Anwendungen sicher ausführen mit Turaya

In Sicherheit

Norbert Pohlmann, Markus Linnemann

Wegen geplanter Rechtebeschränkung auf Nutzerrechnern stieß das von Microsoft & Co. vor einigen Jahren forcierte Trusted Computing auf wenig Gegenliebe in der Öffentlichkeit. Das offene Projekt „Turaya" will sich auf die Stärken des Konzepts konzentrieren und veröffentlicht vertrauenswürdige Pilotanwendungen.

Die Zahl der Angriffe auf Computersysteme durch Malware nimmt stetig zu. Angreifer durchbrechen die vorhandenen Sicherheitsmechanismen der Software- und Betriebssysteme wie Virenscanner und Firewalls, und es stehen zwar zahlreiche Einzelmaßnahmen, aber keine „Allzweckwaffe" oder wirksame Strategie gegen bekannte und unbekannte Angriffe zur Verfügung. Identitätsdaten oder vertrauliche Dokumente sind ebenso gefährdet wie über die IT abgewickelte interne und externe Geschäftsprozesse.

Hier setzt Trusted Computing an. Es soll eine geräte- und netzübergreifende Vertrauens- und Sicherheitsbasis schaffen, die die Integrität aller beteiligten Rechnersysteme gewährleistet und unbefugte Zugriffe auf sie verhindert. Seit 2003 spezifiziert die Trusted Computing Group (TCG), die aus über 160 Firmen wie Sun, Intel, AMD, Microsoft, HP, IBM, Infineon, aber auch deutschen Herstellern wie Fujitsu-Siemens, Utimaco oder Sirrix besteht, diese Technologie. Die Hauptidee besteht darin, manipulationsgeschützte Sicherheitskomponenten in die Hardware zu integrieren. Sie sollen als vertrauenswürdige „Anker" sowohl für die Integrität als auch Authentizität des Rechnersystems garantieren und softwarebasierten Angriffen entgegenwirken. Eine solche Sicherheitskomponente ist das „Trusted Platform Module" (TPM).

Es ist ein kleiner passiver Chip, der fest mit der Systemplattform (Mainboard oder Prozessor) verbunden ist und einen Microcontroller enthält. TPMs werden von mehreren Chip-Produzenten angeboten und inzwischen in die Motherboards von Servern, Desktops und Laptops verbreiteter Marken integriert. Im Jahr 2006 waren circa 60 Millionen Einheiten im Einsatz, für 2008 rechnet die Fachwelt mit bis zu 200 Millionen.

Die Architektur des TPM ähnelt der einer Smartcard. Der Chip beinhaltet einen Krypto-Koprozessor, einen Zufallszahlengenerator und das „Platform Configuration Register" (PCR), in das er die Hash-Werte von Konfigurationszuständen speichert. Diese Messwerte lassen sich überprüfen und machen Änderungen der Soft- oder Hardwarekonfiguration erkennbar.

Die Messung bringt es an den Tag

Sobald ein Softwareangriff oder eine Veränderung von Hardwarekomponenten die Systemkonfiguration verändert, ändern sich die Messwerte und sind dann unter Umständen nicht mehr als vertrauenswürdig einzustufen. Der Messvorgang beginnt während des Systemstarts, dem sicheren Booten. Stimmen die gemessenen Werte nicht mit den Vorgaben überein, kann eine Sicherheitsanwendung diese Information abfragen und als Reaktion beispielsweise den Bootvorgang abbrechen. So wird eine Aussage über die Vertrauenswürdigkeit eines Rechnersystems möglich.

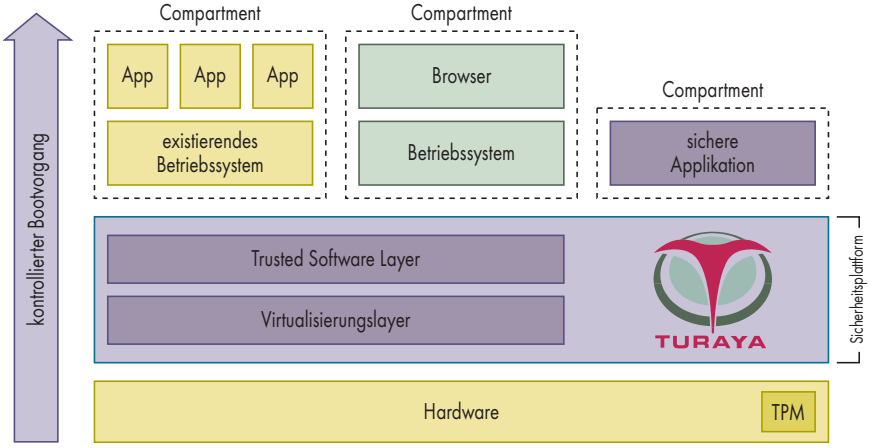
Beim Anwendungsfall Auto würde das etwa bedeuten, dass die Werkstatt das Update eines Autosystems nur durchführen könnte, wenn sich Auto und Werkstattsystem in einer vertrauenswürdigen Systemkonfiguration befinden, definiert durch die Messwerte der Systeme.

Die Grundfunktion der Messbarkeit von Systemkonfigurationen ermöglicht es außerdem, Daten an eine solche Konfiguration zu binden. Dieses

sogenannte „Sealing“ schützt Dokumente eines Anwenders vor fremdem Zugriff. Es gewährleistet auch den Transfer eines Dokuments an ein für den Dokumentenzugriff autorisiertes anderes Rechnersystem – und nur an ein solches.

Man kann mit Trusted Computing beispielsweise den Hash-Wert einer vertrauenswürdigen Systemkonfiguration mit den zu schützenden Dokumenten zu einem Datenpaket verbinden. Die dabei eingesetzte Verschlüsselung gewährleistet, dass die Daten nur auf den Rechnersystemen wieder entschlüsselt werden können, die die definierte Konfiguration vorweisen.

Zusätzlich zum Zustand des eigenen Systems ist es hilfreich, den des Rechnersystems eines Kommunikationspartners zu kennen. Vor einem Dokumentenversand sollte man sicher sein, dass das andere Rechnersystem auch wirklich dasjenige ist, das es vorgibt zu sein, und dass es sich in einem vertrauenswürdigen Systemzustand befindet. Die „Remote Attestation“ überprüft das. Da die TPMs mit ihren Schlüsseln Einzigartigkeit gewährleisten, ist ein Rechnersystem mit Bezug auf seinen Integritätszustand eindeutig identifizierbar.



Turaya schiebt sich als betriebssystemähnliche Sicherheitsschicht zwischen Hardware und Betriebssystem. In sogenannten Compartments kann man sicherheitsrelevante Anwendungen mit eigenem Betriebssystem oder ohne isoliert und parallel ausführen (Abb. 1).

Nur abgeleitete Schlüssel verwenden

Wichtig dabei ist für die Gewährleistung des Datenschutzes, dass nie der Hauptschlüssel (Endorsement Key) des TPM verwendet wird, sondern ausschließlich abgeleitete Schlüssel. Die beteiligten Rechnersysteme übermitteln ihren Systemkonfigurationszustand an eine vertrauenswürdige dritte Instanz und weisen sich durch Schlüssel und Zertifikate ihres TPMs aus. Hat jemand die Systemkonfiguration so verändert, dass sie als nicht vertrauenswürdig gilt, wird eine Kommunikation nicht zugelassen.

Voraussetzung für das Trusted Computing ist eine Infrastrukturkomponente, die sämtliche Vorgänge der beschriebenen Anwendungen steuert. Ihre wichtigste Aufgabe besteht darin, die Integritätsprüfungen durchzuführen und auszuwerten. Das TPM allein bringt noch keine höhere Sicherheit, es ist lediglich ein passives Modul, das Sicherheitsdienste anbietet. Um es nutzen zu können, muss der Besitzer es zuerst aktivieren.

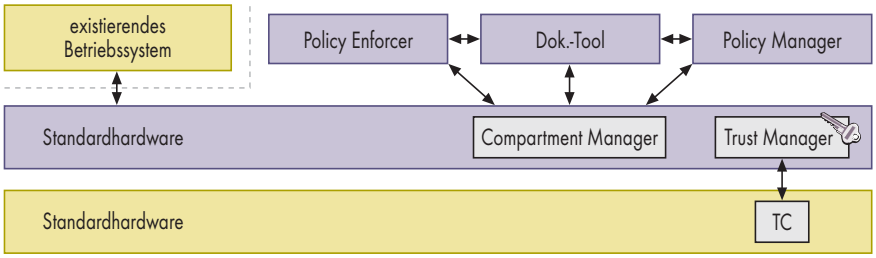
Herkömmliche Betriebssysteme können aufgrund der hohen Fehleranfälligkeit und der monolithischen Struktur den Ansprüchen an eine solche Sicherheitsplattform nicht genügen. Sie können zu einfach kompromittiert werden und vertrauenswürdige Zustände vortäuschen, die nicht den realen entsprechen. Es fehlen entscheidende Strukturen und Konzepte, die zum Beispiel eine strikte Trennung von Speicherbereichen ermöglichen, um bei einem Angriff den Schaden einzuschränken. Auch können sie bisher nicht die Authentizität von Applikationen oder des Rechnersystems gewährleisten, wodurch eine Anwendung nie einen nachweisbaren vertrauenswürdigen Status erreichen kann. Eine Sicherheitsplattform muss selbst möglichst wenig oder gar nicht anfällig für Angriffe sein.

Die Open-Source-Sicherheitsplattform Turaya wählt einen eigenen Ansatz, der die Vorteile des Trusted Computing nutzt und die Diskriminierung von Anwendern oder Anbietern verhindert. Sie wird im Rahmen des Forschungs- und Entwicklungsprojekts EMSCB (European Multilaterally Secure Computing Base, www.emscb.org) entwickelt, einem Konsortium aus dem Institut für Internet-Sicherheit der FH Gelsenkirchen, der Ruhr-Universität Bochum, der TU Dresden und den Firmen Sirrix AG und escrypt GmbH. Das Bundesministerium für Wirtschaft und Technologie fördert das Projekt und Industriepartner wie SAP AG und Bosch/Blaupunkt unterstützen die insgesamt fünf Pilotanwendungen. Ziel ist es, eine Sicherheitsplattform mit offener Architektur und Schnittstellen zu schaffen, die als Basis für vertrauenswürdige IT-Systeme dient.

Turaya zeichnet sich durch einen modularen Aufbau, einen offenen Quellcode und eine geringe Komplexität aus. Zusätzlich bietet sie die Möglichkeit, Rechte und Regeln durchzusetzen (Policy Enforcement). Und das auf faire Art und Weise: Während für Endbenutzer Datenschutzaspekte von Bedeutung

iX-TRACT

- Da einzelne Sicherheitsmaßnahmen nicht immer greifen oder von Kriminellen außer Gefecht gesetzt werden, ist für kritische Geschäftsprozesse eine grundlegende Sicherheitsinfrastruktur erforderlich.
- Die Basis für die europäische Open-Source-Sicherheitsplattform „Turaya“ ist das Trusted Computing. Das dafür erforderliche Trusted Platform Module ist heutzutage in nahezu alle Computersysteme eingebaut.
- Kennzeichnende Eigenschaften der Sicherheitsplattform sind Betriebssystemunabhängigkeit und offengelegter Code sowie Schnittstellen, die einerseits eine Evaluierung aus Sicherheitssicht und andererseits die Nutzung für Produkte aller Hersteller ermöglichen.



Der Policy Enforcer sorgt für die Durchsetzung der vorgegebenen Richtlinien, wie Mitarbeiter mit welchen Dokumenten verfahren dürfen (Abb. 2).

sind, sind für Unternehmen und Behörden die sichere und vertrauliche Behandlung von wichtigen Daten sowie der Schutz der Urheberrechte und Lizenzen gegen unautorisierte Verbreitung und Nutzung relevant.

Um die geforderte Vertrauenswürdigkeit beim Austauschen von Daten zu gewährleisten, ist es notwendig, die Daten mit Rechten verknüpfen zu können, die auf einem fremden Rechnersystem durchsetzbar sind. Doch dürfen diese Regeln nicht mit denen des Empfängers kollidieren und zur Ausführung gebracht werden. So setzt Turaya zum Beispiel nicht nur die Regeln der Softwareanbieter durch, sondern berücksichtigt die aller Beteiligten. Außerdem ist die Sicherheitsplattform für jeden zugänglich und hard- sowie softwareunababhängig. Ein konventionelles Rechnersystem besteht aus Hardware, auf der ein Betriebssystem mit entsprechenden Applikationen arbeitet. Diese Hardware wird um ein TPM-Modul erweitert. Turaya schiebt sich als eigenständige betriebssystemähnliche Sicherheitsplattform zwischen Hardware und Betriebssystem. Die gesamte Ressourcenverwaltung, die Kontrolle über Funktionen und Prozesse im Hinblick auf TC-Funktionen sowie die Rechteverwaltung übernimmt Turaya.

Betriebssystemähnliche Zwischenschicht

Neben dem herkömmlichen Betriebssystem kann die Sicherheitsplattform mithilfe von Isolationsmechanismen und Virtualisierung weitere Betriebssysteme und Applikationen streng voneinander isoliert und parallel in sogenannten Compartments ausführen (Abb. 1). Sie können entweder reine sichere Applikationen enthalten, die an die Sicherheitsplattform angepasst wurden, oder schlanke Betriebssysteme mit Standardapplikationen. Im zweiten Fall misst Turaya das Betriebssystem zusammen mit der Anwendung, um die Unversehrtheit, sprich die Integrität nachweisen zu können. Auf diesem Wege muss man die Applikationen nicht anpassen. Die Architektur der Sicherheitsplattform ist in sich abgeschlossen und bietet Schnittstellen „nach oben“ zum Application Layer und „nach unten“ zum Hardware Layer an. Die Architektur ist in eine Hardware-, eine Sicherheits- und eine Applikationsebene unterteilt.

Fehleranfälligkeit abhängig von Codebasis

Eine Sicherheitsplattform sollte aus einer möglichst kleinen Codebasis bestehen und somit weit weniger komplex sein als etablierte Betriebssysteme. Ein herkömmlicher Betriebssystemkern besteht aus mehr als 3 000 000 Zeilen Code, Turaya dagegen aus weniger als 100 000. Das macht sie weniger fehleranfällig und erleichtert eine Validierung. Zusätzlich ermöglicht die Sicherheitsplattform, dass Anwender anderen ihre Daten zur Verfügung stellen können, zuvor aber bestimmte Bedingungen definieren, ob und in welcher Form der Empfänger sie auf seinem Rechnersystem verarbeiten darf. Der Automobilhersteller kann mit der sogenannten Security Policy zum Beispiel vorschreiben, ob jemand Dokumente anschauen und drucken oder nur anschauen darf. Um zu gewährleisten, dass die Daten gewissen Regeln folgen, muss der Anwender zusätzliche Policies an die Datenpakete binden. Aus dieser Funktion heraus ergeben sich neue Möglichkeiten für den vierten und fünften Meilenstein des Projekts, die voraussichtlich im Februar veröffentlicht und im Folgenden vorgestellt werden.

Derzeit existieren bereits drei Pilotanwendungen, die die Funktionen der Sicherheitsplattform demonstrieren:
– „Turaya.Crypt“ für Device-Verschlüsselung,
– „Turaya.VPN“, ein sicheres VPN-Modul (Zertifikatsmanagement),
– „Turaya.FairDRM“, ein faires Digital-Rights-Management-System.
In Kürze kommen die weiteren Pilotanwendungen „Turaya.ERM“ für das Enterprise-Rights-Management (Dokumentenmanagement) mit SAP sowie „Turaya.Embedded“ für den sicheren Einsatz von embedded Systemen (Automotive, Multimedia) hinzu.

Enterprise Rights Management ist eine Umschreibung für eine Vielzahl von Funktionen, die Daten über ihren gesamten Lebenszyklus schützen und mit entsprechenden Regeln versehen können. Die Automobilindustrie als Beispiel tauscht über ihre Systeme sensible Daten zwischen unterschiedlichen Standorten und Zulieferfirmen aus, um Prozesse zu erleichtern und zu beschleunigen. Der Verlust von Design-Daten würde im Rahmen von Plagiatsfällen einen hohen Schaden verursachen. ERM soll dafür sorgen, das die Design-Daten nur für einen definierbaren Personenkreis einsehbar und zu bearbeiten sind.

Bei Turaya.ERM, der vierten Pilotanwendung, soll die SAP AG als EMSCB-Partner das Problem der sicheren Verteilung von Dokumenten lösen. Dokumente kann man wie oben beschrieben durch eine Sicherheitsplattform auf Basis von Sealing- und Attestation-Funktionen an eigene und entfernte Plattformen binden und in dem Rahmen verschlüsseln.

Verteilt der Chef etwa ein Dokument in der Firma, soll es eventuell für bestimmte Personen lesbar, aber nicht druckbar sein, um eine unsachgemäße Verbreitung zu verhindern. Andere Mitarbeiter mit entsprechender Berechtigung müssen es drucken oder auch weiterleiten können, wieder anderen ist das Öffnen dagegen komplett untersagt. Firmenintern werden die verschieden Rechte gemäß der Stellung häufig durch Rollen abgebildet.

Dokumente sicher verwalten

Turaya kann mit einer Policy gemäß den Rollen des Identitätsmanagementssystems die jeweiligen Rechte in Bezug auf das Dokument durchsetzen – was den Schutz der Dokumente auch über die Unternehmensgrenzen hinaus gewährleisten soll. Mit dem Rights Management ist „Multilevel-Security“ verbunden. Das bedeutet, dass die als

sicherheitsrelevant eingestuften Vorgänge neben den unkritischen im herkömmlichen Betriebssystem auf demselben System parallel und streng isoliert ausgeführt werden können (Abb. 2).

Täglich genutzte Rechnersysteme sollen zunehmend miteinander kommunizieren können. So erwarten viele von einem neuen Auto mehr als einen fahrbaren Untersatz. Es soll etwa Multimediadaten für den DVD-Player der Kinder auf der Rückbank oder Navigationsdaten für die Reise ins Ausland zur Verfügung stellen.

Visionen der Entwickler und potenzielle Sicherheitsfeatures der Zukunft, etwa dass das eigene Auto den Bremsvorgang selbstständig einleiten soll, sobald der Vordermann langsamer fährt, dürfen nur mit vertrauenswürdigen Soft- und Hardwarekomponenten realisiert werden. Das gilt ebenfalls für das in Zukunft realisierbare Update, das die Werkstatt im Vorbeifahren einspielt. Danach muss sichergestellt sein, dass das Rechnersystem vertrauenswürdig ist und die Bremssysteme weiterhin funktionieren. Für diese Anwendungsfälle gibt es schon Konzepte und erste Praxistests.

Die Aufgabe besteht in der Umsetzung der beschriebenen Funktionen auf andere Systeme. Das Rechnersystem, das die Updates der Werkstatt entgegennimmt, ist ein sogenanntes eingebettetes System. Die Turaya-Plattform wird beispielsweise auf ARM-Prozessoren portiert, um diese sicher und vertrauenswürdig zu gestalten. Zu diesem Bereich gehören maschinelle Rechnersysteme ebenso wie Smartphones oder PDAs.

Für die fünfte Pilotanwendung erarbeiten die Verantwortlichen gemeinsam mit Projektpartner Bosch/Blaupunkt ein Szenario. Kartenmaterial für Navigations- oder zukünftige Multimediasysteme in Autos sind kaum durch CDs ständig aktuell zu halten, und für eine Reise ins Ausland möchte man nicht gleich die Karten von ganz Europa bezahlen. Die Anwendung zeigt, wie ein Autobesitzer Kartenmaterial „on demand“ auf eine eingebettete Systemplattform laden kann. Das Kartenmaterial wird explizit für das Rechnersystem zu entsprechenden Konditionen zur Verfügung gestellt. Dieser Vorgang ist stellvertretend für das große Einsatzgebiet im Embedded-Bereich.

Fazit

Neue Informationstechniken bedürfen einer ebenso umfangreichen wie systemübergreifenden Sicherheitslösung. Damit sich Geschäftsprozesse einfacher, effektiver und trotzdem sicher gestalten lassen, muss ein Standard für alle zugänglich und nutzbar sein.

Mit Turaya können Anwender eigene Policies definieren, ihre Netzwerkumgebung auf Vertrauenswürdigkeit hin prüfen und sensible Daten sichern. Zentrale Kriterien sind Fairness und Offenheit, damit kein Hersteller mit seinen Produkten ausgeschlossen ist. Deshalb sind sämtliche Programmierschnittstellen von Turaya und der Quellcode aller sicherheitsrelevanten Komponenten zu Evaluierungszwecken offengelegt, um die Vertrauenswürdigkeit der Implementierung zu garantieren.

Turaya ermöglicht es der Open-Source-Gemeinde, „konkurrenzfähig“ zu bleiben. Zudem bietet die Sicherheitsplattform den Vorteil, dass alle sicherheitskritischen Komponenten und Anwendungen unabhängig von „klassischen“ Betriebssystemen agieren können und damit für zukünftige plattformübergreifende verteilte Anwendungen geeignet sind. Sourcecode, Pilotanwendungen und weitere Informationen finden Interessierte auf der Website des europäischen Konsortiums: www.emscb.org. (ur)

NORBERT POHLMANN UND MARKUS LINNEMANN

vom Institut für Internet-Sicherheit an der FH Gelsenkirchen arbeiten im Turaya-Projekt mit.

Literatur

[1] Informationsfilm über Turaya: www.internet-sicherheit.de/trusted-computing-film.html

[2] N. Pohlmann, H. Reimer; Trusted Computing – Ein Weg zu neuen IT-Sicherheitsarchitekturen; Vieweg-Verlag, Wiesbaden 2008