Schöne neue Welt?!

Die vertrauenswürdige Sicherheitsplattform Turaya

Ein paar Spiele, ein bisschen im Internet surfen, E-Mails lesen und Texte verfassen – das war die Anwendungswelt von Rechnersystemen noch vor einigen Jahren. Inzwischen wird fast jede reale Anforderung digital abgebildet. Es wird eingekauft, hochsensible Kommunikation betrieben, das Kino nach Hause geholt, die Bankgeschäfte abgewickelt, geschäftliche und private Strukturen von Unternehmen und Personen vernetzt. Selbst der Weg zum Ordnungsamt wird in Zukunft ausfallen, oder statt mit einer dicken Aktentasche, mit einem kleinen USB-Token oder einem ePass absolviert. Aber wie sieht es in dieser Entwicklung mit Sicherheit, Datenschutz und Urheberrechten aus? Die Security-Plattform Turaya, die zwischen Betriebssystem und Hardware liegt, schiebt Übeltätern einen Riegel vor.

Aktuelle Betriebssysteme werden täglich durch eine Vielzahl von Attacken bedroht. Phishing, Spam, Viren, Trojanische Pferde, Würmer, Exploits, all diese Begriffe prägen unseren Alltag und zeigen uns, dass herkömmliche Technologien den Anforderungen nicht mehr gewachsen sind. Auch das permanente Ausbessern von Fehlern durch Patches, Firewalls und Virensoftware verbessert die Situation nicht ausreichend. Die aktuellen Technologien müssen der rasanten Entwicklung jedoch gewappnet sein, und mehr noch, durch Innovationen weitere Geschäftsfelder schaffen.

Die aktuelle Situation lässt somit den Schluss zu, dass neue Konzepte entwickelt werden müssen die zuallererst optimale Sicherheit bieten. Sensible Informationen und Daten, wie sie beispielsweise beim Online-Banking genutzt werden, müssen entsprechend geschützt sein. Die vernetzte Struktur und die verteilten Anwendungen des Internets fordern außerdem, gerade im Zusammenhang mit kommunizierten Inhalten, einen Schutz der Urheberrechte, aber auch der Privatsphäre des Anwenders.

Turaya ist eine offene Sicherheitsplattform, die eben jene Sicherheit bietet und sowohl die Regeln und Rechte des Nutzers, als auch die des Inhalts-Anbieters fair und vertrauenswürdig durchsetzt.

Der Sicherheitskern Turaya

Ein Betriebssystem überwacht sämtliche Funktionalitäten eines Rechnersystems und so ziemlich alle angesprochenen Attacken sind darauf ausgelegt das Betriebssystem zu kompromittieren. Ist dieser Zustand erreicht hat der Angreifer Zugriff auf alle Funktionen und Daten des attackierten Rechnersystems. Online-Banking ist eine typische Applikation die heute genutzt wird. Wäre das Rechnersystem von einem Trojanischen Pferd befallen, wäre es sehr leicht möglich an PIN- und TAN-Nummern zu kommen. Außerdem kann man nicht sicher sein, ob die Verbindung tatsächlich zu dem gewünschten und echten Banksystem aufgebaut wurde.

Turaya ist ein Sicherheitskern der unterhalb des Betriebssystems ansetzt. Das herkömmliche Betriebssystem läuft quasi als Applikation des Turaya-Sicherheitskerns, ohne von dessen Existenz zu wissen. Abbildung 1 zeigt diese Architektur. Der Sicherheitskern kontrolliert somit, als Schicht zwischen Betriebssystem und Hardware, sämtlich Zugriffe auf die Ressourcen des Rechnersystems. Dieses Vorgehen wird als Virtualisierung/Paravirtualisierung bezeichnet.

Durch diese Konstellation ist es möglich, Online-Banking nicht in dem gefährdeten Betriebssystem, sondern in einem sicheren isolierten Bereich durchzuführen, in Abbildung 1 durch die „Secure Applikation" dargestellt. In diesem Fall ist es irrelevant, ob

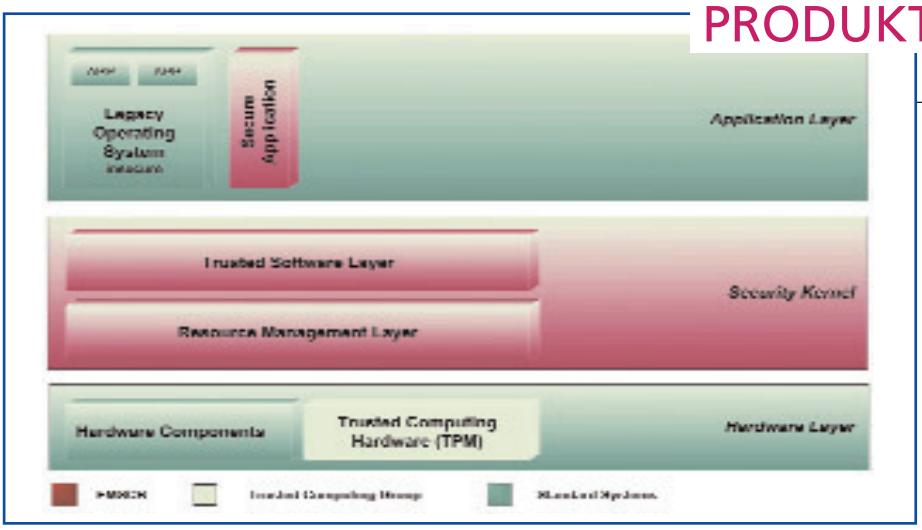

Bild 1: Architektur eines Rechnersystems mit dem Turaya Sicherheitskern

das herkömmliche Betriebssystem kompromittiert ist, da der Prozess von diesem gekapselt ist. Online Banking mit Turaya funktioniert folgendermaßen: Ein Browser funktioniert wie gewohnt und sicherheitsunkritische Anfragen werden an die Netzwerkkarte weitergeleitet. Turaya stellt in diesem Fall zuvor allerdings eine virtuelle Netzwerkkarte zur Verfügung. Kommt nun eine Anfrage an einen vorher im Sicherheitskern definierten Bankserver, dann erkennt Turaya diese Anfrage und übergibt sie an das Turaya-VPN. Dieses initiiert den Aufbau eines VPN-Tunnels zum definierten Bankserver. Alle hierfür notwendigen Schlüssel liegen außerhalb des evtl. kompromittierten Betriebssystems und sind somit geschützt, dasselbe ist möglich für die PIN/TAN-Abfrage. Diese kann ebenfalls vom Betriebssystem isoliert werden. Alle Vorgänge laufen für den Anwender transparent ab.

Das Beispiel zeigt nur eine Anwendungsmöglichkeit des Turaya-Sicherheitskerns. Die Konzepte werden jedoch klar deutlich. Es wird virtualisiert und isoliert, um einen höheren Grad an Sicherheit zu erreichen.

Hardware Sicherheit durch Trusted Computing

In Abbildung 1 wird im Hardware Layer ein Bereich mit dem Namen „Trusted Computing Hardware" bezeichnet. Dieser Zusatz bringt zu dem vorgestellten Konzept einen weiteren hohen Sicherheitszuwachs. Das Rechnersystem wird beim Bootvorgang gemessen, sprich von allen gestarteten Anwendungen wird eine Prüfsumme (Hashwert) gebildet. Diese Ergebnisse werden vom TPM, einem kleinen Trusted Computing Modul auf dem Rechnersystem, festgehalten. So kann ein vertrauenswürdiger Zustand des Rechnersystems gewährleitstet werden. Bei einem Ein(An-)griff in(auf) das Rechnersystem wird der gemessene Wert verändert und es kann nicht mehr von einem vertrauenswürdigen Rechnersystem ausgegangen werden. Das Binden der Konfiguration an das Rechnersystem wird als „Sealing" bezeichnet.

Sicherheit in Verteilten Systemen stellt auch die Forderung, dass ein fremdes Rechnersystem eindeutig als vertrauenswürdig eingestuft werden kann. Beim Online-Banking soll z.B. sichergestellt sein, dass der Bankserver mit dem sich das Rechnersystem verbindet auch wirklich der echte Bankserver ist. Der vertrauenswürdige Zustand des Bankservers kann „gemessen" und diese Information bei einer 3rd Party abgelegt werden. Dort werden die entsprechenden Informationen abgefragt. Stimmen die Werte, die der Bankserver sendet mit denen der 3rd Party überein ist sichergestellt, dass der Bank-Server echt ist. Dieser Vorgang wird als „Attestation" bezeichnet.

Trusted Computing wird im Hinblick auf Möglichkeiten zur Einschränkung der Rechte und der Privatsphäre der Endbenutzer sehr kritisch betrachtet. Durch den Open-Source-Ansatz Turayas ist es jedoch jedem möglich den Quellcode der Entwicklungen einzusehen. Somit wird die Angst vor versteckten Mechanismen, die den Nutzer einschränken könnten, genommen. Der Anwender ist außerdem nicht gezwungen die Funktionen des Rechnersystems zu nutzen, da parallel weiterhin ein herkömmliches Betriebssystem laufen kann.

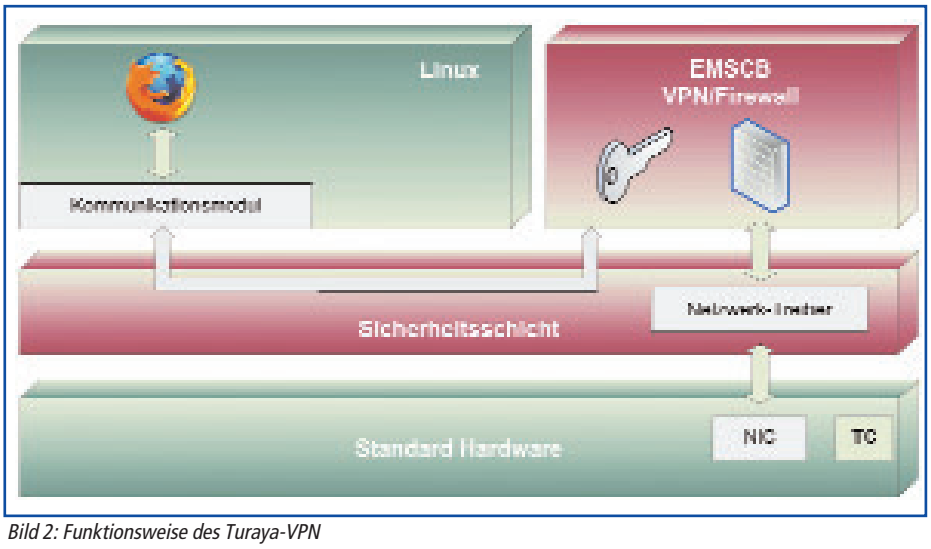

Bild 2: Funktionsweise des Turaya-VPN

Innovative Geschäftsfelder – Digital Rights Management

Zu Beginn wurde darauf eingegangen, dass die heutigen Anforderungen an das Internet die Möglichkeit beinhalten, dass Rechte und Regeln nicht nur auf dem eigenen, sondern auch auf fremden Rechnersystemen durchgesetzt werden müssen.

Der Vorstand einer Bank erstellt ein Dokument, das die Finanzabteilung lesen und verschicken, der Vertrieb aber nur lesen darf. Dieses typische Szenario kann mit Turaya auf fremden Rechnersystemen durchgesetzt werden. Rechte können an Dokumente gebunden und auf fremden Systemen durchgesetzt werden, immer unter der Prämisse, dass die Regeln des Zielsystems mit den Regeln des Anbieters konform gehen.

Digital Rights Management Anwendungen sind damit ein weiteres Einsatzgebiet des Sicherheitskerns. Inhalte können unter Einhaltung des Datenschutzes und des Urheberrechts weitergegeben werden. Die Sicherheitsplattform Turaya vergleicht die vom Benutzer geforderten Sicherheitsanforderungen z.B. mit den Lizenzbedingungen zu installierender Anwendungen und verhindert im Konfliktfall deren Installation. Sämtliche Rechte und Regeln können ausschließlich durch Zustimmung beider Seiten, sowohl des Nutzers, als auch des Anbieters durchgesetzt werden.

Das EMSCB Projekt

Turaya ist die Software, die innerhalb des EMSCB-Projekts entwickelt wird. Das Pro-

jekt-Team besteht aus dem Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen, der Ruhr-Universität Bochum, der TU Dresden, der Sirrix AG, der escrypt GmbH und den strategischen Partnern SAP, Bosch/Blaupunkt und Infineon. Das Projekt wird vom BMWi gefördert [SaSP05].

Turaya nutzt innovative und vertrauenswürdige Konzepte, um den heutigen Anforderungen unserer Informationsgesellschaft zu entsprechen. Viele neue Technologien spielen in diesem Rahmen zusammen, wie Trusted Computing; Virtualisierungstechnologien, usw. Einsetzbar ist der Sicherheitskern mit diesen Technologien nicht nur auf Desktop Systemen, sondern auch auf mobilen Endgeräten, Set-Top-Boxen, Embedded Systemen und allen weiteren Computersystemen. Dies zeigt auch der Projektplan. Die folgenden fünf Piloten werden in drei Jahren realisiert - die ersten beiden sind bereits fertig gestellt:

1. Device Verschlüsselung „Turaya Crypt"; fertig gestellt
2. Sicheres VPN-Modul (Zertifikatsmanagement) „Turaya-VPN"; fertig gestellt
3. Faires DRM; November 2006
4. Dokumentenmanagement mit SAP; November 2007
5. Embedded Systems (Automotiv Multimedia); November 2007

Ausblick

Mit Hilfe des EMSCB-Projektes wird eine vertrauenswürdige, faire und offene Sicherheitsplattform Turaya entwickelt, die allen Anwendungsentwicklern gleiche Marktchancen bietet. Sämtliche Programmierschnittstellen von Turaya und der Sourcecode aller sicherheitskritischen Komponenten werden zu Evaluierungszwecken offen gelegt, um die Vertrauenswürdigkeit der Implementierung zu erhöhen.

Turaya bietet zudem den Vorteil, dass alle sicherheitskritischen Komponenten und Anwendungen unabhängig von „klassischen" Betriebssystemen agieren können und damit für zu-künftige plattformübergreifende verteilte Anwendungen optimal geeignet sind.

Die ersten beiden Meilensteine sind bereits fertig gestellt und eine Vielzahl von Firmen interessiert sich für diesen ersten Prototyp. Innerhalb des geförderten Projekts werden die fünf genannten Meilensteine entwickelt und freigegeben. Das Vorhaben ist, wie durch das Kompetenzzentrum bestätigt wird, auf lange Sicht ausgelegt und motiviert durch neue Partner weitere Piloten zu entwickeln. Dadurch wird die Wissensbasis erweitert, um innovative Geschäftsideen am Standort Deutschland zu inspirieren und zu ermöglichen.

Markus Linnemann
markus.linnemann@internet-sicherheit.de
Prof. Dr. Norbert Pohlmann
norbert.pohlmann@informatik.
fh-gelsenkirchen.de
Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
Neidenburger Str. 43,
D - 45877 Gelsenkirchen
www.internet-sicherheit.de

Literatur

[SaSP05] A.Sadeghi, C. Stüble, N. Pohlmann: "European Multilateral Secure Computing Base - Open Trusted Computing for You and Me", in Datenschutz und Datensicherheit (DUD) 9/2004, Vieweg Verlag (2004) 548-554

[LiPo06] M. Linnemann, N. Pohlmann: „Die vertrauenswürdige Sicherheitsplattform Turaya", in „DACH Security 2006", Hrsg.: Patrick Horster, syssec Verlag, 2006