Trusted Computing Platforms – Zur technischen und industriepolitischen Situation und Vorgehensweise

Dirk Günnewig M. A.,[*] Prof. Dr. Kai Rannenberg,[**] Dr. Ahmad-Reza Sadeghi,[***] Christian Stüble[****]

I. Einleitung

Die Ankündigung der von der Trusted Computing Group entworfenen TCPA-Spezifikation für eine neue Generation sicherer Computerplattformen führte zu diversen und heftigen Debatten über die negativen Folgen, die mit der Anwendung dieser Konzepte einhergehen. Die diskutierten Horrorszenarien, wie die Ausübung von Zensur, die Gefährdung der Privatsphäre des Computernutzers und die Freiheitseinschränkung der Nutzer hinsichtlich der Benutzung ihres Computers und der darauf befindlichen Daten sind jedoch eng mit großen Vorteilen und Chancen verbunden. Die Befürworter preisen u. a. die deutliche Verbesserung des Schutzes sicherheitsrelevanter Daten an. Welches der beiden Szenarien Realität wird, hängt wesentlich von einer bewussten (politischen) Gestaltung der Technik ab. Die existierenden Technologien bieten hierfür die allerbesten Voraussetzungen.

Unsere technische und unabhängige Analyse zeigt, dass letztlich das zugrunde liegende TCPA-fähige Betriebssystem dafür verantwortlich ist, ob die Plattformen gegen den Benutzer missbraucht werden können. Schließlich kontrolliert das TCPA-Betriebssystem die TCPA-Hardwarekomponenten und eröffnet Handlungsspielräume, aber auch -restriktionen für alle beteiligten Parteien – seien es Anbieter von Mediendateien, Softwarehersteller, Inhaber von Daten oder Konsumenten. Deshalb sollte die Frage nicht nur lauten, ob die TCPA-Hardwarespezifikationen vertrauenswürdig sind, sondern vor allem, ob das verwendete TCPA-Betriebssystem sicher und vertrauenswürdig ist. Es stellt sich auch die Frage, wie dieses Vertrauen geschaffen werden kann.

[*] Institut für Algebra und Mathematik, Universität Dortmund, guennewig@digital-rights-management.de.

[**] T-Mobile-Stiftungsprofessur für Mobile Commerce und Mehrseitige Sicherheit, Johann-Wolfgang-Goethe-Universität Frankfurt, kair@m-lehrstuhl.de.

[***] Institut für Informations- und Kommunikationssicherheit, Ruhr-Universität Bochum, sadeghi@crypto.rub.de.

[****] Security and Cryptography Group, Universität des Saarlandes, stueble@acm.org.

Das zentrale Ergebnis unserer Untersuchungen ist, dass vertrauenswürdige Betriebssysteme durch die Verwendung eines Sicherheitskerns sehr effektiv realisiert werden können. Wir erläutern die Architektur eines DRM-fähigen Open-Source-Sicherheitskerns, der basierend auf den TCPA-Spezifikationen die Anforderungen der Industrie und der Benutzer gleichermaßen erfüllen kann. Seit Mitte 1999 wurde mit der Entwicklung des *PERSEUS*[1]-Sicherheitskerns bereits die hierfür dringend erforderliche Grundlage geschaffen. Der Sicherheitskern liegt vor. Insofern sind Annahmen, man würde sich mit der TCPA-Hardwarespezifikation auf ein Betriebssystem eines einzigen Anbieters festlegen, unzutreffend. Wichtiger ist die Frage, wie sich Deutschland technologiepolitisch positioniert, weswegen einige Anmerkungen dazu diesen Text abschließen.

II. Rechnersystemintegrität und TCPA-Hardwareerweiterungen

Existierende Computersysteme bieten lokalen Benutzern und externen Kommunikationspartnern keinerlei Möglichkeiten, die Integrität und damit die Sicherheit der verwendeten Hard- und Softwarekomponenten ohne großen Aufwand zu überprüfen. Dies können Angreifer ausnutzen, indem sie sicherheitskritische Komponenten des Computersystems derart manipulieren, dass Sicherheitsregeln unbemerkt umgangen werden können. Daraus resultieren Gefährdungen der Privatsphäre und sicherheitsrelevanter Daten sowohl im privaten als auch im geschäftlichen Bereich. Die von der Trusted Computing Group (TCG)[2] vorgeschlagenen TCPA-Spezifikationen[3] ermöglichen es, diese gravierende Sicherheitslücke zu schließen.

In der öffentlichen Debatte bemängeln Kritiker, dass die technischen Fähigkeiten der TCPA-Hardware beispielsweise dem Hersteller ermöglichen, die totale Kontrolle über die von Benutzern[4] verwendeten Daten und Informationen zu erlangen und somit ihre Privatsphäre zu verletzen.[5] Obwohl es technisch möglich ist, basierend auf den TCPA-Spezifikationen derartige Funktionen zu realisieren, muss es dazu nicht zwingend kommen.

---

1 http://www.perseus-os.org.

2 Ehemals Trusted Computing Platform Alliance (TCPA).

3 *TCPA, TCPA PC Specific Implementation Specification,* Version 1.00, September 2001; *dies.,* TCPA Main Specification, Version 1.1b, Februar 2002; *Pearson* (Hrsg.), Trusted Computing Platforms – TCPA Technology in Context, Hewlett-Packard Company, Prentice Hall PTR, 2003.

4 Wir unterscheiden zwischen dem Besitzer (Owner) einer Plattform, den Benutzern (User) und den Anbietern (Provider) digitaler Werke.

5 *Anderson,* The TCPA/Palladium FAQ, 2002, http://www.cl.cam.ac.uk/rja14/tcpa-faq.html; *Arbaugh,* IEEE Computer 8/2002, 77.

Die TCPA-Komponenten greifen selbst nicht aktiv in die Geschehnisse eines Computersystems ein.

Die TCPA-Hardwarearchitektur ist grundsätzlich als neutral hinsichtlich ihrer Auswirkungen zu bezeichnen. Sie bietet bestimmte Funktionen an. Erst das Betriebssystem, das die Hardware steuert, entscheidet, ob die Gefahren des Systems eintreten. Daher muss eine bewusste Technikgestaltung hier ansetzen, um Risiken des Technologieeinsatzes zu reduzieren. Entgegen landläufiger Meinungen ist die Zertifizierung von Betriebssystemen und Anwendungen nicht Teil der TCPA-Spezifikation. TCPA-Komponenten können daher nicht darüber entscheiden, welches Betriebssystem oder welche Anwendung geladen wird.

Stattdessen bietet TCPA dem Betriebssystem Funktionen an, die dem Schutz der Integrität und der Vertrauenswürdigkeit von Informationen dienen. TCPA wurde jedoch auch dafür ausgelegt, Digital-Rights-Management-(DRM-)[6]Anwendungen zu unterstützen,[7] weshalb nicht alle Komponenten, speziell die verwendeten kryptographischen Schlüssel, unter der Kontrolle des Benutzers stehen können. Ansonsten bestünde die Gefahr des Missbrauchs und der Verletzung von Urheberrechten.

III. Verbesserungspotential – ein Beispiel

Genau diese DRM-Fähigkeit der TCPA-Komponenten steht in der öffentlichen Kritik, da sie neben dem Schutz von Urheberrechten auch gegen die Interessen und Rechte der Benutzer gerichtet werden kann. Daher besteht insbesondere bei der Kontrolle dieser Funktionen ein erhebliches Verbesserungspotential. Um das Vertrauen in diese Komponenten zu gewährleisten, sollte der Besitzer einer TCPA-Plattform entscheiden können, ob die zugrunde liegende Hardware diese bedenklichen Funktionen unterstützt – oder nicht.

---

6 *National Research Council*, The Digital Dilemma, Intellectual Property in the Information Age, National Academy Press, 2000.

7 Neuere Veröffentlichungen behaupten, dass DRM kein Entwicklungsziel von TCPA gewesen sei, *Safford*, Clarifying Misinformation on TCPA, White Paper, IBM Research, Oktober 2002; *ders.*, The Need for TCPA, White Paper, IBM Research, Oktober 2002. Allerdings sprechen einige Gründe dafür, dass DRM-Fähigkeit eine Anforderung von TCPA war. Beispiele hierfür ist die Bindung von Daten an spezielle Systemkonfigurationen (Sealing), die Zertifizierung des Endorsement Keys (EK) durch den TPM-Hersteller und die Tatsache, dass Attestation zwar gegenüber anderen IT-Systemen, aber nicht gegenüber lokalen Benutzern möglich ist. DRM-Fähigkeit ist auch kein grundsätzlicher Nachteil, solange sie dem Benutzer nicht aufgezwungen werden kann.

Beispielsweise ist die Tatsache, dass der Besitzer einer TCPA-Plattform keine Zugriffsrechte auf den Storage Root Key (SRK) besitzt, Grund für zwei wesentliche Kritikpunkte an TCPA: Erstens verhindert diese Eigenschaft die Möglichkeit, dass Endanwender gesicherte Daten in ein neues System einspielen können. Zweitens ist dem Endanwender dadurch der Zugriff auf Anwendungs- und Benutzerdaten verwehrt, wodurch DRM-Mechanismen erst ermöglicht werden.

Ein möglicher und möglicherweise mehr Vertrauen schaffender Lösungsansatz wäre, den Besitzer der TCPA-Plattform entscheiden zu lassen, ob er Zugriff auf den SRK besitzen möchte oder nicht. Um zu verhindern, dass Endanwender auf diese Weise akzeptierte DRM-Anwendungen oder organisationsinterne Sicherheitsregeln umgehen, muss diese Eigenschaft bei der Bestimmung der Systemkonfiguration berücksichtigt werden, wodurch Content-Provider zwischen Plattformen mit ausgelesenem und nicht ausgelesenem SRK unterscheiden können.

IV. TCPA und Betriebssysteme

Da ausschließlich das Betriebssystem die TCPA-Komponenten kontrolliert, ist bei der Nutzung von TCPA und ähnlichen Architekturen die Vertrauenswürdigkeit des verwendeten Betriebssystems von entscheidender Bedeutung.

Nahezu alle kritisierten Eigenschaften der TCPA-Architektur lassen sich durch ein geeignetes Design des Betriebssystems ausschließen.

Um kritisierte Eigenschaften der TCPA-Spezifikation zu minimieren, dürfte beispielsweise das Betriebssystem keinen *Reference-Monitor*[8] enthalten, der eine systemweite Zensur von Benutzerdaten ermöglichen könnte. Um konform zum Urheberschutzgesetz zu sein, könnte das Betriebssystem Benutzern zwar die Erzeugung von privaten Kopien digitaler Werke erlauben, mittels kryptographischer Mittel jedoch eine Verbreitung dieser Kopien verhindern.

Die Sicherheit des jeweils verwendeten TCPA-fähigen Betriebssystems ist also von entscheidender Bedeutung für die Vertrauenswürdigkeit von TCPA-Systemen. Vertrauen muss, speziell im Kontext der DRM-Nutzung, bei so unterschiedlichen Interessengruppen wie einerseits der (digitale Inhalte vermarktenden) Industrie und andererseits der Verbraucher und individuellen Rechnernutzern erworben werden.

---

[8] Gemeint ist eine abstrakte Maschine, welche Zugriffe auf verschiedene Objekte kontrolliert.

In diesem Zusammenhang ist es bedeutsam, dass eine Auswahl an TCPA-fähigen Betriebssystemen besteht. Befürchtet wird jedoch immer wieder, dass ein im Bereich Betriebssysteme dominanter Hersteller (etwa Microsoft) ein Monopol bei TCPA-fähigen Betriebssystemen erreicht und damit sein „Vertrauensmodell" allen Nutzern aufgenötigt wird. Es wird auch befürchtet, dass dies zu einer massiven Eindämmung der Innovationsfähigkeit vor allem kleiner und mittlerer Unternehmen führt, die keinerlei Einfluss auf die weitere Entwicklung des Betriebssystems besitzen.[9]

Demgegenüber schließen sich jedoch eine Einführung von TCPA und eine Auswahl verfügbarer Betriebssysteme nicht aus. Forderungen nach vertrauenswürdigen Plattformen können basierend auf TCPA erfüllt werden, indem existierende Betriebssysteme um einen DRM-fähigen *Sicherheitskern* erweitert werden, dem die jeweiligen Nutzer vertrauen. Die Verwendung eines Sicherheitskerns ist eine bewährte und effiziente Methode und bietet gleichzeitig eine Lösung für die Sicherheitsprobleme verbreiteter Betriebssysteme, z. B. im Zusammenhang mit qualifizierten digitalen Signaturen.[10] Der Sicherheitskern kontrolliert die TCPA-Hardware derart, dass die Nutzbarkeit der TCPA-Komponenten auf ein sinnvolles Maß eingeschränkt wird.

Die von Sadeghi und Stüble[11] vorgestellte Architektur eines DRM-fähigen Open-Source-Sicherheitskerns verhindert gleichzeitig eine Monopolstellung einzelner Unternehmen (WinTel-Problematik) und erhöht die Vertrauenswürdigkeit, da der Sourcecode öffentlich zugänglich ist. Er kann gegebenenfalls einer technischen und rechtlichen Zertifizierung unterworfen werden. Der Sicherheitskern kann damit bei Bedarf auch eine einheitliche Grundlage für die Betriebssysteme der Softwarehersteller bilden.

Mit der Implementierung der PERSEUS-Sicherheitsplattform[12] wurde bereits gezeigt, dass die Realisierung eines minimalen Sicherheitskerns basie-

---

9 *Koenig*, Trusted Computing im Fadenkreuz des EG-Wettbewerbsrechts, Vortrag im Rahmen der Veranstaltung „‚Trusted Computing' – Neue Herausforderungen für das deutsche und europäische Wirtschaftsrecht" in Bonn am 09.05.2003, http://www.zei.de/download/Konferenzseite/koenig_20030509.pdf; *Ahlborn*, Kartellrechtliche Implikationen von Trusted Computing, Vortrag im Rahmen der Veranstaltung „‚Trusted Computing' – Neue Herausforderungen für das deutsche und europäische Wirtschaftsrecht" in Bonn am 09.05.2003, http://www.zei.de/download/Konferenzseite/ahlborn_20030509.pdf.

10 Siehe http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/4.pdf.

11 *Sadeghi/Stüble*, Bridging the gap between TCPA/Palladium and Personal Security, Technical Report, Saarland University, Germany, 2003.

12 *B. Pfitzmann/Riordan/Stüble/Waidner/Weber*, The PERSEUS System Architecture, in: Fox/Köhntopp/A. Pfitzmann (Hrsg.), VIS 2001, Sicherheit in komplexen IT-Infrastrukturen, DuD-Fachbeiträge, Vieweg Verlag, 2001, S. 1; *dies.*, The PERSEUS System Architecture. Technical Report RZ 3335 (\#93381), IBM Research Division, Zurich Laboratory, April 2001.

rend auf existierenden Hardwarearchitekturen mit wenig Aufwand möglich ist.

Im Gegensatz zu anderen Lösungsansätzen handelt es sich bei der PERSEUS-Sicherheitsplattform um einen sehr kleinen Betriebssystemkern, der – zwischen Hardware und konventionellem Betriebssystem liegend – alle kritischen Hardwareressourcen kontrolliert und damit sicherheitskritische Anwendungen effizient schützen kann. Parallel zu den sicherheitskritischen Applikationen wird ein konventionelles Betriebssystem (bspw. Linux oder auch Microsoft-„Windows“) ausgeführt, das – kontrolliert durch die Sicherheitsplattform – dem Benutzer seine gewohnte Arbeitsumgebung bietet.

V. Gestaltbarkeit von TCPA-Systemen

Wie bereits erwähnt, zeichnet sich die TCPA zugrunde liegende Technologie durch eine große *Gestaltbarkeit* aus: Sie kann umfassenden Vorgaben unterworfen werden, die von der Wirtschaft, aber auch von der Politik und der Gesellschaft definiert werden können.

Vertrauen ist die zentrale Kategorie und muss gesellschaftlich und politisch geschaffen werden.

Dabei ist zu beachten, dass die TCPA-Spezifikationen von einem internationalen Industriekonsortium gestaltet werden und eine Reihe von Funktionen anbieten, auf die nationale Gesetzgeber weitestgehend keinen Einfluss nehmen können, wenn die betreffenden Unternehmen nicht auf dem jeweiligen Staatsgebiet ihren Sitz haben. Bei Betriebssystemen stellt sich die Situation ähnlich dar, denn auch hier ist die Möglichkeit eines regulativen Zugriffes beschränkt. Zwar kann durch Importbestimmungen der entsprechenden Hard- und Software, Dienstleistungen und Daten versucht werden, bestimmte Gestaltungsvorgaben durchzusetzen. Dieses Verfahren ist jedoch langwierig und insbesondere angesichts der häufigen Innovationen und Veränderungen der Technologie in diesem Bereich problematisch. Wird hingegen versucht, eine überschaubare Technologie zu regulieren, können entsprechende Schwierigkeiten für die politische/rechtliche Regulierung abgeschwächt werden.

Aus diesem Grund ist es wichtig, das die TCPA offene Schnittstellen anbietet, die es ermöglichen, lokale Systeme oder Sicherheitskerne, die etwa den lokalen gesetzlichen bzw. gesellschaftlichen Anforderungen entsprechen, mit der jeweiligen TCPA-Hardware zu koppeln. Eine staatliche, staatsnahe oder eine vom Staat benannte gesellschaftliche Institution könnte den Sicherheitskern zertifizieren. Zertifizierungskriterien

wären dann neben technischen Aspekten der IT-Sicherheit vor allem rechtliche Fragen des Datenschutzes und des Urheberrechts.

Entsprechende Betriebssysteme und Software, wie Textverarbeitung und Medienabspielgeräte, müssten noch nicht einmal spezielle Vorkehrungen für den Sicherheitskern enthalten. Der Sicherheitskern würde derart implementiert, dass er Schnittstellen zu den gängigen Applikationen aufweist. Die Vision einer „Regulierung durch Code“ ist in diesem Zusammenhang zwar wohl noch ein erhebliches Stück entfernt, weil die TCPA-Architektur keinerlei Anspruch erhebt (und keinerlei Garantie gibt), sicher gegen Hardwareangriffe zu sein. Allerdings ließen sich durch eine besser gesicherte Zugriffskontrolle in Rechnern sowohl Datenschutz- als auch Urheberrechtsziele besser durchsetzen – wenn es gelingt, sie in computerlesbaren Code zu fassen.

VI. Nötige Schritte zur Gestaltung zukünftiger TCPA-Spezifikationen

Die Diskussion um die Aktivitäten der TCG hat in Deutschland erst recht spät begonnen, ist aber dann umso heftiger aufgeflammt und oft mehr von Aufregung als von präziser Analyse geprägt. Einige Kritiker vermischen z. B. offene Fragen und Kritik an der (verfügbaren) TCPA-Spezifikation mit offenen Fragen und Kritik am Projekt „Next Generation Secure Computing Base“ (NGSCB) (vormals Palladium) der Firma Microsoft und mit vermeintlichen oder tatsächlichen Schwächen der jeweiligen Internetdarstellungen der TCPA-Spezifikation, der TCG oder von Microsoft. Zuweilen wird eindringlich eine Katastrophe für die Wissensgesellschaft beschworen.[13] Eine genauere Analyse der Diskussion und der jeweiligen Motive der (heftig) Propagierenden könnte interessant und aufschlussreich für eine Analyse des Zustands der deutschen Technologiepolitik im Bereich IT sein.

Dringender ist jedoch eine Positionierung dieser deutschen Technologiepolitik in Bezug auf Trusted Computing. Dabei scheinen folgende Aspekte von besonderer Bedeutung:

- Eine Verweigerungshaltung aus Sorge über eine (etwa US-amerikanische) Dominanz der TCG schadet voraussichtlich weniger der TCG als der deutschen IT-Sicherheitsbranche. Insbesondere ein Vergleich der Trusted-Computing-Initiative mit der US-amerikanischen Key-Escrow-Initiative aus den 90er Jahren

---

[13] *Weis,* Ist „Trusted Computing“ wirklich vertrauenswürdig? Konzeptionelle Schwächen und Risiken, Vortrag im Rahmen der Veranstaltung „‚Trusted Computing’ – Neue Herausforderungen für das

des letzten Jahrhunderts ist irrig. Letztere hatte Nutzern keinerlei reale Vorteile zu bieten und war darum bei ernsthafter Betrachtung ein (fast) reiner Versuch, in die Souveränität anderer Staaten (etwa Deutschlands) einzugreifen. Selbst wenn in Teilen der TCG Motive dieser Art verfolgt werden sollten, gibt es doch mindestens einen grundsätzlichen Unterschied zwischen der Trusted-Computing- und der Key-Escrow-Initiative: Die Trusted-Computing-Initiative adressiert ein für sehr viele Nutzer tatsächlich bestehendes Problem, nämlich das der Instabilität und Unterwanderbarkeit von Computerplattformen. Da die von der TCG vorgeschlagenen Lösungen durchaus attraktiv für viele Benutzer sind, wird die Trusted-Computing-Initiative auf dem Weltmarkt sehr populär sein. Selbst wenn das TCG-Konsortium an politischen Problemen scheitern sollte (worauf gegenwärtig nichts hindeutet), würde sich zur Lösung des realen und sehr viele Benutzer betreffenden Problems nicht ausreichend stabiler Computersysteme sehr schnell eine neue Initiative bilden. Deutschland kann es sich nicht leisten, bei der TCG außen vor zu bleiben, sondern muss mitgestalten, insbesondere da einige Initiativen zur Koppelung von Sicherheitssoftware und -hardware von Deutschland ausgingen.

- Ein tieferes Verständnis der TCG-Aktivitäten ist nicht allein durch die Lektüre der Entwurfsdokumente erreichbar. Diese Erkenntnis ergibt sich in fast jedem Standardisierungsprozess und ist von außen zuweilen am Symptom unterschiedlicher Verlautbarungen der am Prozess Beteiligten erkennbar. Die (oft spekulative und oft gezwungenermaßen spekulative) Auslegung der Texte durch Außenstehende trägt jedoch zumeist mehr zur Verwirrung als zur Klärung der Situation bei. Es müssen deshalb über die zwei bisherigen deutschen Mitglieder (Infineon und Utimaco) hinaus Personen und Organisationen aus Deutschland am Prozess beteiligt sein, insbesondere wenn eine Einflussnahme nötig ist. Die neuen Angebote auf vergünstigte Teilnahme an der TCG im Advisory und im Technical Board sollten insofern nicht ungenutzt gelassen werden. Zu fördern ist insbesondere die Vertretung von Vorschlägen, die die Options- und Politikoffenheit des TPM erhöhen.[14]

---

deutsche und europäische Wirtschaftsrecht“ in Bonn am 09.05.2003, http://www.zei.de/download/Konferenzseite/weis_20030509.pdf.

[14] Siehe oben, III.

- Die Arbeit der TCG an den TCPA-Spezifikationen und die Arbeit von Microsoft an der NGSCB sind zwei verschiedene „Baustellen“, die zwar Bezüge haben, aber grundlegend unterschiedliche Aspekte behandeln und unterschiedlichen Regeln folgen. Insbesondere wer nicht nur ein „Horror- oder Paradiesszenario“ malen, sondern gezielt Einfluss nehmen will, sollte sich einerseits mit den Unterschieden zwischen den jeweils behandelten Themen und andererseits mit den grundsätzlichen Unterschieden zwischen überbetrieblichen Initiativen und Initiativen großer Firmen vertraut machen.
- Die Arbeit der TCG wird sich nicht allein auf PCs oder ähnliche Geräte beschränken. Mobile Geräte bis hin zu künftigen Mobiltelefonen liegen im Fokus der TCG, und mit Nokia ist bereits ein starker Vertreter der Mobiltelefonbranche Mitglied der TCG.