Vom PC zum TC

Trusted Computing und Digital Restrictions Management

Dr. Volker Grassmuck

für Sammelband „Trusted Computing“
Schriftenreihe Kommunikation & Recht des Verlages Recht und Wirtschaft

Überarbeitete Fassung des Beitrags auf dem Panel
„Medienwirtschaft, Digital Rights Management und TCG “ auf dem
Symposium „Trusted Computing Group“
des Bundesministeriums für Wirtschaft und Arbeit,
daselbst, am 2. und 3. Juli 2003

Auf dem Umschlag von Pearson (2003), der Prosafassung der von der Trusted Computing Platform Alliance (TCPA[1]) geerbten Spezifikation ver. 1.1b. der Trusted Computing Group (TCG[2]), ist eine Waldszene mit dichtem Farnbewuchs zu sehen. Auf den ersten Blick kann man dies für eine beliebige Bebilderung eines Buches über einen hochabstrakten technischen Gegenstand halten. Hat man jedoch zum wiederholten Male von Vertretern von Intel, HP und anderen TCG-Mitgliedern gesagt bekommen, man dürfe im Zusammenhang mit TCG nicht

[1]http://www.trustedcomputing.org/

[2]https://www.trustedcomputinggroup.org/

über DRM und andere Anwendungen der Technologie sprechen,[3] erschließt sich die Aussage dieses Bildes: Wir bekommen die Bäume gezeigt, damit wir den Wald nicht sehen. Die TCG wird nicht einfach ein neues Bauteil in den PC einfügen. Sie legt das Fundament für eine völlig neue Architektur des Cyberspace, das sich auf unsere grundlegenden Wissenoperationen und Kommunikationsweisen, auf die Beziehungen zwischen Menschen und zwischen Menschen und Daten auswirkt. Dieser Aufsatz fokussiert die TCG-Architektur aus dem Blickwinkel des Digital Restrictions Managements (DRM) und zeigt eine Reihe heute schon absehbarer Folgen auf.

TCG …DRM?

TCG-Vertreter weisen jede Verbindung mit DRM zurück, wie sie namhafte Kritiker wie Prof. Ross Anderson von der Cambridge University[4] vorbringen. TCG habe nichts mit DRM zu tun und umgekehrt.

Begründet wird diese Aussage damit, dass die TCG nur einen Chip spezifiziere, der Schlüssel generiert und speichert und anderen Applikationen kryptographische Dienste anbietet. Sieht man davon ab, dass TCG außerdem eine Fülle von Operationen, weitere Technologien wie ein TCG-konformes BIOS, externe Validierungs- und Zertifizierungsinstanzen und ein ganzes Netzwerk von Rollen definiert, mag man der Behauptung folgen, dass TCG und DRM einander nicht bedingen.

Doch kryptographische Primitiven existieren nicht im luftleeren Raum. Tatsächlich wird „digital content delivery“ als eines der Anwendungsszenarien von TCG angepriesen (Pearson 2003: 7). Auch wenn die Hardware in der aktuellen Spezifikation nicht gegen Angriffe durch den Plattformeigentümer optimiert sein mag, „Remote Attestation“ und „Sealed Storage“ sind die zentralen Neuerungen von TCG und beide eignen sich vorzüglich für die kontrollierte Auslieferung von Content und dessen Nutzungskontrolle auf dem System des Nutzers. Man darf also, allen Beteuerungen des Gegenteils zum Trotz, davon ausgehen, dass DRM ein Anwendungsgebiet der TCG-Architektur sein wird.

Rollendefinitionen von TCG

Die Spezifikation definiert eine Anzahl von Entitäten, die für Aspekte einer Trusted Platform zuständig sind und die auf verschiedene Weisen auf sie einwirken können. Vor der Auslieferung eines Systems an den Nutzer werden drei von ihnen aktiv:

- „Trusted Platform Module Entity“ (TPME) = TPM-Hersteller: generiert und zertifiziert den Endorsement Key (EK), die ID des TPM; behält eine Kopie des öffentlichen Teils des EK, der für die Zertifizierung pseudonymer Identitätsschlüssel, für das Backup der Schlüssel, Migration u.a. Maintenance-Funktionen erforderlich ist. Die TPME kann ein TPM abschalten (Pearson 2003: 31).

[3] Dirk Kuhlmann, HP, wies bei der ZEI-Konferenz im Mai 03 eine Diskussion über die Validation Entities zurück: die gäbe es in der Spezifikation nur als Option, gehörten daher nicht zum Kern des Standards, über den allein man sprechen dürfe.

[4] Homepage Ross Anderson: http://www.cl.cam.ac.uk/users/rja14/

- „Conformance Entity“ = Konformitätslabor oder Plattform-OEM: zertifiziert, dass eine Klasse von TCG-Subsystemen TCG-konform ist
- „Platform Entity“= Plattform-Hersteller: zertifiziert, dass die Integration des TPM TCG-konform ist

Im laufenden Betrieb hat der Eigentümer neben der TPME vor allem mit zwei Entitäten zu tun:

- „Validation Entity“ = Hard- und Software-Hersteller: zertifiziert die Sollwerte für die Integritätsmessung, die auf ROM oder über das Internet bereitgestellt, im DIR (Data Integrity Register) gespeichert und mit Meßwerten in den PCRs (Platform Configuration Register) verglichen werden.
- „Privacy Certification Authority“ = Identitäts-CA der eigenen Wahl: zertifiziert anhand des von der TPME bereitgestellten Endorsement Key pseudonyme Schlüsselpaare und steht damit für die Kopplung eines gültigen TPM und einer gültigen Identität gerade.

Schließlich können drei Parteien von den Diensten des TPM Gebrauch machen:

- Eigentümer
- Nutzer
- Dritte (beliebige Transaktionspartner, z.B. Dienste- und Content-Anbieter)

Eigentümer und Nutzer sind im Falle eines privaten PC identisch, aber getrennt bei einem Unternehmens-PC oder einem öffentlichen Terminal. Der Eigentümer initialisiert das TPM. Beide können *Policies* setzen, z.B. wie sich das System verhalten soll, wenn die Integritätsmessung einen Abweichung von Ist- und Soll-Wert ergibt. Beide könne das TPM abschalten, der Eigentümer vollständig, der Nutzer für die Dauer einer Session bis zum nächsten Boot. Auch der TPM-Hersteller kann ein TPM deaktivieren. Pearson et al. sagen zwar nichts dazu, unter welchen Umständen dies geschieht. Dass es möglich ist, kann man dort nachlesen und vermuten, dass es sich um eine *Revocation* handelt, eine Widerrufung bei Kompromittierung oder anderem Mißbrauch.

Dritte, z.B. eine Bank oder ein Music-on-Demand-Anbieter, können sich vor Beginn einer Transaktion den aktuellen Systemzustand anzeigen lassen (*Remote Attestation*) und die Entschlüsselung der beim Nutzer gespeicherten Daten an einen bestimmten Systemzustand koppeln (*Sealed Storage*).

Alle genannten Parteien verfügen über ihre *Policies*, Bedingungen, unter denen Eigenschaften zertifiziert oder Operationen zugelassen werden. Die letzten drei legen *Policies* auf einem initialisierten System fest. Schon heute setzen Unternehmen ein Hausrecht auf den Rechnern ihrer Mitarbeiter durch. Die Innovation von TCG besteht darin, nun auch externen Parteien die Durchsetzung ihrer Nutzungsbedingungen auf den Rechnern ihrer Transaktionspartner zu ermöglichen. Das ist der Wald, den wir vor lauter Bäumen nicht sehen sollen.

Digital Content Delivery

Die Auslieferung von kommerziellen Inhalten erfolgt nach dem TCG-Modell in zwei Schritten: 1.) Der Anbieter fragt (per Smart Card, MS Passport, Biometrie etc.) die Identität

des Käufers und dessen Systemzustand ab (*Remote Attestation*). Hat der Empfänger sich korrekt ausgewiesen, läuft ein Betriebssystem mit den aktuellen Sicherheits-Upgrades, läuft ein Viren-Checker mit den aktuellen Viren-Definitionen, haben alle laufenden Programme den erwarteten Hash-Wert, läuft kein Programm-Monitor oder Debugger usw. usw. (vgl. Pearson 2003: 77), liefert er den gewünschten Content aus. Dazu werden

2.) die Daten (vor oder nach der Auslieferung) „versiegelt", d.h. an einen nicht-migrierbaren Schlüssel im TPM und an die spezifische Software-Konfiguration zum Zeitpunkt der Versiegelung (i.e. an den aktuellen Wert im *Platform Configuration Register* (PCR)) gekoppelt (für eine ausführlichere Beschreibung s. Pearson 2003: 48) Migrierbare Schlüssel werden für Nutzerdaten verwendet, damit diese kopiert, z.B. ge-backupt werden können. Nicht-migrierbare Schlüssel werden für Daten von Dritten eingesetzt, damit diese genau nicht kopiert werden können (Pearson 2003: 86 f.). Und natürlich werden die Daten nur dann entschlüsselt, wenn keine der vom Anbieter in der Lizenz und dem dazugehörigen *Rights Expression Language* Mechanismus festgelegten Nutzungsbedingungen dagegen spricht, z.B. ein Verfallsdatum oder eine nicht verlängerte Subskription.

Fragile Daten

Bei den meisten der genannten Schritte handelt es sich um generische DRM-Funktionen. Was TCG außer einem Hardware-Schutz für die verwendeten Schlüssel hinzufügt, ist die Kopplung an einen bestimmten Systemzustand.

Doch der Systemzustand eines üblichen PCs ändert sich. Nutzer installieren neue Hardware, neue Software und neue Versionen alter Programme. Microsoft installiert ungefragt neue Software.

> "Microsoft may provide security related updates to the OS Components that will be automatically downloaded onto your computer. These security related updates may disable your ability to copy and/or play Secure Content and use other software on your computer." (Microsoft, Windows Media Player EULA)

Das ist keine Besonderheit von Microsoft. „System Renewal" und „Auto Update" sind Standardfeatures aller aktuellen DRM-Systeme. Auf diese Weise werden Patches gegen den neuesten Hack eingespielt und regelmäßig neuentwickelte Kontrollmechanismen nachgeladen.

Wenn sich der Systemzustand ändert, ändern sich auch die Meßwerte in den *Platform Configuration Registern* (PCR). Was geschieht dann mit den daran gekoppelten Daten?

Eine Antwort darauf gab Brian LaMacchia, Sicherheitsexperte von Microsoft, auf dem TCG-Symposium des Bundesministeriums für Wirtschaft und Arbeit im Juli 2003[5]: Da NGSCB (Next Generation Secure Computing Base, formerly known as Palladium[6]) nicht sämtliche laufende Software vermißt, erfolge die Kopplung nur an den Nexus und die jeweilige gesicherte Anwendung für die Darstellung der Daten.

---

[5]http://www.webpk.de/bmwa/willkommen.php

[6]http://www.microsoft.com/resources/ngscb/

Nicht zufrieden mit dieser Auskunft, befragte ich noch zwei weitere Vortragende der BMWA-Veranstaltung danach. Die Antwort von Michael Waidner, Kryptographieexperte am IBM Zürich Lab,[7] war verblüffend: Bei TCG sei es tatsächlich so, dass durch die kleinste Systemänderung alle daran gekoppelten Daten unlesbar werden. Es sei ja gerade Sinn von TCG, sensible Daten zu schützen, wenn sich ein Trojaner oder Virus eingeschlichen hat. Hat man diese beseitigt und das System neu gebootet, stimmen -- idealerweise -- die Werte in den PCRs wieder mit den Erwartungen überein und die Schlüssel sind wieder verfügbar.

Diese Antwort weist auf zwei Möglichkeiten: entweder eine Trusted Platform ist ein statisches System. Flexibilität, Offenheit, Erweiterbarkeit wären dahin. Im Unternehmenskontext, wo die IT-Abteilung ohnehin nicht will, dass Nutzer eigenständig Software installieren, wäre ein solches System vielleicht vorstellbar, doch selbst hier müssen die für die Arbeit notwendigen Programme regelmäßig ge-updatet werden. In fast allen anderen Einsatzbereichen von PCs ist eine solche Einzementierung nicht vorstellbar.

Die zweite Möglichkeit wäre, dass der Eigentümer einer Trusted Platform nach jeder Systemänderung sämtliche eigenen Daten und die Dritter mit aktualisierten PCR-Werten versieht, respektive von allen beteiligten Parteien versehen läßt. Dazu findet sich nichts in der Spezifikation. Diese Lösung scheint ebenfalls unwahrscheinlich. Denn von dem immensen Aufwand abgesehen, würde sie auch einen weiteren Angriffskanal bieten. Ein bösartiges Programm könnte darüber u.U. seinen eigenen Hash in ein PCR schreiben.

Auch die Antwort von Bob Meinschein, Desktop Platform Architecture Engineering Manager bei Intel und Sprecher für die TCG, war erstaunlich. Es werden gar nicht sämtliche Meßwerte in PC-Registern gespeichert, sondern nur die des Security Kernels und anderer sicherheitsrelevanter Komponenten, so wenige wie möglich, denn es werden nur 8 Register im TPM verwendet. Für die Attestierung könne der Security Kernel dann weitere Meßwerte zur Verfügung stellen, die offenbar außerhalb des TPM gespeichert werden. Auch diese Erläuterung läßt sich nicht in der Spezifikation wiederfinden. Und sie hat die gleichen Probleme. Zwar kann eine Nutzerin hier nicht sicherheitsrelevante Soft- und Hardware installieren, ohne den Zugriff auf sämtliche versiegelten Daten zu verlieren, doch auch die Sicherheitssoftware wird nicht ohne Updates ein- für allemal sicher sein.

Für die Migration der Schlüssel im TPM, einschließlich des *Endorsement Key* sieht die Spezifikation einen Mechanismus in Kooperation mit dem Plattformhersteller vor. Doch selbst wenn man die Schlüssel auf einer neuen Trusted Plattform installiert hat, wird deren Systemzustand kaum dem entsprechen, an den die Daten gekoppelt sind.[8]

Es scheint also, als sei bei der TCG mit „Datenschutz“ der Schutz des Nutzers vor Zugriff auf seine Daten gemeint. Die Revolution des Cyberspace beruht auf den offenen Architekturen von PC und Internet. Die Konterrevolution von TC-gestütztem DRM soll den Allzweckrechner zu einer dedizierten Unternehmens- und eCommerce-Plattform schließen. Und selbst hier wird der offensichtlich noch nicht ausreichend durchdachte Mechanismus des *Sealed Storage* zu strukturellen Problemen führen. TCG versetzt private, Unternehmens- und

---

[7] http://www.zurich.ibm.com/~wmi/

[8] Wie auch immer man es dreht und wendet: es bleibt eine ausgesprochen dumme Idee, Daten an Systemzustände zu binden. Und überflüssig dazu: das TPM „weiß“ durch den laufenden Vergleich von PCR und DIR jederzeit, ob das System „integer“ ist oder nicht. Die Entschlüsselung von Daten könnte somit ebenso gut an eine von der jeweils aktuellen Systemkonfiguration abstrahierten Integrität gebunden werden.

Unterhaltungsindustrie-Daten in einen äußerst fragilen Zustand. Die Lehre daraus ist wiederum generisch für Kryptographie: Sie führt in Teufels Küche, wenn die Nutzer nicht die vollständige Kontrolle über die Schlüssel haben.[9]

Informationelle Nachhaltigkeit

Es mag deutlich geworden sein, welche Probleme schon im täglichen Betrieb mit einer „vertrauenswürdigen Plattform" auf uns zukommen. Noch eklatanter wird die Lage, wenn man den kurzfristigen Verwertungs- und Profitinteresse von wirtschaftlichen Akteuren die Anforderungen entgegenstellt, die eine Erhaltung von Kulturgütern für kommende Generationen mit sich bringt. Um Daten langfristig zu bewahren und zugänglich zu halten, müssen Privatpersonen, Institutionen, Firmen, Bibliotheken und Archive sie 1.) kopieren, um dem Verfall von Datenträgern entgegenzuwirken, 2.) konvertieren, um dem Verfall von Datenformaten entgegenzuwirken, und 3.) ihre Laufumgebungen emulieren, um dem Verfall von Plattformen entgegenzuwirken.

Diese Operationen zu verhindern, ist erklärtes Ziel von DRM. Und auch TCG ohne weitere DRM-Mechanismen außer *Sealed Storage* kann offenbar sehr leicht jeden Zugriff nachhaltig sperren.

Die einzige Lösung, um digitale Kulturgüter für die Nachwelt zu bewahren, ist ein digitales Pflichtbibliothekengesetz, wie es das Bundesland Berlin bereits hat und in Frankreich und Schweden derzeit diskutiert wird, und damit verbunden natürlich eine Ablieferungspflicht in einem unverschlüsselten offenen Format.

DRM „funktioniert nicht" und „ist dumm"

Solche Behauptungen lassen sich leicht aufstellen. Doch wenn sie aus den Häusern Microsoft und IBM kommen, haben sie Gewicht.

Peter Biddle spielt seit mindestens fünf Jahren eine zentrale Rolle für die DRM-Entwicklung bei Microsoft, u.a. in der CPTWG und in der DVD-CCA. Heute ist er Product Unit Manager für NGSCB. Zusammen mit drei Kryptographie-Kollegen von Microsoft trug er auf dem 2002 ACM Workshop zu Digital Rights Management ein aufsehenerregendes Papier vor. In „The Darknet and the Future of Content Distribution" sehen sie keinerlei Behinderung von peer-to-peer File-sharing durch DRM. Sie sagen einige weitere Eskalationsrunden zwischen den Konstrukteuren von DRM-Systemen und ihren Hackern voraus, bis die Konsumenten endgültig nicht mehr mitspielen. „Increased security (e.g. stronger DRM systems) may act as a disincentive to legal commerce. ... Finally, consumers themselves are likely to rebel against ‚footing the bill' for these ineffective content protection systems." (Biddle et al., 2002) Am Ende dieses technologischen Irrwegs werde sich die Erkenntnis durchsetzen: „if you are competing with the darknet, you must compete on the darknet's own terms: that is convenience and low cost rather than additional security." (ebd.) Eine Allerweltsweisheit, die der Erfolg von Apple's iTunes Music Store mit gemäßigtem DRM und gemäßigten Preisen jüngst bestätigte.

---

[9]Deshalb lautet die erste der vom Chaos Computer Club an IBM gerichteten Forderungen: „Vollständige Kontrolle des Anwenders über sämtliche gespeicherten Schlüssel" (TCPA - Whom do we have to trust today?, March 18, 2003, http://www.ccc.de/digital-rights/forderungen)

Auch David Saffords Meinung hat Gewicht. Er ist Kryptoexperte und Manager für Netzwerksicherheit bei IBMs Thomas J. Watson Research Center. Er ist auch verantwortlich für den Linux-Treiber für IBMs TCG-konformen Chip, z.B. in Thinkpads. In seiner Erwiderung auf Ross Andersons FAQ (Anderson o.J.) stellt Safford TCPA als ein schlichtes Werkzeug hin, dass für gute und für schlechte Zwecke verwendet werden könne. Für die guten verteidigt er TCPA. Zu den schlechten zählt er vor allem DRM: „My personal opinion (not speaking for IBM) is that DRM is stupid, because it can never be effective, and it takes away existing rights of the consumer." (Safford 2002)

Bedrohte Rechte

Zu diesen durch DRM bedrohten Rechten gehören der Datenschutz, die informationelle Selbstbestimmung, das Hausrecht im eigenen Gerät, die Schrankenbestimmungen des Urheberrechts.

Datenschutz

TCG mag pseudonyme Identitäten ermöglichen, doch ob sich Bank, Arbeitgeber oder Content-Industrie damit zufrieden geben werden, bleibt abzuwarten. Letzteren werden DRM-Systeme ja gerade damit angepriesen, dass sie hochpräzise Profile aus Personen-, und Werknutzungsdaten generieren.

Hausrecht

Das Recht auf die Unverletzlichkeit der Wohnung war Thema, als das Bundesverfassungsgericht ab dem 1. Juli 2003 über den Großen Lauschangriff verhandelte. Ich will nun keineswegs TCG oder DRM auf die gleiche Stufe stellen mit dem richterlich angewiesenen Abhören von Privatwohnungen in Ermittlungen gegen schwere Straftaten. Doch auch bei TCG geht es um weitreichende technologische Fernwirkung Dritter in den Privatraum hinein -- mit dem wichtigen Unterschied, dass sie hier in einem weitgehend rechtsfreien Raum stattfindet. Das neue Urheberrechtsgesetz schützt DRM pauschal vor Umgehung, hat aber den Systemen keinerlei Auflagen gemacht. Die Bundesregierung argumentiert, dass ein DRM genauso wie jedes andere System, das Personendaten verarbeitet, den Bestimmungen des Datenschutzrechts genügen müsse. Das könnte eine Lösung sein, wären die Datenschützer durch mangelnde Kapazitäten und Eingriffskompetenzen nicht schon heute überfordert, auch ohne Trusted Computing. Hinzu kommt, dass die Content-Industrie Datenschutz als lästiges Übel sieht. So forderte Alexander Felsenberg vom Deutschen Multimedia-Verband dmmv jüngst: „Der Datenschutz darf die Medienanbieter bei der Strafverfolgung im Netz nicht behindern." (nach Sietmann 2003) Wie die Fernsteuerung aussehen wird, hängt also weitgehend davon ab, was technisch machbar und je nach Geschäftsmodell opportun ist.

Schrankenbestimmungen des Urheberrechts

Am ersten Verhandlungstag vor dem Verfassungsgericht erläuterte einer der Sachverständigen, Oberstaatsanwalt Achim Thiel aus Frankfurt, warum es seit der Verfassungsänderung nur so wenige Lauschangriffe gegeben hat. Ein Lauschangriff sei sehr aufwendig und teuer. Es erfordere oft mehrwöchige Vorbereitungen, bis eine Wohnung mit Mikrofonen bestückt ist. Auch die Auswertung der Aufnahmen sei sehr aufwendig. Darauf fragte Verfassungsrichter Brun-Otto Bryde verdutzt: "Die Grundrechte werden also am

besten durch technische Schwierigkeiten geschützt?" Und niemand widersprach (nach Rath 2003).

Ein Grundrecht existiert, weil es die reibungslose Technologie zu seiner Beseitigung noch nicht gibt -- genau so wird in Bezug auf die Schrankenbestimmungen des Urheberrechts argumentiert. Bildung, Forschung, Presse, und, in Form der Privatkopie, jedermann gesteht das Gesetz bislang eng umrissene, zustimmungsfreie und pauschal vergütete Nutzungen urheberrechtlicher Werke zu. DRM erlaube nun eine punktgenaue individuelle Lizenzierung und Vergütung. In einem auf dem BMWA-Symposium verteilten Papier nimmt Microsoft die Möglichkeit individueller Vergütungsmodelle sogar in die Definition von DRM auf. Deshalb lobbyied der Branchenverband der Gerätehersteller Bitkom unter Führung von HP seit geraumer Zeit massiv für die Abschaffung der Pauschalvergütungen zugunsten einer DRM-gestützten individuellen Abrechnung, die dann die Verlage gleich mit abwickeln würden.[10]

Die Pauschalvergütungen und die sie verwaltenden Verwertungsgesellschaften wären damit technisch überholt. Alexander Wolf, stellvertretender Direktor der Direktion Industrie der GEMA, zeigte sich auf dem Panel zu Medienwirtschaft, DRM und TCG des BMWA-Symposiums nur zu bereitwillig, die Verwertungsgesellschaften zuzumachen, wenn sich das Problem, auf das sie eine Antwort waren, besser lösen ließe. Damit würden aber auch die Schrankenbestimmungen selbst abgeschafft, deren wesentlicher Sinn in einer zustimmungsfreien und anonymen Nutzung besteht. In dem Grundsatzurteil, das zur Einführung der Pauschalvergütungen ins deutsche Urheberrechtsgesetz führte, entschied der Bundesgerichtshof 1964, dass die GEMA Einzelhändler nicht zwingen könne, ihnen die Personalausweisdaten der Käufer von Audioaufnahmegeräten zu übermitteln. Eine solche Kontrollmaßnahme widerspreche dem Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 GG).[11] Eine DRM-gestützte individuelle Lizenzierung beruht aber gerade auf einer Personenerfassung.

Die pauschalvergüteten Schranken verkörpern somit einen zentralen Werte: das Recht, anonym zu lesen und zu kopieren, der Schutz der Privatsphäre. Urheberrechtsspezialisten leiten sie aus der Sozialbindung des Eigentums (Art. 14 GG) ab, die ein Abwägen zwischen den Interessen der Eigentümer und des Allgemeinwohls vorschreibt. „Im Grunde ist das ganze Urheberrechtsgesetz nichts anderes als das Gesetz, das diese Balance herstellen soll. Insofern ist auch die Privatkopieschranke im Grundgesetz verankert.“ (Kreutzer 2003)

Bei der Pauschalvergütung steht also mehr auf dem Spiel als die wirtschaftlichen Interessen von Bitkom und GEMA. Entspricht die Beschränkung des geistigen Eigentums im Gemeinwohlinteresse der grundgesetzlichen Sozialbindung des Eigentums oder begründet sie sich nur in „technischen Schwierigkeiten“? Auch zu dieser Frage wäre ein Verfassungsgerichtsentscheid hilfreich.

---

[10] s. diverse Stellungnahmen des Bitkom-Arbeitskreises Urheberrechtliche Abgaben: http://www.bitkom.org/index.cfm?gbAction=FD4873D5-1C35-4C94-8790C4CA9AB0833A&CategoryNodeID=E3F2D1C2-2D01-4EA2-B297850237E0FA40

[11] BGH, 29. Mai 1964 - Aktz.: Ib ZR 4/63 (Personalausweise), in GRUR 02/1965, S. 104

Open Source
IBM hat bereits einen Treiber für den TCG-Chip unter der GPL, HP arbeitet an einem (s. Krempel 2002). Quelloffenheit ist natürlich im Prinzip eine gute Sache. Sie ermöglicht, den Code auf Hintertüren und Schwachstellen hin zu überprüfen. Ein Allheilmittel, um aus einer problematischen Technologie eine gute zu machen, ist sie nicht.

- Den Quellcode einsehen, aber nicht verändern zu dürfen, wie Microsoft es für den Nexus unter der Shared Source Initiative angekündigt hat, ist sinnlos.
- Ebenfalls sinnlos ist es, wenn man den Quellcode unter GPL modifizieren und verbreiten darf, ihn aber nicht benutzen kann, weil alle Dienste eine Zertifizierung voraussetzen.
- Selbst wenn weder Patentansprüche noch Zertifizierung die Freiheit der Software verhindern: Sobald die Open Source Implementierung die TCG-Spezifikationen mit ihren zwei zentralen Neuerungen -- *remote attestation* und *sealed storage* unter Kontrolle Dritter -- umsetzt, führt sie zu exakt denselben Problemen. Wenn man Dummheiten quelloffen implementiert, sind es eben quelloffene Dummheiten.

Es entspricht nicht der Idee von freier Software, dass ein Industriekonsortium eine Architektur entwirft und die freie Software Community dann mit der Software experimentieren darf. Wäre es den Beteiligten ernst mit einer Open Source Strategie, müßte schon das Basis-Design in einer offenen Struktur, etwa einer IETF Arbeitsgruppe, diskutiert werden, also die grundlegenden Fragen von Angreifermodell, Schlüsselkontrolle, Datenschutz und informationeller Nachhaltigkeit.

Vertrauen
Da wir in diesen Tagen Orwells 100. Geburtstag begingen, möchte ich damit enden, „Trusted Computing“ als Newspeak zu enttarnen. Tatsächlich ist es das in Technologie gegossene Mißtrauen gegenüber den Nutzern. „Trusted systems presume that the consumer is dishonest,“ (Stefik 1996) schrieb Mark Stefik vom Xerox PARC in einer Zeit, als DRM noch „Trusted Systems“ hieß. Intel-Vizepräsident Don Whiteside begründete im vergangenen Jahr die aktuellen „Trusted Systems“ wie folgt: „Wir können nicht weiter vertrauen, dass die Technik von den Konsumenten fair benutzt wird“ (nach Scheffler 2002). Wer zu allen anderen Problemen mit dieser neuen Technologie ihre potentiellen Kunden auch noch als Dieb hinstellt, wird kaum mit ihrer Kooperation rechnen können.

Literatur

Anderson, Ross, Trusted Computing Frequently Asked Questions, O.J., http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

Biddle, Peter, Paul England, Marcus Peinado und Bryan Willman (Microsoft Corporation), „The Darknet and the Future of Content Distribution“, 2002 ACM Workshop on Digital

Rights Management, November 18, 2002, Washington DC,
http://crypto.stanford.edu/DRM2002/darknet5.doc

BMWA Symposium: "Trusted Computing Group" (TCG), am 2. und 3. Juli 2003 im Bundesministerium für Wirtschaft und Arbeit (BMWA), Berlin,
http://www.timekontor.de/home/veranstaltungen/26.html#26

Krempl, Stefan, 19C3: HP-Forscher wirbt für Allianz von Open-Source-Bewegung und TCPA, Heise News, 28.12.2002, http://www.heise.de/newsticker/data/se-28.12.02-003/

Kreutzer, RA Till, Redebeitrag auf der „Alternativen Anhörung zur Novelle des Urheberrechtsgesetzes“, 23. Januar 2003, Humboldt-Universität zu Berlin,
http://privatkopie.net/files/aktuell2.htm

Pearson, Siani (Hrsg.), Trusted Computing Platforms. TCPA Technology in Context, HP Books, Prentice Hall, Upper Saddle River, N.J., 2003

Rath, Christian , „Profi-Lauscher haben viele Freunde. Das Bundesverfassungsgericht verhandelt über Zulässigkeit des Großen Lauschangriffs“, taz, 2.7.03, S. 6,
http://www.taz.de/pt/2003/07/02/a0082.nf/text

Safford, David, IBM Research, „Clarifying Misinformation on TCPA“, October, 2002,
http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf

Scheffler, Sven, „Schluss mit Raubkopien“, SonntagsZeitung, 22.9.2002, S. 143

Sietmann, Richard, „Nachholbedarf. Nationale Breitbandstrategie für Deutschland gesucht“, c't 13/2003, S.38

Stefik, Mark J., Letting Loose the Light: Igniting Commerce in Electronic Publication, in: Stefik, M. (Hrsg.), Internet Dreams: Archetypes, Myths, and Metaphors, MIT Press, Cambridge Mass. 1996; http://www.parc.xerox.com/istl/projects/uir/pubs/pdf/UIR-R-1996-10-Stefik-InternetCommerce-IgnitingDreams.pdf

TCG Main Specification Version 1.1b
http://www.trustedcomputinggroup.org/downloads/tcg_spec_1_1b.zip