

TCPA und Palladium

Der gläserne PC-Spieler

Die Industrie will Ihren Rechner kontrollieren! Das behaupten zumindest Kritiker der neuen Technologien TCPA und Palladium. GameStar nennt die Fakten.

Haben Sie MP3-Dateien auf Ihrer Festplatte? Oder Filme? Die können Sie vielleicht bald nicht mehr nutzen. Denn 170 Hersteller unter der Führung von Microsoft und Intel arbeiten mit dem TCPA¹-Standard an einer massiven Kontrolle aller Vorgänge auf Ihrem PC. Künftig könnten Internet-Server darüber entscheiden, welche Datei Sie mit welchem Programm öffnen, welche Spiele Sie installieren und welche Websites Sie besuchen dürfen. TCPA ist keine Zukunftsmusik, sondern steckt bereits heute in den Thinkpad-Notebooks von IBM. Spätestens 2004 soll jeder neue PC diese Technologie besitzen. In den USA plant der republikanische Senator von South Carolina, Fritz Hollings, sogar das Verbot TCPA-inkompatibler Rechner. Mit Palladium integriert Microsoft eine ähnliche Technik in das neue Windows. Datenschützer und Sicherheitsexperten befürchten eine Entmündigung des PC-Nutzers, oder schlimmer noch einen Überwachungsstaat wie in Orwells 1984. GameStar hat sich für Sie durch die TCPA-Spezifikation gewühlt und geprüft, welche Auswirkungen TCPA und Palladium für Sie wirklich haben.

Das TCPA-Konsortium

Offiziell will die TCPA die PC-Sicherheit durch einen Schutz gegen Hacker erhöhen und so das Vertrauen des Nutzers in die Industrie stärken. Im Kontrast dazu steht die derzeit geheime TCPA-Mitgliederliste. Laut Gründungsmitglied Intel fehle die aber nur



TCPA und Palladium können lästige Cheater von CounterStrike-Servern werfen.

auf der Homepage (www.gamestar.de Quicklink: [38](#)), weil dort aufgeführte Firmen mit E-Mails überschwemmt würden. Eine neue Liste ohne Kontaktdaten soll bald online gehen. Auf www.notcpa.org (www.gamestar.de Quicklink: [40](#)) finden Sie eine ältere Liste mit rund 170 Herstellern, darunter Branchenriesen wie Microsoft, Intel, AMD, Nvidia, HP und IBM. Geht es nach der TCPA, steckt 2004 in jedem neuen PC ein Verschlüsselungschip namens TPM (Trusted Platform Module). Der kann Dokumente vor unerlaubtem Zugriff schützen und auf Änderungen durch Viren oder Trojaner untersuchen (Integritätstest). Anders als oft behauptet darf jeder Entwickler den offenen TCPA-Standard gratis für seine Programme nutzen. Ältere Spiele und Programme laufen ohnehin problemlos auf einem TCPA-Rechner.

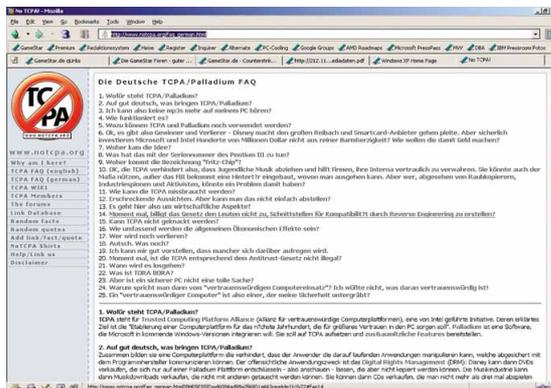
Standardmäßig deaktiviert

Der für TCPA notwendige Verschlüsselungschip TPM ist standardmäßig deaktiviert. Sie als Anwender entscheiden also, ob Sie das System nutzen. Dabei gibt es im Mainboard-Bios voraussichtlich drei Stufen. Entweder schalten Sie TCPA komplett aus, oder Sie ak-

tivieren nur die lokale Datenverschlüsselung. In diesem Betriebsmodus brauchen Sie keinen Internetzugang. Die dritte Einstellung ermöglicht den Zugriff auf TCPA-abgesicherte Webseiten, zum Beispiel für Homebanking. Allerdings funktioniert TCPA nur, wenn Hard- und Software zusammenarbeiten. Bevor der Chip also einen Dienst aufnimmt, müssen Sie die passenden Funktionen des Betriebssystems aktivieren. Nach aktuellem Stand unterstützt Linux TCPA ab Ende 2003 und Windows ab dem XP-Nachfolger Longhorn Ende 2004. Laut Microsoft und Intel lassen sich die TCPA-Komponenten des Betriebssystems jederzeit an- und abschalten, fraglich ist allerdings, ob dies so bleibt.

Sicherheitsmechanismus

Während Zugriffssicherungen wie Passwörter oder mobile Speichermedien (Compact Flash Card) den Anwender authentifizieren, authentifiziert TCPA die PC-Hard- und Software. Es stellt also sicher, dass kein Hacker oder ein anderer Unbefugter den PC verändert hat. Die dazu nötigen Schlüssel hält er laut einer FAQ der TCPA (www.gamestar.de Quicklink: [42](#)) stets geheim, um Hackern



Auf www.notcpa.org formulieren sich Kritiker von TCPA und Palladium.

¹TCPA: Die Trusted Computing Platform Alliance (Allianz für vertrauenswürdige Computer-Plattformen) verspricht sichere PCs. Das System kann Sie aber auch ausspionieren.



IBM verbaut bereits heute in den Thinkpad-Notebooks den TCPA-Chip.

keinen Angriffspunkt zu bieten. Für die Kommunikation außerhalb des TPM ist von den Schlüsseln lediglich ein Hash sichtbar, also ein einmaliges Abbild, das keine Rückschlüsse ermöglicht und so die Privatsphäre schützt. Wenn Sie TCPA aktiviert haben, prüft das TPM beim PC-Start die Integrität Ihres Systems: zuerst das Bios, dann folgt wie heute auch eine eventuelle Passwort-Abfrage. Anschließend kontrolliert es Bootloader², Betriebssystem-Kernel³ und Software wie Virens Scanner. Das erschwert Hackern, Anti-Viren-Tools auszutricksen – die PC-Sicherheit steigt. Nachteil: Mittels TCPA verschlüsselte Dateien werden unbrauchbar, wenn der Schlüssel weg ist. Erst auf Nachfrage von GameStar verrät Intels Security Architect David Grawrock die Backup-Strategie. So lassen sich die Eigenschaften des TPMs auf einer Diskette passwortgeschützt speichern und später auf ein neues TPM übertragen.

Palladium

Zu Microsofts Softwareprojekt Palladium gibt es derzeit noch wenig Informationen. Offiziell heißt es »Next Generation Secure Computing Base« (NGSCB) und soll wie TCPA zusammen mit einem Chip auf dem Mainboard den PC sicherer machen. Allerdings ist Palladium inkompatibel zum derzeitigen TPM und erfordert einen eigenen SSC-Chip (System Security Component). Laut Microsofts Chief Security Officer Gerald Hübnert bemüht sich das Unternehmen aber zusammen mit der TCPA, beide Chips in einem TPM zu vereinen.

Im Gegensatz zu TCPA unterstützt Palladium mit dem Programmbestandteil Nexus getrennte Speicherbereiche. Die schützen Virens Scanner oder Homebanking-Anwendungen vor Hackern. Auch Online-Spiele könnten von Palladium profitieren:

Durch Prüfen der Spieldateien entlarvt ein Counterstrike-Server Cheater und wirft sie aus dem Spiel. Kritische Stimmen vermuten hingegen, das Palladium Informationen über den Nutzer und den PC an Microsoft übermittelt. Zwar machen das bereits Windows XP und vermutlich auch dessen Nachfolger Longhorn, aber Nexus wird laut Microsoft-Sprecher Frank Mihm einen öffentlichen Quelltext haben. Jeder Programmierer könnte also etwaige Spionagefunktionen leicht nachvollziehen. Übrigens erfahren wir aus Microsoft nahestehenden Quellen, dass Palladium für Windows XP mit einem Service Pack nachgeliefert werden könnte.

Wirtschaftliche Interessen

Gegen Raubkopien sind TCPA und Palladium allein machtlos. Erst sogenannte DRM⁴-Systeme schützen die Urheberrechte per digitalem Wasserzeichen und einem Internet-Server. Beispielsweise lässt sich eine Software dann nur noch auf einem PC installieren. Allerdings kann eine DRM-Software in Kombination mit dem TPM auch die Rechte der Kunden untergraben. Vorerst bleiben selbst erstellte Filme und MP3s nutzbar, im schlimmsten Fall lassen sich aber zum Beispiel Word-Dokumente nur noch mit Microsoft Office öffnen, nicht aber mit selbst geschriebener Software oder der quelloffenen Microsoft-Konkurrenz Open Office ([www.gamestar.de Quicklink: \[41\]](http://www.gamestar.de Quicklink: [41])). Der Windows Media Player dürfte in der neuen Version 10 ein integriertes DRM-System haben, wie bereits jetzt der Real Media Player. Mit DRM könnte ein Spielehersteller unerwünschte Mods leicht ausperren. Düster wird's, wenn der DRM-Server abstürzt. Dann verweigern Spiele nämlich ihren Dienst genauso wie MP3s und Filme.

Fazit

Zwar verbessern TCPA und Palladium die PC-Sicherheit, aber auch sie bieten nur begrenzten Schutz gegen Hacker-Angriffe. Es ist keine Frage, ob ein System geknackt wird, sondern wann. Besonders Microsoft ist für Sicherheitslöcher in seinen Programmen bekannt. Eine Kontrolle von Downloads bieten TCPA und Palladium ohnehin nicht. Daher sollten Sie auch künftig aufpassen, von

Daniel Visarius



Sie bestimmen Ihre Zukunft!

Sie als Anwender entscheiden über den Erfolg von TCPA und Palladium. Denn Sie müssen die Systeme erst aktivieren, und das ist gut so. Ich jedenfalls werde sie nicht nutzen, weil ich selbst bestimmen will, welche Dateien ich herunterlade und welche ich ausführe. Als Sicherheitssysteme haben TCPA und Palladium gute Ansätze. Bei Missbrauch der Technologien durch die Industrie empfehle ich Ihnen einen kompromisslosen Wechsel auf alternative Plattformen wie Linux, bei denen sich TCPA stets abschalten lassen wird. In Kombination mit DRM werden TCPA und Palladium schnell zu einer Gefahr für den freien Datenverkehr im Internet – GameStar bleibt für Sie am Ball!



Laut Microsoft macht das kommende Windows Longhorn mit Palladium den PC sicherer.

welchen Internet-Servern Sie Dateien herunterladen, damit ungebetene Software-Gäste draußen bleiben. Beweise für Vermutungen, nach denen amerikanische Geheimdienste einen Universalschlüssel für TCPA-PCs bekommen, fehlen derzeit. Dennoch: Die Kombination aus TCPA/Palladium, passendem Betriebssystem und DRM bringt den gläsernen PC-Nutzer in Reichweite und leistet Industrie-Monopolen Vorschub. Wenn Sie auf Nummer sicher gehen wollen, rüsten Sie Ihren Rechner am besten noch 2003 mit TCPA-freier Hardware auf. GameStar verfolgt das brisante Thema weiter und hält Sie auf dem Laufenden. **DV**

²Bootloader: Nach dem Booten sucht das Mainboard-Bios einen sogenannten Startsektor. Der enthält den Bootloader, der das eigentliche Betriebssystem startet.
³Kernel: Der Kernel ist der Kern des Betriebssystems. Er enthält Routinen zur Speicher- und Gerätetreiberverwaltung. Unter Linux lässt er sich individuell konfigurieren.
⁴DRM: Digital Rights Management regelt in Kombination mit einem digitalen Wasserzeichen und Internet-Servern die Nutzungsrechte in MP3s und Filmen.