Ein Kryptochip allein macht noch kein Trusted Computing

Michael Hartmann, SAP AG, TeleTrusT Arbeitsgruppenleiter AG2 „Personal Security Environment“ PSE

Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen, Vorstandsvorsitzender des TeleTrust Vereins

Unternehmensweite Sicherheitskonzepte verfolgen Ziele auf unterschiedlichen Ebenen. Auf der primären Ebene ist die Verfügbarkeit der IT-Infrastruktur sicherzustellen. Auf der darüber liegenden Ebene der Applikationen sind die Authentizität, Integrität und Vertraulichkeit der Daten zu garantieren. Auf der Ebene der Geschäftsprozesse müssen die Rechteverwaltung, Revisionssicherheit, Auditierbarkeit, Datenschutz und die Trennung von Verantwortlichkeiten gewährleistet werden. Die Konzepte und Technologien des Trusted Computing können helfen, die Sicherheitsziele auf Applikations- und Prozessebene zu erreichen.

Der Begriff Trusted Computing wird in der öffentlichen Diskussion fälschlicherweise oft mit der Trusted Computing Group und dem von ihr spezifizierten Trusted Platform Module (TPM) gleichgesetzt. Das TPM ist vereinfacht gesagt nichts weiter als eine SmartCard, die fest mit einem elektronischen Gerät (Desktop PC, Server, PDA, Mobiltelefon etc.) verbunden ist und physikalisch geschützt kryptographische Schlüssel speichert.

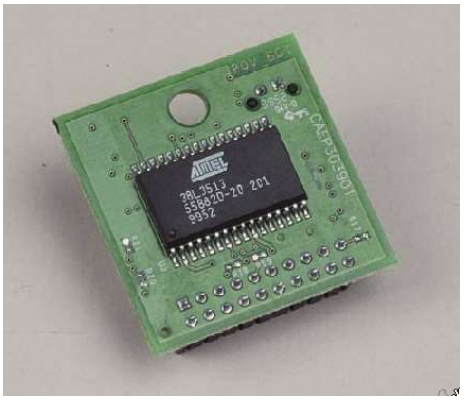

Abbildung 1: Beispiel eines TPMs

Das TPM ist wert- und nutzlos, wenn es nicht vom Betriebssystem und den Applikationen unterstützt wird. Wie jegliche Technologie sind Trusted Computing und das TPM zunächst wertfrei und können sowohl für Zwecke verwendet werden, die vielen Anwendern oder aber auch nur einigen wenigen nützen. Der Nutzen weniger einzelner auf Kosten von vielen wird berechtigterweise kritisiert und in der Öffentlichkeit bereits kontrovers diskutiert. Zur Zeit werden die erste Versionen der Trusted Computing Group Spezifikation schon als Grundlage für die millionenfache Produktion von TPM-Chips und deren Integration in Informationstechnik verwendet.

In diesem Artikel werden die möglichen Vorteile der Technologie herausgestellt.

Die Szenarien, die mit Trusted Computing möglich sind, reichen von erhöhtem Datenschutz bei Online-Transaktionen über Kontrolle von informationellen Werten eines Unternehmens („Digital Rights Management“) bis zur Verhaltenskontrolle durch einen öffentlichen Diensteanbieter für staatliche Belange.

Im Unternehmensumfeld besteht das berechtigte Interesse, die eigene IT-Infrastruktur zu kontrollieren, vorhandene (Security-) Policies durchzusetzen und somit einen reibungslosen Ablauf der Applikationen und Geschäftsprozesse zu ermöglichen. Das vertrauenswürdige Zusammenspiel der einzelnen Komponenten (TPM, Betriebssystem, Applikation, etc.) kann es den Verantwortlichen ermöglichen, nicht

nur auf Applikationsebene zu kontrollieren, wer die Applikationen/Ressourcen nutzt, sondern auch mit welchem Equipment. Als Stichwort sei an dieser Stelle Remote Attestation genannt. Mit diesem Mechanismus kann die Integrität, der Zustand eines Systems gegenüber einem Dritten (in diesem Fall dem Unternehmensnetzwerk) nachgewiesen werden. Dadurch kann aus Sicht des IT-Verantwortlichen garantiert werden, dass die Systeme einem aktuellen Patchlevel entsprechen, so dass nur zugelassene Applikationen in gewünschter Konfiguration betrieben werden. Damit wird verhindert, dass das Sicherheitskonzept des Unternehmens unterlaufen wird.

Die einzelnen Applikationen werden auf Betriebssystemebene gegeneinander abgeschirmt. Das Betriebssystem bedient sich dazu der Mechanismen „Memory curtaining“, „Secure input and output” und “Sealed storage”. Diese Mechanismen schirmen die Speicherbereiche der einzelnen Applikationen gegeneinander ab, bauen einen sicheren Kanal der Applikation zu Ein- und Ausgabegeräten auf und erlauben es der Applikation, ihre Daten in einem kryptographisch gesicherten Bereich auf den Massenspeichern abzulegen. Diese Mechanismen werden allerdings nicht alleine durch das TPM ermöglicht, sondern erfordern zusätzlich noch spezielle Hardware und Betriebssysteme.

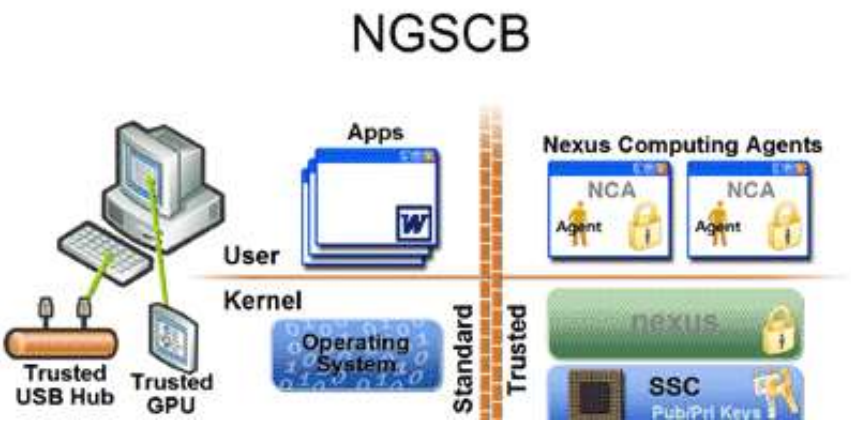

Abbildung 2: Beispiel NGSCB von Microfoft

In der Abbildung 2 ist eine Übersicht der Vorstellung, die Microsoft mit dem NGSCB unterstützt wollen. Ein Kleiner, überschaubarer, in Windows integrierter Sicherheitskern (Nexus) kontrolliert einen neuen Trusted Mode. Die Software kann unter der NGSCB "hinter der Mauer" im Trusted Mode (sog. "Nexus Computing Agents (NCA)") besonders sicher ausgeführt werden. Damit sollen weder Schadprogramme (Viren, Trojaner etc.) noch andere Applikationen oder Betriebssystemkomponenten können NCAs beeinträchtigen. Neben Microsoft arbeiten noch andere Firmen und Hochschulen an solchen Realisierungen von Secure Computing Base. Beispiele sind: EMSCB (European Multilateral-Secure Computing Base) von der Uni Bochum und LaGrand von Intel.

Durch eine derartige Absicherung kann sichergestellt werden, dass die einzelnen Applikationen nur genau die gewünschte Funktionalität zur Verfügung stellen. Auf dieser Grundlage können durch organisatorische Maßnahmen bei der Implementierung der Applikationen die o.g. Sicherheitsziele auf Prozessebene erreicht werden.

Von allen auf einander aufbauenden Komponenten, die für ein durchgängiges Trusted Computing notwendig sind, ist das TPM die grundlegendste - aber auch nur der erste Schritt. Solange die einzelnen Hardwarekomponenten, Betriebssysteme und Applikationen nicht konzeptionell angepasst werden, bleibt Trusted Computing nur ein hehres, aber wünschenswertes Ziel, das seine Praxistauglichkeit noch unter Beweis stellen muss.

Die Bandbreite der neuen Szenarien und Missbrauchsmöglichkeiten wird durch die starke Mehrseitigkeit der Anforderungen an mehr Sicherheit bestimmt. Denn je nach Blickwinkel ergibt sich ein anderer Bedarf an mehr Sicherheit: aus Sicht von Privatpersonen ist es der Datenschutz, aus Sicht von Firmen der Schutz von geistigem Eigentum und vertrauenswürdiger Geschäftsprozesse und aus Sicht des Staatsschutzes die Überwachung. Dieses Spannungsverhältnis existiert auch ohne Trusted Computing. Durch die neue Technologie wird auf Grund ihrer voraussichtlich flächendeckenden Verbreitung - ähnlich wie bei der Verwendung von Kryptographie im Allgemeinen – die Diskussion verschärft und beschleunigt.

Umso wichtiger ist eine frühzeitige, fundierte Beschäftigung mit der neuen Technologie. Ein wesentliches Merkmal, Monopole und damit die potenzielle einseitige Verwendung zu kontrollieren, besteht in einer offenen Standardisierung der zu Grunde liegenden Technologien. Damit ist es nicht nur anderen, kleineren Organisationen möglich, alternative Angebote zu machen, sondern mittelbar ist damit auch die freie Verwendung sichergestellt.

In den Arbeitsgruppen des TeleTrusT Deutschland e.V. werden die unterschiedlichen Aspekte und Ebenen vertrauenswürdiger Geschäftsprozesse betrachtet. So werden beispielsweise Geschäftsprozesse und Identitätsmanagement in der AG 9 bearbeitet, die juristischen Aspekte werden in der AG 1 diskutiert und die Betrachtung der zu Grunde liegenden Technologien erfolgt in der AG 2.