Eine vertrauenswürdige, faire und offene Sicherheitsplattform Turaya

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

Zusammenfassung

Das vom Bundeswirtschaftsministerium geförderte EMSCB-Projekt schafft die~~eine~~ vertrauenswürdige, faire und offene Sicherheitsplattform Turaya, welche eine vertrauenswürdige Verarbeitung von Informationen auf dem eigenen und auf fremden Rechnersystemen möglich macht.

1 Motivation

Aktuelle Sicherheitstechnologien wie beispielsweise SmartCards und Firewall-Systeme können die Sicherheit existierender Betriebssysteme auf Dauer nicht entscheidend verbessern, da sie immer nur Teilaspekte betrachten, bzw. nur partielle Sicherheitsprobleme lösen. Die Identifizierung und Beseitigung konzeptioneller Schwachstellen vorhandener Betriebssysteme führt daher zum kontinuierlichen Ausbessern von Fehlern und Sicherheitslücken durch Patches.

Viele innovative Ideen ersticken im Keim. Anwendungen bei denen die Vertrauenswürdigkeit von fremden Rechnersystemen eine besondere Rolle spielen, wie z.B. im Bereich des Digital Rights Management werden nicht genutzt oder weiterentwickelt, da die Gefahren auf Seiten der Inhalte-Anbieter wie auf Seiten der Nutzer zu groß sind. Tägliche Berichte über neue Sicherheitslücken, Viren, Würmer, Trojaner und Phishing-Attacken verunsichern Hersteller und Anbieter wie auch (potenzielle) Anwender und be- oder verhindern Online-Angebote, die für beide Seiten wegen ihres praktischen und ökonomischen Nutzens wünschenswert sind. Dies zeigt deutlich, dass wir eine neue Sicherheitsplattform benötigen, der alle Seiten vertrauen können: Turaya ist eine Sicherheitsplattform, die sichere Anwendungen ermöglicht, indem sie sowohl die Regeln und Rechte des Nutzers, als auch die des Inhalte-Anbieters fair und vertrauenswürdig durchsetzt.

2 Anforderungen & Ziele

Der Einsatz komplexer Applikationen und die rapide Zunahme der Vernetzung von Rechnersystemen im B2B und B2C Bereich stellen uns vor neue Herausforderungen hinsichtlich ihrer Sicherheit und Benutzbarkeit.

2.1 Anforderungen

Im Rahmen der Benutzbarkeit beschränken sich heutige Anwendungen nicht mehr nur auf PC- und Server-Systeme von Unternehmen. Neue Geschäftsmodelle erfordern die Realisierung innovativer Anwendungen z.B. auch für eingebettete Systeme, dazu zählen mobile Geräte (PDAs, SmartPhones), aber auch Systeme im Automobilbereich (PS-Steuerung, Infotainment). Die zu entwickelnde Technologie muss den Anspruch erfüllen auf einem breiten Spektrum von Plattformen einsetzbar und von diesen unabhängig zu sein.

Im Bereich der Sicherheit agieren in diesem Zusammenhang verschiedene Parteien mit unterschiedlichen Interessen 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. Hinzu kommt, dass mit zunehmendem Einsatz von IT-Systemen in sicherheitsrelevanten Szenarien auch die Gefahren und folglich die Sicherheitsanforderungen an die zugrunde liegenden Rechnerplattformen und die verwendete Software wachsen. Heutigen Applikationen fordern Benutzer-Endgeräte, die Sicherheitsziele wie Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit im Sinne multilateraler Sicherheit sowohl software-, wie auch hardwareseitig garantieren können.

Existierende Rechnerplattformen, vor allem die heutigen Betriebssysteme, erfüllen diese Sicherheitsanforderungen nicht in gewünschtem Maße. Die Vielzahl von notwendigen Sicherheits-Updates und Exploits, kleine Computerprogramme, die Sicherheitslücken ausnutzen, unterstreichen diese Aussage. Besonders auf Windows-Ebene kommen noch Viren, Würmer und Trojaner-Angriffe hinzu. Die Ursachen sind vielfältig und liegen sowohl in den heutigen Betriebssystemen, als auch in der genutzten Hardware begründet.

Einige wichtige Probleme sind:

- Schutz zwischen Anwendungen: Übliche Betriebssysteme bieten keine angemessenen Mechanismen, um verschiedene Applikationen voreinander zu schützen. Durch Sicherheitslücken in einer Anwendung können alle weiteren Anwendungen kompromittiert werden.
- Installation und Originalität: Bisher gibt es kein generelles Verfahren, das einerseits Programme auf ihre Originalität, bzw. einen beglaubigten Zustand testet und andererseits dessen Zugriffsrechte auf Systemressourcen zuverlässig einschränkt und kontrolliert.
- Authentifikation: Es fehlen Authentifikationsmöglichkeiten von Programmen, die dem Benutzer gegenüber garantieren, dass keine unerwünschte Veränderung der Applikation stattgefunden hat. Ausserdem ist es bisher nicht möglich gewesen, dass eine Authentifizierung der Hardware gegenüber dem Nutzer durchgeführt wird, um eventuelle Manipulationen am gesamten System sichtbar zu machen

- Darstellungsproblem: Digital signierte Dokumente können zwar nicht unbemerkt verändert werden, aber bereits vor der Signatur fehlerhaft dargestellt worden sein (What You See Is *Not* What You Get). Außerdem werden Dokumente auf unterschiedlichen (Sicherheits-)Plattformen möglicherweise unterschiedlich dargestellt. Es ist keine Trusted Chain (Verkettung vertrauenswürdiger Vorgänge für den gesamten Ablauf einer Aktion) vorhanden, die die Originalität des Dargestellten garantieren kann.

Die existierenden Rechnerplattformen bieten keine geeigneten Mechanismen, um lokale Sicherheitsrichtlinien des Benutzers (Datenschutz) oder des Unternehmens (Firmengeheimnis), sowie die Richtlinien externer Instanzen (Inhalte-Anbieter) durchzusetzen. Maßnahmen zum Urheberschutz digitaler Inhalte lassen sich über die bisher zur Verfügung stehenden Möglichkeiten nicht mit Sicherheitsrichtlinien, beziehungsweise den Interessen des Benutzers, in Einklang bringen.

Aufgrund konzeptioneller Schwächen von heutigen Betriebssystemen ist nicht zu erwarten, dass sich die Sicherheit der Rechnerplattformen in den nächsten Jahren entscheidend verbessern kann. Dies betrifft sowohl Windows- als auch Linux-basierte Betriebssysteme. Bedingt sind diese Schwächen durch die monolithische (z.B. Linux), bzw. hybride (z.B. Windows) Struktur der Systeme. Diese Strukturen implizieren, dass eine Vielzahl von Funktionalitäten in den Kern des Betriebssystems integriert wird. Dadurch entsteht~~en~~ eine sehr hohe Komplexität und damit eine sehr hohe Fehleranfälligkeit. Im Gegensatz dazu ist die Komplexität von mikrokernbasierten Systemen wesentlich geringer. Außerdem sehen die herkömmlichen Systeme selten eine Isolation von sicherheitskritischen Prozessen vor. Die dadurch bestehenden Bedrohungen verzögern oder verhindern dabei die Realisierung vieler nützlicher Anwendungen und Geschäftsmodelle im Bereich des elektronischen Handels.

Um die gewünschten Sicherheitseigenschaften zu garantieren, besonders auch in einer potenziell unsicheren Umgebung, wird offensichtlich eine neue Generation von Betriebssystemen benötigt. Trusted-Computing-Technologie bietet hierzu wichtige Funktionen, kann jedoch alleine - *ohne* ein sicheres und vertrauenswürdiges Betriebssystem - die heutigen Probleme nicht lösen, denn das Betriebssystem kontrolliert alle Vorgänge, allem voran die Hardware, und hat somit in letzter Instanz den Zugriff auf alle sicherheitsrelevanten Informationen.

Bisher existiert jedoch keine vertrauenswürdige, faire und offene Sicherheitsplattform, die basierend auf den Spezifikationen der TCG die notwendige Grundlage für die Realisierung multilateral sicherer Anwendungen bietet.

2.2 Ziele

Die Anforderungen zeigen die Notwendigkeit eine vertrauenswürdige, faire und offene Sicherheitsplattform zu schaffen. Dabei zielt das Projekt nicht ausschließlich auf die Lösung technischer Probleme ab. Vielmehr ist das Ziel die IT vertrauenswürdiger zu machen. Das bedeutet die Einhaltung der Rechte jedes Teilnehmers.

Das Projekt schafft einen Wissenspool, im Rahmen eines Kompetenzzentrums, der Firmen und vor allem dem IT-Standort Deutschland zu gute kommt. Durch das offene Forschungsprojekt wird angestrebt einen Standard zu schaffen, der jedem Entwickler zugänglich ist, unabhängig von bestimmten Herstellern auf Hardware- und Softwareebene.

3 Die Sicherheitsplattform

Im Wesentlichen bietet die EMSCB-Sicherheitsplattform Turaya einen Mikrokern-basierten Sicherheitskern der „unterhalb“ von herkömmlichen Betriebssystemen agiert. Im Grunde handelt es sich um ein eigenes Betriebssystem. Die gesamte Ressourcenverwaltung und die Kontrolle über Prozesse im Hinblick auf die Rechteverwaltung werden von Turaya übernommen. Das Trusted Plattform Module (TPM) der Trusted Computing Group (TCG) bietet die Möglichkeit sicherheitsrelevante Prozesse durch Hardwaresicherheit zu stützen und somit um ein wesentliches sicherer zu machen.

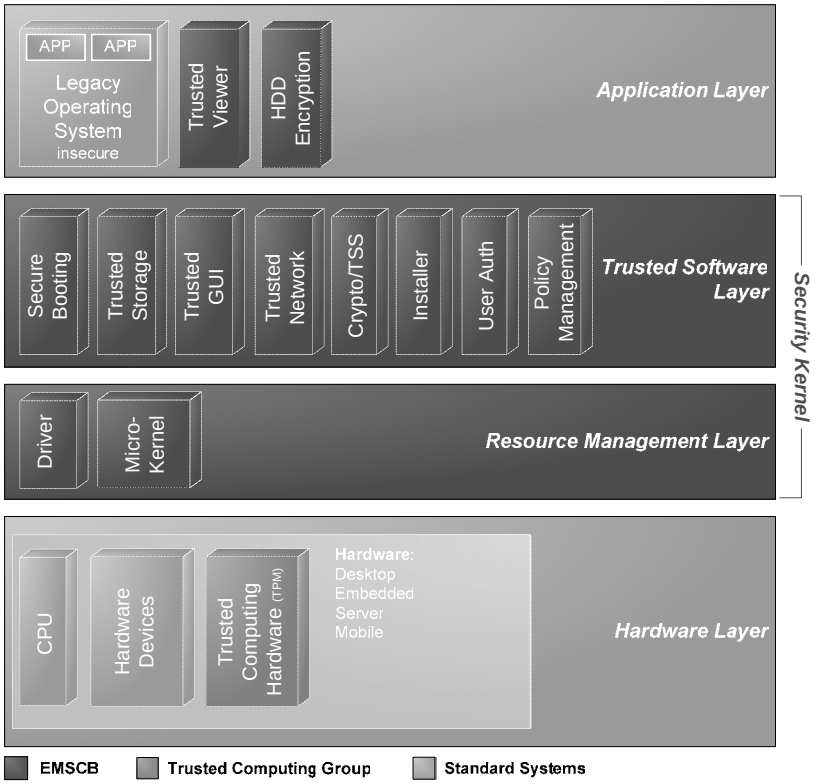

Abb. 2: Security Software Layer als Kontrollinstanz zwischen konventionellem Betriebssystem, sicherheitskritischen Anwendungen und der Hardware

3.1 Der Aufbau

Die wichtigsten Aspekte und Komponenten der Sicherheitsplattform Turaya sind im Folgenden aufgeführt und werden kurz erläutert:

3.1.1 Trusted Computing Support:

Trusted Computing stellt erstmalig Hardware bereit, die die geeignete Grundlage für die Realisierung eines durchgängig sicheren Betriebssystems bildet. Somit besteht die Möglichkeit der Integritätsprüfung der zugrunde liegenden Rechnerplattform (Attestation). Diese Integritätsprüfung ist insbesondere von fremden Rechnern aus durchführbar. Damit erreichen wir eine sehr sichere Hardware-basierte Client-Authentifizierung. Ein weiterer Vorteil ist das Binden eines geheimen Schlüssels an eine Plattformkonfiguration (Sealing). Des Weiteren kön-

nen sichere Zufallszahlen für kryptographische Funktionen erzeugt und kryptographische Schlüssel sicher in einem softwareseitig nicht kompromittierbaren Stück Hardware gespeichert werden. Dieses Hardware-Sicherheitsmodul stellt die nicht manipulierbare Grundlage für viele Sicherheitsdienste dar. Schon Ende 2006 sollen ca. 60-100 Mio. TPMs in unterschiedliche Rechnersysteme eingebaut sein [Roge05].

3.1.2 Hardwareunabhängigkeit

Die Sicherheitsplattform soll universell sein, d.h. unabhängig von der konkreten Realisierung der TC-Hardware. Sie soll von dem von der Trusted Computing Group (TCG) spezifizierten und bereits verfügbaren TPM-Chip ebenso profitieren wie von der gegen Ende 2005 erwarteten LaGrande-Technologie (TPM-ähnliche Technologie), die Intel im Zusammenhang mit Microsofts NGSCB entwickelt hat. Der Sicherheitskern ist also eigenständig und auch ohne Trusted Computing Hardware einsetzbar, allerdings mit einem geringeren Sicherheitsniveau und ohne Technologien, wie Sealing und Attestation.

3.1.3 Trusted Software Layer

Bei dem Trusted Software Layer handelt es sich um den Teil des OpenSource Sicherheitskerns, der alle kritischen Hardwareressourcen (inkl. TC-Hardware) policy-basiert kontrolliert und damit sicherheitskritische Anwendungen und Daten schützen kann. Auf dieser Ebene befinden sich sämtliche schützenswerte Softwaremodule, die nicht Teil des Mikrokerns sind, wie zum Beispiel die persistente Datenspeicherung (Trusted Storage), die auch für Benutzerdaten verwendet wird.

3.1.4 Ressource Management Layer

Der Ressource Management Layer hat hauptsächlich die Aufgabe, eine abstrakte Schnittstelle zu darunter liegenden Hardware-Ressourcen (zum Beispiel Interrupts, Speicher etc.) zur Verfügung zu stellen. Auf dieser Ebene werden den darüber liegenden Schichten alle Funktionen der Hardware angeboten, quasi als Virtualisierung der Hardware. Der Mikrokern leistet dann den realen Zugriff auf die Hardware. Der Ressource Management Layer wird insbesondere durch einen Micro-Kernel und spezielle vertrauenswürdige Treiber definiert.

3.1.5 Secure Application

Basierend auf der zur Verfügung gestellten Schnittstelle können sicherheitskritische Anwendungen (Festplattenverschlüsselung, digitale Signaturen, faire DRM etc.) ausgeführt werden, welche die neuen Möglichkeiten der Trusted Computing Base und der TC-Technologie nutzen. Die Sicherheitsschicht schützt diese Anwendungen vor externen und lokalen Manipulationsversuchen (z.B. durch Malware oder lokale Benutzer), ermöglicht jedoch auch eine kontrollierte Kommunikation mit einem „klassischen“ Betriebssystem.

3.2 Konzepte

Aus verschiedenen Ideen und Anforderungen heraus wurden zwei wichtige Konzepte entwickelt, um die Ansprüche an die SicherheitspPlattform Turaya erfüllen zu können:

3.2.1 Sicherheit durch Minimalisierung und Isolation

Der Sicherheitskern isoliert Prozesse voneinander und steuert jegliche Interprozess-Kommunikation. Dadurch sind kompromittierte Anwendungen (z.B. Linux auf einem Sicher-

heitskern) für das restliche System ungefährlich, da kein Zugriff auf andere Ressourcen möglich ist. Sowohl für den Sicherheitskern programmierte sichere Applikationen, als auch herkömmliche Betriebssysteme werden als parallel laufende Prozesse behandelt. Die Hardware wird von dem Sicherheitskern quasi für jede einzelne Anwendung virtualisiert.

Der Sicherheitskern basiert auf einem Mikrokern mit Schnittstellen gringer Komplexität und Modulen, die sich durch eine geringe Zahl von Codezeilen auszeichnen. Dadurch werden die Wahrscheinlichkeit von Programmierfehlern und die dadurch entstehenden Sicherheitslücken sehr stark reduziert.

3.2.2 Existierende Betriebssysteme

Parallel zu den sicherheitskritischen Applikationen wird ein konventionelles Betriebssystem (derzeit Linux) ausgeführt, das durch die Sicherheitsplattform Turaya kontrolliert wird und es dem Benutzer ermöglicht, seine gewohnte Arbeitsumgebung zu verwenden. Somit entstehen keine Kompatibilitätsprobleme und existierende Anwendungen sind weiter verwendbar.

3.3 Eigenschaften der EMSCB-Sicherheitsplattform

Die Sicherheitsplattform Turaya kombiniert in innovativer Weise die Vorteile eines vertrauenswürdigen Open Source Sicherheitskerns mit den Vorteilen von Trusted Computing:

3.3.1 Multilaterale Sicherheit

Die Sicherheitsplattform Turaya ermöglicht die Durchsetzung lokaler (z.B. Endbenutzer) und externer (z.B. Inhalte-Anbieter) Sicherheits- bzw. Zugriffsregeln. Dadurch bietet sie dem Benutzer einen wirksamen Schutz gegen Verletzung von Datenschutzrichtlinien. Inhalte-Anbietern gegenüber bietet die Sicherheitsplattform einen Schutz gegen eine Umgehung ihrer Lizenzbedingungen, wenn diese von Konsumenten bereits akzeptiert worden sind.

3.3.2 Vertrauenswürdige Sicherheitsplattform

Durch die geringe Komplexität des Sicherheitskerns, die bereits als Minimalisierung beschrieben wurde, erreicht die Sicherheitsplattform Turaya eine sehr hohe Vertrauenswürdigkeit. Die Fehlerwahrscheinlichkeit wird durch die geringe Komplexität, die offene Implementierung und die Evaluierung nach Sicherheitsstandards minimiert.

3.3.3 Faire Sicherheitsplattform

Trusted Computing wird im Hinblick auf die Einschränkung der Rechte und der Privatsphäre der Endbenutzer sehr kritisch betrachtet. Durch den OpenSource-Ansatz ist es 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 der Plattform zu nutzen, da parallel weiterhin ein herkömmliches Betriebssystem laufen kann. Die EMSCB-Sicherheitsplattform Turaya vergleicht die vom Benutzer geforderten Sicherheitsanforderungen 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.

3.3.4 Offene Sicherheitsplattform

Mit Hilfe der EMSCB-Sicherheitsplattform Turaya soll ein offener Standard zur Erhöhung der Interoperabilität geschaffen werden.

Turaya ist zudem so konzipiert, dass sie sich effizient auf weitere Geräte portieren lässt, beispielsweise auf Personal Digital Assistants (PDAs), Smartphones und Embedded Systems. Um die TC-Funktionalitäten nutzen zu können, müssen diese Geräte mit entsprechender Hardware ausgerüstet werden. Spezifikationen für diese Bereiche stehen kurz vor dem Abschluß [Trus05]. Weitere Anwendungen können Multimedia- und Informationssysteme in Kraftfahrzeugen sein.

Ausserdem ist die EMSCB-Sicherheitsplattform Turaya offen für Partner, und stellt keine Diskriminierung einzelner Anbieter/Anwender dar.

4 Technischer Einblick in die Sicherheitsplattform

Grundsätzlich wird unterschieden zwischen sicherheitsunkritischen und sicherheitskritischen Anwendungen. Für Anwendungen die als sicherheitsunkritisch gelten existieren keine Besonderheiten, da sie sich im Legacy Betriebssystem befinden und sie keinerlei Information darüber besitzen, dass sie auf einem mikrokernbasierten Betriebssystem im User Mode ausgeführt werden.

Für Anwendungen die als sicherheitskritisch gelten müssen viele Faktoren berücksichtigt werden. Jede sicherheitskritische Anwendung besitzt eine Komponente (Client) im Legacy Betriebssystem. Diese Komponente ist lediglich dafür verantwortlich einen bestimmten Vorgang im Sicherheitskern, der auch Trusted Computing Base (TCB) genannt wird, zu initiieren. Sie besitzt zwar das Wissen das sie sich auf einem mikrokernbasiertem Betriebssystem befindet, erhält aber keine sicherheitskritischen Informationen. Über diese Komponente lässt sich die entsprechende sicherheitskritische Anwendung, die sich als Modul (Server) im Sicherheitskern befindet, starten. Diese Anwendung ist in der Lage weitere Prozesse zu starten oder für den Client Aufgaben zu übernehmen, die er auf Grund seines Sicherheitsstatus` nicht kontrollieren darf.

Client und Server kommunizieren über IPC (Inter Process Communication) Aufrufe die vom Client an den Server gesendet und vom Server beantwortet werden. Eine Datenübertragung kann in beide Richtungen erfolgen.

Für den Server gelten hohe Sicherheitsanforderungen, da er Teil der TCB ist und Zugriff auf sicherheitskritische Daten besitzt. Bei der Implementierung des Servers muss darauf geachtet werden, dass er keine sicherheitskritischen Daten an den Client gibt, da sich dieser im Legacy Betriebssystem befindet und dort von jedem Rootprozess ausgelesen werden kann. Das bedeutet, dass alle Daten die man an den Client sendet von jedem Rootprozess des Legacy Betriebssystems gelesen werden können.

Sowohl beim Design der Serveranwendung, als auch bei deren Implementierung muss besonders viel Wert auf die Sicherheit und Korrektheit gelegt werden, da ein Implementierungsfehler (Buffer Overflow) die gesamte TCB gefährdet.

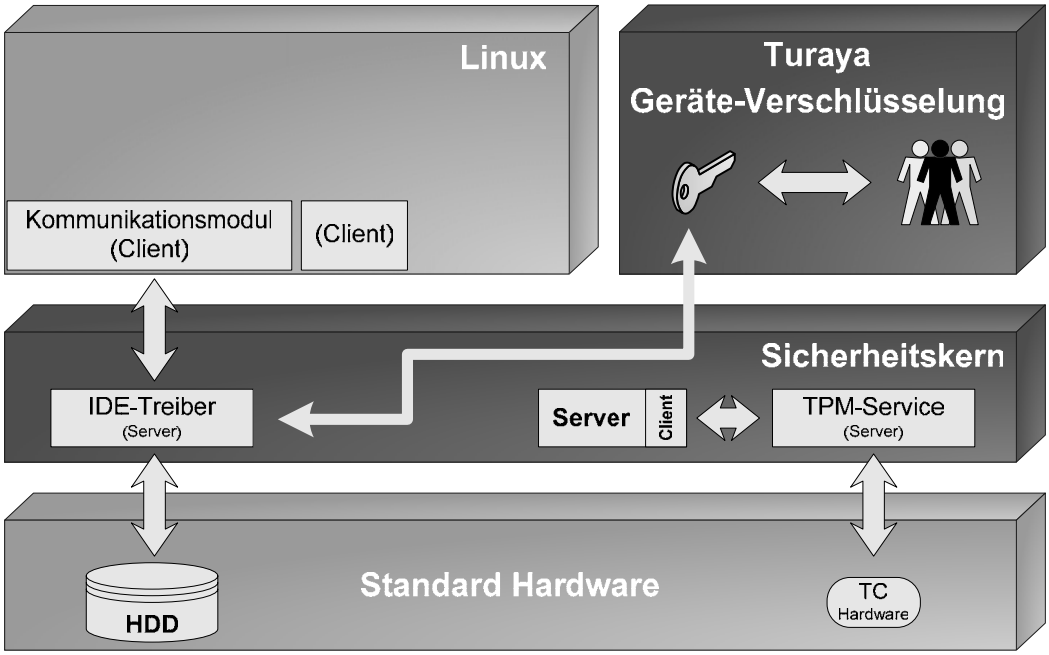

Abb. 3: Das Client-Server-Konzept der TCB am Beispiel der Festplattenverschlüsselung

4.1 Die Entwicklung sicherer Applikationen

Die Entwicklung von Anwendungen auf Turaya-Basis erfordert ein hohes Maß an Planung und Vorbereitung. Ein bereits definiertes Interface zwischen Client und Server lässt sich später nur schwer ohne grundlegende Modifikation des gesamten Servers verändern.

Bei der Entwicklung von Client und Server wird ein IDL (Interface Description Language)-Compiler verwendet. Mit Hilfe dieses Compilers wird das Interface zwischen Client und Server definiert. Sämtliche Aufrufe des Clients für den Server werden mit allen Parametern und ihren Datenrichtung in der IDL Sprache beschrieben. Der Compiler erstellt alle benötigten (Header-)Dateien für den Client und den Server. Die Funktionen im entstandenen Grundgerüst müssen nun vom Entwickler implementiert werden.

Der Client verwendet die vom IDL-Compiler generierten (Header- und Source-)Dateien in denen alle beschriebenen Interfacefunktionen implementiert sind. Diese Interfacefunktionen senden die Client-Aufrufe über IPC an den entsprechenden Server der innerhalb der TCB existieren muss.

Der vom IDL-Compiler generierte Sourcecode des Servers enthält standardmäßig eine Plausibilitätsprüfung aller übergebenen Parameter und muss um die eigentliche Aufgabe der Serverfunktionen erweitert werden. Der Server ist ein Modul der Sicherheitsplattform und wird vom „Trusted Bootloader“ beim Start des Rechners geladen. Während dieses Vorgangs wird der Server gemessen, das bedeutet, dass ein Hash der Binärdatei berechnet wird, der im TPM (genau in den PCR Registern des TPM) gespeichert wird. Somit ist man in der Lage eine Veränderung des Servers durch Viren oder Trojaner zu erkennen und entsprechend zu handeln.

Jeder Server kann weitere Threads starten oder Aufrufe an vorhandene Threads delegieren. Um komplexe Aufgaben zu erledigen, ist es dem Server möglich weitere Server aus der TCB zu verwenden. Dazu müssen lediglich die entsprechenden Header und die Sourcen des zu verwendenden Servers eingesetzt werden. Es ist sichergestellt, dass ein Server sowohl von

Clients aus einem Legacy Betriebssystem, als auch von Clients aus der TCB aufgerufen werden können.

4.2 Beispiele für Server der Trusted Computing Base

Um ein Gespür für die eingesetzten Server und deren Funktionen zu bekommen, werden im Folgenden einige beispielhaft aufgeführt:

Application Manager

Teil von Turaya ist ein Application Manager über den die verschiedenen Module geladen und verwaltet werden. Der Application Manager verfügt über detaillierte Informationen der Clients, da sich jeder Client beim Application Manager anmelden muss, um einen Server verwenden zu können. Der Server nutzt diese Informationen, um eine verlässliche Aussage darüber treffen zu können, welche Sicherheitsstufe der Aufrufende Client besitzt.

User Manager

Unabhängig vom Login des Legacy Betriebssystem besitzt Turaya eine eigene User Verwaltung. Die Server benötigen Informationen darüber, welcher Nutzer aktuell am System angemeldet ist. Diese Informationen stellt der User Manager zur Verfügung. Das Login des Users wird unabhängig von jeglichem Legacy Betriebssystem vorgenommen. Ein Server kann über den User Manager den Login von Usern prüfen oder initiieren.

Storage Manager

Der Storage Manager ist der einzige Server innerhalb der TCB, der in der Lage ist Daten persistent zu Speichern. Jeder Server der TCB ist zwingend mit dem Storage Manager verbunden.

TPM Service

Dieser Service verwaltet die Zugriffe auf den TPM und stellt eine Virtualisierungsschicht zwischen den Servern und dem TPM da. Alle Prozesse, die den TPM verwenden, müssen über den TPM Service auf ihn zugreifen.

5 Anwendungen

Die Sicherheitsplattform Turaya ermöglicht die Realisierung von Geschäftsmodellen in Bereichen, die auf die Existenz (verteilter) vertrauenswürdiger Dritter angewiesen oder dadurch erheblich effizienter zu gestalten sind. Im Folgenden werden die wichtigsten Anwendungen vorgestellt, wobei als erster Entwicklungsschritt die Realisierung neuer, sicherer und fairer DRM-Geschäftsmodelle betrachtet werden soll.

5.1 Multilaterally Policy Enforcement

Existierende technische Maßnahmen zur Handhabung von Urheberrechten im Bezug auf digitale Inhalte und Dienste können bisher nur einen mäßigen Erfolg für die Anbieter vorweisen. Dies gilt ebenso für die entsprechenden Endgeräte, da die meisten dieser technischen Lösungen aufgrund fehlender Manipulationssicherheit der Hardware oder Software vollständig von ihren Benutzern umgangen werden können und somit keine ausreichende Sicherheit bieten.

Im Gegensatz zu bisherigen unsicheren Lösungen kann die Sicherheitsplattform Turaya die Realisierung von sicheren DRM-Anwendungen ermöglichen. Insbesondere handelt es sich

hierbei um die Durchsetzung von Lizenzbedingungen, die Konsumenten digitaler Inhalte bereits akzeptiert haben: Beispielsweise soll das System einerseits sicherstellen, dass, je nach vereinbarten Lizenzbedingungen, die Benutzer Online-Informationen (z.B. Reise- und Navigationsinformationen, elektronische Zeitschriften) nur gegen entsprechende Gebühren in Anspruch nehmen und nicht beliebig weiter verbreiten können. Andererseits soll durch die Sicherheitsplattform verhindert werden, dass Anbieter über den angebotenen Dienst Zugriff auf private Informationen des Anwenders erlangen, soweit dies im Vertrag nicht anders vereinbart wurde.

Mögliche Anwendungen der in diesem Projekt entwickelten Rechnerplattform mit kurz- und mittelfristigem Realisierungspotenzial liegen im Bereich der Handhabung von Urheberrechten (beispielsweise bei eLearing, eBooks, Geokarten- und Informationssystemen), sowie im Telematikbereich (Fahrzeugnavigationssysteme). Langfristig ist auch der hoch umsatzträchtige Bereich von Multimediainhalten, wie Audio und Video, ein attraktives Anwendungsfeld, um unerlaubte und großflächige Vervielfältigungen digitaler Inhalte erheblich zu erschweren.

5.2 Sicheres Dokumentenmanagement

Geschäftsprozesse zwischen Unternehmen erfordern häufig den Austausch von sensitiven Daten und Dokumenten (z.B. Finanzbuchhaltung, Patentanträge, technische Kooperationen), deren Verwendung vertraglich reglementiert wird (z.B. durch Geheimhaltungsvereinbarungen). Auch unternehmensintern sind dann technische Schutzmaßnahmen essentiell, die Zugriffe auf Dokumente außerhalb des vorgesehenen Workflows verhindern. So ist beispielsweise zu unterbinden, dass Mitarbeiter geheime Dokumente lesen, sensitive Dokumente (versehentlich oder vorsätzlich) außerhalb des Unternehmens verbreiten oder unbefugte Änderungen vornehmen.

Bisher können Benutzer die Kontrollmechanismen umgehen, indem sie die entsprechenden vorhandenen Funktionen für ihre Zwecke einsetzen oder Softwarekomponenten durch Ausnutzung von Sicherheitslücken manipulieren.

Erst eine Sicherheitsplattform wie EMSCB kann externe und unternehmensweite Sicherheitsregeln mit den ausgetauschten Dokumenten verbinden und zuverlässig durchsetzen (Mandatory Policy Enforcement). Dies stellt die Basis für die Realisierung eines den praktischen Gegebenheiten angepassten Systems mit MultiLevel Security[1] (MLS) dar. MLS-Lösungen existieren zwar bereits, sind aber aufgrund ihrer hohen Komplexität, bzw. ineffizienten Gestaltung, (streng getrennte Hardware) bislang nicht befriedigend.

5.3 Sichere Server und PCs

Eine weitere wichtige Beispielanwendung für eine sichere Rechnerplattform sind Multi-Server-Systeme, bei denen verschiedene sicherheitskritische Dienste - wie beispielsweise eine virtuelle Poststelle und ein Security Gateway - parallel auf einem Server laufen, aber hermetisch gegeneinander abgeschottet werden sollen. Ebenso ist es möglich sichere Firmennetze mit vereilten Clients aufzubauen, da durch den Trusted Computing Support eine hochsichere Hardware-Client-Authentifizierung möglich ist.

[1] Multi Level Security beschreibt die Möglichkeit, dass auf einem System Daten unterschiedlicher Sicherheitsstufen verarbeitet werden können.

5.4 Sichere Endbenutzersysteme

Viele Sicherheitsprobleme entstehen zudem dadurch, dass Unternehmen oder Behörden nicht effektiv verhindern können, dass ihre Mitarbeiter - versehentlich oder absichtlich - gegen Sicherheitsrichtlinien verstoßen. Häufig können Mitarbeiter eigene Programme installieren oder das System anderweitig manipulieren. Insbesondere die bei eCommerce und eGovernment-Anwendungen geforderte Rechtssicherheit kann vor diesem Hintergrund nicht gewährleistet werden. Erst eine Sicherheitsplattform wie Turaya bietet, durch einen geschützten Boot- und Authentifizierungsmechanismus, die notwendige und hinreichende Basis für sicherheitskritische Anwendungen, wie beispielsweise Signaturerzeugung oder Onlinebanking. Insbesondere für Unternehmen eröffnet dies einen deutlichen Sicherheitsgewinn, da sich unternehmensweite Sicherheitsregeln zentral durchsetzen lassen und die Wartung und Sicherheitskonfiguration der IT-Infrastruktur deutlich erleichtert wird.

5.5 Embedded Security

Ein weiterer, wichtiger Anwendungsbereich für die Sicherheitsplattform Turaya ergibt sich aufgrund der stetig steigenden Integration von Computer Plattformen in andere Produkte (Embedded Systems), z.B. in der Automobilindustrie. Die eingesetzte Software wird immer komplexer. Dies führt zu einer erhöhten Fehlerwahrscheinlichkeit, die sich durch Einsatz des Sicherheitskerns über die bereits beschriebenen Konzepte minimieren lässt. Außerdem wird in Zukunft die Integration von Informations- und Multimediasystemen in Kraftfahrzeugen eine immer wichtigere Rolle spielen, wodurch sich für die Hersteller neuartige Marktmöglichkeiten ergeben. Die Sicherheitsplattform Turaya bietet hierfür die notwendige Grundlage und ermöglicht insbesondere der deutschen Automobilindustrie die Entwicklung innovativer Produkte.

5.6 Ergebnisse des Projekts

Die Ergebnisse des Projektes werden in unterschiedlichen Entwicklungsschritten zur Verfügung gestellt. Die Entwicklungsschritte sind:

- Festplattenverschlüsselung (November 2005),
- Zertifikatsmanagement (Februar 2006),
- Faires DRM (Dezember 2006),
- Dokumentenmanagement (Dezember 2007 mit SAP) und
- DRM-Anwendung für Embedded Systems (Dezember 2007 mit Bosch/Blaupunkt).

Der erste Entwicklungsschritt, eine Festplattenverschlüsselung auf Basis des EMSCB-Sicherheitskerns und der TPM-Hardware ist bereits abgeschlossen und steht zur Verfügung.

6 Konsortium und Kompetenzzentrum

Um dieses Vorhaben in die Tat umzusetzen, wurde ein Konsortium gebildet, das das notwendige Know-How in sich vereint. Es besteht aus den Hochschuleinrichtungen eurobits, Ruhruniversität Bochum, dem Institut für Internet-Sicherheit, FH Gelsenkirchen und dem Institut für Systemarchitektur, TU Dresden, sowie den Unternehmen escrypt GmbH und Sirrix AG. Als strategische Firmenpartner sind SAP und Bosch/Blaupunkt mit von der Partie. Das Projekt wird vom Bundesministerium für Wirtschaft und Technologie BMWi gefördert.

Basierend auf dem Konsortium wird ein Kompetenzzentrum aufgebaut, dem die Aufgabe zukommt das Wissen über die Sicherheitsplattform zu bündeln und darzustellen. Das vereint auch alle angewandten Technologien, wie Trusted Computing oder den Einsatz von Mikrokernen. Auf lange Sicht wird forciert offene Standards im Bereich sichere Computerplattformen zu erreichen. Zum Ausbau der Vorreiterstellung in diesen Bereichen werden Partnerschaften mit Firmen, Instituten und weiteren Einrichtungen angestrebt, nicht zuletzt um den Technologiestandort Deutschland zu fördern.

7 Ausblick

Die vorgestellte Architektur ist kompatibel zu existierenden Betriebssystemen. Die zukünftige Bedeutung von TC-unterstützten Betriebssystemen wird durch die beständigen Anstrengungen des bisherigen Monopolanbieters Microsoft im Zusammenhang mit der Entwicklung ihrer Sicherheitsplatttform, der Next Generation Secure Computing Base (NGSCB), untermauert. Eine alternative, offene Sicherheitsplattform macht sicherheitskritische Anwendungen unabhängig von einzelnen Betriebssystemanbietern und sichert somit auch in Zukunft die Einsatzfähigkeit solcher Systeme vor dem Hintergrund neuer Erfordernisse.

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. In der momentanen Entwicklungsphase steht fest, dass EMSCB unter den Open-Source Lizenzen GPL (Plattform) und LGPL (Libs) veröffentlicht wird. Eventuell werden weitere Lizenzen hinzukommen. EMSCB ermöglicht daher nicht zuletzt auch der OpenSource- und Linux-Gemeinde „konkurrenzfähig“ zu bleiben.

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

Der erste Meilenstein ist 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.

Literatur

[Trus05] Trusted Computing Group: Mobile Phone Work Group.
In: https://www.trustedcomputinggroup.org/groups/mobile (2005)

[Kay05] Roger L. Kay: The Future of Trusted Computing.
In: https://www.trustedcomputinggroup.org/home/IDC_Presentation.pdf (2005)

[Vert05] Vertrauenskrise, Einsichten und Aussagen vom Trusted-Computing-Symposium.
In: kes (2003*4) 20

[Doll04] Wilhelm Dolle: Trusted Computing: Stand der Dinge. In: kes (2004*4) 20

[Casp04] Thomas Caspers: Der schmale Grad zwischen Vertrauensbeweisen und Datenschutz. In: BSI-Forum/kes (2004*6) 35

[Trus06] Trusted Computing Group (TCG) In: www.trustedcomputinggroup.org (2006)

[SaSP05] Ahmad-Reza Sadeghi, Christian Stüble, Norbert 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