

Trusted Computing und Digital Rights Management

Der Besitz und der Schutz von Information hat in den vergangenen Jahren vermehrt zu Anstrengungen geführt Technologien zu entwickeln, die zum Schutz von Informationen dienen sollen. Die Konsequenzen dieser Entwicklungen werden viel zu oft unterschätzt oder nicht richtig durchdacht. Dieser Artikel von Rene Pfeiffer soll einige kritische Ideen aufwerfen und über die Technologien informieren.

• Trusted Computing und Digital Rights Management

Wegen der weiten Verbreitung erweitern Rechnerplattformen wie die PC-Architektur ihre Einflüsse in eine Vielzahl von neuen Business- und Heimanwendungen. Fragen zur Computersicherheit und digitalen Kontrollmechanismen haben in der Vergangenheit viele Projekte ins Leben gerufen. Die Trusted Computing Platform Alliance (TCPA) Arbeitsgruppe ist eine von ihnen. Sie wurde im Oktober 1999 von Compaq, HP, IBM, Intel und Microsoft gegründet. Die TCPA zielt darauf ab, sogenannte "trust controls" in zukünftigen Hardwarekomponenten zu implementieren, die wiederum von Betriebssystemen und anderer Software genutzt werden kann. Derzeit besteht die Architektur aus einer Spezifikation, die bei den TCPA erhältlich ist (Spezifikation 1.1 ist veröffentlicht, Spezifikation 1.2 ist nur unter einer Geheimhaltungsvereinbarung verfügbar). Die ersten Chips, die TCPA unterstützen, sind bereits vorhanden.

Die Idee einer "Trusted Computing"-Plattform selbst hört sich schon verlockend an. TCPA selbst ist vielleicht keine schlechte Idee, aber wenn man die Implikationen für Enduser miteinbezieht, so zeigen sich ebenso Nachteile. Microsoft entwickelt eine neue Komponente mit dem früheren Code-Namen "Palladium" (laut einer Pressemeldung heißt sie jetzt "next-generation secure computing base for Windows"). Dessen Zweck ist es, eine "Trusted Computing"-Plattform für das Microsoft Windows Betriebssystem zur Verfügung zu stellen. Es verwendet die Hardware, die von der TCPA spezifiziert ist, und arbeitet als eine Art paralleles Betriebssystem, das sicher von Windows getrennt ist. Durch die TCPA-Hardware kann es sicherstellen, dass es nicht kompromittiert wurde. Dies funktioniert über Kryptographie. Danach übernimmt das "Palladium"-Subsystem, welches dann feststellt, was vertrauenswürdig ist oder nicht. Ein MSNBC-Artikel streicht die Fähigkeiten mit folgenden Features heraus:

- ◆ "Erzählt Ihnen, mit wem Sie es zu tun haben, und was sie tun. Bei Palladium geht es nur darum, zu entscheiden, was vertrauenswürdig ist."
- ◆ "Schützt Information."
- ◆ "Stoppt Viren und Würmer."
- ◆ "Bewacht die Privatsphäre. Mit Palladium ist nicht nur möglich, Daten am eigenen Computer zu versiegeln, sondern auch, diese an Agenten zu senden, die nur die diskreten Stücke verteilen, die sie an die richtigen Personen freigeben wollen."
- ◆ "Kontrolliert Ihre Informationen, nachdem Sie sie versandt haben. Palladium wird den Studios und Plattenfirmen als ein Weg angeboten, um Musik und Filme zu verteilen [...]"

Während beide Entwicklungen verschiedene Schichten der Computerarchitektur betreffen, so haben sie doch etwas gemeinsam. In Kombination können sie genutzt werden, um ein sog. Digitales Rechte-Management (Digital Rights Management, DRM) in Anwendungen einzubauen. Palladium kann auch genutzt werden, um die Interoperabilität mit anderen Plattformen zu behindern. Vertreter Freier Software haben ihre Bedenken über Szenarien geäußert, in denen eine Kombination von Technologien für "Trusted Computing" und der Verbot von Reverse Engineering durch den DMCA (Digital Millennium Copyright Act) die Entwicklung von Freien Software Projekten schädigt. Der Samba Dateiserver ist ein prominentes Beispiel. Konsumenten können ebenso davon betroffen sein, indem sie Geld ausgeben für ein Computersystem, das sie nicht so verwenden dürfen, wie sie gerne

würden. Es sind bereits Audio-CDs am Markt erhältlich, die nicht auf allen CD-Playern abgespielt werden können. DRM ermöglicht es Firmen, Software auszuliefern, die nicht auf allen Computern funktioniert, obwohl dafür bezahlt wurde. An diesem Punkt wird das "Digital Rights Management" zu einem "Digital Restriction Management" und sollte für jeden von Belang sein, der heutzutage Computer verwendet.

Forscher von IBM Watson Research haben kürzlich zwei Artikel über die TCPA-Infrastruktur veröffentlicht. Beide Dokumente erklären die Motivation, eine "Trusted Computing"-Plattform zu kreieren, sowie die Aufgaben der TCPA-Hardware, die hauptsächlich daraus bestehen, kryptographische Schlüssel nach einem Systemboot zu speichern und zu schützen. Es ist möglich, Laufzeitmodifikationen des BIOS, des Betriebssystems oder anderer Anwendungen zu erkennen. Die Kommunikation zwischen TCPA-Chip und Betriebssystem ist nicht abgesichert und kann belauscht werden. Laut David Safford von IBM ist der einzige Zweck des Chips der, die kryptographischen Schlüssel, die während des Bootvorgangs erzeugt oder akquiriert wurden, wegzusperren. Es ist sogar ein experimenteller Linux-Treiber für den TCPA-Chip auf deren Webseite verfügbar. Er ist unter der GPL lizenziert. Eine genauere Betrachtung des Codes zeigt, dass dieser Treiber es dem Linux-Kernel ermöglicht, mit dem TCPA-Chip zu kommunizieren. Programmierer können dies benutzen, um die Fähigkeiten des TCPA-Chips für ihre Zwecke einzusetzen. Dieses Design betont die Unterschiede zu DRM. DRM baut auf TCPA auf. Das bedeutet, dass es vielleicht nicht genug ist, einen Treiber unter der GPL für die TCPA-Hardware zu besitzen, da die wichtigen Aufgaben in den Schichten darüber geschehen. Und diese könnten von Rechten zum Schutz des geistigen Eigentums geschützt sein.

Verwandte Links:

- ◆ <http://www.trustedcomputing.org/> - Trusted Computing Platform Alliance (TCPA)
 - ◆ <http://www.gnu.org/philosophy/can-you-trust.html> - Can you trust your computer?
 - ◆ <http://www.research.ibm.com/gsal/tcpa/> - IBM Watson Research - Global Security Analysis Lab: TCPA resources
 - ◆ <http://www.epic.org/privacy/consumer/microsoft/palladium.html> - Microsoft Palladium
 - ◆ <http://www.counterpane.com/crypto-gram-0208.html#1> - Crypto-Gram newsletter August 15, 2002
- Dieser Text ist Copyright 2003 Rene Pfeiffer und darf über jedes Medium beliebig zitiert oder verteilt werden, sofern dieser Hinweis erhalten bleibt.