Sicherheitsgewinn durch vertrauenswürdige IT-Systeme

Eine Diskussion über Trusted Computing

Trusted Computing (TC) ist eine seit ihrer Einführung kontrovers diskutierte IT-Sicherheits- und Vertrauenswürdigkeitstechnologie. Seitdem stehen sich Befürworter und Gegner oft uneinsichtig gegenüber. Die Befürworter betonen die Möglichkeiten dieser modernen und intelligenten Technik, um für mehr Robustheit und ein höheres Sicherheitsniveau auf einem IT-System zu sorgen, während die Gegner oftmals nur die nutzereinschränkende Seite in den Vordergrund stellen. Dabei haben beide Seiten gleichermaßen Recht in ihrer Einschätzung. Trusted Computing bietet sowohl eine Grundlage für weiterführende IT-Sicherheits- und Vertrauenswürdigkeitstechnologie, als auch die Möglichkeit, die Nutzer bewusst in ihrem Handeln einzuschränken. Dieser Artikel beleuchtet beide Seiten und versucht, aus persönlichen Erfahrungen und Einschätzungen heraus, aufzuzeigen, warum Trusted Computing heute noch nicht so eingesetzt wird, wie es eigentlich möglich wäre und sein sollte. Darüber hinaus gehen wir darauf ein, welche heutigen IT-Sicherheits- und Vertrauenswürdigkeitsprobleme mit Trusted Computing zu lösen wären.

Der Begriff des Trusted Computing wurde primär durch die Trusted Computing Group (1) (TCG) geprägt, welche die grundlegenden Spezifikationen für ein vertrauenswürdiges IT-System erarbeitet hat. Die TCG ist ein Industriekonsortium, zusammengeschlossen aus über 170 Firmen. Darunter befinden sich Weltmarktführer wie Microsoft, Intel, AMD, HP, IBM, Cisco und Infineon, aber auch deutsche Hersteller wie zum Beispiel Sophos und Sirrix. Die Gruppe hat sich zur Aufgabe gemacht, offene Spezifikationen für vertrauenswürdige IT-Systeme zu entwickeln, um die IT-Sicherheit verteilter Anwendungen mit vertretbarem Aufwand zu erhöhen. Kern aller Bemühungen der TCG ist die Bildung einer „Trusted Platform", einer sicheren und vertrauenswürdigen Basis für Anwendungen. Die Trusted Platform, in der Form einer Sicherheitsplattform (2), stellt auf der Basis von intelligenten kryptographischen Verfahren eine sichere Umgebung zum Schutz von sicherheitskritischen Daten für sicherheitskritische Operationen bereit, die sehr viele heutige IT-Sicherheitsprobleme reduzieren würde.

Sehen wir uns nun an, mit welcher Sicherheitsarchitektur, mit welchen Sicherheitsprinzipien und IT-Sicherheitsmechanismen ein vertrauenswürdiges IT-System aufgebaut werden kann. Beginnen wir mit den Sicherheitsaspekten, die die Robustheit und die Modularität betreffen.

Trusted Computing Base (TCB): Per Definition ist die „Trusted Computing Base" der kritische Teil eines IT-Systems. Wenn im TCB eine Schwachstelle vorhanden ist, dann ist das ganze IT-System betroffen. Gibt es außerhalb der TCB eine Schwachstelle, kann anhand einer Sicherheitspolicy der potenzielle Schaden sehr eingeschränkt

und beschrieben werden. Aus diesem Grund ist eine TCB sehr sorgfältige designt und implementiert. Eine auf einem Micro-Kernel basierende TCB hat etwa 100.000 Code-Zeilen und ist von daher eine sehr vertrauenswürdige Basis, die in der Regel auch schon semiformal verifiziert werden kann. Es gibt aber auch TCBs, die beispielsweise aus einem sehr abgespeckten und speziell gehärteten Linux bestehen, das auch schon vertrauenswürdiger ist als übliche Betriebssysteme.

Ein weiterer Sicherheitsaspekt ist die Virtualisierung. Hier kann der Robustheitsvorteil genutzt werden, der schon seit langem bei Servern genutzt wird. Es ist sehr einfach möglich, die verschiedenen virtuellen Maschinen wieder in einen stabilen Urzustand zu versetzen und von da aus neu zu starten.

Der Sicherheitsaspekt Isolierung sorgt dafür, dass die virtuellen Maschinen isoliert und sicher getrennt voneinander laufen und sich nicht gegenseitig beeinflussen können. Daher haben Schwachstellen in einer isolierten virtuellen Maschine keinen Einfluss auf die anderen virtuellen Maschinen. Eine solche stark isolierte virtuelle Maschine wird im Bereich von TC auch Compartment (3) genannt.

Der Sicherheitsaspekt der Modularisierung gibt uns die Möglichkeit, Anwendungen, die zusammengehören, in einer virtuellen Maschine laufen zu lassen, und Anwendungen, die getrennt sein sollten, in verschiedenen virtuellen Maschinen zu positionieren. Hier haben wir einen interessanten Gestaltungsspielraum, mit dem sehr hohe IT-Sicherheit erzielt werden kann, weil für verschiedene Sicherheitsprobleme unterschiedliche virtuelle Maschinen genutzt werden können.

Mit dem generellen Sicherheitsaspekt „Integritätsüberprüfung" kann die Integrität und damit der vertrauenswürdige Zustand eines IT-Systems überprüft werden. Der Trusted Software Layer stellt dazu vertrauenswürdige Sicherheitsdienste zur Verfügung, die helfen, IT-Systeme (Hardware, Software und Konfigurationen) vertrauenswürdig zu gestalten und messbar zu machen. Das Security Module ist zum Beispiel ein TPM (Trusted Platform Module) mit intelligenten kryptographischen Verfahren auf dem Level von SmartCard-Sicherheit, ergänzt um weitere Sicherheitsdienste wie das Platform Configuration Register (PCR), welches die sichere Speicherung und Überprüfung von Messdaten organisiert. Das TPM ist ein kleiner passiver Sicherheitschip, der fest mit dem Mainboard verbunden ist. Die Vorteile eines Sicherheitsmoduls sind:

- hohe Sicherheit bei geringer Investitionssumme, da ein TPM nicht mehr als einen Euro kostet.
- weite Verfügbarkeit auf dem überwiegenden Teil der IT-Systeme. Das heißt, die flächendeckende Einführung einer Sicherheitsplattform ist einfach. Zum aktuellen Zeitpunkt wurden bereits weit über 300 Millionen TPMs verbaut.
- Einbindung in eine Sicherheitsinfrastruktur (PKI …). Die Module sind daher einfach im Sicherheitsmanagement zu behandeln.

Trusted Boot sorgt dafür, dass das IT-System nur in einem definierten vertrauenswürdigen Zustand aktiv wird. Remote Attestation gibt die Möglichkeit, die Vertrauenswürdigkeit von anderen, auch fremden IT-Systemen zu messen, bevor eine Interaktion mit diesem IT-System begonnen wird. Binding und Sealing sind weitere Trusted-Computing-Funktionen, mit denen moderne IT-Sicherheitssysteme intelligent umgesetzt werden können. Unter dem Begriff Trusted Interaction werden Sicherheitsdienste im Trusted Software Layer zusammengefasst, die dafür sorgen, dass Informationen vertrauenswürdig eingegeben, gespeichert, übertragen und dargestellt werden können. Trusted Process vereint die Sicherheitsaspekte, welche die Abläufe in den und mit den verschiedenen IT-Systemen betreffen.

Security Management fasst die wichtigen Funktionen zusammen, die notwendig sind, um das proaktive Sicherheitssystem vertrauenswürdig nutzbar zu machen. Mithilfe des Policy Enforcement sind wir in der Lage, die definierte Regel auf unserem eigenen, aber auch auf fremden IT-Systemen vertrauenswürdig umzusetzen. All diese Sicherheitsaspekte zusammen stellen die vertrauenswürdige Basis, eine Trusted Platform, dar.

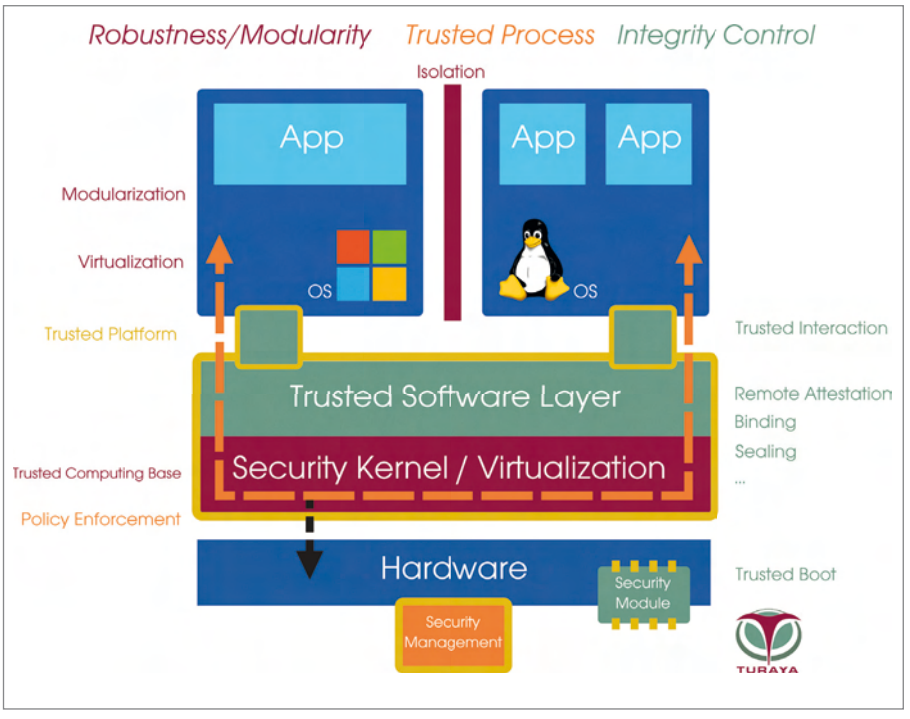

Bild 1: Architektur der Trusted Computing-Plattform. Quelle: ifis

Das Für und Wider einer modernen und intelligenten IT-Sicherheits- und Vertrauenswürdigkeitstechnologie

Oft wird im Zusammenhang mit dem Begriff Trusted Computing ein negatives Bild assoziiert, das meist aus Vorurteilen und einseitigen Darstellungen entstanden ist.

Kurz nach Einführung der Spezifikationen, insbesondere der des Trusted Platform Module, wurden die ersten Stimmen aus der Industrie laut, diese IT-Sicherheits- und Vertrauenswürdigkeitstechnologie zur Sicherung von Marktpositionen und multimedialen Inhalten zu nutzen. Hierbei wurde die einseitige Ausnutzung von Digital Rights Management (DRM) schnell in Bezug zu Trusted Computing und den TPMs gebracht. Inhaltlich drehten sich die Diskussionen um die Bindung von Inhalten an eine bestimmte Hardware, welche das ungehinderte Kopieren von Inhalten auf weitere IT-Systeme unterbinden soll. Auch wenn in den folgenden Jahren von Seiten der Content-Industrie primär in Bezug auf digital verbreitete Musik von DRM Abstand genommen wurde, ist die Assoziation in vielen Köpfen erhalten geblieben und damit auch der schlechte Ruf dieser TC-Technologie. Analog dazu gab es ebenfalls Diskussionen, diese IT-Sicherheits- und Vertrauenswürdigkeitstechnologie zur Einschränkung von Soft- und Hardware zu nutzen. So ließe sich ein IT-System realisieren, das nur noch Software eines bestimmten Herstellers erlaubt. Dies ist bei Betriebssystemherstellern besonders kritisch zu betrachten. Oder IT-Systeme, die nur noch die Hardware eines bestimmten Herstellers unterstützen, da nur entsprechende, an das IT-System gebundene Treiber erlaubt werden. Dies ist unter dem Begriff „Vendor Lock" bekannt.

Natürlich ermöglicht die Trusted-Computing-Technologie all diese Einschränkungen, die ihre Kritiker vorbringen. Genau diese Möglichkeiten erlauben auf der anderen Seite aber auch, die IT-Sicherheit und Vertrauenswürdigkeit eines IT-Systems deutlich zu verbessern. So kann eine Trusted Platform unter anderem auch genutzt werden, um die persönlichen oder beruflich kritischen Daten sicher an ein IT-System zu binden und diese dadurch vor unerlaubtem Zugriff zu schützen sowie deren Integrität vertrauenswürdig sicherzustellen.

IT-Sicherheit und Vertrauenswürdigkeit

Das Thema Trusted Computing muss von mehreren Seiten betrachtet werden. So sind die Vorstellungen der Forschung und der Industrie, trotz häufiger Kooperationen, oftmals voneinander abweichend. Die IT-Industrie hat das Ziel der erfolgreichen Vermarktung, daher sind Innovationen diesem Ziel unterworfen. Ein großes Problem für die europäische IT-Industrie ist, dass sie auf dem Weltmarkt nur eine sehr kleine Rolle spielt. Die Aufgabe der Forschung sollte sein, intelligente Ansätze zu entwickeln, die noch keine direkte Umsetzung für den Nutzer beinhalten müssen, aber in Zukunft unsere Sicherheitsprobleme lösen. Die dritte Gruppe sind die Nutzer, welche die TC-Technologie einsetzen. Ihre Bedürfnisse unterscheiden sich hier oftmals noch einmal deutlich von den beiden anderen Parteien. Einfachheit der Nutzung und der Preis sind hier die leitenden Kriterien für oder gegen die Nutzung neuer und hoffnungsvoller Technologien. Aber auch eine gute Technologie allein kann keine hohe IT-Sicherheit und Vertrauenswürdigkeit garantieren.

Moderne Internetdienste wie soziale Netzwerke sind mit dem Einzug des Web 2.0 aufgekommen und haben sich seitdem in allen Themenbereichen verbreitet. Sie sind nicht mehr wegzudenken. Viele IT-Dienste im Internet sind unserer Einschätzung nach gerade dadurch sehr beliebt, dass diese vermeintlich kostenlos sind. Aber sind sie es wirklich? Kein Unternehmen kann durch die Bereitstellung von kostenlosen Internet-Diensten lange überleben. Auch wenn der Nutzer diese Internet-Dienste nicht kaufen muss, so bezahlt er doch mit seinen persönlichen Daten und Nutzungsinformationen, bei denen er weitere Spuren über sich hinterlässt, die wiederum auf unterschiedliche Arten durch den Anbieter vermarktet werden können.

Wer seine persönlichen Daten besser schützen will, ist hier bereits sehr eingeschränkt. Dabei muss ausdrücklich darauf hingewiesen werden, dass es auch bei kommerziellen Angeboten keine Garantie für die IT-Sicherheit und Vertrauenswürdigkeit der Daten gibt. Besonders sind hierbei die rechtlichen Aspekte der Herkunftsstaaten der Anbieter zu beachten und nicht nur der Standort des Rechenzentrums, über das der jeweilige IT-Dienst bereitgestellt wird, wie zurzeit überall zu lesen ist.

Hinter der intensiven Umsetzung von Cloud Computing steckt weit mehr als nur ein Onlinespeicher. Es werden zunehmend ganze Geschäftsprozesse samt Geschäftsdaten an einen IT-Dienstleister übergeben. Neben dem preislichen Aspekt bleibt die Frage: Wie groß ist mein Vertrauen gegenüber den Anbietern und der eingesetzten IT-Technik? Des Weiteren muss auch ein gänzlich anderes Problem diskutiert werden, denn der Schutz von Privatsphäre in der digitalen Welt ist ebenfalls ein Teil der IT-Sicherheit und insbesondere der Vertrauenswürdigkeit.

Gewinn von Vertrauenswürdigkeit

Welche Möglichkeiten bietet uns nun Trusted Computing, um mehr IT-Sicherheit und Vertrauenswürdigkeit zu gewinnen und womit muss diese bezahlt werden? Dies sind wohl zwei der wichtigsten Fragen, die es zu beantworten gilt. Ein Beispiel, mit dem sich die Möglichkeiten des Trusted Computing gut darstellen lassen, ist Cloud Computing, allen voran Cloud Storage, einer der wohl meistgenutzten Internet-Dienste schlechthin. Hierbei handelt es sich um einen Online-Speicher, der durch einen Internet-Dienstleister bereitgestellt wird. Durch die potenziell große Menge an Daten, die hinterlegt werden kann, muss ein besonderes Augenmerk auf IT-Sicherheit und Vertrauenswürdigkeit gelegt werden. Es sollte verhindert werden, dass Unbefugte Zugriff auf Daten und somit Einblick in die darin enthaltenen Informationen erhalten oder diese gar verändern können. Diese IT-Sicherheit sollte möglichst unabhängig vom Herkunftsland des IT-Dienstanbieters gewährleistet werden.

Trusted Computing bietet hier die Möglichkeit einer „transparenten Verschlüsselung". Hierbei werden die Daten vor der Übertragung durch die Sicherheitsplattform im IT-System automatisch verschlüsselt, ohne dass der Nutzer explizit eingreifen muss. Eine einmalige Konfiguration der Sicherheitsplattform des IT-Systems ist hierbei ausreichend. Dabei bewahrt ein vertrauenswürdiges IT-System auch die für die Verschlüsselung benötigten Schlüssel sicher auf, indem es diese an die Hardware des jeweiligen IT-Systems bindet. Hierbei wird das TPM für die Verschlüsselung des

Für Abonnenten ist dieser Artikel auch digital auf www.datakontext.com verfügbar

Schlüsselmaterials verwendet und nur dieses kann das Schlüsselmaterial auch wieder entschlüsseln und somit nutzbar machen. Diese einfache Technik eignet sich ebenfalls für die sichere Aufbewahrung von Passwörtern. Ebenso kann das beschriebene Prinzip mit kryptographischen Verfahren sogar auf mehrere IT-Systeme ausgedehnt werden, sodass beispielsweise ein gesamtes Unternehmen davon profitiert. Auch lassen sich die Daten mithilfe der Sicherheitsplattform und des TPM signieren, sodass die Integrität sichergestellt ist.

Ebenso erlaubt ein solches vertrauenswürdiges IT-System die Einrichtung getrennter Compartments. Damit lassen sich beispielsweise ein privat und ein geschäftlich genutztes Compartment parallel auf einem IT-System betreiben, ohne das Risiko eines ungewollten Datenaustauschs. Auch ist es möglich, die Integrität einer Sicherheitsplattform feststellen zu lassen. Dieser Funktion kann zum Beispiel eine Kommunikation mit einem anderen IT-System vorausgehen, damit sichergestellt ist, dass keine ungewollte Manipulation vorliegt. Dies stärkt das Vertrauen in den Kommunikationspartner – hier also in das entsprechende IT-System. Dies könnte zum Beispiel auch im Falle sozialer Netze genutzt werden. So ist es vorstellbar, dass diese IT-Systeme von öffentlichen Instanzen geprüft werden und dass IT-Systeme (PC, Notebook, Smartphone ...) des Nutzers die dafür hinterlegten Integritätsdaten vor einem Datenaustausch prüfen.

Um die Vorteile einer Sicherheitsplattform nutzen zu können, muss diese auf den IT-Systemen zur Verfügung stehen. Ein Nutzer eines vertrauenswürdigen IT-Systems muss sich daher auf Mehraufwand einstellen, der aber auch zu einem Mehr an IT-Sicherheit und Vertrauenswürdigkeit führt. Ein wünschenswertes Ziel ist, dass eine solche Sicherheitsplattform zukünftig fester Bestandteil von IT-Systemen wird.

Positive Entwicklungen

Seit einigen Jahren nimmt die Verbreitung von TPMs deutlich zu – vorwiegend im Business-Umfeld. Als Übergangslösung stehen zudem sogenannte Steck-TPMs zur Verfügung, um jedes IT-System mit TPMs zu bestücken.

Microsoft hat kürzlich bekannt gegeben, dass ab 1. Januar 2015 nur noch IT-Systeme mit eingebautem TPM 2.0 (4) die Zertifizierung für Microsoft Windows erhalten werden (5). Dies spricht zum einen für eine Nutzung dieser IT-Sicherheits- und Vertrauenswürdigkeitstechnologie auf allen IT-Systemen und setzt zugleich ein wichtiges Zeichen für die gesamte Branche. Demzufolge ist zu erwarten, dass innerhalb kurzer Zeit die Verbreitung dieser Sicherheitschips in allen Klassen der Hardware stark zunehmen wird. Auf lange Sicht wird jedes neue IT-Gerät über ein TPM verfügen. Ebenso wird erwartet, dass diese Entwicklung auch im Bereich der eingebetteten Hardware, speziell bei Tablets und Smartphones, Einzug halten wird. Die Chips nennen sich hier Mobile Trusted Module (MTM) (6), ein TPM speziell für die Anforderungen eingebetteter IT-Systeme, deren Spezifikation ebenfalls durch die Trusted Computing Group erarbeitet wurde.

Wichtig dabei ist, dass alle Beteiligten an diesem Entwicklungsprozess mitwirken. So ist es notwendig, dass sowohl die Forschung weiterführende Konzepte und Prototypen entwickelt, als auch die Industrie diese Technologie in Produkten angemessen nutzt. Vor allem aber ist hierbei auch der Nutzer von entscheidender Relevanz, da er diese IT-Sicherheitstechnologie auch einfordern muss, auch wenn er hierdurch eventuell einige Einschränkungen in Kauf nehmen muss. Es hilft die beste IT-Sicherheits- und Vertrauenswürdigkeitstechnologie nichts, wenn diese nicht auch genutzt wird … ■

ANDREAS SPEIER,
Wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen und Leiter des Forschungsbereiches „Vertrauenswürdige IT-Systeme"

NORBERT POHLMANN,
Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie geschäftsführender Direktor des Instituts für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen

(1) https://www.trustedcomputinggroup.org/
(2) M. Linnemann, N. Pohlmann: „Turaya – Die offene Trusted-Computing-Sicherheitsplattform", in „Open Source Jahrbuch 2007", Hrsg.: B. Lutterbeck, M. Bärwolff, R. Gehring, Lehmanns Media, Berlin, 2007
(3) Compartment – Logisch oder durch Virtualisierung stark von den restlichen Systemressourcen getrennt laufende Anwendung oder Betriebssystem
(4) https://www.trustedcomputinggroup.org/resources/tpm_20_library_specification_faq
(5) Windows Certification Program – Hardware Certification Taxonomy & Requirements – Systems Windows 8.1 – June 26, 2013, p. 6 (Verfügbar unter: http://msdn.microsoft.com/en-us/library/windows/hardware/hh748188.aspx)
(6) Windows Certification Program – Hardware Certification Taxonomy & Requirements – Systems Windows 8.1 – June 26, 2013, p. 6 (Verfügbar unter: http://msdn.microsoft.com/en-us/library/windows/hardware/hh748188.aspx)