

# Trusted Computing Platform Alliance

Mythen, Wirklichkeit und Lösungswege

Dirk Günnewig      Ahmad-Reza Sadeghi      Christian Stübke

## Zusammenfassung

Freude bei den einen und Sorgenfalten bei den anderen erzeugte die Ankündigung der Trusted Computing Group<sup>1</sup> (TCG), eine sichere Generation von Computerplattformen spezifiziert zu haben. Die Befürworter preisen die Vorteile für einen verbesserten Schutz sicherheitsrelevanter Daten, während die Kritiker zu bedenken geben, dass diese Technologie genutzt werden könne, um Zensur auszuüben, die Privatsphäre der Benutzer zu verletzen und sie in ihrer Freiheit hinsichtlich der Nutzung ihres Computers und der darauf befindlichen Daten zu beschneiden.

Unsere technische und unabhängige Analyse zeigt, dass letztlich das zugrundeliegende TCPA<sup>2</sup>-fähige Betriebssystem dafür verantwortlich ist, ob diese 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. Das Betriebssystem nutzt die TCPA-Hardware, um Nutzungsregeln effektiv durchzusetzen. 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.

Der Vortrag geht aus einem technischen und sozialwissenschaftlichen Blickwinkel auf folgende Aspekte ein:

- Welche Kritikpunkte an den TCPA-Spezifikationen können bestätigt und welche entkräftet werden?
- Wie können Vorteile für die verschiedenen Benutzer bzw. Rollen durch die TCPA-Spezifikationen ermöglicht werden?
- Welche Lösungsmöglichkeiten existieren, um die potentiellen Gefahren des Einsatzes von TCPA zu reduzieren?
- Wie können technische Lösungsmöglichkeiten gesellschaftlich und politisch gestaltet werden, um eine Interessenbalance zwischen den verschiedenen Beteiligten zu erreichen?

Die zentrale Aussage des Vortrages ist, dass vertrauenswürdige Betriebssysteme durch die Verwendung eines *Sicherheitskerns* sehr effektiv realisiert werden können. Wir erläutern die Architektur eines DRM-fähigen OpenSource 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*<sup>3</sup> Sicherheitskerns bereits die hierfür dringend erforderliche Grundlage geschaffen. Der Sicherheitskern liegt vor.

---

<sup>1</sup>ehemals Trusted Computing Platform Alliance (TCPA)

<sup>2</sup>Trusted Computing Platform Alliance

<sup>3</sup>[www.perseus-os.org](http://www.perseus-os.org)

## Überblick

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 in den TCPA-Spezifikationen [13, 12, 5] vorgeschlagenen Hardwareerweiterungen ermöglichen es, diese gravierende Sicherheitslücke zu schließen — (trotz der Kritik).

In der öffentlichen Debatte bemängeln Kritiker, dass die technischen Fähigkeiten der TCPA-Hardware bspw. dem Hersteller ermöglichen, die totale Kontrolle über die von Benutzern verwendeten Daten und Informationen zu erlangen und somit ihre Privatsphäre zu verletzen [2, 11, 3]. Obwohl es technisch möglich ist, basierend auf den TCPA-Spezifikationen derartige Funktionen zu realisieren, muss es dazu nicht zwingend kommen.

*Die TCPA Komponenten greifen selbst nicht aktiv in die Geschehnisse in einem Computersystems ein.*<sup>4</sup>

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) Anwendungen zu unterstützen<sup>5</sup>, weshalb nicht alle Komponenten, speziell die verwendeten kryptographischen Schlüssel, unter der Kontrolle des Benutzers stehen können.<sup>6</sup> Ansonsten bestünde die Gefahr des Missbrauchs und der Verletzung von Urheberrechten. Die entsprechenden Eigenschaften von TCPA ermöglichen jedoch auch den Missbrauch der von TCPA bereitgestellten Funktionen, z.B. eine systemweite Zensur aller Dokumente durch die Industrie. 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 gezieltes Design des Betriebssystems ausschließen.*

Um kritisierte Eigenschaften der TCPA-Spezifikation zu minimieren, dürfte beispielsweise das Betriebssystem keinen *Reference-Monitor*<sup>7</sup> 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.

---

<sup>4</sup>Die Zertifizierung von Softwarekomponenten ist nicht Teil der TCPA-Spezifikation. TCPA Komponenten können daher nicht darüber entscheiden, welches Betriebssystem oder welche Anwendung geladen wird.

<sup>5</sup>Neuere Veröffentlichungen behaupten, dass DRM kein Entwicklungsziel von TCPA gewesen sei [10, 9]. Allerdings sprechen sehr viele Gründe dafür, dass DRM-Anforderungen aus der Industrie ein Grund für die Entwicklung von TCPA waren. Dies ist auch kein grundsätzlicher Nachteil, solange DRM-Fähigkeiten dem Benutzer nicht aufgezwungen werden können.

<sup>6</sup>Werden die DRM-Anforderungen ausgeschlossen, dann könnte eine Plattform bereitgestellt werden, die den Benutzern ein gleiches Maß an Sicherheitsfunktionen bietet, wie TCPA, jedoch die befürchteten Szenarien effektiv unterbindet.

<sup>7</sup>Gemeint ist eine abstrakte Maschine, welche Zugriffe auf verschiedene Objekte kontrolliert.

Da die Sicherheit eines TCPA-fähigen Betriebssystems von entscheidender Bedeutung für seine Vertrauenswürdigkeit gegenüber der Industrie, aber eben auch gegenüber den Benutzern ist, sollte es nicht unter der Kontrolle einzelner Softwarehersteller stehen. Durch eine Monopolstellung bei TCPA-Betriebssystemen könnte der Schutz der Benutzer nicht mehr garantiert werden. Zudem führt dies zu einer massiven Eindämmung der Innovationsfähigkeit vor allem kleiner und mittlerer Unternehmen, die keinerlei Einfluss auf die weitere Entwicklung des Betriebssystems besitzen [4, 1].

Die Forderungen der Industrie und der Benutzer nach vertrauenswürdigen Plattformen können basierend auf TCPA erfüllt werden, indem existierende Betriebssysteme um einen DRM-fähigen *Sicherheitskern* erweitert werden, dem die Benutzer und die Industrie 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<sup>8</sup>. Der Sicherheitskern kontrolliert die TCPA-Hardware derart, dass die Nutzbarkeit der TCPA-Komponenten auf ein sinnvolles Maß eingeschränkt wird.

Wie bereits erwähnt, zeichnet sich die TCPA zugrundeliegende 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 generiert werden.*

*Open Source* in Verbindung mit einem System politischer oder gesellschaftlicher Kontrolle kann helfen, nicht beabsichtigte Folgen des Technologieeinsatzes zu reduzieren.

Die von uns vorgestellte Architektur eines DRM-fähigen OpenSource Sicherheitskerns (siehe [8]) verhindert gleichzeitig eine Monopolstellung der Industrie und erhöht die Vertrauenswürdigkeit, da der Source-Code öffentlich zugänglich ist. Er kann gegebenenfalls einer technischen und rechtlichen Zertifizierung unterworfen werden. Der Sicherheitskern bildet eine einheitliche Grundlage für die Betriebssysteme der Softwarehersteller.

*Mit der Implementierung der PERSEUS Sicherheitsplattform [6, 7] wurde bereits gezeigt, dass die Realisierung eines minimalen Sicherheitskerns basierend 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.

Die TCPA-Spezifikationen werden von einem Industriekonsortium gestaltet und bieten eine Reihe von Funktionen an, auf die nationale Gesetzgeber weitestgehend keinen Einfluß nehmen können, wenn die betreffenden Unternehmen nicht auf dem eigenen Staatsgebiet ihren Sitz haben. Bei Betriebssystemen stellt sich die Situation ähnlich dar, denn auch hier ist die Möglichkeit zum regulativen Zugriff beschränkt.

---

<sup>8</sup>siehe [www.regtp.de/imperia/md/content/tech\\_reg\\_t/digisign/4.pdf](http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/4.pdf)

Durch Importbestimmungen der entsprechenden Hard- und Software, Dienstleistungen und Daten kann versucht werden, bestimmte Gestaltungsvorgaben durchzusetzen. Dieses Verfahren ist jedoch langwierig und ist insbesondere angesichts der häufigen Innovationen und Updates der Technologie in diesem Bereich problematisch.

Der Sicherheitskern ist Open Source. Eine staatliche, staatsnahe oder eine vom Staat benannte gesellschaftliche Institution könnte den Sicherheitskern zertifizieren. Zertifizierungskriterien sind neben technischen Aspekten der IT-Sicherheit vor allem rechtliche Fragen des Datenschutzes und des Urheberrechts. Ein System politischer Kontrolle bzw. Zertifizierung des Sicherheitskerns stellt sicher, dass die im demokratischen, politischen Prozess definierte Ziele u.a. hinsichtlich der Privatsphäre und des Urheberrechts effektiv durchgesetzt werden können.

## Autoren

Dirk Günnewig ist Politikwissenschaftler im interdisziplinären Forschungsprojekt zum Thema “Digital Rights Management” an der Universität Dortmund. Sein Forschungsschwerpunkt liegt im Bereich der technologiepolitischen Steuerung, speziell der Steuerung von DRM-Systemen und der Analyse der Interessen relevanter Akteure im Politikfeld Urheberrecht.

Weitere Informationen: <http://guennewig.digital-rights-management.de>  
email: [guennewig@digital-rights-management.de](mailto:guennewig@digital-rights-management.de)

Ahmad-Reza Sadeghi ist Junior-Professor am Horst-Görtz Institut für Sicherheit in der Informationstechnik an der Ruhr-Universität Bochum. Er promovierte im Bereich des kryptographischen Urheberschutzes am Fachbereich Informatik an der Universität des Saarlandes. Sein Forschungsschwerpunkt liegt im Entwurf und in der Entwicklung von DRM-Systemen und kryptographischen Protokollen.

Weitere Informationen:  
<http://www-krypt.cs.uni-sb.de/research/>  
email: [sadeghi@crypto.rub.de](mailto:sadeghi@crypto.rub.de)

Christian Stüble ist wissenschaftlicher Mitarbeiter in der “Cryptography and Security Group” im Fachbereich Informatik der Universität des Saarlandes. Sein Forschungsschwerpunkt liegt im Entwurf und in der Implementierung von Trusted Computing Plattformen, insbesondere sicherer Betriebssysteme.

Weitere Informationen:  
<http://www-krypt.cs.uni-sb.de/research/> und <http://www.perseus-os.org>  
email: [stueble@acm.org](mailto:stueble@acm.org)

## Literatur

- [1] C. Ahlborn. Kartellrechtliche Implikationen von Trusted Computing. Linklaters London, [http://www.zei.de/download/Konferenzseite/ahlborn\\_20030509.pdf](http://www.zei.de/download/Konferenzseite/ahlborn_20030509.pdf), 2003.
- [2] R. J. Anderson. The TCPA/Palladium FAQ. <http://www.cl.cam.ac.uk/rja14/tcpa-faq.html>, 2002.
- [3] W. A. Arbaugh. Improving the TCPA specification. *IEEE Computer*, pages 77–79, Aug. 2002.

- [4] C. Koenig. Trusted Computing im Fadenkreuz des EG-Wettbewerbsrechts. Zentrum für Europäische Integrationsforschung (ZEI), [http://www.zei.de/download/Konferenzseite/koenig\\_20030509.pdf](http://www.zei.de/download/Konferenzseite/koenig_20030509.pdf), 2003.
- [5] S. Pearson. *Trusted Computing Platforms - TCPA technology in context*. Hewlett-Packard Company, Prentice Hall PTR, 2003.
- [6] B. Pfitzmann, J. Riordan, C. Stübke, M. Waidner, and A. Weber. The PERSEUS system architecture. In D. Fox, M. Köhntopp, and A. Pfitzmann, editors, *VIS 2001, Sicherheit in komplexen IT-Infrastrukturen*, DuD Fachbeiträge, pages 1–18. Vieweg Verlag, 2001.
- [7] B. Pfitzmann, J. Riordan, C. Stübke, M. Waidner, and A. Weber. The PERSEUS system architecture. Technical Report RZ 3335 (#93381), IBM Research Division, Zurich Laboratory, Apr. 2001.
- [8] A.-R. Sadeghi and C. Stübke. Bridging the gap between TCPA/Palladium and personal security. Technical report, Saarland University, Germany, 2003.
- [9] D. Safford. Clarifying misinformation on TCPA. White paper, IBM Research, Oct. 2002.
- [10] D. Safford. The need for TCPA. White paper, IBM Research, Oct. 2002.
- [11] B. Schneier. Palladium and the TCPA. <http://www.counterpane.com/telegram-0208.html#1>.
- [12] Trusted Computing Platform Alliance (TCPA). TCPA PC specific implementation specification, Sept. 2001. Version 1.00.
- [13] Trusted Computing Platform Alliance (TCPA). Main specification, Feb. 2002. Version 1.1b.