Allseits vertrauenswürdig

European Multilaterally Secure Computing Base (EMSCB)

Das EMSCB-Projekt will eine vertrauenswürdige, faire und offene Sicherheitsplattform schaffen, welche die Interessen von Anbietern und Nutzern gleichermaßen schützt und eine neutrale technische Sicherungsschicht zwischen Trusted-Computing-Hardware und klassischem Betriebssystem einschiebt.

Von Norbert Pohlmann, Gelsenkirchen, Ahmad-Reza Sadeghi und Christian Stüble, Bochum

Heutige Betriebssysteme bergen immense Risiken. Viele innovative Geschäftsideen ersticken im Keim, weil die Missbrauchsgefahr zu hoch erscheint. Anwendungen 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 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 und mehr zeigt deutlich, dass wir eine Sicherheitsplattform benötigen, der alle Seiten vertrauen können: Eine multilaterale Sicherheitsplattform, die wirklich sichere Anwendungen ermöglicht.

Aus diesem Grund hat sich ein Konsortium aus Wirtschaft und Wissenschaft zum Projekt EMSCB – European Multilaterally Secure Computing Base – zusammengeschlossen, das diese dringend notwendige vertrauenswürdige, faire und offene Sicherheitsplattform gemeinsam entwickeln will (www.emscb.de). Das Konsortium besteht aus den Hochschuleinrichtungen eurobits an der Ruhr-Universität Bochum, dem Institut für Internet-Sicherheit der FH Gelsenkirchen und dem Institut für Systemarchitektur der 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 zudem vom Bundesministerium für Wirtschaft und Arbeit (BMWA) gefördert.

Motivation

Aktuelle Sicherheitsmechanismen wie Smartcards oder Firewall-Systeme können die Sicherheit existierender Betriebssysteme nicht entscheidend verbessern, weil sie immer nur Teilaspekte betrachten. Die Identifizierung und Beseitigung konzeptioneller Schwachstellen vorhandener Betriebssysteme führt daher zum kontinuierlichen Ausbessern von Fehlern und Sicherheitslücken durch Patches.

Um dennoch eine Sicherheitsplattform für kritische Geschäftsanwendungen bieten zu können, hat die Trusted Computing Group (TCG) als sichere Hardwarekomponente das Trusted Platform Module (TPM) entwickelt und zur Verfügung gestellt (vgl. [1,2,3,4]). Diese Spezifikation soll als Grundlage für die Realisierung eines durchgängig sicheren Betriebssystems dienen.

Mit der Next Generation Secure Computing Base (NGSCB, s. [5,6]) hat Microsoft eine auf der TCG-Spezifikation basierende Sicherheitsplattform in Aussicht gestellt, die in kommende Windows-Versionen integriert werden soll. Im Moment erscheint unklar, wie viel davon bereits in Windows Vista (vormals: Longhorn) umgesetzt wird (vgl. [7,8]).

EMSCB versteht sich als offene Alternative und will die Funktionen jeglicher Trusted-Computing-(TC)-Hardware als Black-Box benutzen und daher sowohl in Kombination mit einem TPM als auch mit möglicher anderer NGSCB-Hardware und zukünftiger TC-Technik benutzbar sein. Ein wesentlicher Aspekt bei EMSCB ist zudem die Durchsetzung *multilateraler* Sicherheit.

Anforderungen

Der Einsatz komplexer Applikationen und die rapide Zunahme der Vernetzung von Rechnersystemen stellen uns vor neue Herausforderungen hinsichtlich ihrer Sicherheit und Benutzbarkeit. Heute beschränken sich diese Anwendungen nicht mehr auf PC- und Server-Systeme von Unternehmen. Neue Geschäftsmodelle erfordern die Realisierung solcher Anwendungen bis hin zu eingebetteten Systemen in mobilen Geräten (PDAs, SmartPhones) sowie im Automobilbereich (PS-Steuerung, Infotainment).

In diesem Zusammenhang agieren verschiedene Parteien mit unterschiedlichen Interessen und Sicherheitsstrategien: Während für Endbenutzer Datenschutzaspekte

verstärkt von Bedeutung sind, stellen für Unternehmen und Behörden die sichere und vertrauliche Behandlung wichtiger Daten sowie der Schutz von Urheberrechten und Lizenzen gegen unautorisierte Verbreitung und Nutzung relevante Aspekte dar. Man benötigt daher multilaterale Sicherheit. Hinzu kommt, dass mit der zunehmenden Vernetzung von IT-Systemen auch die Gefahren und folglich die Sicherheitsanforderungen an die zugrunde liegenden Rechnerplattformen und die verwendete Software wachsen. Die heutigen Applikationen fordern Endgeräte, die Sicherheitsziele wie Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit im Sinne multilateraler Sicherheit garantieren können.

Die Erfahrungen der letzten Jahre zeigen, dass existierende Rechnerplattformen, vor allem die heutigen Betriebssysteme, diese Sicherheitsanforderungen nicht im gewünschten Maße erfüllen. Dies wird vor allem durch die Vielzahl von Exploits, Viren, Würmern und Trojaner-Angriffen sowie notwendigen Sicherheits-Updates bestätigt. Die Ursachen sind vielfältig und liegen sowohl in den heutigen Betriebssystemen als auch in der verwendeten Hardware begründet. Einige wichtige Probleme sind:

_____ Schutz zwischen Anwendungen: Übliche Betriebssysteme bieten keine angemessenen Mechanismen, um verschiedene Applikationen voreinander zu schützen.

_____ Installation: Es gibt kein generelles Verfahren, das die Korrektheit eines Programms feststellt oder dessen Zugriffsrechte auf Systemressourcen einschränkt.

_____ Es fehlen Authentifizierungmöglichkeiten für Programme gegenüber dem Benutzer.

_____ Darstellungsproblem: Digital signierte Dokumente können zwar nicht unbemerkt verändert werden, aber die Präsentation oder auch das Dokument selbst können vor einem Signiervorgang möglicherweise manipuliert worden sein (What You See Is *Not* What You Get). Außerdem werden Dokumente auf unterschiedlichen (Sicherheits-)Plattformen möglicherweise unterschiedlich dargestellt.

_____ Unsichere Hardware: Auch bei einem korrekt implementierten Betriebssystem können sicherheitsrelevante Systemkomponenten umgangen werden, zum Beispiel indem Applikationen direkter Zugriff auf die Hardware gewährt wird (häufig aus Performance-Gründen).

Heutige IT-Sicherheitsmechanismen wie Kryptographie, Firewalls, Virenschutz- und Intrusion-Detection-Systeme sowie Smartcards können offenbar die Benutzer vor Manipulationen, böswilligen Codes (Malware) sowie Konfigurationsfehlern nicht effektiv genug schützen.

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

Aufgrund konzeptioneller Schwächen in Betriebssystemen (z. B. ihre monolithische Struktur) und hoher Komplexität ist nicht zu erwarten, dass sich die Sicherheit der Rechnerplattformen in den nächsten Jahren entscheidend verbessern kann; dies betrifft wohlbemerkt sowohl Windows- als auch Linux-basierte Betriebssysteme. Die dadurch bestehenden Bedrohungen verzögern oder verhindern dabei die Realisierung vieler nützlicher Anwendun-

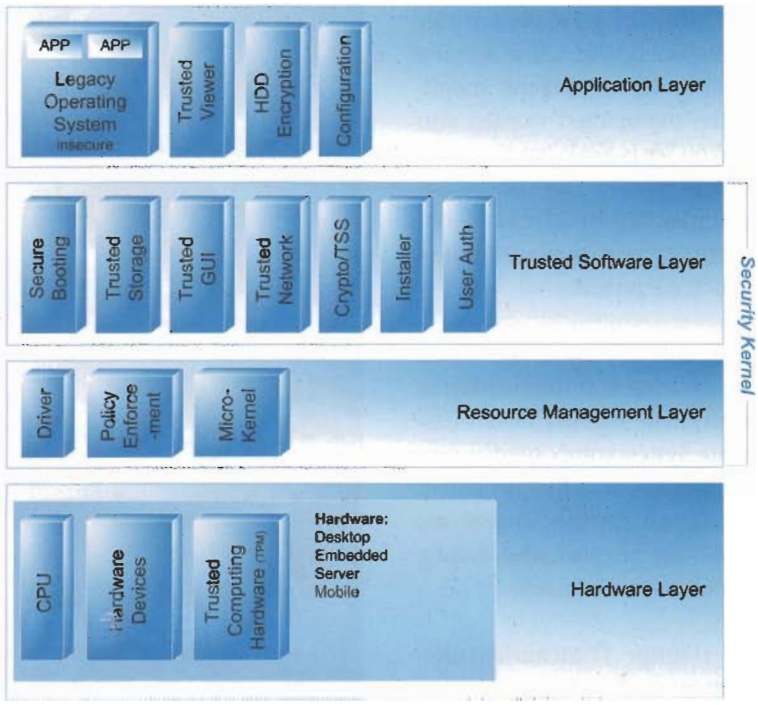

Abbildung 1: Security Layer fungieren als Kontrollinstanz zwischen konventionellem Betriebssystem, sicherheitskritischen Anwendungen und der Hardware

gen 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-(TC)-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 letztlich Zugriff auf alle sicherheitsrelevanten Informationen. Bisher existiert keine vertrauenswürdige, faire und offene Sicherheitsplattform, die basierend auf den Spezifikationen der TCG die notwendige Grundlage für die Realisierung multilateral sicherer Anwendungen böte.

EMSCB

Eben hier will die European Multilaterally Secure Computing Base (EMSCB) als vertrauenswürdige, faire und offene Sicherheitsplattform ansetzen und als zusätzliche Sicherheitsebene existierende Betriebssysteme mit einem Security Kernel und TC-Hardware kombinieren (vgl. Abb. 1). Wesentliche Aspekte und Komponenten der geplanten Sicherheitplattform EMSCB sind im Folgenden aufgeführt.

Trusted-Computing-Support

Trusted Computing stellt erstmalig Hardware bereit, die eine geeignete Grundlage für die Realisierung eines durchgängig sicheren Betriebssystems bildet. Somit besteht die Möglichkeit der Integritätsprüfung der zugrunde liegenden Rechnerplattform (Attestation), des Bindens geheimer Schlüssel an eine Plattformkonfiguration (Sealing), der Erzeugung sicherer Zufallszahlen und der sicheren Speicherung von kryptographischen Schlüsseln.

Hardwareunabhängigkeit

Die EMSCB-Sicherheitsplattform soll universell sein, das heißt unabhängig von der konkreten Realisierung der TC-Hardware. Sie soll vom durch die Trusted Computing Group (TCG) spezifizierten und bereits verfügbaren TPM-Chip ebenso wie von der gegen Ende 2005 erwarteten La-Grande-Technologie profitieren, die Intel im Zusammenhang mit Microsoft NGSCB entwickelt hat.

Trusted Software Layer

Bei diesem Security Software Layer handelt es sich um einen sehr kleinen Open-Source-Sicherheitskern, der alle kritischen Hardwareressourcen (inkl. TC-Hardware) Policy-basiert kontrolliert beziehungsweise virtualisiert und damit sicherheitskritische Anwendungen und Daten schützen kann.

Ressource Management Layer

Der Ressource Management Layer hat hauptsächlich die Aufgabe, eine abstrakte Schnittstelle zu darunter liegenden Hardware-Ressourcen (z. B. Interrupts, Speicher etc.) zur Verfügung zu stellen. In dieser Schicht werden die Ressourcen über eine konfigurierbare Policy kontrolliert. Der Ressource Management Layer besteht aus einem Micro-Kernel, einem Enforcement-Modul und einem speziellen vertrauenswürdigen Treiber.

Secure Application

Basierend auf der zur Verfügung gestellten Schnittstelle können sicherheitskritische Anwendungen (digitale Signaturen, DRM etc.) ausgeführt werden, welche die neuen Möglichkeiten der TC-Hardware 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.

Existierende Betriebssysteme

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

Multilaterale Sicherheit

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

Kritiker des Trusted Computing geben zu bedenken, dass die eingeschränkte Kontrolle durch den Endbenutzer prinzipiell auch dazu genutzt werden kann, Zensur auszuüben, die Privatsphäre der Anwender zu verletzen oder ihre Rechte einzuschränken. Dieser inhärente Konflikt zwischen den Interessen und Sicherheitsanforderungen der Endbenutzer (Schutz der Privatsphäre und Selbstbestimmung) gegenüber denen der Inhalte- und Anwendungsanbieter kann nur durch eine multilateral vertrauenswürdige, faire und offene Sicherheitsplattform gelöst werden, die eine Ausgewogenheit zwischen den Interessen aller beteiligten Parteien garantiert. Daher vergleicht die EMSCB-Sicherheitsplattform die vom Benutzer geforderten Sicherheitsanforderungen mit den Lizenzbedingungen zu installierender Anwendungen und verhindert im Konfliktfall deren Installation.

Offene Architektur

Aufgrund einer offenen Architektur und auf sinnvollem Niveau gehaltenen Komplexität sicherheitskritischer Komponenten weist EMSCB eine hohe Vertrauenswürdigkeit auf, nicht zuletzt durch verringerte Fehlerwahrscheinlichkeit im Entwicklungs- und Wartungsprozess.

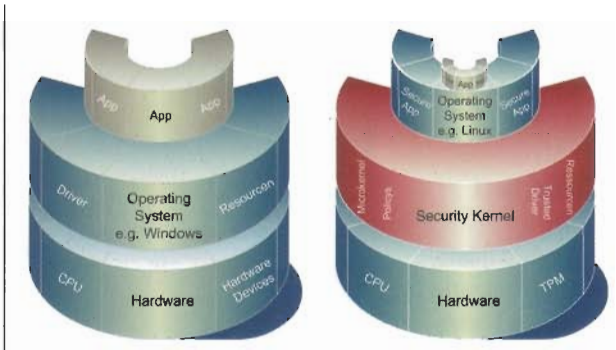

Abbildung 2: Standard-System-Architektur im Vergleich zu EMSCB mit Sicherheitskern

Darüber hinaus wird eine Evaluierung nach Sicherheitsstandards möglich (bspw. den Common Criteria).

Die Sicherheitsplattform ist zudem so konzipiert, dass sie sich effizient auf weitere Geräte portieren lässt, beispielsweise auf Personal Digital Assistants (PDAs), Smartphones und Embedded Systems. Weitere Anwendungen können Multimedia- und Informationssysteme in Kraftfahrzeugen sein.

Anwendungen

EMSCB ermöglicht vor allem auch 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 angegangen werden soll.

Multilateral Policy Enforcement

Existierende technische Maßnahmen zur Handhabung von Urheberrechten auf digitale Inhalte oder Dienste sowie die entsprechenden Endgeräte können bisher nur einen mäßigen Erfolg vorweisen, da die meisten Lösungen aufgrund fehlender Manipulationssicherheit der Hard- oder Software vollständig von ihren Benutzern umgangen werden können und somit keine ausreichende Sicherheit bieten.

EMSCB will hier Abhilfe schaffen. Ein wesentlicher Punkt ist hierbei die Durchsetzung von Lizenzbedingungen, die Konsumenten digitaler Inhalte bereits akzeptiert haben: Beispielsweise soll das System einerseits sicherstellen, dass – je nach vereinbarten Lizenzbedingungen – 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 aber auch verhindert werden, dass Anbieter über den angebotenen Dienst Kenntnis von privaten Benutzerinformationen erlangen, soweit dies nicht im Vertrag vereinbart wurde und soweit dies den Sicherheitsregeln des Benutzers widerspricht.

Sicheres Dokumentenmanagement

Geschäftsprozesse zwischen Unternehmen erfordern häufig den Austausch sensitiver Daten und Dokumente (z. B. Finanzbuchhaltung, Patentanträge, technische Kooperationen), deren Verwendung vertraglich reglementiert wird (z. B. durch Geheimhaltungsvereinbarungen). Auch unternehmensintern sind dann technische Schutzmaßnahmen essenziell, 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.

Existierende Rechnerplattformen können auch hier keinen wirksamen Schutz bieten. Erst eine Sicherheitsplattform 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 prakti-

Literatur

[1] Vertrauenskrise, Einsichten und Aussagen vom Trusted-Computing-Symposium, <kes> 2003#4, S. 12

[2] Wilhelm Dolle, Trusted Computing: Stand der Dinge, <kes> 2004#4, S. 20

[3] Thomas Caspers, Der schmale Grat zwischen Vertrauensbeweisen und Datenschutz, BSI-Forum/<kes> 2004#6, S. 35

[4] Trusted Computing Group (TCG), www.trustedcomputinggroup.org

[5] Microsoft Next-Generation Secure Computing Base (NGSCB), Homepage, www.microsoft.com/resources/ngscb/

[6] Microsoft Next-Generation Secure Computing Base, Technical FAQ, www.microsoft.com/technet/archive/security/news/ngscb.mspx

[7] Microsoft, Trusted Platform Module Services in Windows Longhorn, www.microsoft.com/resources/ngscb/WinHEC05.mspx

[8] Microsoft Technet, Security and Protection in Windows Vista, www.microsoft.com/technet/windowsvista/secprot/

[9] European Multilaterally Secure Computing Base, The EMSCB Project, www.emscb.de

schen Gegebenheiten angepassten Systems mit Multi Level Security (MLS) dar – MLS-Lösungen existieren zwar bereits, sind aber aufgrund ihrer hohen Komplexität beziehungsweise ineffizienten Gestaltung (streng getrennte Hardware) bislang nicht befriedigend.

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.

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 IT-System anderweitig manipulieren. Insbesondere die bei E-Commerce- und E-Government-Anwendungen geforderte Rechtssicherheit kann vor diesem Hintergrund nicht gewährleistet werden. Erst eine Sicherheitsplattform bietet durch einen geschützten Boot- und Authentifizierungsmechanismus die notwendige und hinreichende Basis für sicherheitskritische Anwendungen wie beispielsweise Signaturerzeugung oder auch Homebanking.

Fazit

Mit EMSCB soll eine vertrauenswürdige, faire und offene Sicherheitsplattform geschaffen werden, die allen Anwendungsentwicklern gleiche Marktchancen bietet. Sämtliche Programmierschnittstellen von EMSCB und der Source-Code aller sicherheitskritischen Komponenten werden zu Evaluierungszwecken offen gelegt, um die Vertrauenswürdigkeit der Implementierung zu erhöhen. EMSCB ermöglicht daher nicht zuletzt auch der Open-Source- und Linux-Gemeinde, „konkurrenzfähig" zu bleiben.

EMSCB bietet zudem den Vorteil, dass alle sicherheitskritischen Komponenten und Anwendungen unabhängig vom „klassischen" Betriebssystem agieren können und damit für zukünftige plattformübergreifende, verteilte Anwendungen optimal geeignet sind. ■

Prof. Dr. Norbert Pohlmann (norbert.pohlmann@informatik.fh-gelsenkirchen.de) ist Leiter des Instituts für Internet-Sicherheit der FH Gelsenkirchen. Prof. Dr.-Ing. Ahmad-Reza Sadeghi (sadeghi@crypto.rub.de) ist Leiter der Forschungsgruppe für angewandte Datensicherheit des Horst Görtz Institut für Sicherheit in der Informationstechnik / eurobits der Ruhr-Universität Bochum. Christian Stüble (stueble@acm.org) ist technischer Projektleiter von EMSCB.