Xpert.press

Thomas Müller

Trusted Computing Systeme

Springer

Xpert.press

Thomas Müller

Trusted Computing Systeme

Springer

Xpert.press

Die Reihe **Xpert.press** vermittelt Professionals in den Bereichen Softwareentwicklung, Internettechnologie und IT-Management aktuell und kompetent relevantes Fachwissen über Technologien und Produkte zur Entwicklung und Anwendung moderner Informationstechnologien.

Thomas Müller

Trusted Computing Systeme

Konzepte und Anforderungen

Mit einem Vorwort von Thomas Caspers

Springer

Thomas Müller
Hagenholzstrasse 92
CH-8050 Zürich
Schweiz
Thomas.Mueller@tmxm.de

Korrigierter Nachdruck 2008

ISBN 978-3-540-76409-0 e-ISBN 978-3-540-76410-6

DOI 10.1007/978-3-540-76410-6

ISSN 1439-5428

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

© 2008 Springer-Verlag Berlin Heidelberg

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland vom 9. September 1965 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten waren und daher von jedermann benutzt werden dürften.

Einbandgestaltung: KünkelLopka, Heidelberg
Satz und Herstellung: le-tex publishing services oHG, Leipzig

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

Vorwort

Mit der heute in vielen Lebensbereichen erforderlichen Nutzung der Informationstechnik (IT) ergeben sich nicht nur Fragen zur Sicherheit und Verfügbarkeit dieser Technik. Die IT-Durchdringung wirkt sich auf unsere Gesellschaft und ihr Normensystem aus. Deutlich wird dies durch den Urteilsspruch des Ersten Senats des Bundesverfassungsgerichts aus dem Februar 2008 zu den so genannten Online-Durchsuchungen. Erstmals formuliert das Gericht ein „Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“[1]. Damit wird die IT-Nutzung als Teil der durch die Verfassung geschützten Privatsphäre anerkannt. In seiner Urteilsbegründung führt das Gericht aus: „Die Nutzung der Informationstechnik hat für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt. Die moderne Informationstechnik eröffnet dem Einzelnen neue Möglichkeiten, begründet aber auch neuartige Gefährdungen der Persönlichkeit.“[2] Derzeit ist noch nicht abzuschätzen, welche konkreten Auswirkungen aus dem Urteil des Bundesverfassungsgerichtes auf die IT-Branche sowie die Wirtschaft und Verwaltung insgesamt resultieren. Unstrittig ist, der Schutz der digitalen Privatsphäre ist zunehmend von vertrauenswürdiger Informationstechnik abhängig.

Die rasante Entwicklung und Verbreitung der Computertechnik in den letzten Jahrzehnten hat sowohl bei der Hardware als auch bei Betriebssystemen und Anwendungen dazu geführt, dass IT-Sicherheit oftmals als lästiges, die Benutzerfreundlichkeit einschränkendes Beiwerk empfunden wurde. Auf dem Markt bestimmten andere Faktoren den Erfolg und Misserfolg von Produkten und Unternehmen. Die IT-Wirtschaft gelangte aber spätestens dann an einen Scheideweg, als das Internet mit seinen elektronischen Transaktions- und Banking-Plattformen das Interesse der international strukturierten Kriminalität fand. Die IT-Systeme erlaubten Raubzüge, die mit relativ einfachen Mitteln und geringem Risiko durchgeführt

[1] Erster Leitsatz zum Urteil des Ersten Senats des Bundesverfassungsgerichts vom 27. Februar 2008

[2] Begründung des Urteils des Ersten Senats des Bundesverfassungsgerichts vom 27. Februar 2008, Absatz 170

werden konnten. Die Verantwortbarkeit der Nutzung von Informationstechnik und des Internets für Geschäfte aller Art war dadurch mit Zweifel belastet.

In der Folge wurden seit Ende der Neunziger Jahre zahlreiche Sicherheitslösungen von der Industrie angeboten. Heute werden technische Schutzmaßnahmen – wie Virenschutzprogramme und Firewalls – nicht nur von professionellen IT-Anwendern eingesetzt, sondern sind auch bei vielen Privat-PCs vorhanden. Jedoch rüsten auch die Angreifer immer wieder auf. Und mit ständig ausgefeilteren Angriffstechniken gelingt es ihnen, die ihnen in den Weg gestellten Hindernisse zu überwinden.

Eine grundlegende Lösung muss gefunden werden, um die Integrität von IT-Systemen nachhaltig zu gewährleisten. Hier setzen die Ideen des Trusted Computing an. Seit 1999 versucht ein Industriekonsortium, das sich inzwischen zur Trusted Computing Group (TCG) zusammenschloss, einen Standard für sichere IT-Systeme zu schaffen, der sich auch unter den harten Bedingungen des schnelllebigen IT-Marktes durchsetzen kann. Eine kostengünstige Sicherheitshardware verbunden mit verlässlichen Integritätsmessungen soll den Durchbruch bringen. Eine Schlüsselrolle nimmt dabei das Trusted Platform Module (TPM) ein, das über geschützte kryptografische Funktionen und speziell abgeschirmte Speicherbereiche diese Anforderungen abdecken soll.

Bereits heute ist Standardhardware von so gut wie allen Anbietern erhältlich, die mit einem TPM ausgerüstet ist. In 2008 werden vermutlich erstmals mehr als 200 Millionen TPMs einsatzbereit sein. Doch schon steht die Industrie am nächsten Scheideweg: Trusted Computing, insbesondere die Integritätssicherung von IT-Systemen, muss auch von Betriebssystemen und Anwendungen genutzt werden. Es gibt bis heute keine massentaugliche Applikation, die einen tatsächlichen Nutzen aus dem angesichts der Verkaufszahlen praktisch allgegenwärtigen TPM und seinen sicherheitstechnischen Vorteilen schöpft. Aufgrund der starken Marktposition bei den Betriebssystemen ist Microsoft hier in einer besonderen Verantwortung. Ausgehend von Palladium über die Next-Generation Secure Computing Base (NGSCB) startete Microsoft in 2002 einen Paradigmenwechsel hin zu sicheren Betriebssystemen, konnte aber diesen Wandel selbst nicht erzwingen. Die Wunschvorstellungen abgeschotteter sicherer Bereiche, seien es die Palladium-Quadranten oder NGSCB-Compartments, wurden von der Trägheit in der Windows-Entwicklung eingeholt. Aus viel versprechenden Ideen in Longhorn verblieb bei Windows Vista lediglich ein abgesicherter Bootprozess, und zwar ausschließlich in den teuren Vista-Versionen für professionelle Anwender. Dennoch ist Microsoft damit eine für den Massenmarkt taugliche Pilotanwendung für das TPM gelungen, die den zukünftigen Weg aufzeigt, die Integrität für alle zu sichern. Microsoft trägt nun die Verantwortung, diese Integritätssicherung in der kommenden Windows-Version allen Anwendern anzubieten und die Technik für jeden bedienbar zu machen. Gleiches gilt für die Mitbewerber wie die Anbieter von Linux-Distributionen oder Apple. Dafür bedarf es sowohl auf Herstellerseite als auch bei den Kunden, die eine Nachfrage nach sicherer Informationstechnik schaffen müssen, noch einiger Überzeugungsarbeit.

Das vorliegende Buch gibt einen umfassenden Überblick über die Möglichkeiten, die Trusted Computing bereits heute bietet. Dabei werden alle wesentlichen

Facetten des Trusted Computing tiefgehend beleuchtet, ohne sich jedoch in technische Spezialfragen zu verlieren. Die Gesamtsicht auf das eigentliche Ziel der Technologie bleibt im Fokus, so dass sich die Vision des Trusted Computing auch in den Detailbetrachtungen erschließt. Damit stellt dieses Buch einen wichtigen Beitrag dazu dar, das grundlegende Verständnis für Trusted Computing auch bei einem breiten Publikum zu schaffen und die damit verbundenen Möglichkeiten im Bewusstsein zu verankern. Gleichzeitig zeigt es die Grenzen von Trusted Computing auf und verschweigt auch nicht die Themen, bei denen auf Herstellerseite Anspruch und Wirklichkeit noch auseinander klaffen.

Die Integrität unserer Computersysteme und die Vertrauenswürdigkeit einer kritischen Infrastruktur sind nicht zuletzt durch die zunehmende Cyberkriminalität massiv bedroht. Integritätssicherung ist möglich – alle sind dafür verantwortlich, sich zu informieren, wie sie ihren Beitrag dazu leisten können.

Dieses Buch kann Anregung und Ausgangspunkt dafür sein, auf welchem Weg Vertraulichkeit und Integrität von IT-Systemen zu erreichen sind und wie der Schutz der Integrität der Persönlichkeit mit Hilfe technischer Systeme gelingen kann.

Bundesamt für Sicherheit in der Informationstechnik, *Thomas Caspers*
März 2008

Inhaltsverzeichnis

Abbildungsverzeichnis