1 TCPA/Palladium

1.1 Wofür steht TCPA/Palladium?

TCPA steht für Trusted Computing Platform Alliance (Allianz für vertrauenswürdige Computerplattformen)
Palladium ist eine Software, die Microsoft in kommende Windows-Versionen integrieren will. Sie soll auf TCPA aufsetzen und zusätzliche Features bereitstellen.

1.2.1 Offizielle Motivation ist security-by-default

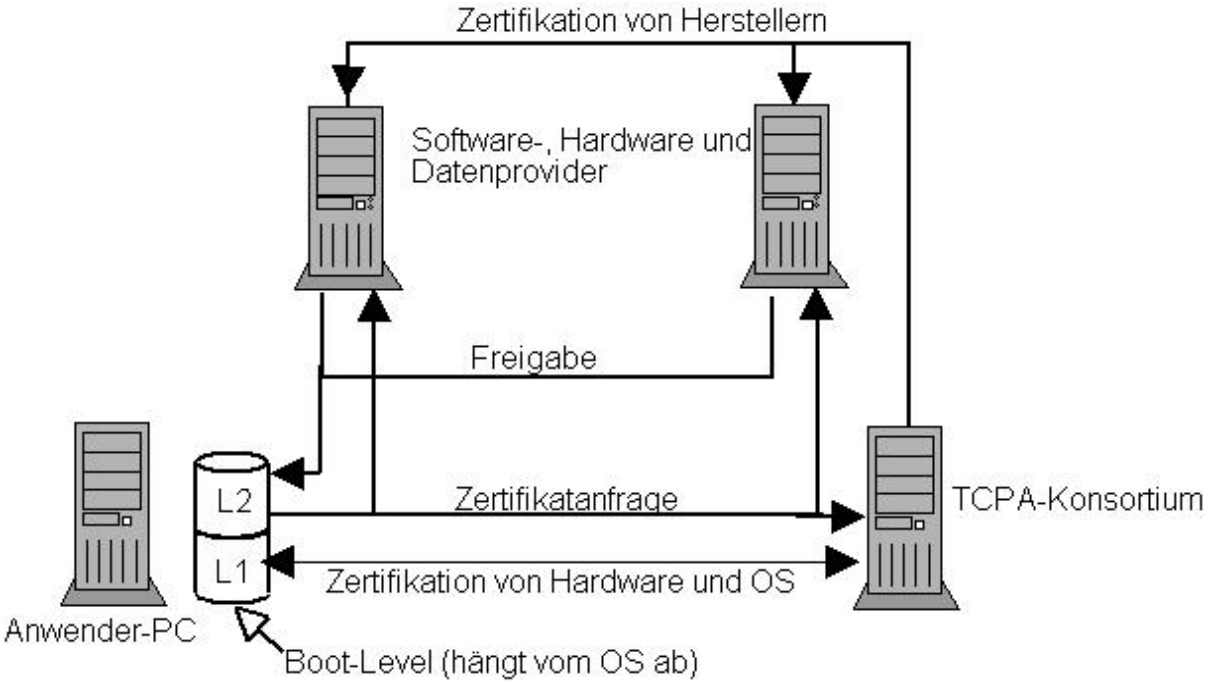
- Ver-/Entschlüsselung beschleunigen und sicherer machen
- digitale Signaturen für Daten/Programme erzwingen (Pro für Virenschutz)
- erzwungene Zugangskontrolle** zu Netzwerken/Terminals/Client-PCs usw.
- Systemintegrität beim bootup testen (Passt die Grafikkarte zu Mainboard und OS?)
- Identitätenverwaltung (Admin, Users, Useraliases)

1.2.2 inoffizielle Motivation

- uneingeschränktes DRM (Digital Rights Management = digitale Rechteverwaltung), auch wenn dies offiziell verneint wird erst durch sichere Verschlüsselung und erzwungene Zugangskontrolle** ermöglicht.

1.3 Wie funktioniert es?

1.3.1 Das Zertifikatnetzwerk (grobe Skizze nach den whitepapers von http://www.trustedcomputer.org):



1.3.2 lokale Komponenten und Zugriff vom und auf das Zertifikatnetzwerk

TCPA sorgt für den Einbau einer Überwachungs- und Meldekomponente in künftige PCs. Die bevorzugte Variante in der ersten Phase der Einführung ist ein Fritz-Chip* - ein Smartcard-Chip oder Dongle, der aufs Motherboard gelötet wird oder später sogar Prozessorintegriert.

Sobald der PC gebootet wird, übernimmt der Fritz-Chip* die Kontrolle. Er überprüft, ob das Boot ROM TCPA-konform ist, führt es aus und bewertet den Zustand des Rechners. Dann wird der erste Teil des Betriebssystems überprüft, geladen und ausgeführt. Anschließend wird wieder der Zustand des Systems bewertet und so weiter. Die Vertrauensgrenze, die Hardware und Software als bekannt und überprüft bewertet, wird kontinuierlich erweitert.

In einer Tabelle werden Hardware (Soundkarte, Grafikkarte, etc.) und Software (Betriebssystem, Treiber, etc.) gespeichert. Dabei können Hardware, BootROM und OS durch eine Hardwareliste (PLA oder Statischer RAM) mit kontinuierlichem update via Internet gespeichert werden. Der Fritz-Chip* überprüft also, ob die Hardwarekomponenten auf der TCPA-genehmigten Liste stehen und die

Softwarekomponenten signiert sind und dass keine dieser Komponenten eine erloschene Seriennummer bzw. Datum etc. (also entgegen offizieller Aussagen DRM) aufweist.

Diese Liste wird regelmäßig heruntergeladen und mit den Dateien, die die Anwendung öffnet, verglichen. Die Löschung von Dateien kann dann anhand des Inhaltes, ihrer Seriennummer oder zahlreicher anderer Kriterien erfolgen. Die Idee dahinter ist nicht nur Raubkopieren zu verhindern. Zusätzlich sorgt man nämlich dafür, dass weltweit jeder TCPA-konforme PC ein öffnen von Dokumenten verweigert, die mit dieser raubkopierten Version erstellt wurden.

Sollten bedeutsame Änderungen an der PC-Konfiguration vorgenommen worden sein, muss der PC online gehen, um sich erneut zu zertifizieren.

Die Kontrolle der TCPA-Konformität wird dann an den Teil des Betriebssystems, der die Einhaltung der Richtlinien überwacht (z.B. Palladium in Windows), abgegeben und TCPA-zertifizierte Software- und Datenproduzenten können nun die Richtlinien für die Nutzung ihrer Daten festlegen (weiter zertifizieren).

z.B. wird Disney per Authentifizierungsprotokoll versichert, dass der Rechner ein geeigneter Empfänger von "Schneewittchen" ist. D.h., dass der Rechner momentan eine autorisierte Anwendung laufen hat - Mediaplayer, Disneyplayer, was auch immer. Der Disney-Server sendet darauf hin die verschlüsselten Inhalte mit einem Schlüssel, den der Fritz-Chip* zur Entschlüsselung derselben verwendet. Diesen Schlüssel stellt der Fritz-Chip* nur der autorisierten Anwendung zur Verfügung und auch nur so lange, wie die Rechnerumgebung als "vertrauenswürdig" gilt. Daher müssen zuvor die Sicherheitsrichtlinien, die den Rechner als "vertrauenswürdig" definieren vom Server des Herstellers der Playersoftware heruntergeladen werden.

1.4.1 Ängste vor TCPA/Palladium bzw. Implikationen

Die offiziellen Motivationen scheinen rein positiv und werden auch für Werbezwecke genutzt, aber es bestehen berechtigte Ängste um die Informations-„Freiheit“ durch DRM, falls TCPA zum Standard wird.

Durch DRM würden Raubkopien auf TCPA-Systemen nicht mehr funktionieren und jedem Datum kann ein Ablaufdatum beigemessen werden, so dass der TCPA-Chip oder eine entsprechende Software-Implementierung bzw. –Erweiterung das Datum zum Verfallsdatum auf Eis gelegt oder gelöscht wird oder ein update über Internet eingespielt wird. Dies soll z.B. video-on-demand oder ähnliche Geschäftsmodelle ermöglichen bzw. kalkulierbar machen.

Relativ gesicherten Informationen zu Folge sollen auch bestimmte Regierungen bzw. zugehörigen Geheimdiensten (z.B. der USA) einen Generalschlüssel erhalten, so dass Zensur und Manipulation von Dateien Tor und Tür geöffnet wären. Dieses würde aber wiederum auch bedeuten, dass wenn der Generalschlüssel einmal korrumpiert ist vollständiger Zugriff auf das System von außen herrscht. D.h. jemand im Besitz des Generalschlüssels kann auch Dateien löschen oder TCPA-Viren installieren. Weiterhin kann generell die Kommunikation zwischen TCPA-Computern und nicht TCPA-Computern verhindert werden.

Die eigene Computer-Konfiguration (Hardware & Software) ist allen Generalschlüssel-Besitzern (nur diese gelten als vertrauenswürdig) bekannt.

Elektronische Bücher (generell private Veröffentlichungen) sind angreifbar, sobald sie einmal veröffentlicht wurden; die Gerichte können durchsetzen, dass sie "unveröffentlicht" werden (analog 1984 von Orwell), und die TCPA-Infrastruktur wird die Drecksarbeit übernehmen.

1.4.2 Die Verlierer

Es sieht z.B. so aus, als würde die europäische Smartcard-Industrie Schaden nehmen, da die Funktionen ihrer Produkte in die Fritz-Chips* von Laptops, PDAs und Mobiltelefone der dritten Generation wandern werden. (Wie schon bei integrierten WaveLAN-Karten) Tatsächlich wird sich ein Großteil der Informationssicherheitsindustrie Sorgen machen, wenn TCPA zum großflächigen Einsatz kommt.

Microsoft behauptet, dass Palladium Spam, Viren und so ziemlich alles schädliche („böse“) im Cyberspace stoppen wird - falls das stimmt wird den Herstellern von Antivirensoftware, den Spammern, den Spamfilter-Herstellern, den Firewall-Firmen und den Leuten aus dem Bereich der Intrusion-Detection die Butter vom Brot genommen.

Mit Sicherheit nicht zertifiziert werden Open Source-Projekte, denn die werden immer mehr zu ernsthaften Konkurrenten. Kleinere Software-Firmen können sich die Zertifizierungskosten nicht leisten.

Im Wesentlichen sind aber Datenschutz, Privatsphäre und andere persönliche Freiheiten in Gefahr.

1.4.3 Die Gewinner

TCPA bietet den zertifizierten Firmen, wie Microsoft, Intel, AMD, Siemens, Samsung etc. die Möglichkeit lästige (zumeist kleinere) Konkurrenten loszuwerden und nebenbei noch eine Menge Geld zu verdienen.

1.5 Was hat das mit der Seriennummer des Pentium III zu tun?

Das Modell von Hardware-Zertifizierung ist nicht neu. Mitte der 90er startete Intel ein früheres Programm, das bis zum Jahr 2000 die Funktionalität des Fritz-Chip* in den Hauptprozessor oder den Cache Controller integrieren sollte. Die Pentium Seriennummer war ein erster Schritt auf diesem Weg.

Die ablehnenden öffentlichen Reaktionen scheinen sie erst zum Abwarten, dann zur Bildung eines Konsortiums mit Microsoft und anderen und schließlich zu einem erneuten Anlauf mit vereinten Kräften gebracht zu haben.

1.6 Kann man TCPA umgehen bzw. abschalten (Schwächen von TCPA)

Lässt man seinen PC mit Administratorprivilegien laufen, kann man auch unsichere Anwendungen benutzen, aber selbst in diesem Modus kann man den Fritz-Chip* nicht dazu bringen, raubkopierte Software zu ignorieren. Selbst wenn der Chip weiß, dass der Rechner in einem unsicheren Zustand bootet, wird er immer noch überprüfen, ob sich das verwendete Betriebssystem auf der schwarzen Liste befindet.

Man kann den Bus zwischen Prozessor und Fritz-Chip* abhören und so nach einiger Zeit sein eigenes Passwort herausfinden, so lange der Fritz-Chip* noch nicht im Prozessor integriert ist, so dass hier Korruption des Schlüssels möglich ist, wenn auch sehr schwer. Eine weitere Möglichkeit ist die eigene Telefonleitung anzuzapfen.

Es gibt weiterhin die Möglichkeit Schwächen die eine TCPA-Software oder –Hardware hat, die bei Zertifizierung nicht erkannt (oder ignoriert) wurden auszunutzen.

1.7 Begriffsklärung

1.7.* Woher kommt die Bezeichnung "Fritz-Chip"?

Der Name wurde zu Ehren des Senators von South Carolina - Fritz Hollings - gewählt, der unermüdlich im Kongress daran arbeitet, TCPA als zwingend für sämtliche Konsumelektronik vorzuschreiben.

1.7.** Was ist erzwungene Zugangskontrolle?

Software und Hardware, die auf TCPA/Palladium-Plattformen laufen soll muss zuvor vom TCPA-Konsortium zertifiziert worden sein. Dateien, die als vertraulich markiert sind nur auf dem System zu öffnen sein sollen, auf denen sie erstellt oder explizit freigeschaltet werden.

1.8 Material

die offizielle Seite:
http://www.tustedcomputing.org/

Chaosradio Mitschnitt:
http://www.againsttcpa.com/download.html

allgemeine Infos:
http://www.notcpa.org/faq_german.html#
http://www.againsttcpa.com/tcpa-faq-en.html
http://www.againsttcpa.com/what-is-tcpa.html
http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

auf heise:
http://www.heise.de/newsticker/data/anw-09.04.03-000/