Turaya – Die offene Trusted-Computing-Sicherheitsplattform

NORBERT POHLMANN UND MARKUS LINNEMANN

Mit Turaya stellt die Forschungs- und Entwicklungsgemeinschaft des Projekts *European Multilaterally Secure Computing Base (EMSCB)* die erste vertrauenswürdige, faire und offene Sicherheitsplattform zur Verfügung, die auf Trusted-Computing-Technologie aufbaut. Sie bietet eine derart hohe Sicherheit, dass durch sie Möglichkeiten für innovative Geschäftsmodelle und kreative Anwendungen geschaffen werden können. Das als manipulationssichere Komponente in der Hardware eingesetzte „Trusted Platform Module" (TPM) ermöglicht die zuverlässige Überprüfung der Integrität und Authentizität eines IT-Systems – auch aus der Entfernung. Der Open-Source-Ansatz bietet die Möglichkeit, die viel diskutierte Trusted-Computing-Technologie vertrauenswürdig einzusetzen.

Schlüsselwörter: EMSCB · Turaya · Trusted Platform Module

1 Einleitung

Die Zahl der Angriffe auf Computersysteme durch Viren und Trojanische Pferde nimmt stetig zu. Der Zeitraum für die Ausnutzung von gerade bekannt gewordenen Schwachstellen in Softwaresystemen liegt derzeit bei 6,4 Tagen (Barnitzke 2005) und sinkt weiter. Des Weiteren nimmt die Komplexität der Angriffe immer weiter zu (Windows IT Pro 2004), während gleichzeitig immer weniger Kenntnisse notwendig sind, um solche Angriffe durchzuführen. Auch die starke Verbreitung von Bot-Netzen[1] stellt eine nicht zu unterschätzende Bedrohung für die Betroffenen dar. Angreifer durchbrechen die vorhandenen Sicherheitsmechanismen der Software- und

1 Bot-Netze sind Netzwerke, bestehend aus Rechnersystemen, die ohne Wissen der Besitzer unter die Kontrolle von Außenstehenden gebracht wurden und beispielsweise Spam-Mails versenden oder Denial-of-Service-Angriffe durchführen.

Betriebssysteme, und es stehen zur Zeit keine schärferen Sicherheitsmaßnahmen zur Verfügung, die dieser Problematik entgegenwirken könnten. Auch zusätzliche konventionelle Sicherheitslösungen wie Firewalls oder Intrusion-Detection-Systeme (IDS)[2] bieten diesbezüglich oft keinen ausreichenden Schutz. Die statischen Infrastrukturen einzeln stehender Systeme sind in den vergangenen Jahren von heterogenen und dynamischen Netzen verdrängt worden. Dabei verschwammen die einst klaren Firmen- und Systemgrenzen, die mit herkömmlichen Sicherheitsmechanismen, wie z. B. Firewalls abgesichert werden konnten.

Was wäre wenn:

- Sie ein vertrauliches Dokument verschlüsselt an einen Kollegen sendeten, der es auf dem Flurdrucker ausdruckt und vergisst? Für solche Fälle hätten Sie gerne die Möglichkeit gehabt, das Drucken Ihres Dokuments auf fremden Rechnersystemen zu untersagen!
- Ein Trojanisches Pferd einen *keylogger* auf Ihrem Rechnersystem installierte und all Ihre Passworteingaben mitläse? Dann wollten Sie, dass Ihre sicherheitsrelevanten Daten nicht unter dem Zugriff des Betriebssystems stünden!
- Ein Schädling die privaten Schlüssel Ihrer Zertifikate ausläse und versendete? Dann würden Sie einen sicheren Zertifikatsspeicher herbeisehnen!
- Sich jemand als externer Mitarbeiter mit dem *PDA* an Ihrem Firmenserver anmeldete und gar nicht Ihr Mitarbeiter wäre? Dann wünschten Sie, dass Sie das externe Rechnersystem mit hoher Vertrauenswürdigkeit authentifizieren könnten!
- Sie ein Sicherheitssystem einer Firma einsetzten und herausfänden, dass es eine Hintertür eingebaut hätte? Dann würden Sie beim nächsten Mal auf ein Rechnersystem zurückgreifen, welches eindeutig und offen evaluiert werden könnte!

Die dargestellten Szenarien unterstreichen die Motivation zur Realisierung einer vertrauenswürdigen, fairen und offenen Sicherheitsplattform, die im Rahmen dieses Artikels vorgestellt werden soll.

2 Anforderungen und Ziele

Daten besitzen einen hohen Wert und sollten daher mit angemessenen Sicherheitsmechanismen geschützt werden. Um auf private und vertrauliche Daten zugreifen zu können, ist folglich eine Authentifizierung notwendig. Diese kann auf unterschiedliche Arten durchgeführt werden und reicht vom Passwortschutz bis zur Zwei-Faktor–

2 Intrusion-Detection-Systeme sind Programme, deren Aufgabe darin besteht, Einbrüche in Rechnersysteme zu detektieren.

Authentifizierung[3], z. B. mit einer *SmartCard*. Ein allen gemeinsames Sicherheitsproblem bei diesen herkömmlichen Verfahren ist die Allmächtigkeit des Betriebssystems. Sobald das Betriebssystem kompromittiert wird, hat der Angreifer die volle Kontrolle über jegliche Aktion und damit auch über sämtliche Daten, zu denen auch Zugangsdaten, Zertifikate und Schlüssel gehören. Durch die Strukturen der am häufigsten eingesetzten Betriebssysteme ist eine „echte" Sicherheit nicht möglich. Dies verdeutlicht allein die Vielzahl an Sicherheits-Patches, die fortlaufend herausgegeben werden, um entdeckte Sicherheitslücken zu schließen. Dies lässt den Schluss zu, dass neue Sicherheitskonzepte notwendig sind, um eine höhere Sicherheit und Vertrauenswürdigkeit zu erreichen und trotzdem die Arbeitsfähigkeit herkömmlicher Rechnersysteme zu erhalten. Die erste Anforderung an ein vertrauenswürdiges Rechnersystem[4] ist somit, dass alle bisherigen Anwendungen weiterhin genutzt werden können und zusätzlich alle sicherheitskritischen Daten geschützt werden, indem diese nicht mehr unter der Kontrolle eines herkömmlichen Betriebssystems stehen.

Heutige IT-Anwendungen beschränken sich nicht mehr nur auf reine PC- und Server-Systeme von Unternehmen. Neue Geschäftsmodelle erfordern die Realisierung innovativer Anwendungen zum Beispiel auch für eingebettete Rechnersysteme. Dazu zählen mobile Geräte, wie *PDAs* und *Smartphones*, aber auch Rechnersysteme im Automobilbereich wie Leistungssteuerungs- und Infotainment-Systeme. Die zu entwickelnde Sicherheitstechnologie muss den Anspruch erfüllen, auf einem breiten Spektrum von Rechnersystemen einsetzbar und von diesen unabhängig zu sein.

Verteilte Anwendungen fordern die Vernetzung voneinander entfernter Rechnersysteme. Ein externer Mitarbeiter einer Firma greift etwa mit einem mobilen Gerät auf den gesicherten Firmenserver zu. Ist das System des mobilen Gerätes jedoch kompromittiert, so ist der Server nun ebenfalls in Gefahr. Wenn Zugangsdaten durch kriminelle Handlungen oder auch durch die Unachtsamkeit des externen Mitarbeiters in die falschen Hände geraten sind, dann ist auch der Server nicht mehr als sicher einzustufen. Einem Angreifer ist im oben beschriebenen Fall die Möglichkeit gegeben, von einem fremden Rechnersystem auf den Server zuzugreifen. Um in solchen Szenarien wirklich eine vertrauenswürdige Verbindung etablieren zu können, muss sich demnach nicht nur der Anwender, sondern auch das Rechnersystem mit all seinen Hard- und Softwarekomponenten und seiner Konfiguration authentifizieren und das System muss zusätzlich garantieren können, dass es nicht kompromittiert worden ist.

Wünschenswert erscheint also eine Sicherheitsplattform, die die verwendete Soft- und Hardwarekonfiguration verlässlich für den Benutzer, und gegebenenfalls auch für seine Kommunikationspartner, überprüfbar macht.

Im Geschäftsverkehr agieren verschiedene Parteien mit unterschiedlichen Interes-

3 Zusätzlich zu einem Passwort wird ein Hardwareelement zur Authentifizierung verwendet. Die zwei Faktoren sind zumeist definiert als Wissen (bspw. PIN) und Besitz (bspw. EC-Karte).

4 Ein vertrauenswürdiges Rechnersystem ist ein Computersystem, welches sich immer so verhält, wie sein Benutzer es von ihm erwartet und die Daten integer und vertraulich hält.

sen und Sicherheitsstrategien: Während für Endbenutzer Datenschutzaspekte von Bedeutung sind, stellen für Unternehmen und Behörden die sichere und vertrauliche Behandlung von wichtigen Daten sowie der Schutz der Urheberrechte und Lizenzen gegen unautorisierte Verbreitung und Nutzung relevante Aspekte dar. Um die geforderte Vertrauenswürdigkeit beim Austauschen von Daten zu gewährleisten, ist es notwendig, dass die Daten mit Rechten verknüpft werden können, die auf einem fremden Rechnersystem durchsetzbar sind. Doch dürfen diese Regeln nicht mit denen des Empfängers kollidieren und trotzdem zur Ausführung gebracht werden. Ein Beispiel hierfür wäre ein Dokument, welches eine andere Person lesen darf, aber nur unter der Einschränkung, dass das Dokument weder gedruckt, noch verschickt werden kann.

Zusammengefasst werden folgende Anforderungen an eine Sicherheitsplattform definiert:

- Überprüfbarkeit der Vertrauenswürdigkeit eines Rechnersystems
- Durchsetzbarkeit von Rechten auf einem entfernten Rechnersystem im Sinne multilateraler Sicherheit
- Hardware- und Softwareunabhängigkeit
- Nutzbarkeit herkömmlicher Rechnersysteme
- Hohe Sicherheit und Vertrauenswürdigkeit

Um diese Anforderungen in Ziele münden zu lassen, wurde das EMSCB-Konsortium[5] gebildet, das gefördert durch das Bundesministerium für Wirtschaft und Technologie (BMWi) eine vertrauenswürdige, faire und offene Sicherheitsplattform realisiert (Sadeghi et al. 2004). Die aus diesem Konsortium heraus entstandenen und zukünftigen Sicherheitstechnologien und Ergebnisse werden unter dem Namen Turaya geführt. *Turaya* ist ein Fantasie-Name, der im Gegensatz zum Projektnamen *EMSCB* eingängig und leicht zu merken ist.

3 Trusted Computing mit Turaya

Trusted Computing ist eine Sicherheitstechnologie, die seit 2003 von der *Trusted Computing Group (TCG)* spezifiziert wird. Die *TCG* ist ein Industriekonsortium aus über 140 Firmen. Darunter befinden sich alle „Global Player“, wie *SUN*, *Intel*, *AMD*, *Microsoft*, *HP*, *IBM* sowie *Infineon* als Promoter, aber auch weitere deutsche Hersteller wie *Fujitsu Siemens*, *Utimaco Safeware AG*, *Sirrix AG* und andere, die es sich zur Aufgabe gemacht haben, offene Spezifikationen für vertrauenswürdige Rechnersysteme zu entwickeln, um die Sicherheit verteilter Anwendungen mit vertretbarem Aufwand zu erhöhen.[6]

5 *EMSCB* steht für *European Multilaterally Secure Computing Base*.

6 Siehe die Webseite der *Trusted Computing Group* unter http://www.trustedcomputinggroup.org.

Die Hauptidee besteht darin, manipulationssichere Sicherheitskomponenten in die Hardware zu integrieren, die als vertrauenswürdige „Anker" für die Sicherheit des Rechnersystems genutzt werden sollen, indem sie die Integrität und Authentizität des Rechnersystems garantieren. Die wichtigste Komponente ist das Trusted-Platform–Modul (TPM). TPMs werden bereits eingesetzt und sind bisher vor allem in Notebooks eingebaut worden. Ende des Jahres 2006 sollten es bereits 60–100 Millionen sein (vgl. Kay 2005).

3.1 Das Trusted-Platform-Modul

Das TPM ist ein kleiner passiver Chip, der einen Mikrokontroller enthält. Der Chip ist fest mit dem Mainboard oder dem Prozessor verbunden und rein von der Architektur her mit einer *SmartCard* vergleichbar. Es beinhaltet einen Crypto-Coprozessor, einen Zufallszahlengenerator und die *Platform Configuration Register (PCR)*, in denen Hashwerte[7] von Konfigurationszuständen gespeichert werden. Um die Vertrauenswürdigkeit eines Rechnersystems zu erhöhen, bietet das TPM ein Zertifikat mit einem Schlüsselpaar, dem *Endorsement Key (EK)*, welches das TPM niemals verlässt und die Eindeutigkeit und Einzigartigkeit des TPMs definiert. Um eine gewisse Anonymität wahren zu können, werden in den meisten Anwendungsfällen stets Schlüssel verwendet, die vom *EK* abgeleitet wurden. Diese Schlüssel werden *Attestation Identity Keys (AIK)* genannt. Die *AIKs* können nur für die Signatur von Werten des PCR-Registers eingesetzt werden. Für alle weiteren Verfahren stellt der *Storage Root Key (SRK)* die Wurzel des Schlüsselbaums dar. Der Schlüsselbaum besteht aus einer nicht endlichen Menge an Schlüsseln, die mit dem *SRK* verschlüsselt werden. Diese sind für sämtliche Verschlüsselungs- und Signaturvorgänge, die von der vertrauenswürdigen Plattform kontrolliert werden, einsetzbar.

3.2 Die Funktionen

Das TPM ist ein passives Sicherheitsmodul. Um das TPM nutzen zu können, muss es zuerst vom Besitzer aktiviert werden. Dieser Vorgang wird als *take ownership* bezeichnet. Zur sinnvollen Verwendung der TPM-Funktionen wird eine Software–Sicherheitsplattform benötigt, die sämtliche Vorgänge sicher und vertrauenswürdig steuert. Herkömmliche Betriebssysteme können aufgrund der hohen Fehleranfälligkeit und der ihnen eigenen Struktur den Ansprüchen an eine solche Sicherheitsplattform nicht genügen. Es fehlen entscheidende Strukturen und Konzepte, die zum Beispiel eine strikte Trennung von Speicherbereichen ermöglichen, um bei einem Angriff den Schaden einzuschränken. Eine Authentifizierung von Applikationen oder der

7 Hashwerte sind Werte, die mit Hilfe einer Hashfunktion berechnet werden. Hier berechnet eine Hashfunktion zu einer binärwertigen Folge einen binärwertigen Block fester Länge (den sog. Hashwert; derzeit übliche Länge ist 160 Bit). Der Vergleich zweier Hashwerte erlaubt den Ausschluss von Gleichheit der Ausgangsdaten bei deren Ungleichheit. Der Hashwert entspricht einem Fingerabdruck.

Sicherheitsplattform kann bisher ebenfalls nicht gewährleistet werden, wodurch eine Anwendung nie einen nachweisbar vertrauenswürdigen Status erreichen kann. Die Sicherheitsplattform Turaya ist speziell für diesen Einsatz konzipiert worden und ist in der Lage, z. B. die im Folgenden aufgeführten und wichtigsten Sicherheitsfunktionen zu steuern.

Secure boot

Das TPM alleine bringt einem Rechnersystem noch keinen Vorteil. Es ist auch notwendig, dass vertrauenswürdige Sicherheitsmechanismen greifen, sobald das Rechnersystem startet. Die erste Instanz, die unmittelbar zu Beginn des Bootvorgangs eingreift, ist das *Core Root of Trust for Measurement (CRTM)*, welches zusammen mit dem TPM den *Trusted Building Block* bildet (vgl. Abb. 1). Der *CRTM* ist ein ausführbarer Code, der einen Messvorgang über einzelne Systemzustände durchführt und dann die Ergebnisse in den *PCR* hinterlegt.[8] An dieser Stelle wird der Grundstein für ein vertrauenswürdiges Rechnersystem gelegt. Alle folgenden Bootvorgänge bzw. Systemzustände werden kontrolliert „aufgezeichnet". Diese Aufgabe übernimmt der *trusted bootloader*. Im Falle von Turaya ist dies der *Trusted Grub*. Er lädt die folgenden Module und führt deren Messung, wie im Folgenden beschrieben, durch (vgl. Abb. 1).

Die Hardware und die Software, die zu einer vertrauenswürdigen Komponente gehören, werden mit Hilfe einer Hashfunktion gemessen. Der daraus gebildete Hashwert repräsentiert diese Messung und wird im *PCR* hinterlegt. Einige Speicherplätze des *PCR* sind für bestimmte Messungen der Hardware vordefiniert (vgl. Abb. 1). Der Zustand des Rechnersystems ist also ab diesem Moment vertrauenswürdig nachweisbar. Wird an der Konfiguration des Rechnersystems nun etwas verändert, zum Beispiel durch einen Angriff auf eine gemessene Software-Konfiguration oder durch den Austausch einer Hardwarekomponente, würde der aktuelle Konfigurationszustand nicht mehr dem gemessenen entsprechen. Wird ein solches Rechnersystem erneut gestartet, können die im vertrauenswürdigen Zustand registrierten und beispielsweise auf einem USB-Stick abgelegten Messwerte mit den Messungen des aktuellen Bootvorgangs verglichen werden. So entsteht ein Trusted-(Authenticated)-Boot-Vorgang. Stimmt ein Wert im *PCR* nicht mit dem als vertrauenswürdig geltenden Wert überein, kann dem User diese Erkenntnis beispielsweise durch eine Warnung mitgeteilt werden. Per Definition ist das System oder die Applikation in diesem Zustand nicht vertrauenswürdig. Von einem *secure boot* wird gesprochen, wenn der Bootvorgang direkt abgebrochen wird, falls das System als nicht vertrauenswürdig eingestuft wurde.

Um die beschriebenen Funktionen sinnvoll nutzen und steuern zu können, wird eine vertrauenswürdige Sicherheitsplattform benötigt, beispielsweise um Applikationen eindeutig voneinander zu trennen, damit sie separat auf Vertrauenswürdigkeit

8 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2006).

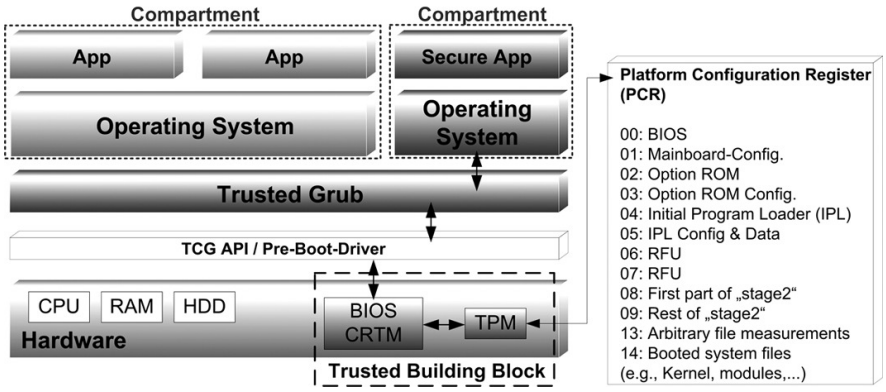

Abbildung 1: Vorgang und Architektur des secure boot unter Verwendung des Trusted Grub

überprüft werden können oder um den vertrauenswürdigen Zustand weitergeben zu können, um sich „auszuweisen". Die Messwerte lassen sich etwa nutzen, um sie mit Werten von Applikationen zu vergleichen, die vom Hersteller mitgegeben wurden und einen unveränderten Zustand widerspiegeln. Turaya ist eine solche Sicherheitsplattform. Die beschriebenen Verfahren bilden die Grundlage für alle Funktionen, die durch TC-Technologie ermöglicht werden.

Sealing (Versiegeln)

Ein Grundanliegen der Anwender ist das Bedürfnis, die eigenen Daten vor fremdem Zugriff zu schützen. Idealerweise kombiniert mit der Möglichkeit, die Daten auch an ein anderes Rechnersystem übergeben zu können mit der Gewissheit, dass die Daten auf dem entfernten Rechnersystem gemäß den eigenen Vorstellungen behandelt werden. Durch den Einsatz der TC-Technologie ist es nun möglich, Daten an eine Systemkonfiguration zu binden. Diesen Vorgang nennt man *sealing*. Durch *sealing* sind diese Daten nur auf dem Rechnersystem mit der entsprechenden Konfiguration abrufbar. Beispielsweise wird der Hashwert einer vertrauenswürdigen Konfiguration mit den zu schützenden Daten zu einem Datenpaket verbunden (vgl. Abb. 2). Hierbei kommt eine Verschlüsselung zum Einsatz, die gewährleistet, dass die Daten nur auf den Systemen wieder entschlüsselt werden können, die die entsprechende Konfiguration vorweisen. In Abbildung 2 verfügt System 1 über diese Konfiguration und kann somit das Datenpaket auslesen, System 2 jedoch nicht. Die mit einem bestimmten Konfigurationszustand verknüpften Daten könnten auch zusätzlich mit einem Schlüssel des TPMs verschlüsselt werden. Diese Daten wären dann nur auf diesem Rechnersystem mit genau diesem TPM verfügbar.

Binding (Auslagern)

Es ist zudem möglich, die Daten mit einer so genannten *security policy* für die Verarbeitung auf entfernten Rechnersystemen zu versehen. Diesen Vorgang nennt

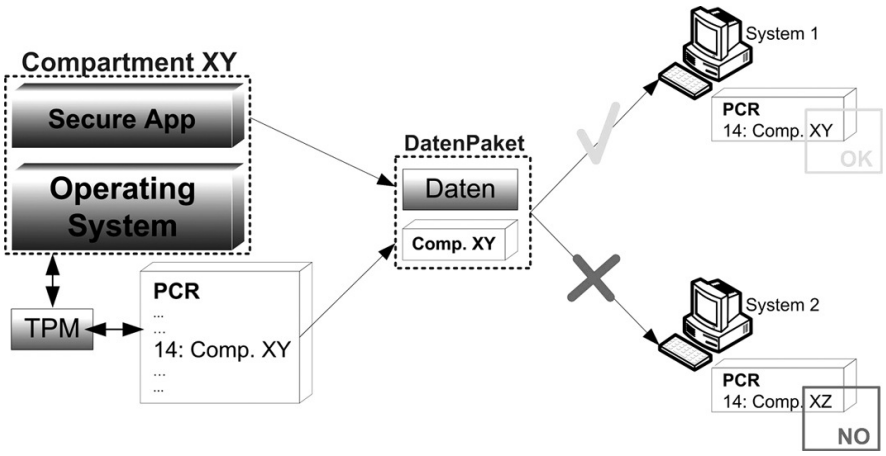

Abbildung 2: Der prinzipielle Vorgang beim sealing

man *binding*. Dadurch wird es möglich, jemand anderem seine Daten zur Verfügung zu stellen, aber nur unter bestimmten Bedingungen. Der Besitzer der Daten könnte etwa durch eine *security policy* vorschreiben, dass keine E-Mail- oder Druckertools auf dem Rechnersystem verfügbar sein dürfen, solange seine Daten genutzt werden, damit diese nicht versendet oder gedruckt werden können.

Attestation (Beglaubigung der Rechnersystemintegrität)

Zusätzlich zu dem Binden der Daten an das eigene Rechnersystem ist das genaue Wissen über den Zustand des Rechnersystems eines Kommunikationspartners ein sehr nützliches Sicherheitsfeature. Mit Hilfe der Attestierung kann der Zustand eines Rechnersystems überprüft werden. Bevor Daten an ein anderes Rechnersystem versendet werden, sollte erst sichergestellt sein, dass das andere Rechnersystem auch wirklich das Rechnersystem ist, das es vorgibt zu sein. Es sollte außerdem eine Hard- und Softwarekonfiguration aufweisen, welche die gewünschte Vertrauenswürdigkeit besitzt. Da die TPMs mit ihren Schlüsseln Einzigartigkeit mit sehr hoher Wahrscheinlichkeit gewährleisten, ist ein Rechnersystem eindeutig identifizierbar. Über eine vertrauenswürdige dritte Instanz, die die jeweiligen Rechnersysteme zertifiziert hat, wäre es also möglich, ein Rechnersystem zu identifizieren, indem sich die Rechnersysteme über die Schlüssel und Zertifikate ihrer TPMs ausweisen. Dies eröffnet erstmals die Möglichkeit, nicht nur Anwender, sondern auch die Rechnersysteme selbst authentifizieren zu können. Die Funktion wird als *(remote) attestation* bezeichnet. So ergeben sich weitere Sicherheitsmerkmale, beispielsweise für Netze mit externen Mitarbeitern.

Manipulationen durch Angreifer, die mit ihrem eigenen Rechnersystem einen Angriff durchführen, sind somit nahezu unmöglich und falls Angreifer das Rechnersystem eines externen Mitarbeiters übernehmen wollten, kämen sie weder an Daten, die durch *sealing* verschlüsselt wurden, noch könnten sie in das Firmennetz eindringen, da das gesamte Rechnersystem durch den Angriff die vertrauenswürdige Konfigurati-

on verloren hätte. In der TPM-Spezifikation 1.2 wird neben dem Einsatz einer dritten Partei auch ein Sicherheitsverfahren zur Attestierung angeboten, das ohne einen vertrauenswürdigen Dritten auskommt. Dieses Verfahren nennt sich *Direct Anonymous Attestation (DAA)*.

Diese Attestierungsfunktion besitzt Potenzial im Hinblick auf *grid computing*, Webservices, Peer-to-Peer- und Unternehmenskommunikation, da derartige gegenseitige Attestierungen das Vertrauen in solche Technologien stärken.

3.3 Wie kann Trusted Computing die Sicherheitssituation verbessern?

Der Einsatz von zusätzlicher sicherer Hardware, also beispielsweise der Einsatz von TPMs, erhöht das Maß an Sicherheit und Vertrauenswürdigkeit eines Rechnersystems beträchtlich. Durch die beschriebenen Sicherheitsfunktionen ist also eine Steigerung der Vertrauenswürdigkeit von Rechnersystemen möglich, da Daten effektiver geschützt und Anwendungen wesentlich besser kontrolliert werden können.

Es eröffnen sich die Möglichkeiten zu neuen Geschäftsfeldern, in deren Arbeitsgebiet aufgrund der Unsicherheit des Mediums *Computer* bisher keine Möglichkeit gesehen wurde, die IT zu nutzen. Firmengeheimnisse können effizient geschützt werden.

4 Die Sicherheitsplattform Turaya

Im Wesentlichen bietet die Sicherheitsplattform Turaya einen mikrokernbasierten Sicherheitskern, der „unterhalb“ von herkömmlichen Betriebssystemen agiert. Turaya ist ein eigenständiges, sicheres kleines Betriebssystem. Die gesamte Ressourcenverwaltung, die Kontrolle über Funktionen und Prozesse im Hinblick auf TC-Funktionalitäten und die Rechteverwaltung werden von Turaya übernommen. Das Konzept der Isolation durch Virtualisierung (vgl. 4.1) ermöglicht den Einsatz herkömmlicher Betriebssysteme neben hoch sicher geschützten Anwendungen. Das TPM bietet die Möglichkeit, sicherheitsrelevante Prozesse durch Hardwaresicherheit zu stützen.

4.1 Architektur

Die Architektur der Sicherheitsplattform Turaya ist so angelegt, dass sie hardware- und softwareunabhängig agieren kann. Die Architektur ist in sich abgeschlossen und bietet entsprechende Schnittstellen „nach oben“ zur Anwendungsschicht (*Application Layer*) und „nach unten“ zur Hardwareschicht (*Hardware Layer*) an.

Die Architektur des *Security Kernel* von Turaya spaltet sich in zwei Teile, den *Resource Management Layer (RML)* und den *Trusted Software Layer (TSL)*. Die Abbildung 3 zeigt die Einordnung dieser Layer in die Gesamtarchitektur eines Rechnersystems. Die dunklen Komponenten stellen ein herkömmliches, nicht vertrauenswürdiges Rechnersystem dar. Die helleren Komponenten zeigen die Sicherheitsplattform

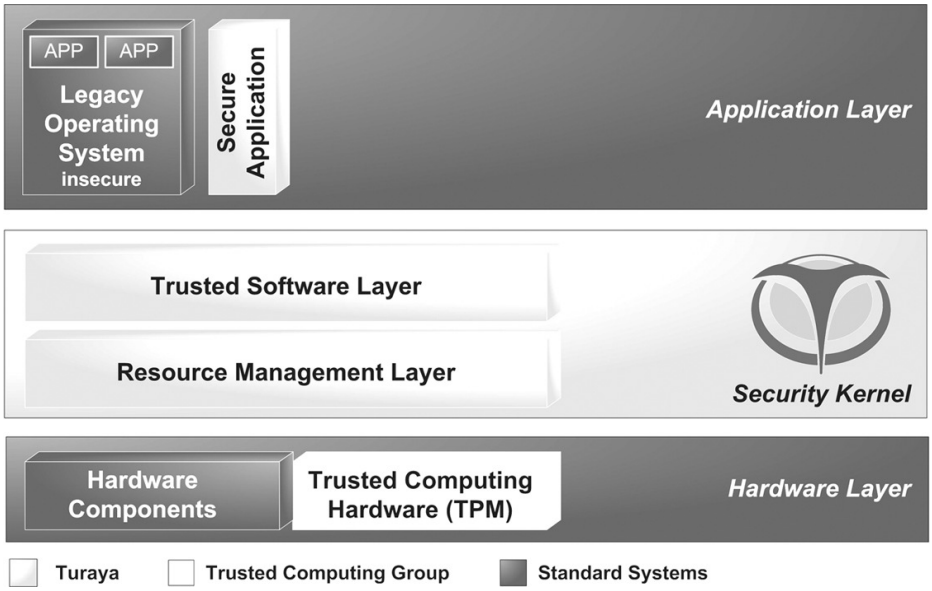

Abbildung 3: Die Turaya-Architektur im Überblick

Turaya und auf der Application-Layer-Ebene die sicheren Applikationen, die nur auf Turaya zugreifen (Linnemann und Pohlmann 2006*a*). Die hellgrau gefärbte Trusted–Computing-Hardware nimmt in diesem Zusammenhang eine besondere Stellung ein, da die Technologie lediglich durch Turaya genutzt und gesteuert wird. Ein TPM ist für den Einsatz von Turaya nicht grundsätzlich notwendig. Jedoch können die genannten TC-Funktionalitäten ohne den TPM nicht genutzt werden. Dies hätte ein wesentlich geringeres Sicherheitsniveau zur Folge.

Isolation durch Virtualisierung

Der *Resource Management Layer* Turayas steuert und kontrolliert den Zugriff auf die Hardware des Rechnersystems. Eine der wichtigsten Aufgaben dieser Schicht ist die Virtualisierung der Hardware. Umgesetzt wird dies aktuell durch einen L4-Mikrokernel[9], der zusammen mit den Gerätetreibern den *RML* bildet. Durch die Virtualisierung ist es möglich, mehrere „Rechnersysteme“ zu simulieren. Diese Technik wird bereits vielfach angewendet, zum Beispiel, um auf einem realen Server mehrere virtuelle Maschinen laufen zu lassen, die jeweils wie ein selbstständiger Server agieren. Bekannte Virtualisierungssoftwaresysteme sind beispielsweise *Xen* oder *VMware*. Durch die Virtualisierung wird ein sicherheitstechnisch entscheidendes Konzept umgesetzt – die Isolation. Ein herkömmliches Betriebssystem läuft auf der Sicherheitsplattform Tura-

9 *L4* ist ein Betriebssystemkern (Kernel), der ursprünglich von Jochen Liedtke entwickelt wurde. *L4* bezeichnet heute vor allem die *API* (Anwendungsprogrammschnittstelle). In diesem Projekt wird die L4-Implementierung *Fiasco* der TU Dresden verwendet und angepasst. *L4* ist ein sehr kleiner Betriebssystemkern, der zumeist als Basis für Echtzeitbetriebssysteme verwendet wird. Sein Vorteil ist, dass er wesentlich kleiner ist als Betriebssystemkerne von herkömmlichen monolithischen Systemen.

ya, anstatt wie bisher direkt auf der Hardware. Zusätzlich ist die Sicherheitsplattform in der Lage, parallel und vollständig isoliert voneinander weitere Betriebssysteme oder Applikationen laufen zu lassen. Die strikte Trennung erlaubt es, sicherheitskritische Anwendungen auch dann auszuführen, wenn das herkömmliche, parallel laufende Betriebssystem bereits kompromittiert wurde. Das gesamte zu schützende Gut, wie beispielsweise Zertifikate, Schlüssel und *credentials* aller Art, kann auf diesem Wege vor Angriffen wirkungsvoll geschützt werden. Die einzelnen voneinander isolierten Applikationen und Betriebssysteme oberhalb der Sicherheitsplattform Turaya werden als *compartments* bezeichnet (vgl. Abb. 4).

Die Möglichkeiten der Turaya-Architektur am Beispiel Onlinebanking

Sicherheitskritische Prozesse werden durch die Virtualisierung von unsicheren Prozessen getrennt. Onlinebanking beispielsweise lässt sich mit der Sicherheitsplattform Turaya hoch sicher betreiben. Um eine entsprechende Vertrauenswürdigkeit zu erreichen, wird die Onlinebanking-Applikation in einem Compartment ausgeführt. An dieser Stelle sind zwei unterschiedliche Szenarien denkbar: Zum einen wäre es möglich, ein Compartment mit einem Betriebssystem und einem Browser auszustatten; dazu sind keine Anpassungen an der Software notwendig. Zum anderen würde eine Banking-Software so modifiziert werden, dass sie direkt auf den Schnittstellen der Sicherheitsplattform aufsetzte. Im Folgenden wird das Beispiel der modifizierten Banking-Software weiterverfolgt. Sobald der Anwender seine Banking-Applikation startet, „springt" er in das entsprechende Compartment. Für den Anwender ist dieser Vorgang transparent. Er startet die Applikation, beispielsweise durch einen Klick auf das Icon seiner Anwendung im herkömmlichen Betriebssystem. Dadurch wird ein Aufruf an die Turaya-Plattform gesandt. Diese startet die Banking-Software in einem neuen Compartment. Daraufhin öffnet sich die Anwendung in einem Fenster. Dieses Fenster ist bereits das sichere Compartment. Der Bankserver wird angewählt. Über die Attestierungsfunktion kann vertrauenswürdig nachgewiesen werden, dass der Anwender wirklich mit dem Server seiner Bank verbunden ist und sich dieser Bankserver in einem vertrauenswürdigen Zustand befindet. Die Attestierung könnte folgendermaßen realisiert werden:

Die Banking-Software besitzt beispielsweise den öffentlichen Teil eines Schlüsselpaares, der sich aus der vertrauenswürdigen Konfiguration in Verbindung mit einem *AIK* des TPMs des Bankservers zusammensetzt. Eine mit diesen Informationen verschlüsselte Zufallszahl wird an den Bankserver übermittelt. Ist dieser in der Lage, mit seinem einmaligen privaten Schlüssel die Zufallszahl zu entschlüsseln und gibt dieses Wissen an den anfragenden Server zurück, so ist die Authentizität und Vertrauenswürdigkeit des Servers sichergestellt, da nur dieser Server in der Lage sein kann, die verschlüsselte Zufallszahl zu entschlüsseln.

Der Anwender gibt seine transaktionsrelevanten Daten ausschließlich innerhalb des sicheren Compartments ein. Das herkömmliche Betriebssystem hat keinen Zu-

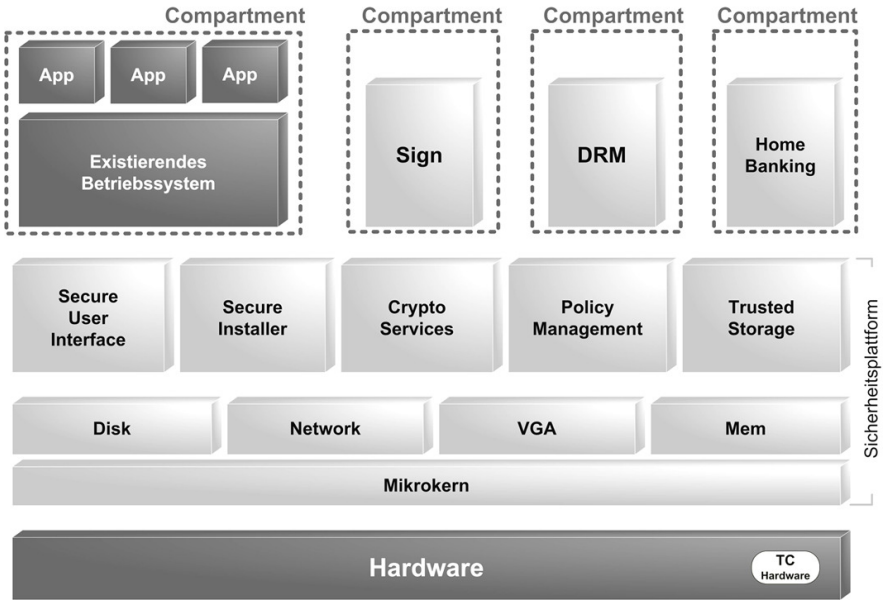

Abbildung 4: Die Turaya-Architektur im Detail

griff. Dadurch ist evtl. vorhandene Malware nicht in der Lage, die Eingaben des Anwenders zu missbrauchen. Das Compartment wurde in einem unveränderten Zustand gemessen. Wenn ein Angriff auf dieses Rechnersystem erfolgt wäre, der das Compartment beeinflusst hätte, wäre das Compartment aufgrund des beschriebenen Secure-Boot-Vorgangs jedoch erst gar nicht gestartet worden, da die Messwerte nicht mehr übereingestimmt hätten und damit die Vertrauenswürdigkeit nicht gewährleistet war.

Im Rahmen des Onlinebankings lässt sich ein weiterer Vorteil der Sicherheitsplattform Turaya lokalisieren. Das Onlinebanking-Verfahren *HBCI*[10] verlangte bisher mindestens einen teuren Klasse-3-Kartenleser für ein höheres Sicherheitsniveau. Turaya stellt eine vertrauenswürdige Middleware und somit einen *trusted path*[11] zwischen Kartenleser und Banking-Applikation dar. Dadurch ist der Einsatz eines simplen kostengünstigen Kartenlesers zusammen mit Turaya völlig ausreichend für ein hohes Sicherheitsniveau. Dieses Szenario zeigt, wie die Technologien *Trusted Computing* und *SmartCard* zusammenspielen. Das TPM ist fest mit einem Rechnersystem verbunden, während die *SmartCard* für mobile Anwendungen eingesetzt wird. So besteht die Aufgabe der *SmartCard* darin, einen Nutzer zu authentifizieren, während die Hauptaufgabe des TPMs in der Authentifizierung des Rechnersystems liegt.

10 *HBCI* steht für *Home Banking Computer Interface* – ein nationaler Standard des Zentralen Kreditausschusses.

11 Als *trusted path* wird ein Mechanismus beschrieben, der die direkte Kommunikation zwischen einer *Trusted Computing Base*, wie Turaya, und einem Terminal oder Nutzer beschreibt. Der Kommunikationsweg ist nicht manipulierbar. Er basiert darauf, dass sich alle daran beteiligten Instanzen als vertrauenswürdig ausweisen können.

Das beschriebene Beispiel zeigt die Aufgaben des *TSL*. Die Kontrolle über sämtliche Vorgänge wird in dieser Architekturschicht umgesetzt. Die sichere Installation von Komponenten, das Starten von Compartments, die Erzeugung von Zufallszahlen oder die sichere Eingabe von Nutzerdaten über die *Secure GUI*[12] sind nur einige Beispiele der Vorgänge, die in dem *TSL* ablaufen oder von diesem gesteuert werden.

Policy enforcement[13]

Zusätzlich zu diesen Sicherheitsfunktionen bietet die Sicherheitsplattform Turaya eine weitere Funktion, die innerhalb des *TSL* genutzt wird. Daten, die innerhalb der Sicherheitsplattform verarbeitet werden, können mit so genannten *policies* versehen werden. Die *policies* enthalten Regeln, die angeben, auf welche Art die Daten verarbeitet werden sollen. Turaya als vertrauenswürdige Instanz bindet die *policies* an die Daten und sorgt dafür, dass diese *policies* auf einem anderen Rechnersystem durchgesetzt werden unter der Voraussetzung, dass die *policy* mit der des Rechnersystembesitzers übereinstimmt. Eine Regel, die das Ausdrucken einer Datei untersagt, würde Turaya innerhalb des *TSL* umsetzen, indem sie dem Compartment, das diese Datei anzeigt, den Zugang zum Druckertreiber verwehren würde. Über diese Vorgänge lassen sich Digital-Rights-Management-Funktionen[14] mit der Sicherheitsplattform Turaya anwenden.

4.2 Die Applikationen

Die Sicherheitsplattform Turaya wird im Rahmen des EMSCB-Projekts entwickelt. Dieses ist ein Konsortium aus der Ruhr-Universität Bochum, dem Institut für Internet-Sicherheit der FH Gelsenkirchen, der TU Dresden sowie den Firmen *Sirrix AG* und *escrypt GmbH*. Unterstützt wird das Projekt über drei Jahre vom Bundesministerium für Wirtschaft und Technologie. Nach Ablauf dieser Zeitspanne wird Turaya im Trusted-Computing-Kompetenzzentrum, das Anfang 2007 gegründet werden soll, weiterentwickelt und gepflegt werden. Innerhalb des Projektzeitraumes sollen die folgenden fünf Piloten umgesetzt werden, die die Funktionalitäten der Sicherheitsplattform demonstrieren (Linnemann und Pohlmann 2006*b*):

1. *Turaya.Crypt* – Device-Verschlüsselung; fertiggestellt
2. *Turaya.VPN* – Sicheres VPN-Modul (Zertifikatsmanagement); fertiggestellt
3. *Turaya.FairDRM* – Faires DRM-System; fertiggestellt

12 *Secure GUI* beschreibt das vertrauenswürdige *Secure Graphical User Interface*, das vom Sicherheitskern kontrolliert wird und somit nicht von Anwendungen manipuliert werden kann.

13 Aus dem Englischen: *policy* = Verfahrensweise, Grundsatz; *enforcement* = Durchsetzung, Erzwingung.

14 *Digitales Rechtemanagement (DRM)* ermöglicht Rechteinhabern die Durchsetzung ihrer Rechte bei geschützten Daten wie etwa Musik- oder Filmdateien.

4. *Turaya.ERM – Enterprise Rights Management* (Dokumentenmanagement) mit *SAP*; November 2007

5. *Turaya (embsys)* – Embedded-Systems-Einsatz (Automotiv Multimedia); November 2007

Die ersten beiden fertig gestellten Piloten demonstrieren den Einsatz der Trusted–Computing-Technologie und die Isolation sicherheitskritischer Komponenten. Alle sicherheitsrelevanten Daten stehen in diesen Applikationen unter der Kontrolle der Sicherheitsplattform und erlauben keinerlei Zugriff durch das herkömmliche Betriebssystem. Die Piloten stehen auf der EMSCB-Webseite[15] als Demo-Image zum Testen zur Verfügung. Der dritte Pilot beschäftigt sich mit dem Einsetzen und Durchsetzen von *policies*. Auf diesen Ergebnissen aufbauend werden die Piloten vier und fünf im Verbund mit strategischen Partnern entwickelt. Das *Enterprise Rights Management* wird mit der *SAP AG* und Turaya auf Embedded-Rechnersystemen mit der Bosch/Blaupunkt-Gruppe gemeinsam umgesetzt. Dies führt zu einer marktnahen Entwicklung der Sicherheitsplattform, basierend auf Anforderungen von Herstellern.

5 Das Besondere an Turaya – TC kritisch diskutiert

Es fragt sich hier nicht nur, ob Turaya die aufgestellten Anforderungen erfüllen kann, sondern auch auf welche Weise. *Microsoft* kündigte bereits weit vor dem Jahr 2003 ein System mit dem Namen *Palladium*[16] an, das TC-Funktionalitäten unterstützt. Aufgrund der negativen Schlagzeilen um dieses Projekt änderte *Microsoft* den Namen 2003 in *NGSCB (Next Generation Secure Computing Base)*. Es wurden eine Menge von Funktionen auf Basis von *Trusted Computing* versprochen, die immer im engen Verbund zu DRM-Funktionen standen, welche im neuen Betriebssystem eingesetzt werden sollten. Im jetzt erschienenen Microsoft-Betriebssystem *Vista* ist von all den ursprünglich versprochenen Funktionen lediglich eine Festplattenverschlüsselung mit Namen *BitLocker* übrig geblieben, die das TPM nutzt.

Durch *Trusted Computing* ist es möglich, das Rechnersystem eines Anwenders zu kontrollieren und Informationen über denselben zu bekommen. Zusätzlich kann einem Anwender vorgeschrieben werden, welche Software er nutzen darf und welche nicht. Dies sind Aussagen der Gegner der TC-Technologie und die Punkte, die dazu beigetragen haben, dass die TC-Technologie in ein schlechtes Licht gerückt wurde. Tatsächlich hätte *Microsoft* die Möglichkeit, sein Betriebssystem so zu entwickeln, dass es andere Betriebssysteme oder Anwendungen von bestimmten Anbietern auf seinem Rechnersystem zur Laufzeit nicht zulässt (vgl. The Information Security Journal 2003; Dolle 2004; Caspers 2004). Dieses Szenario wird zu Recht kritisiert. Dem entgegen steht jedoch die aktuelle Entwicklung des zunehmenden Einsatzes der IT

15 http://www.emscb.de

16 Siehe http://www.microsoft.com/resources/ngscb.

im sicherheitskritischen Umfeld. Hier ist eine Sicherheitsplattform, wie einleitend beschrieben, für innovative und hochsichere Anwendungen notwendig.

Die Sicherheitsplattform Turaya wählt daher einen eigenen Ansatz, der die Vorteile der TC-Technologie nutzt und die Diskriminierung von Anwendern oder Anbietern verhindert. Turaya ist eine Open-Source-Sicherheitsplattform, die unter der GPL–Lizenz veröffentlicht wird. Dies ermöglicht dem Anwender genau zu verfolgen, ob die Sicherheitsplattform schon von der Struktur und Funktionsweise her in irgendeiner Form die Rechte des Anwenders untergräbt. Hintertüren, wie sie in Closed-Source–Systemen vermutet und eingesetzt werden könnten, wären in der Sicherheitsplattform Turaya sofort sichtbar. Bei der Konnektivität setzt Turaya auf offene Standards und möchte in diesem Bereich selbst einen offenen Standard definieren. Zur Steigerung der Vertrauenswürdigkeit und um den Einsatz im Hochsicherheitsbereich zu ermöglichen, wird eine Evaluierung z. B. nach *Common Criteria EAL 4*[17] angestrebt.

Um die Verarbeitung von Daten und Dokumenten auf fremden Rechnersystemen vertrauenswürdig durchführen zu können und um Datenschutz und Urheberrecht zu gewährleisten, ist der Einsatz von *policies* notwendig. In diesem Zusammenhang lassen sich, wie bereits erwähnt, auch DRM-Funktionalitäten einsetzen. Turaya wählt hierfür einen fairen Ansatz: Ein Anwender definiert seine eigenen *policies*. Wenn eine Datei oder Anwendung eines Anbieters auf dem Rechnersystem ausgeführt werden soll, die als *policy* vorgibt, dass die Datei nur einmal angezeigt werden kann und dafür ein bestimmter Geldwert zu entrichten ist, wird dies nur durchgesetzt, wenn die *policy* des Anwenders dies zulässt. Diese Eigenschaft wird als multilaterale Sicherheit bezeichnet. Somit ist es selbstverständlich möglich, Rechte auf fremden Rechnersystemen durchzusetzen, aber nur, wenn der Anwender des Rechnersystems dies zulässt.

Hinzu kommt, dass die Sicherheitsplattform Turaya sowohl hardware- als auch softwareunabhängig ist. So gibt es einerseits keine Diskriminierung von Anbietern und andererseits ein sehr hohes Maß an Kompatibilität.

6 Fazit

Der Bedarf für vertrauenswürdige Rechnersysteme in verschiedensten Geschäftsfeldern und Anwendungen scheint klar ersichtlich und notwendig. In diesem Kontext sollten Daten- und Urheberschutzaspekte berücksichtigt werden. Eine Sicherheitsplattform, die den Anforderungen eines vertrauenswürdigen Rechnersystems entspricht, darf weder Anwender noch Anbieter benachteiligen.

Die vertrauenswürdige, faire und offene Sicherheitsplattform Turaya berücksichtigt diese Aspekte und bietet die notwendige Sicherheit und Vertrauenswürdigkeit für Rechnersysteme. Die definierten Anforderungen können vollständig von Turaya erfüllt werden, indem die Trusted-Computing-Technologie im positiven Sinne genutzt

17 *Common Criteria* ist ein ISO-Standard für die Bewertung der Sicherheit von Informationstechnologien.

wird. Sämtliche Programmierschnittstellen von Turaya und der Sourcecode aller sicherheitskritischen Komponenten werden zu Evaluierungszwecken offengelegt, um die Vertrauenswürdigkeit der Implementierung zu erhöhen. Turaya ermöglicht daher auch der Open-Source-Gemeinde, „konkurrenzfähig" zu bleiben.

Zudem bietet Turaya den Vorteil, dass alle sicherheitskritischen Komponenten und Anwendungen unabhängig von „klassischen" Betriebssystemen agieren können und damit für zukünftige plattformübergreifende verteilte Anwendungen optimal geeignet sind. Die Autoren wünschen sich, dass möglichst viele Anwendungen auf die Sicherheitsplattform Turaya aufbauen, um eine sichere und vertrauenswürdige Zukunft von Rechnersystemen zu ermöglichen.

Literatur

Barnitzke, A. (2005), 'Exploit und Wurm folgen dem Patch schon auf dem Fuße', *Computer Zeitung* **35**, S. 6.

Bundesamt für Sicherheit in der Informationstechnik (2006), 'Das Trusted Platform Module', http://www.bsi.de/sichere_plattformen/trustcomp/infos/tpm_report/tpm_crtm.htm [20. Dez 2006].

Caspers, T. (2004), 'Der schmale Grad zwischen Vertrauensbeweisen und Datenschutz', *<kes> – The Information Security Journal* (6), S. 35.

Dolle, W. (2004), 'Trusted Computing: Stand der Dinge', *<kes> – The Information Security Journal* (4), S. 20.

Kay, R. L. (2005), 'The Future of Trusted Computing'. https://www.trustedcomputinggroup.org/home/IDC_Presentation.pdf [20. Dez 2006].

Linnemann, M. und Pohlmann, N. (2006*a*), Die vertrauenswürdige Sicherheitsplattform Turaya, *in* P. Horster (Hrsg.), 'DACH Security 2006', syssec Verlag.

Linnemann, M. und Pohlmann, N. (2006*b*), 'Schöne neue Welt?! Die vertrauenswürdige Sicherheitsplattform Turaya', *IT-Sicherheit – Management und Praxis* (3).

Sadeghi, A., Stüble, C. und Pohlmann, N. (2004), 'European Multilateral Secure Computing Base – Open Trusted Computing for You and Me', *Datenschutz und Datensicherheit* (9), S. 548–554.

The Information Security Journal (2003), 'Vertrauenskrise – Einsichten und Aussagen vom Trusted-Computing-Symposium', *<kes> – The Information Security Journal* (4), S. 12. http://www.kes.info/archiv/online/03-4-012.htm [25. Jan 2007].

Windows IT Pro (2004), 'Die Bedrohung von morgen', *Windows IT Pro* (4), S. 14.