Entwicklung des Internet von einer offenen Wissensgesellschaft zur geschlossenen Copyright-Gesellschaft. Trusted Computing und Digital Restrictions Management

Volker Grassmuck

Helmholtz-Zentrum für Kulturtechnik
Humboldt-Universität zu Berlin
Unter den Linden 6
10099 Berlin
vgrass@rz.hu-berlin.de

Abstract: Dieser Text betrachtet die weitere Entwicklung des Internet unter dem Fokus der Trusted Computing Group (TCG) Architektur und ihrer Anwendung für das Digital Restrictions Management (DRM). Er zeigt die Probleme auf, die entstehen, wenn man die Entschlüsselung von Daten an Systemzustände koppelt. Er schließt mit grundlegenden Einwänden gegen DRM.

1 Einleitung

TCG-Vertreter weisen jede Verbindung mit DRM zurück. 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 [Pe03]. Die Hardware mag in der aktuellen Spezifikation nicht gegen Angriffe durch den Plattformeigentümer optimiert sein. Die zentralen Neuerungen von TCG sind „Remote Attestation“ und „Sealed Storage“. Dritte, z.B. eine Bank oder ein Music-on-Demand-Anbieter, können sich damit vor Beginn einer Transaktion den aktuellen Systemzustand anzeigen lassen und die Entschlüsselung der beim Nutzer gespeicherten Daten an einen bestimmten Systemzustand koppeln. Die beiden Mechanismen eignen sich somit 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.

2 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. [Pe03], 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. 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 [Pe03]. 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.

3 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. Auch Microsoft installiert ungefragt neue Software und sogar Betriebssystemkomponenten, wie es sich in der Lizenz des Windows Media Players von dessen Nutzer abbedungen hat. Das ist keine Besonderheit von Microsoft. „System Renewal" und „Auto Update" sind Standardfeatures aller aktuellen DRM-Systeme.

Wenn sich der Systemzustand ändert, ändern sich auch die Meßwerte in den *Platform Configuration Registern* (PCR). Was geschieht dann mit den daran gekoppelten Daten? Auf dem TCG-Symposium des BMWA im Juli 2003[1] erhielt ich darauf mehrere Antworten. Die von Michael Waidner, Kryptographieexperte am IBM Zürich Lab, 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.

[1] 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

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 Vorstand von 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.

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 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.

4 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“ [BEPW02] 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." [BEPW02]. Am Ende dieses technolgischen 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. 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 [An 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." [Sa02]

5 Vertrauen

„Trusted Computing" ist Orwellscher Newspeak. Tatsächlich ist es das in Technologie gegossene Mißtrauen gegenüber den Nutzern. „Trusted systems presume that the consumer is dishonest," [St96] 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" [Sc02]. Wer zu allen anderen Problemen mit dieser neuen Technologie ihre potentiellen Kunden auch noch als Dieb hinstellt, wird kaum mit ihrer Kooperation rechnen können.

[Pe03] Pearson, S. (Hrsg.): Trusted Computing Platforms. TCPA Technology in Context, HP Books, Prentice Hall, Upper Saddle River, N.J., 2003, S. 7. Das Buch bezieht sich auf die TCG Main Specification Version 1.1b, http://www.trustedcomputinggroup.org/downloads/tcg_spec_1_1b.zip

[BEPW02] Biddle, P.; England, P.; Peinado, M.; Willman, B. (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

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

[Sa02] Safford, D., IBM Research: „Clarifying Misinformation on TCPA", October, 2002, http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf

[St96] Stefik, M. 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

[Sc02] Scheffler, S.: „Schluss mit Raubkopien", SonntagsZeitung, 22.9.2002, S. 143