengo; independientemente si yo te odio o soy tu amigo, no puedo hacer nada para afectar tu política de que los informes médicos deben ser confidenciales. Tu doctor puede, sin embargo; y el hecho es que está en una posición de hacerte daño es por que tu confías en él. Puede que te parezca una persona agradable, o simplemente que te tengas que fiar de él por que es el único doctor en la isla en que vives; independientemente, la definición del DoD elimina esos aspectos emocionales y difusos de la 'confianza' (que confunden a la gente).

Recuerda que a finales de los 90, cuando la gente debatía el control del gobierno sobre la criptografía, Al Gore propuso una 'Tercera Parte Fiable' – un servicio que contendría una copia de tu clave de descifrado, solamente por si tú (o el FBI o la NSA) la necesitaba en algun momento. El nombre se derivaba de un ejercicio de marketing que vio la colonia rusa de Alemania del Este, llamada 'Republica Democrática'. Pero realmente tiene que ver con el pensamiento del DoD. Una Tercera Parte Fiable es una tercera parte que puede romper tu política de seguridad.

25. *Entonces, ¿un 'Ordenador Fiable' es aquel que puede romper mi seguridad?*



Lo has pillado.

[Ross Anderson](#)⁽¹⁾

Aquí hay una [traducción China](#)⁽³⁵⁾.

Aquí está el link a la primera versión online de este FAQ : [la version 0.2](#)⁽³⁶⁾.

Más comentarios sobre TCPA / Palladium de [ZDNet](#)⁽³⁷⁾, la [BBC](#)⁽³⁸⁾, [Internetnews](#)⁽³⁹⁾, [PBS](#)⁽⁴⁰⁾, [O'Reilly](#)⁽⁴¹⁾, [Linux Journal](#)⁽⁴²⁾, [Salon.com](#)⁽⁴³⁾, y [Extremetech](#)⁽⁴⁴⁾. Los comentarios de [Larry Lessig en un seminario Harvard](#)⁽⁴⁵⁾ son relevantes. Hay una [historia contada por un antiguo trabajador de Microsoft](#)⁽⁴⁶⁾ acerca de cómo se lanzó Palladium, y dos entradas en un Blog ([aquí](#)⁽⁴⁷⁾ y [aquí](#)⁽⁴⁸⁾) de Seth Schoen del adiestramiento de Microsoft a la EFF. La Unión Europea está [empezando a tomar nota](#)⁽⁴⁹⁾. Todo el revuelo que hemos creado ha [deprimido a los Analistas del mercado de PCs en Australia](#)⁽⁵⁰⁾. Hay un discurso del [ciberzar de Bush, Richard Clark](#)⁽⁵¹⁾ elogiando el TCPA (ver p 12); en la misma conferencia, el CEO de Intel, Craig Barrett dice que el gobierno debería dejar que la industria hiciera el control de derechos digitales, en lugar de obligar a una solución. Esto puede tener relación con [esta historia](#)⁽⁵²⁾ de Intel enfrentándose a la ley Hollings, al mismo tiempo que apoyan el TCPA.

Lista de enlaces de este artículo:

1. <http://www.cl.cam.ac.uk/~rja14/>
2. [http://bulmalug.net/mailto:frang_lAT\[terra D.O.T es](mailto:bulmalug.net/mailto:frang_lAT[terra D.O.T es)
3. <http://www.trustedpc.org>
4. <http://www.theregister.co.uk/content/4/25852.html>
5. <http://www.activewin.com/articles/2002/pd.shtml>
6. <http://www.theregister.co.uk/content/archive/23387.html>
7. <http://www.cw.com.hk/Comment/c990713001.htm>
8. <http://www.newscientist.com/news/news.jsp?id=ns99992483>
9. <http://www.vmware.com/>
10. <http://www.highcriteria.com/>
11. <http://www.dtc.umn.edu/~odlyzko/doc/history.communications1b.pdf>
12. <http://www.openoffice.org/>
13. <http://www.cis.upenn.edu/%7Ewaa/aegis.ps>
14. <http://comment.zdnet.co.uk/story/0,,t479-s2118863,00.html>
15. <http://cryptome.org/ms-drm-os.htm>
16. <http://cryptome.org/ms-drm-os2.htm>
17. <http://www.cl.cam.ac.uk/~mgk25/trustno1.pdf>
18. <http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf>
19. <http://www.nytimes.com/2002/07/04/business/04SCEN.html>
20. http://www.motorola.com/GSS/CSG/Help/PR/pr980723_wirelessbatt.html
21. <http://socrates.berkeley.edu/%7Eescotch/re.pdf>
22. <http://www.cl.cam.ac.uk/ftp/users/rja14/lucky>
23. <http://www.defcon.org/dc-speakers.html>
24. <http://www.cnn.com/2002/TECH/ptech/06/24/diagnosing.cars.ap/>
25. <http://www.playstation2-linux.com/faq.php>
26. <http://www.amazon.com/exec/obidos/ASIN/1578515149/rossandersshomep>
27. <http://www.trustedcomputing.org/>
28. <http://www.atmel.com/atmel/products/prod50a.htm>
29. <http://commerce.www.ibm.com/cgi-bin/ncommerce/CategoryDisplay?cgfnbr=2072541>
30. <http://yro.slashdot.org/article.pl?sid=02/07/07/0522219172>
31. <http://www.wave.com>
32. <http://www.cl.cam.ac.uk/ftp/users/rja14/toulouse.pdf>
33. <http://www.idei.asso.fr/ossconf.html>
34. <http://cryptome.org/palladium-sl.htm>
35. http://chat.ttv.com.tw/TCPA-Palladium_FAQ.html
36. <http://www.cl.cam.ac.uk/~rja14/tcpa-faq-0.2.html>
37. <http://zdnet.com.com/2100-1107-941111.html>
38. http://news.bbc.co.uk/hi/english/sci/tech/newsid_2094000/2094167.stm



39. <http://www.internetnews.com/asp-news/article.php/1378731>
40. <http://www.pbs.org/cringely/pulpit/pulpit20020627.html>
41. <http://www.oreillynet.com/pub/a/webservices/2002/07/09/udell.html>
42. <http://www.ssc.com/pipermail/suitwatch/2002q2/000024.html>
43. <http://www.salon.com/tech/feature/2002/07/11/palladium/index.html>
44. <http://www.extremetech.com/article2/0.3973.274309.00.asp>
45. <http://slashdot.org/articles/02/07/10/1820236.shtml?tid=123>
46. <http://www.kuro5hin.org/story/2002/7/9/17842/90350>
47. <http://vitanuova.loyalty.org/2002-07-03.html>
48. <http://vitanuova.loyalty.org/2002-07-05.html>
49. <http://www.theregister.co.uk/content/4/25988.html>
50. <http://australianit.news.com.au/articles/0.7204.4653378%5e15321%5e%5enbv%5e15306>
51. <http://www.bsa.org/resources/2002-03-16.99.pdf>
52. http://www.eff.org/IP/SSSCA_CBDTPA/20020308_eff_sssca_alert.html
53. <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>

E-mail del autor: kyle@navegalia.com

Podrás encontrar este artículo e información adicional en: <http://bulmalug.net/body.phtml?nIdNoticia=1398>