

Die nötige Hardware gibt es schon

TCPA wird von den Kritikern oft mit NGSCB in einen Topf geworfen – fälschlicherweise. Die Trusted Computing Platform Alliance (TCPA), gegründet 1999, ist ein Zusammenschluss von 200 Hard- und Software-Herstellern. Ziel der Organisation war es, einen Standard für vertrauenswürdige Computer zu entwickeln. Mittlerweile sind die Tage der TCPA gezählt. Fünf ihrer wichtigsten Mitglieder – Intel, AMD, HP, IBM und Microsoft – haben eine Nachfolgeorganisation gegründet, die Trusted Computing Group (TCG), die nun die Entwicklung einer NGSCB-kompatiblen TCPA-Version 1.2 vorantreibt.

Die Mitglieder der TCPA wurden aufgefordert, der TCG beizutreten – knapp 30 haben dies bisher getan. TCPA gilt ebenso wie Palladium als verbrannte Marke.



IBMs Thinkpad T30 ist eines der ersten Produkte mit TCPA-Unterstützung.
Foto: IBM

Anders als NGSCB ist TCG nicht nur ein Phantom – Version 1.1b der Spezifikation steht seit Mai 2002 im Netz, kompatible Hardware wie IBMs Thinkpad T30 ist bereits im Handel erhältlich. Besonders vertrauensbildend wirkt die Spezifikation indes nicht: In der Fußzeile des Dokuments ist das Datum September 2001 über 332 Seiten hinweg durchgängig falsch als „Setember 2001“ geschrieben. In Programmen und Hardware macht ein solcher kleiner Fehler den Unterschied zwischen sicher und nicht sicher. Kern der TCG-Spezifikation ist ähnlich wie bei NGSCB ein ausschaltbarer Sicherheits-Chip, der in etwa einer nicht entnehmbaren Smartcard entspricht. Er prüft während des Bootvorgangs die Systemintegrität und enthält Schlüssel, mit denen der Rechner eindeutig identifizierbar ist. Zugleich dienen sie der Ver- und Entschlüsselung von Daten. Einsatzgebiete für TCG sind nicht nur Rechner, sondern beispielsweise auch PDAs und Handys. Abgeschottete Speicherbereiche sieht die Spezifikation allerdings nicht vor, ebenso wenig die Zertifizierung von Software. Microsofts NGSCB geht somit deutlich über die aktuelle TCG-Spezifikation hinaus. Ob Version 1.2 die Microsoft-Anforderungen vollständig erfüllen wird, ist offiziell noch offen – es spricht jedoch vieles dafür.

Der Anwender hat die Wahl – noch. Unter NGSCB bestimmt der Rechteinhaber, welches Programm seine Musikstücke wiedergeben darf.



Microsoft gar, unter welchen Bedingungen ein Zertifikat ausgestellt werden darf?

Spyware darf kommunizieren

NGSCB ermöglicht es, Programme und Dokumente eindeutig an einen PC zu binden – einige nicht exportierbare Schlüssel im Sicherheits-Chip machen es möglich. Ein Vorgang wie die Windows-Aktivierung lässt sich so kaum mehr überlisten. Unklar ist dabei, inwieweit die Technik und entsprechenden Anwendungen bei jedem Programmaufruf auf zentrale Server zugreifen werden. Fragt Office künftig bei jedem Programmstart am Microsoft-Server nach: „Bin ich eine Raubkopie?“ Und was fragen oder übermitteln die Programme noch?

Dass Anwendungen ungefragt „nach Hause telefonieren“, ist auch heute schon der Fall. Welche Daten sie übermitteln, finden Hacker in der Regel binnen kurzer Zeit heraus und machen die Infos öffentlich. NGSCB-Programme werden sich nicht so einfach auspähen lassen – laut Spezifikation ist schon der Einblick in ihren Speicherbereich unmöglich.

Hintertüren für Geheimdienste

Wenig Gefallen an abhörsicheren Programmen dürften Polizei und Geheimdienste finden, aber auch Finanzämter und andere staatliche Stellen. Amerikanischen Sicherheitsbehörden ist starke Verschlüsselung seit jeher ein Dorn im Auge. Zwar war sie mit Programmen wie PGP auch bisher schon möglich – aber die meisten Anwender verzichte-

ten aus Bequemlichkeit darauf. Trusted Computing macht Verschlüsselung tauglich für den Masseneinsatz, das ist der entscheidende Unterschied. Dementsprechend sprießen im Internet die Gerüchte, Microsoft könnte in Palladium Hintertüren (Backdoors) für staatliche Stellen einbauen. Rüdiger Weis, Diplom-Mathematiker und Chief Cryptographer der Cryptolabs Amsterdam, hält die Gefahr für real – der Einbau von „hidden channels“ könne im Nachhinein nicht nachgewiesen werden.

Microsoft dementiert nach Kräften. Der Hersteller will den Quelltext von NGSCB sogar offen legen – jedoch nur unter der hauseigenen Shared-Source-Lizenz. Die kennt bislang strenge Einschränkungen: Nur Großkunden bekommen den Quelltext zu sehen, auch das nur nach Unterzeichnung diverser Stillhalteabkommen – und beileibe nicht immer den kompletten Code.

Sicherheitslücken im System

Den größten Schaden könnte Trusted Computing genau dann anrichten, wenn Anwender glauben, ihr PC sei nun endgültig sicher – und somit jede Vorsicht überflüssig. Eine irrige Vorstellung, da jedes System geknackt werden kann. Zwar scheint die Technik vergleichsweise sicher vor Software-Attacken, doch hat ein Hacker physikalischen Zugang zum PC, kann für nichts mehr garantiert werden, das stellt auch Microsoft klar. Nicht-NGSCB-Anwendungen bleiben obendrein so unsicher, wie sie es schon immer waren.

Wie sicher die Daten sind, die NGSCB-Programme auf Festplatte spei-