



LINUXA – Asociación Usuarios GNU/Linux de Cantabria

Preguntas frecuentes sobre Informática Fiable

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

Creado el 09/08/2003 20:38 y modificado por última vez el 09/08/2003 20:38

Esta es la Actualización de Agosto de 2003 para las antiguas [Preguntas Frecuentes sobre TCPA y Palladium](#)⁽¹²⁹⁾. En este artículo compañías se han aliado para implementar tecnología para el Control de Derechos Digitales y otros oscuros métodos para redu

Preguntas Frecuentes sobre Informática Fiable

TC / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA

Versión 1.1 (Agosto 2003)

Este documento se publica bajo la [Licencia de Documentación Libre GNU](#)⁽¹⁾. Están disponibles versiones en [alemán](#)⁽²⁾, español, [ita](#)⁽³⁾, [sueco](#)⁽⁷⁾, [finlandés](#)⁽⁸⁾, [húngaro](#)⁽⁹⁾, [hebreo](#)⁽¹⁰⁾ y [francés](#)⁽¹¹⁾. Recomendamos visitar la [Página de Recursos sobre Economía y Seguridad](#) complementaria a los temas expuestos aquí.

1.- ¿Qué es esta historia de la "Informática Fiable"?

El Grupo para la Informática Fiable ([Trusted Computing Group](#)⁽¹³⁾ TCG) es una alianza de Microsoft, Intel, IBM, HP, y AMD que "seguro". Su definición de "seguridad" es controvertida; las máquinas construidas según sus especificaciones serán mas fiables desde software y la industria del contenido, pero menos fiable desde el punto de vista de los dueños. De hecho, las especificaciones TCG quienquiera que escribiera el software que este ejecuta. (Sí, incluso más que ahora)

Al proyecto TCG se le conoce por una variedad de nombres. "Informática Fiable" (Trusted Computing) fue el original, que todavía Trustworthy Computing (NT: en castellano tendría un sentido similar a informática fiable) y la Free Software Foundation (FSF) lo computing. De aquí en adelante, lo llamaré simplemente TC. Entre otros nombres también puedes encontrar TCPA (el nombre original nombre de Microsoft para la [versión](#)⁽¹⁶⁾ que se publicaría en el 2004) y [NGSCB](#)⁽¹⁷⁾ (el nuevo nombre de Microsoft). Intel en este m más segura" (Safer computing). Muchos observadores creen que esta confusión es deliberada los promotores quieren distraer la at



2.– ¿Qué hace TC, en castizo?

TC aporta una plataforma informática donde las aplicaciones no pueden ser alteradas o modificadas, y donde éstas se pueden comunicar. Su aplicación original era el [Control de Derechos Digitales](#)⁽¹⁸⁾ (digital rights management – DRM): Disney podrá venderte DVD en plataformas TC, pero que no podrás copiar. La industria discográfica podrá venderte descargas de música que no podrás intercambiarlas muchas veces, o solamente el día de tu cumpleaños. Toda una nueva gama de posibilidades en marketing a su alcance.

TC hará también muy difícil ejecutar Software sin licencia. En la primera versión de TC, el software pirateado se podía detectar y borrar. Microsoft ha denegado en algunas ocasiones que quisiera que TC hiciera esto, pero en el [WEIS 2003](#)⁽¹⁹⁾ un director senior se negó a una meta: "Ayudar a que la gente ejecute software robado simplemente no es nuestra meta en la vida". Los mecanismos ahora propuestos protegerá los [procesos de registro](#)⁽²⁰⁾ de las aplicaciones, de tal forma que el software sin licencia esté bloqueado. Además, las aplicaciones TC, de tal forma que ya no merecerá la pena usar aplicaciones no-TC (incluyendo las piratas). Del mismo modo, algunos ficheros de viejas aplicaciones cuyos números de serie hayan sido prohibidos. Si Microsoft opina que tu copia de Office es pirata, y los documentos que intercambies con ellos se pueden volver ilegibles. TC también hace más fácil alquilar software que comprarlo; el software dejará de funcionar, si no probablemente también los ficheros creados con él. Así que si dejas de pagar actualizaciones para todas las canciones que compraste con él.

Durante años, Bill Gates ha soñado con una forma de [hacer pagar a los chinos por el software que usan](#)⁽²¹⁾, esta puede ser la respuesta.

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

También hay desventajas. Por ejemplo, puede que haya censura remota. En su forma más simple, se pueden diseñar aplicaciones para las que una se extrae canción protegida de una plataforma TC comprometida (crackeada) y es puesta en el Web como un fichero MP3, el receptor puede que lo detecte usando una marca de agua, informe de ello y sea informado de que debe borrarlo (del mismo modo que cualquier aplicación comprometida). Este modelo de negocio, denominado *traitor tracing* (búsqueda del traidor) ha sido investigado extensivamente por los investigadores digitales creados usando sistemas TC, permanecen bajo control de sus creadores, en lugar de bajo control de los dueños de las máquinas (actualidad). Entonces, el autor de un escrito designado como difamatorio por un tribunal, puede ser requerido a censurarlo y la emisor ordenada a borrar el fichero si el autor se niega. Dadas estas posibilidades, debemos esperar que TC sea usado para suprimir cualquier cosa a líderes políticos.

Las desventajas para las empresas es que los proveedores de software pueden hacer muy difícil cambiarse a un producto de un competidor. Sus documentos con claves a las que solo tendrían acceso otros productos de Microsoft; de tal forma que solo tendrías acceso usando otro procesador de textos de la competencia. Un bloqueo tan clamoroso probablemente sea prohibido por las autoridades antimonopolísticas sutiles que son mucho más difíciles de regular (Explicaré algunas de ellas más adelante).

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

Con los MP3s existentes, quizá no pase nada durante algún tiempo. Microsoft dice que TC no hará que nada deje de funcionar de momento. Windows Media Player ha causado [gran controversia](#)⁽²²⁾ insistiendo en que los usuarios deben aceptar una licencia que permita futuro borrado de contenido 'pirateado' encontrado en el ordenador. Del mismo modo, es poco probable que programas que dan a las peñas [VMware](#)⁽²³⁾ y [Total Recorder](#)⁽²⁴⁾, funcionen bajo TCPA. Así que tendrás que usar un reproductor diferente – y si éste reproduce MP3 no 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. Es difícil averiguar bajo qué condiciones se debe reproducir un determinado título protegido. De esta forma, yo espero que Microsoft haga algo pudiendo éstos experimentar con nuevos modelos de negocios: quizá puedas comprar CDs a un tercio de su precio, pero que solo si obtienes derecho a oírlo cuantas veces quieras. Quizá se te permita dejar tu copia digital de un disco a un amigo, pero entonces tu parte te la devuelva. Con más probabilidad, no podrás dejar música a tu amigo en absoluto. Estas políticas harán la vida más incómoda a 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 TC impida a Microsoft hacer más fácil a Microsoft controlar los parches y actualizaciones, será imposible escapar. El control sobre el software de reproducción antimonopolio de la Unión Europea [están proponiendo](#)⁽²⁵⁾ penalizar a Microsoft por su comportamiento anticompetitivo mediante la inclusión en el sistema operativo Windows herramientas de terceros. La profundidad y ámbito del control sobre medios será ampliado.

4.– ¿Cómo funciona TC?

TC provee métodos para monitorizar los componentes de los PCs ensamblados en el futuro. La implementación elegida en la primera generación es una arquitectura inteligente soldada a la placa madre. La versión actual tiene 5 componentes: el chip Fritz, una función de memoria acortinada (curtained memory) para la seguridad en el sistema operativo ("Nexus", en lenguaje Microsoft), un núcleo de seguridad en las aplicaciones TC (NCA según Microsoft), un conjunto de servidores de seguridad en línea mantenidos por los fabricantes de hardware y software para englobar todo.

Fritz supervisaba el arranque en la versión inicial de TC, de modo que el PC acababa en un estado predecible, con hardware y software. Un componente de monitorización pasivo que almacena el hash del estado de la máquina al arrancar. Este hash se calcula usando datos de hardware (sonido, vídeo, etc) y el software (sistema operativo, drivers, etc). Si la máquina finaliza en el estado aprobado, Fritz pondrá a disposición las claves criptográficas necesarias para descifrar aplicaciones TC y sus datos. Si no finaliza en un estado aprobado, el hash será incorrecto y no se podrá ejecutar aplicaciones no-TC y acceder a datos no-TC, pero el material protegido no estará disponible.

El núcleo de seguridad del sistema operativo ("Nexus") hace de puente entre el chip Fritz y los componentes de seguridad de las aplicaciones. Los componentes hardware estén en una lista TCPA aprobada, y que los componentes software han sido firmados y que ninguno de ellos ha sido revocado. Si se hacen cambios significativos a la configuración de un PC, el ordenador debe conectarse a Internet para poder ser verificado. El servidor encargado de todo esto. El resultado es un PC que arranca en un estado conocido con una combinación aprobada de hardware y software. Finalmente, Nexus funciona junto a la nueva "memoria acortinada" para impedir que ninguna aplicación TC lea o escriba los datos. Los fabricantes denominan [Lagrande Technology](#)⁽²⁶⁾ (LT) para CPUs Intel y [TrustZone](#)⁽²⁷⁾ para ARM.

Una vez que la máquina esté en este estado aprobado, con aplicaciones TC cargadas y aisladas de interferencias causadas por otros programas: por ejemplo, puede autenticarse ante Disney para probar que la máquina es un receptor adecuado de "Blancanieves". Esto significa que en ese momento un programa autorizado – MediaPlayer, DisneyPlayer, lo que sea – con su NCA correctamente cargado y aislado por la arquitectura (debuggers) u otras herramientas diseñadas para copiar el contenido. El servidor de Disney entonces manda datos encriptados, con la clave solamente pondrá la clave a disposición de la aplicación mientras el entorno permanezca 'fiable' (trustworthy). En este caso, fiable significa Seguridad bajada del servidor de políticas diga. Esto significa que Disney podría ofrecer sus contenidos solamente al autor de un programa que respetar ciertas condiciones. Éstas pueden ser pagos, por ejemplo: Disney puede insistir en que la aplicación cobre 1 dólar cada vez que se use. La misma también puede ser alquilada. Parece que las posibilidades están solamente limitadas por la imaginación de los vendedores...

5.– ¿Para qué mas se puede usar TC?

Se puede usar TCPA para implementar controles de acceso mucho más fuertes para documentos confidenciales. Estos controles ya existen en Windows Server 2003, bajo el nombre de "Enterprise rights management", y la gente está empezando a experimentar con ellos.

Una característica interesante es la [destrucción automática de documentos](#)⁽²⁸⁾. Después de sufrir embarazosas revelaciones de emails, Microsoft desarrolló una política interna en la que todos los emails se destruyen al cabo de 6 meses. TC haría que esto esté disponible en la plataforma Microsoft (piensa qué utilidad habría tenido esto para Arthur Andersen durante el caso Enron). También se podrá utilizar para que una 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. Los controles más sutiles: por ejemplo, si mandas un correo criticando a tu jefe, éste puede mandar un mensaje de cancelación que borra el correo. También funciona a través de dominios: por ejemplo, una compañía puede decidir que su correspondencia legal solamente pueda ser leída por los abogados y sus secretarías.

TC también se podrá usar para sistemas de pago. Una de las ideas de Microsoft es que mucha de la funcionalidad existente en las tarjetas de crédito una vez que este sea resistente a alteraciones. Esto nos llevará a un futuro donde paguemos por los libros que leemos y la música que escuchamos.



por página o por minuto. La industria de la banda ancha [impulsa esta idea](#)⁽²⁹⁾, mientras que alguna gente con una visión más amplia pensando que Microsoft quiera cobrar un porcentaje en todas sus ventas. Incluso si los micropagos no funcionan como modelo de [persuasivos](#)⁽³⁰⁾ diciendo que no habrá grandes cambios en los sistemas de pago online, con un efecto dominó para el usuario. Si, de una tarjeta de crédito si no tienes TC, será un momento duro para los usuarios de Mac o GNU/Linux.

El atractivo de TC para la gente de sistemas de los gobiernos es que se use ERM para implementar "control obligatorio de acceso", acceso independiente de los deseos del usuario, si no simplemente basadas en su status. Por ejemplo, un ejército puede decidir que documentos Word marcados como 'Confidenciales' o superior, y que sólo un ordenador TC con un certificado expedido por su propio documento como este. De esta forma, los soldados no podrían enviar documentos a la prensa (ni mandárselos a su propia casa, vía organizaciones grandes y complejas como un gobierno, por que los controles de acceso dificultan el trabajo diario de las personas, duda tendrán que aprender por las malas (El control obligatorio de acceso puede ser más útil para organizaciones más pequeñas como de la cocaína puede hacer que una hoja de cálculo con los últimos embarques de droga para este mes solamente se pueda leer en 5 minutos de validez hasta fin de mes. Entonces las claves utilizadas para cifrarlo expirarán y los chips Fritz en esas 5 máquinas nunca más las h

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

Para Intel, que inició todo este proyecto, era una jugada defensiva. Dado que hacen la mayor parte de su dinero a través de los micropagos parte del mercado, solo podían hacer crecer la compañía agrandando el mercado. Estaban decididos a que el PC fuera el centro de los entretenimientos será la aplicación principal, y el DRM será una tecnología crítica para ello, los PCs tiene que proveer DRM o corre

Las motivaciones de Microsoft también vienen del deseo unir el mercado del entretenimiento a su imperio. Pero por otra parte, también se convierte en popular. Hay dos razones. La primera, y menos importante, es reducir grandemente la copia ilegal de Software. 'Hacer de las grandes metas de Bill Gates; con TC, puede ligar a cada PC una única copia registrada de Windows y Office, y evitar que corra un universo TC.

El segundo, y más importante, beneficio para Microsoft es que TC aumentará enormemente los costes de migrar desde productos Microsoft (como [OpenOffice](#)⁽³¹⁾). Por ejemplo, si un bufé de abogados desea migrar de Office a OpenOffice hoy mismo, solamente tendría que convertir los ficheros existentes. Dentro de 5 años, cuando hayan recibido documentos protegidos por TC de una centena de clientes (con certificado digital) para migrar estos ficheros a una plataforma diferente. En la práctica, el bufé no hará esto, de tal forma que no te preocupes por los precios cuanto desee.

Los economistas que han estudiado la industria del software han llegado a la conclusión que el valor de una empresa de software es el que se cambien a uno de sus competidores; ambos son iguales al valor neto presente de futuros pagos de los clientes. Esto significa que una empresa maduro, como Microsoft con Office, solamente puede crecer más rápidamente que el mercado si encuentra una forma más agresiva de esta teoría, pero la idea es muy conocida por los ejecutivos de las empresas de software. Esto explica el comentario de Bill Gates: "[nos hemos dado cuenta que el correo electrónico y los documentos son mucho más interesantes](#)"⁽³²⁾.

7.– ¿De dónde viene la idea?

El concepto de TC de iniciar una máquina en un estado conocido está implícita en los primeros PCs donde la ROM estaba en la BIOS y un virus se pudiera esconder. La idea de una secuencia de arranque fiable para máquinas modernas apareció por primera vez en un ensayo de Jonathan Smith, '[Una Arquitectura Segura y Fiable para Secuencias de Arranque \(Bootstraps\)](#)'⁽³³⁾, en los procesos del Simposio IEEE de 1965–71. Esto llevó a la patente US 'Arquitectura Segura y Fiable para Secuencias de Arranque', U.S. Patent No. 6,185,678, February 1999, que parte del trabajo sobre firmado de código que hizo mientras estaba en la NSA en 1994. Este chico de Microsoft también solicitó un [sistema operativo](#)⁽³⁴⁾. (Los textos de las patentes están [aquí](#)⁽³⁵⁾ y [aquí](#)⁽³⁶⁾.)

Puede que existan bastantes desarrollos anteriores (prior art). Markus Kuhn escribió hace años sobre el [Procesador TrustNo1](#)⁽³⁷⁾ y la 'Referencia' fiable que supervisa las funciones de control de acceso de un ordenador – se remontan al menos a [un escrito de James](#) que 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 mediados de los 90 que hubiera añadido la funcionalidad de los chips Fritz dentro del propio controlador de caché, en el 2000. El número de serie del Pentium 3 fue un paso previo en esta dirección. La adversa respuesta pública en forma que se creó un consorcio junto a Microsoft y otros. El consorcio que crearon, [Trusted Computing Platform Alliance \(TCPA\)](#)

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

En honor al senador Fritz Hollings, de Carolina del Sur, que [trabajó incansablemente](#)⁽⁴¹⁾ en el congreso para hacer TC una parte obvia del consumo. (La ley de Hollings fracasó; perdió su sillón en el Comité de comercio, ciencia y transporte del Senado y se jubilará en el futuro). Como ejemplo, Microsoft se está gastando una fortuna en Bruselas promoviendo una directiva borrador sobre Propiedad Intelectual [realmente](#)

10.– **OK, entonces el TCPA impide que los críos intercambien música, y ayuda también a que los datos confidenciales. También puede ayudar a la Mafia, a no ser que el FBI tenga una puerta de escape. Pero a parte de piratas, espías industriales y activistas, quien estará en desacuerdo?**

Muchas compañías tienen mucho que perder, como los proveedores de Seguridad de la Información. Cuando Microsoft lanzó TC básicamente eliminaría el spam, los virus y prácticamente cualquier otra cosa en el ciberespacio – si esto es así, las compañías de software antivirus, anti-spam, las firmas que desarrollan firewalls y los detectores de intrusiones ya no tendrían nada que comer. Ahora han rebajado sus intenciones: [admite](#)⁽⁴⁴⁾ (cypherpunk33/cypherpunk) que Microsoft atacará el mercado de seguridad de forma agresiva: "Dado que es un área de alta prioridad de nuestras intenciones".

Mientras tanto, las preocupaciones sobre los efectos sobre la [innovación y la competencia](#)⁽⁴⁵⁾ continúan creciendo. Los efectos sobre la [reciente columna del New York Times](#)⁽⁴⁶⁾ escrita por el distinguido economista Hal Varian.

Pero hay problemas mucho más profundos. El tema fundamental es que quien controle la infraestructura TC obtendrá una inmensa ventaja. El control es como hacer que todo el mundo use el mismo banco, o el mismo contable o el mismo abogado. Hay gran cantidad de foros

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' de TC, dado que TC hará inviolable el proceso de registro de una aplicación. Pero, ¿qué pasa con los vídeos o canciones pirateados? ¿se puede hacer esto si es necesario poniendo un micrófono al lado de los altavoces de una máquina TC, y grabándolo como MP3? La solución propuesta es de agua digital, y los reproductores autorizados que no detecten esta marca de agua no reproducirán la canción a no ser que venga en un dispositivo. Pero, ¿qué pasará si alguien hackea un chip Fritz y realiza una transacción que legítimamente le transfiere la propiedad de la tecnología de búsqueda del traidor para encontrar desde qué PC se extrajo esa canción. Entonces, pasarán dos cosas. Primero, el dueño será juzgado judicialmente (Esa es la teoría al principio, probablemente no funcionará por que los piratas usarán PCs hackeados o no-TC). Segundo, esa máquina se pondrán en una lista negra, que los reproductores TC actualizarán de vez en cuando vía Internet.

Las listas negras tienen más usos a parte de impedir la copia de música. Se pueden usar para monitorizar todos los ficheros que abren un número de serie de la aplicación que los creó, o por cualquier otro criterio deseable. El propósito de esto es que si todo el mundo usa una máquina TC, evitas este uso en una máquina TC; simplemente motivas a que todos los chinos usen PCs normales en lugar de ordenadores TC. Todos los ordenadores TC del mundo se nieguen a abrir ficheros que han sido creados por este programa pirata. Esto creará una presión enorme para los c



spammers empezaron a usar cuentas en China, muchos ISP americanos [simplemente aislaron toda China](#)⁽⁴⁷⁾, cosa que obligó al gob

El potencial de abusos va más allá de intimidaciones entre empresas o batallas económicas si no que llega a la censura política. Esp alguna fuerza policial bienintencionada obtendrá una orden contra una imagen pornográfica de algún niño, o un manual de cómo sa ordenadores TC simplemente borrarán o informarán sobre estos documentos. Entonces un denunciante en un proceso judicial o en juez contra un documento ofensivo; quizá los Cienciólogistas intenten censurar al famoso [Fishman Affidavit](#)⁽⁴⁸⁾. La policía secreta panfleto disidente simplemente borrando todo lo que él creó usando ese sistema su nuevo libro, sus declaraciones de hacienda, inc de sus hijos todo borrado. En el este, los jueces apoyándose en la doctrina de confiscar, pueden "aislar" una máquina que ha sido u un niño. Una vez que los abogados, jueces y policías se den cuenta del potencial, el goteo se convertirá en un aluvión

La edad moderna empezó cuando Gutenberg inventó la imprenta móvil en Europa, que permitió que la información se preservara y querían prohibirla. Por ejemplo, cuando Wycliffe tradujo la Biblia al inglés en 1380–1, el movimiento Lollard que el inició fue red el nuevo testamento en 1524–5, fue capaz de imprimir más de 50000 copias antes que le cogieran y quemaran en la hoguera. El vie era comenzó. Las sociedades que han intentado controlar la información se convirtieron en poco competitivas, y con la caída de la democrático liberal había ganado. Pero ahora, TC pone en riesgo la incalculable herencia que Gutenberg nos dejó. Los libros electr los juzgados pueden prohibir su publicación, y la infraestructura TCPA les hará el trabajo sucio.

La Unión Soviética intentó mantener un registro y controlar todas las máquinas de escribir y faxes. Del mismo modo, TC intenta re problema es que todo el mundo está empezando a usar ordenadores. No tenemos ni idea de dónde nos llevará un sistema de control

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. administrador, y usar aplicaciones inseguras.

Sin embargo hay un pequeño problema. Si desactivas TC, Fritz no te dará las claves adecuadas para descifrar tus propios ficheros o TC no funcionarán bien, o incluso no lo harán en absoluto. Sería como cambiarse de Windows a Linux en estos días; tienes más lib las aplicaciones que usan TC son más atractivas para la mayoría de la gente o para los vendedores de software, puedes acabar simp forma que mucha gente tienen que usar Microsoft Word porque todos sus amigos y colegas les envían documentos en formato Mic que los costes de desactivar TC son simplemente intolerables.

Esto tiene algunas implicaciones interesantes para la seguridad nacional. En el [Simposio TCG](#)⁽⁴⁹⁾ en Berlín, lo expuse de esta forma 2 botones rojos en su escritorio uno que mande misiles a China y otro que desactive todos los PCs de China y adivinas a cual le te los asistentes a la charla dijo "¿y qué pasa con el botón para Europa?") Esto puede parecer una exageración, pero es una exageración poder han estado entrelazadas desde el Imperio Romano, y un dirigente prudente no puede descartar las implicaciones estratégicas tener que migrar de Windows a GNU/Linux en medio de una crisis internacional.

13.– ¿Entonces los motivos económicos y políticos van a ser importantes aquí?

Exactamente. Los beneficios más altos en el mercado de bienes y servicios de tecnologías de la información llegan a aquellas empr pueden establecer la compatibilidad con ellas; lo suficiente como para controlar los mercados de productos complementarios. Un e [ordenador](#)⁽⁵⁰⁾. Desde que la Xerox N24 apareció en 1996, muchos fabricantes de impresoras han comenzado a poner [chips de auten](#) forma que las impresoras pueden reconocer cartuchos de terceras partes o cartuchos recargados, negándose a funcionar con ellos. E llevando a un conflicto comercial entre Europa y Estados Unidos. En los Estados Unidos, un juez ha otorgado a Lexmark un [mand](#) con chips que funcionen con sus impresoras. Mientras tanto, la Comisión Europea ha adoptado una [Directiva sobre residuos de apa](#) los estados miembro, a finales del 2007, a ilegalizar caso omiso sobre las leyes de reciclado en la Unión Europea que realizan las c impiden que sean reciclados.

Este no es un problema solamente de impresoras. Algunos [fabricantes de móviles](#)⁽⁵⁴⁾ usan chips de autenticación embebidos para as



no de otra empresa. La Playstation 2 de Sony también usa una autenticación similar para asegurarse de que los cartuchos de memoria no sean de una empresa competidora más barata. La Xbox de Microsoft no es diferente. Hasta ahora, todo el mundo que quería embarcarse en esta tecnología hardware. Esto puede que sea fácil para fabricantes de hardware, pero era demasiado caro para la mayor parte de compañías.

TC permitirá que los fabricantes de software lleven a cabo tantas restricciones en sus productos como deseen. Dado que el fabricante de políticas de seguridad, puede dictar los términos bajo los cuales cualquier software de otro fabricante interoperará con el suyo propio, el software era rápida y furiosa por que había millones de PCs ahí fuera, con datos cuyo formato era conocido y entendido. Si tenía una libreta de direcciones, podrías programar una aplicación que tratara con la media docena de formatos comunes en PCs, PDAs y teléfonos móviles, millones de clientes potenciales. En el futuro, los dueños de estos formatos estarán fuertemente tentados de restringirlos usando TC. Los fabricantes alquilarán a terceras partes que quieran acceder a ellos. Esto será [muy malo para la innovación](#)⁽⁵⁵⁾. Esto será posible porque el servicio de asegurarse de que las políticas sobre qué otras aplicaciones acceden a un fichero creado por una aplicación TC se cumplen.

Entonces una aplicación TC exitosa valdrá mucho más dinero para la empresa de software que la controla, dado que pueden alquilar el mercado en el que estén. Entonces, la mayoría de desarrolladores de aplicaciones las harán compatibles con TC; y si Windows es el estándar tendrá una gran ventaja competitiva sobre GNU/Linux y MacOS en 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, [Ingeniería Inversa](#)⁽⁵⁶⁾, Yale Law Journal, May 2002, 1575–1663. Pero la ley, en la mayoría de los casos, sólo te da la oportunidad de hacer ingeniería inversa para compatibilidad. Hacer ingeniería inversa significaba tener que jugar con los formatos de ficheros, había una disputa real – Cuando Word y Word Perfect querían hacer ingeniería inversa para ellos intentaba leer los ficheros del otro e impedir que leyera los propios. Sin embargo, con TCPA se acabó el juego; sin acceso a los formatos de ficheros, 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 TC: ver [un post](#)⁽⁵⁷⁾ de [Con](#)⁽⁵⁸⁾ para oír más. Es una táctica que va más allá del mundo informático. El congreso está [molesto](#)⁽⁵⁹⁾ por que los fabricantes de coches quieren evitar que sus clientes reparen sus coches en talleres independientes. Y el chico de Microsoft dice que quieren TC en todas partes, y las implicaciones económicas en todo el mundo 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., con Fritz). Sin embargo, a partir de la fase 2, Fritz simplemente desaparecerá dentro del microprocesador. Llamémosle 'Hexium' – y las herramientas de ingeniería inversa de un 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 hace. En Europa tendremos que tratar con [Directiva Europea sobre Copyright](#)⁽⁶⁰⁾ (si ésta es aprobada) y el borrador de [Directiva para su cumplimiento](#) (la Directiva sobre copyright hace ilegal la investigación sobre criptografía)

Por otra parte, en muchos productos el control sobre compatibilidad se mezcla deliberadamente con el control sobre copia. Los chips de DVD también contienen el algoritmo de encriptación de los DVD, por lo que los que hagan ingeniería inversa pueden ser acusados de burlar el control de copia 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 sir Michael Jagger sea un p... económico más significativo sea el fortalecimiento de los poseedores de derechos en los mercados de bienes y servicios de la inform... Esto puede significar un aumento en el tope del mercado para firmas como Intel, Microsoft e IBM – pero a costa del crecimiento y [documenta](#)⁽⁶¹⁾ cómo la mayor parte de innovaciones que generan crecimiento económico no son anticipadas por los desarrolladores... cambios tecnológicos en los mercados de bienes y servicios de tecnologías de la información son habitualmente acumulativos. Dar... métodos para impedir que la gente de nuevos usos a sus productos es una mala idea.

La inmensa centralización de poder económico que TC representa favorecerá a las empresas grandes sobre las pequeñas; habrá efectos... grandes compañías obtener más de sus actividades económicas, como con las empresas de coches forzando a los dueños a hacer su... Como el mayor crecimiento en el empleo tiene lugar en el sector pequeño o mediano, esto podría tener consecuencias para los pue...

También puede que haya distintos efectos regionales. Por ejemplo, el patrocinio durante muchos años por parte de los Gobiernos E... inteligentes muy fuerte, a costa de impedir otras innovaciones. Según los veteranos de la industria a los que he consultado predican... inserte las funcionalidades de Fritz en el procesador principal, esto destruirá las ventas de tarjetas inteligentes. Muchas de las funci... quieren que éstas hagan se podrán hacer con los Fritz de tu portátil, tu PDA o tu teléfono móvil. Si esta industria es eliminada debie... gran parte de la industria en seguridad de la información desaparecería.

17. ¿Quién más perderá?

Hay muchos sitios donde los actuales procesos de negocios se alteran para permitir que los poseedores del copyright obtengan nuev... solicité permisos para convertir un campo que tenemos en un jardín; para hacer esto, necesitaba aportar seis copias de un mapa 1:1... podía obtener un mapa de la biblioteca local y fotocopiarla. Ahora los mapas están en un servidor en la biblioteca, con control de c... 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. I... habitualmente acabarán pagando mucho más a las compañías de mapas. Eso puede parecer un pequeño problema; multiplícalo para... economía en general. Parece ser que las transferencias de beneficios, una vez mas, serán desde las pequeñas empresas a las grandes...

Un muy conocido abogado británico ha dicho que las leyes de copyright solamente se toleran por que no se asegura su cumplimiento... infractores. Y puede que haya algunos casos particularmente resaltables de buena suerte. Entiendo que las [regulaciones de copyright](#)... eliminarán el derecho de uso–justo a los invidentes para usar sus programas de interpretación para leer libros electrónicos. Normal... puede que no importe mucho, dado que mucha gente simplemente la ignoraría y la policía no sería tan idiota como para perseguir a... las regulaciones sobre copyright a través de una protección hardware que son difícilmente rompibles, entonces los invidentes pueden... grupos menores en situación similar)

18. Uhh! ¿Qué más?

TC puede minar la General Public License (GPL), la licencia bajo la cual se distribuyen muchos productos libres y de código abier... los frutos del trabajo voluntario y en común sean secuestrados por compañías privadas para su beneficio. Cualquiera puede usar y r... licencia, pero si distribuyes una copia modificada, tienes que ponerla disponible al mundo junto con el código fuente para que otros... mismos.

IBM y HP ya ha iniciaron aparentemente un programa de desarrollo de una versión de GNU/Linux que soporte TC. Esto supondrá... características. Para obtener un certificado de evaluación aceptable para el TCG, el patrocinador enviará el código recortado a un la... cantidad de documentación describiendo el trabajo hecho, incluyendo un número de análisis probando por qué varios ataques ya co... evaluación está a nivel EAL3, suficientemente cara para mantener fuera a la comunidad del software libre, aunque relajada como p... hacer pasar su infestado código fuente). El truco es éste. Aunque el programa modificado esté cubierto por la GPL, y sea libre para... características TC a no ser que sea firmado, y tenga un certificado que le permita usar la infraestructura de clave pública (PKI) de T... principio, sí en algún momento)



Se podrán hacer modificaciones al código modificado, pero no podrás obtener ningún certificado que te permita entrar en el maravilloso mundo de [linux distribuido por Sony](#)⁽⁶²⁾ para su Playstation 2; los mecanismos de protección anticopia de la consola impiden la ejecución de programas que no sean compatibles con las características del hardware. Incluso si un filántropo hiciera un GNU/Linux seguro y sin buscar beneficios, el producto resultante no sería un sistema operativo TCPA, si no un sistema operativo propietario que el filántropo podría dar libremente. (Hay todavía aspectos sobre quién debería emitir los 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. Pero TC cambia eso. Una vez que sean compatibles TC, la GPL no funcionará como se preveía. El beneficio para Microsoft no es que esto destruirá el software libre, sino que este: una vez que incluso el código GPL pueda ser secuestrado para propósitos comerciales, los programadores estarán mucho menos interesados en contribuir.

19. Mucha gente se molestará con esto

Y hay muchos otros aspectos políticos – la transparencia del procesado de datos personales que la directiva Europea sobre protección de datos, la soberanía, sobre qué regulaciones sobre copyright promulgará cada país, como en el presente; o si Microsoft utilizará TCPA para impedir que otros sean como por ejemplo Apache; y si la gente estará de acuerdo con que sus PCs, en realidad, estén efectivamente, bajo control remoto – por jueces o agencias gubernamentales sin su conocimiento.

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

En Estados Unidos, probablemente no. Intel ha empleado una 'plataforma de liderazgo', en la cual ellos conducen los esfuerzos de la industria para 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](#)⁽⁶³⁾. Intel quiere compartir el desarrollo de la tecnología, hacer que los miembros fundadores ponga algo de Propiedad Intelectual (PI) en ello, publicarlo y licenciarlo a la industria bajo la condición de que los licenciatarios, en retorno, licencien cualquier propiedad intelectual suya que involucre a 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 dominante en ninguna tecnología pueda amenazar la dominancia de Intel en la plataforma PC. Así, del mismo modo que Intel no puede ser 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 una gama alta. El efecto en términos estratégicos es similar a la antigua práctica romana de demoler todas las casas y cortar todos los árboles. Ninguna estructura rival será permitida cerca de la plataforma de Intel; todas deben ser niveladas en comunes. Pero comunes ordenadas para 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 del consorcio – mientras que los estándares sean abiertos y accesibles a todas las compañías. Quizás necesiten llegar a ser un poco más estrictos.

En Europa, la ley cubre específicamente los consorcios, y se está endureciendo. Hubo una [conferencia en Berlín sobre TC](#)⁽⁴⁹⁾, organizada por el Parlamento Europeo y el Trabajo, en donde ponentes pro y anti TC exponían sus motivos. Si lees alemán, hay un [análisis muy cuidadoso de los aspectos sobre TC](#) de Christian Koenig; el resumen es que TC aparentemente viola la ley Europea de competencia en un número de aspectos. Los grupos de consumidores tienen una excepción a la ley antimonopolio solamente si son no exclusivos abiertos y no discriminatorios. TCG no lo es. Discrimina contra negocios que los pequeños negocios sean socios, y sus licencias de pago discriminan al software libre. Hay además un número de problemas de independencia de este. La Unión Europea está a [punto de encontrar culpable a Microsoft](#)⁽⁶⁵⁾ de intentar extender su monopolio en sus interfaces. Si se pueden bloquear los interfaces mediante TC, esto lo empeorará aún más. TC permitirá a Microsoft extender su monopolio en sus servicios de música online o a software de móviles.

Sin embargo, una cosa es la ley y otra es hacer que se cumpla. A finales del 2003, la Unión Europea deberá haber condenado a Microsoft en su relación a Netscape y en relación a los interfaces de servidores. Este juicio llega muy tarde como para resucitar a Netscape o para condenar a los navegadores. Para cuando la Unión Europea intente condenar a Microsoft por TC, estaremos en el 2008. En esa fecha quizá nuestra ley sea políticamente posible hacer algo efectivo.



21. ¿Cuándo llegará a la calle todo esto?

Ya lo ha hecho. La primera [especificación](#)⁽⁶⁶⁾ se publicó en 2000. Atmel ya está vendiendo un [chip Fritz](#)⁽⁶⁷⁾, y aunque hace falta un [Disclosure Agreement – NDA](#) para obtener una hoja de especificaciones, puedes comprarlo instalado en [la serie Thinkpad de IBM](#). Las características en Windows XP y en la X-Box son características de TC: por ejemplo, si tu cambias la configuración hardware de tu empresa de Redmond. Desde Windows 2000, Microsoft ha estado trabajando en certificar todos los controladores (drivers): si interviene el [Enterprise Rights Management](#)⁽⁶⁹⁾ ya se incluye con Windows Server 2003. Hay también un creciente [interés del gobierno de los Estados Unidos](#) en la estandarización técnica. El tren está en marcha.

22. ¿Qué es TORA BORA?

Parece que es un chiste interno de Microsoft: mira la [presentación de Palladium](#)⁽⁷¹⁾. La idea es que 'Trusted Operating Root Architecture Once Run Anywhere' que significa que un contenido 'pirateado', una vez desprotegido, puede ser enviado a la red y usado por cualquier usuario sin "tracing" la tecnología de censura omnipresente.

Parece ser 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 de 2003, el eslogan había cambiado a 'BORE-resistance', donde BORE significa 'Break Once Run Everywhere'. (Por cierto, el ponente describió 'contenidos' (content screening), un término que usó para referirse a impedir que los menores vean pornografía: ¡la maquinaria de restricción de contenidos! También nos contó que no funcionaría si no todo el mundo usase un sistema operativo 'fiable'. Cuando le pregunté si esto significaría que los usuarios de GNU/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 TC no solucionará eso: los virus (como Microsoft Office y Outlook) utilizan el scripting. Puede que le moleste el SPAM, pero eso no será arreglado tampoco. (Microsoft filtra todos los mensajes no firmados. Pero acabas antes configurando tu cliente de correo actual para que filtre el correo de la gente que te interesa echas un vistazo todos los días). Puede que te preocupes sobre la privacidad, pero TC no solucionará eso: casi todas las violaciones de privacidad son autorizadas; TC [incrementa los incentivos](#)⁽⁷²⁾ para que las compañías recojan y vendan tu información personal. La compañía de seguridad no quiere compartir sus datos con tu jefe, y con cualquiera a la que quiera vendérselos, no va a parar simplemente por que sus PCs sean ahora 'fiables'. Probable que los vendan más ampliamente, por que los ordenadores son ahora 'fiables'. Los economistas llaman a esto trampa social: hacer algo menos peligroso, o hacerlo parecer menos peligroso, causa habitualmente que la gente lo use más o más descuidadamente, por lo que el resultado clásico es que los conductores de Volvo tienen más accidentes.

El [aspecto más caritativo de TC](#)⁽⁷³⁾ nos lo muestra [Roger Needham](#)⁽⁷⁴⁾ ex-director de investigación de Microsoft en Europa: hay algo que puede restringir las acciones del usuario. Por ejemplo, tú quieres impedir que la gente manosee el cuentakilómetros de un coche antes de comprarlo. El Control de Derechos Digitales (DRM) en un PC, tienes que tratar al usuario como el enemigo.

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



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

Es prácticamente un chiste interno. En el Departamento de Defensa de los Estados Unidos, un 'sistema o componente fiable' es aquel que puede parecer anti-intuitivo en un principio, pero simplemente párate a pensarlo. Un guardián de correo o un firewall que está diseñado para romper la política de seguridad que dice que el correo solamente puede ir de Secreto a Top Secret, pero nunca cumple con 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 tu información si fuera poco cuidadoso o malicioso. Tu no te fías de mí para mantener tus informes médicos, por que no los tengo; independientemente, puedo hacer nada para afectar tu política de que los informes médicos deben ser confidenciales. Tu doctor puede, sin embargo; y el 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 un profesional. 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 Copia' de tu clave de descifrado, solamente por si tú (o el FBI o la NSA) la necesitaba en algún momento. El nombre se derivaba de la República Democrática de Alemania del Este, llamada 'Republica Democrática'. Pero realmente tiene que ver con el pensamiento del DoD. Una Tercera Copia puede romper tu política de seguridad.

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

Es una forma cortés de decirlo :-)

[Ross Anderson](#)⁽⁷⁵⁾

- Recomendamos visitar la [Página de Recursos sobre Economía y Seguridad](#)⁽¹²⁾, que aporta mucha información complementaria.
- Están disponibles versiones en [alemán](#)⁽²⁾, español, [italiano](#)⁽³⁾, [holandés](#)⁽⁴⁾, [chino](#)⁽⁵⁾, [noruego](#)⁽⁶⁾, [sueco](#)⁽⁷⁾, [finlandés](#)⁽⁸⁾, [húngaro](#)⁽⁹⁾.

Lecturas Complementarias (orden más o menos cronológico desde julio de 2002)

- Enlace para la [versión 0.2](#)⁽⁷⁶⁾ de este FAQ, y otro para [la 1.0](#)⁽⁷⁷⁾, que ha estado online desde Julio de 2002 hasta Agosto de 2002.
- Más comentarios sobre TCPA / Palladium de [ZDNet](#)⁽⁷⁸⁾, la [BBC](#)⁽⁷⁹⁾, [Internetnews](#)⁽⁸⁰⁾, [PBS](#)⁽⁸¹⁾, [O'Reilly](#)⁽⁸²⁾, [Linux Journal](#)⁽⁸³⁾, y comentarios de [Larry Lessig en un seminario Harvard](#)⁽⁸⁶⁾ son relevantes. Hay una [historia contada por un antiguo trabajador de Palladium](#), y dos entradas en un Blog ([aquí](#)⁽⁸⁸⁾ y [aquí](#)⁽⁸⁹⁾) de Seth Schoen del adiestramiento de Microsoft a la EFF. La Unión Europea también ha estado involucrada. Todo el revuelo que hemos creado ha [deprimido a los Analistas del mercado de PCs en Australia](#)⁽⁹¹⁾. Hay un discurso del [Congreso de los Estados Unidos](#) sobre TCPA (ver p 12); en la misma conferencia, el CEO de Intel, Craig Barrett dice que el gobierno debería dejar que la industria decida si quiere un lugar de obligar a una solución. Esto puede tener relación con [esta historia](#)⁽⁹³⁾ de Intel enfrentándose a la ley Hollings, al menos hay [un email de Bill](#)⁽⁹⁴⁾.
- Muchos de los aspectos expuestos fueron previstos por Richard Stallman en su famoso artículo [El derecho a leer](#)⁽⁹⁵⁾.
- Uno de los inventores de TC, Bill Arbaugh, tenía otras ideas e [hizo unas propuestas](#)⁽⁹⁶⁾ sobre como rediseñar TC para mitigar los problemas de seguridad dejando que los usuarios introduzcan sus propios certificados raíz (root certificates) o simplemente apagar Fritz completando el protocolo.
- [Lucky Green](#)⁽⁹⁷⁾ es uno de los primeros investigadores de TC, que más tarde se arrepintió. Su presentación en el Def Con 2 fue muy interesante.



- En este [intercambio de correos en la lista de criptografía](#)⁽⁹⁸⁾, Peter Biddle, director técnico de TC en Microsoft, explica algo con TC 1.0, un ordenador que estuviera ejecutando un proceso seguro e iniciara uno inseguro, debía matar el proceso seguro a TC inusable en la práctica por las nuevas formas de trabajar. Fue necesario ampliar las especificaciones y hacer que Intel que se pudieran ejecutar aplicaciones seguras e inseguras al mismo tiempo).
- Un correo de [John Gilmore](#)⁽⁹⁹⁾ a la lista cypherpunk, y algunos comentarios subsiguientes de [Adam Back](#)⁽¹⁰⁰⁾, [Seth Schoen](#)⁽¹⁰¹⁾.
- La [opinión de Bruce Schneier](#)⁽¹⁰²⁾; un poco de [polémica](#)⁽¹⁰³⁾ creada por Bill Thompson, que aparentemente se cree que de él tendrá ni virus ni spam y te permitirá ejercer tus derechos de uso-justo; y algunas [reacciones](#)⁽¹⁰⁴⁾...
- Microsoft editó un [FAQ sobre Palladium](#)⁽¹⁰⁵⁾ en Agosto de 2002 en el que desmentían que Palladium fuera a eliminar virus iniciales.
- En Septiembre de 2002, [Intel anunció Lagrande](#)⁽¹⁰⁶⁾. Este chip será el sucesor de su Pentium 4 y soportará el modo de *menor consumo* siguientes. Recibió este nombre debido a [un pueblo del este de Oregón](#)⁽¹⁰⁷⁾ (USA). Las reacciones iniciales fueron [hostiles](#) y empezaron a despertarse; apareció una [página web](#)⁽¹⁰⁹⁾ en EPIC, por ejemplo.
- En Octubre de 2002 vi un [artículo en Linux Devices](#)⁽¹¹⁰⁾ sobre los problemas que TCPA puede causar a los sistemas empujados a *ci*⁽¹¹¹⁾. Pero el punto fuerte del mes fue [Richard Stallman denunciando TC](#)⁽¹¹⁴⁾.
- El 7 de de noviembre tuvimos un [debate público sobre TCPA](#)⁽¹¹²⁾ entre los trajeados (Microsoft, HP, Infineon) y los *geeks* (desafortunadamente Channel 4 nos quitó del web), y un debate más corto al día siguiente en Cambridge, que formaba parte de [seguridad](#)⁽¹¹³⁾.
- En noviembre, TC entró en el mundo de la ciencia ficción, en la [más reciente historia corta de Cory Doctorow](#)⁽¹¹⁴⁾.
- El interés para los franceses seguía aumentando durante enero del 2003, con este [artículo en Le Monde](#)⁽¹¹⁵⁾.
- Sin embargo, el evento más importante de enero fue, sin embargo, que la versión propuesta por Microsoft para TC (Palladium) que si tienes un problema ente manos, ¡le tienes que cambiar el nombre! Desde entonces se conoce a Palladium oficialmente como Computing Base)
- En febrero de 2003, Microsoft anunció que incluiría muchas de las características de TC a nivel de aplicación en su Windows, el [control de derechos](#)⁽¹¹⁶⁾ que permitiría que un email se evaporara en la bandeja del receptor a los 30 días. Esto todavía se discute cuando el receptor tiene un servidor o cliente compatible con Microsoft, y se puede burlar parcheando el software (aunque en otra forma, vamos a empezar a tener esta funcionalidad en el mercado, y allanar el camino para TC más tarde. Hay comentario en [Zdnet](#)⁽¹¹⁹⁾.
- En abril, los distinguidos criptógrafos Whit Diffie y Ron Rivest [denunciaron a TC](#)⁽¹²⁰⁾ en una conferencia de RSA.
- En mayo, TCPA fue relanzado como [TCG](#)⁽¹²¹⁾ (el Trusted Computing Group, que anunció que estaban trabajando en la versión vendiéndose a finales del 2004 o en el 2005; y que el ámbito de TC se ampliaría de PCs a PDAs y teléfonos móviles. Lee [la continuación](#)⁽¹²³⁾; también puedes leer sobre la presentación de Bill en la [conferencia sobre ingeniería de hardware para Windows](#) (NGSBC).
- En Julio, Bill Gates [admitió ante el New York Times](#)⁽⁴⁴⁾ (cypherpunk33/cypherpunk) que Microsoft entraría agresivamente en un área de expansión, no debemos revelar nuestras intenciones". También insistió en que la mayor apuesta de la compañía era en el hardware (Longhorn). En otras palabras, la tecnología antiguamente conocida como Palladium se llama ahora NGSCB. Estás avisado.

Hablé en público sobre TC el 2 de julio en Berlín en el [simposio "Trusted Computing Group"](#)⁽⁴⁹⁾; más tarde en Bruselas el 8 de julio y otra vez el 14 de Julio en el [PODC](#)⁽¹²⁵⁾. Espero hablar en el [Helsinki IPR workshop](#)⁽¹²⁶⁾ en agosto. Estoy seguro que de habrá mas o menos. [mi estudio económico de TC](#)⁽¹²⁷⁾ ha aparecido en [una edición especial de Upgrade](#)⁽¹²⁸⁾ que trata sobre Propiedad Intelectual y asuntos de [seguridad](#)⁽¹²⁹⁾. [más amplia del documento](#)⁽⁴⁵⁾ trata en detalle algunos de los problemas aquí expuestos sobre políticas de competencia.

Ross Anderson

Cambridge, Inglaterra, Agosto de 2003

Lista de enlaces de este artículo:



1. <http://www.gnu.org/copyleft/fdl.html>
2. <http://moon.hipjoint.de/tcpa-palladium-faq-de.html>
3. <http://www.complixita.it/tcpa/>
4. <http://home.wanadoo.nl/squell/tcpa-faq.html>
5. http://chat.ttv.com.tw/TCPA-Palladium_FAQ.html
6. <http://www.efn.no/tcpa-faq-no.html>
7. <http://www.refactor.fi/pen/tcpa/faq.html>
8. <http://www.ffi.org/tcpa-palladium-faq-fi.html>
9. <http://tcpa.vajko.hu/>
10. <http://www.penguin.org.il/faq/downloads/tcpa-faq/>
11. <http://www.lebars.org/sec/tcpa-faq.fr.html>
12. <http://www.cl.cam.ac.uk/users/rja14/econsec.html>
13. <https://www.trustedcomputinggroup.org/home>
14. <http://linuca.org/body.phtml?nIdNoticia=54>
15. <http://www.theregister.co.uk/content/4/25852.html>
16. <http://www.activewin.com/articles/2002/pd.shtml>
17. <http://www.theregister.co.uk/content/4/29039.html>
18. <http://www.theregister.co.uk/content/archive/23387.html>
19. <http://www.cpppe.umd.edu/rhsmith3/index.html>
20. <http://www.geek.com/news/geeknews/2003Jul/gee20030729021057.htm>
21. <http://www.cw.com.hk/Comment/c990713001.htm>
22. <http://www.newscientist.com/news/news.jsp?id=ns99992483>
23. <http://www.vmware.com/>
24. <http://www.highcriteria.com/>
25. http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/03/1150/0|RAPID&style=Press_Room
26. <http://news.com.com/2100-1001-985156.html>
27. http://www.arm.com/news.nsf/html/TrustZone270503?OpenDocument&style=Press_Room
28. <http://www.theregister.co.uk/content/4/19368.html>
29. http://www.broadbanduk.org/news/bsg_press_release_23_07_03.htm
30. <http://www.dtc.umn.edu/~odlyzko/doc/history.communications1b.pdf>
31. <http://www.openoffice.org/>
32. <http://www.wininformant.com/Articles/Index.cfm?ArticleID=25681>
33. <http://www.cis.upenn.edu/~waa/aegis.ps>
34. <http://comment.zdnet.co.uk/story/0,,t479-s2118863,00.html>
35. <http://cryptome.org/ms-drm-os.htm>
36. <http://cryptome.org/ms-drm-os2.htm>
37. <http://www.cl.cam.ac.uk/~mgk25/trustno1.pdf>
38. <http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf>
39. <http://www.google.com/search?q=cache:bSqUxOLdZyoJ:www.trustedpc.org/+Computer+Platform+Alliance+Trusted&>
40. <http://news.com.com/2100-1009-996032.html>
41. http://www.salon.com/tech/feature/2002/03/29/hollings_bill/
42. <http://www.fipr.org/copyright/draft-ipr-enforce.html>
43. <http://web.archive.org/web/20020628074926/http://www.msnbc.com/news/770511.asp?cp1=1>
44. <http://www.nytimes.com/2003/07/25/technology/25SOFT.html>
45. <http://www.cl.cam.ac.uk/ftp/users/rja14/tcpa.pdf>
46. <http://www.sims.berkeley.edu/~hal/people/hal/NYTimes/2002-07-04.html>
47. <http://www.computing.co.uk/News/1129699>
48. <http://www.xs4all.nl/~kspaink/fishman/home.html>
49. <http://www.timekontor.de/home/veranstaltungen/26.html#26>
50. <http://www.ipjustice.org/030303.scc.shtml>
51. <http://www.scc-inc.com/special/oemwarfare/whitepaper/default.htm>
52. <http://slashdot.org/article.pl?sid=03/01/09/1228217&mode=thread&tid=123>
53. http://europa.eu.int/comm/environment/docum/00347_en.htm
54. http://www.cl.cam.ac.uk/ftp/users/rja14/mototola_battery_auth.html
55. <http://www.nytimes.com/2002/07/04/business/04SCEN.html>
56. <http://socrates.berkeley.edu/~scotch/re.pdf>



57. <http://www.cl.cam.ac.uk/ftp/users/rja14/lucky>
58. <http://www.defcon.org/dcx-speakers.html>
59. <http://www.cnn.com/2002/TECH/ptech/06/24/diagnosing.cars.ap/>
60. http://www.fipr.org/copyright/eucd_intro.html
61. <http://www.idei.asso.fr/Commun/Conferences/Internet/OSS2002/Papiers/VonHippel.pdf>
62. <http://www.playstation2-linux.com/faq.php>
63. <http://www.amazon.com/exec/obidos/ASIN/1578515149/rossandersshomep>
64. <http://www.tkrecht.de/index.php4?direktmodus=vortraege>
65. http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/03/1150/0|RAPID&mode=thread&tid=172
66. <http://www.trustedcomputing.org/>
67. <http://www.atmel.com/atmel/products/prod50a.htm>
68. <http://linuca.org/link/?l63>
69. <http://www.microsoft.com/windowsserver2003/techinfo/overview/wrm.msp>
70. <http://yro.slashdot.org/article.pl?sid=02/07/07/0522219&mode=thread&tid=172>
71. <http://cryptome.org/palladium-sl.htm>
72. <http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf>
73. <http://www.idei.asso.fr/Commun/Conferences/Internet/OSS2002/Papiers/Needham.PDF>
74. <http://www.cl.cam.ac.uk/~ksj/RogerNeedham.html>
75. <http://www.cl.cam.ac.uk/~rja14/>
76. <http://www.cl.cam.ac.uk/~rja14/tcpa-faq-0.2.html>
77. <http://www.cl.cam.ac.uk/~rja14/tcpa-faq-1.0.html>
78. <http://zdnet.com.com/2100-1107-941111.html>
79. http://news.bbc.co.uk/1/hi/english/sci/tech/newsid_2094000/2094167.stm
80. <http://www.internetnews.com/asp-news/article.php/1378731>
81. <http://www.pbs.org/cringely/pulpit/pulpit20020627.html>
82. <http://www.oreillynet.com/pub/a/webservices/2002/07/09/udell.html>
83. <http://www.ssc.com/pipermail/suitwatch/2002q2/000024.html>
84. <http://www.salon.com/tech/feature/2002/07/11/palladium/index.html>
85. <http://www.extremetech.com/article2/0.3973.274309.00.asp>
86. <http://slashdot.org/articles/02/07/10/1820236.shtml?tid=123>
87. <http://www.kuro5hin.org/story/2002/7/9/17842/90350>
88. <http://vitanuova.loyalty.org/2002-07-03.html>
89. <http://vitanuova.loyalty.org/2002-07-05.html>
90. <http://www.theregister.co.uk/content/4/25988.html>
91. <http://australianit.news.com.au/articles/0.7204.4653378^15321^^nbv^15306.00.html>
92. <http://www.bsa.org/resources/2002-03-16.99.pdf>
93. http://www.eff.org/IP/SSSCA_CBDTPA/20020308_eff_sssca_alert.html
94. <http://microsoft.com/mscorp/execmail/2002/07-18twc.asp>
95. <http://www.gnu.org/philosophy/right-to-read.es.html>
96. <http://www.cs.umd.edu/~waa/TCPA/TCPA-goodnbad.html>
97. <http://www.cypherpunks.to/>
98. <http://www.cl.cam.ac.uk/~rja14/biddle.txt>
99. <http://www.cl.cam.ac.uk/~rja14/gilmore.txt>
100. <http://www.mail-archive.com/cryptography@wasabisystems.com/msg02526.html>
101. <http://www.mail-archive.com/cryptography@wasabisystems.com/msg02510.html>
102. <http://www.counterpane.com/crypto-gram-0208.html#1>
103. <http://www.theregister.co.uk/content/6/26695.html>
104. <http://www.theregister.co.uk/content/6/26740.html>
105. <http://www.napolifirewall.com/MicrosoftPalladium.htm>
106. <http://yro.slashdot.org/yro/02/09/10/1514236.shtml?tid=118>
107. <http://www.lagrandeobserver.com/>
108. <http://www.theregister.co.uk/content/4/27065.html>
109. <http://www.epic.org/privacy/consumer/microsoft/palladium.html>
110. <http://www.linuxdevices.com/articles/AT7225637142.html>
111. <http://www.heise.de/ct/02/22/204/>
112. http://www.netproject.com/courses/TCPA_Update.html



113. <http://www.cl.cam.ac.uk/Research/Security/group-meetings.html>
114. <http://archive.salon.com/tech/feature/2002/08/28/0wnz0red/index.html>
115. <http://www.lemonde.fr/article/0,5987,3244--305691-,00.html>
116. <http://www.microsoft.com/windowsserver2003/evaluation/news/bulletins/wrm.mspix>
117. <http://www.geek.com/news/geeknews/2003Feb/gee20030225018810.htm>
118. <http://www.vnunet.com/News/1139309>
119. <http://news.zdnet.co.uk/story/0,,t269-s2130914,00.html>
120. <http://www.eetimes.com/story/OEG20030415S0013>
121. <http://www.trustedcomputinggroup.org/home>
122. <http://www.eetimes.com/story/OEG20030408S0046>
123. <http://www.eweek.com/article2/0,3959,1053556,00.asp>
124. <http://www.wired.com/news/privacy/0,1848,58745,00.html>
125. <http://turing.acm.org/podc/podc2003/>
126. <http://www.hiit.fi/de/mobileipr/workshop/>
127. <http://www.upgrade-cepis.org/issues/2003/3/up4-3Anderson.pdf>
128. <http://www.upgrade-cepis.org/issues/2003/3/upgrade-vIV-3.html>
129. <http://linuca.org/body.phtml?nIdNoticia=93>

E-mail del autor: kyle@navegalia.com

Podrás encontrar este artículo e información adicional en: <http://linuca.org/body.phtml?nIdNoticia=207>