



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

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](http://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“<sup>1</sup>. 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.“<sup>2</sup> 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

---

<sup>1</sup> Erster Leitsatz zum Urteil des Ersten Senats des Bundesverfassungsgerichts vom 27. Februar 2008

<sup>2</sup> 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 schnelllebrigen 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,  
März 2008

*Thomas Caspers*

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Motivation	1
1.2	Ziele des Buches	2
1.3	Gliederung des Buches	3
<b>2</b>	<b>Grundlagen</b>	<b>5</b>
2.1	CPU-Ringe	5
2.2	Verwendung der CPU-Ringe	7
2.3	Virtualisierung und die CPU-Ringe	8
2.4	Zero-Knowledge-Beweis	10
2.5	Clark-Wilson-Integritätsmodell	11
<b>3</b>	<b>Trusted Computing</b>	<b>13</b>
3.1	Definition des Begriffs „Trusted Computing“	14
3.2	Ziele des Trusted Computing	16
3.3	Das Trusted Computing System (TCS)	19
3.3.1	Die Trusted Computing Platform (TCP)	21
3.3.2	Das Trusted Operating System (TOS)	21
3.3.3	Die Trusted Computing Base (TCB)	21
3.4	Trusted Computing und Secure Computing	22
<b>4</b>	<b>Die TCP der Trusted Computing Group</b>	<b>25</b>
4.1	PC-Referenzarchitektur	26
4.2	Trusted Building Block (TBB)	27
4.2.1	Root of Trust for Measurement (RTM)	28
4.2.2	Root of Trust for Reporting (RTR)	28
4.2.3	Root of Trust for Storage (RTS)	29
4.3	Das Trusted Platform Module (TPM)	29
4.3.1	TPM-Einheiten	31
4.3.2	TPM-Zugriffskontrolle und Kommunikationsprotokoll	37
4.3.3	TPM-Initialisierung	40

4.3.4	Betriebszustände des TPM (Opt-In) .....	41
4.3.5	Erweiterte TPM-Konfiguration (Opt-In) .....	43
4.3.6	TPM-Eigentümer einrichten und entfernen .....	44
4.3.7	TPM-Schlüsseltypen und Schlüsselverwaltung .....	46
4.3.8	TPM-Selbstschutzmaßnahmen (Tamper-Resistant) .....	50
4.4	Sicherheitsfunktionen der TCP .....	51
4.4.1	Integrity Measurement, Storage and Reporting .....	51
4.4.2	Initialisierung der Chain of Trust .....	52
4.4.3	Remote Attestation .....	55
4.4.4	Kryptographische Operationen .....	56
4.5	Identität der TCP und entstehende Datenschutzprobleme .....	57
4.5.1	Erzeugung eines Attestation-Identity-Zertifikats .....	58
4.5.2	Direct Anonymous Attestation (DAA) .....	60
4.5.3	Löschen des Endorsement Key .....	60
4.5.4	Deaktivieren des TPM .....	61
4.6	Plattform-Zertifikate (Platform Credentials) .....	61
4.7	Probleme und Einschränkungen der TCP .....	63
<b>5</b>	<b>Erweiterungen und Alternativen zur TCG .....</b>	<b>65</b>
5.1	Intel Trusted Execution Technology (TXT) .....	65
5.2	AMD Presidio Technology .....	68
5.3	IBM SecureBlue .....	69
<b>6</b>	<b>Anforderungen an vertrauenswürdige Betriebssysteme .....</b>	<b>71</b>
6.1	Dynamic Chain of Trust (Integrity Measurement) .....	71
6.2	Dynamic Chain of Trust (Integrity Protection) .....	72
6.3	Bewertung der Systemintegrität (Integrity Validation) .....	73
6.4	Remote Attestation (Remote Integrity Validation) .....	74
6.5	Trusted Software Stack .....	75
6.5.1	TPM Device Driver .....	76
6.5.2	TCG Device Driver Library (TDDL/TDDLI) .....	76
6.5.3	TSS Core Services (TCS/TCSI) .....	77
6.5.4	TCG Service Provider (TSP/TSPI) .....	77
6.5.5	Einsatzszenarien des TSS .....	78
6.6	Protected Execution .....	79
6.7	Trusted-GUI und Trusted Input/Output .....	80
<b>7</b>	<b>Trusted-Computing-Infrastruktur .....</b>	<b>83</b>
7.1	Public Key Infrastructure (PKI) .....	84
7.1.1	Ausstellung der Plattform-Zertifikate .....	84
7.1.2	Ausstellung der AIK-Zertifikate .....	85
7.1.3	Verwendung der AIK-Zertifikate .....	86
7.1.4	Zusammenfassung .....	88
7.2	Certificate-Management-Protokoll .....	89
7.3	Remote-Attestation-Protokoll .....	89

<b>8</b>	<b>Theoretische und praktische Lösungsansätze</b>	91
8.1	Integrity Measurement und Integrity Protection	91
8.1.1	AEGIS	91
8.1.2	SEBOS	92
8.1.3	Copilot	93
8.1.4	<i>Trusted Grub</i>	94
8.1.5	IBM Integrity Measurement Architecture (IMA)	95
8.1.6	BIND – Binding Instructions and Data	98
8.2	Remote Attestation	100
8.2.1	Trusted Network Connect (TNC)	100
8.2.2	Microsoft Network Access Protection (NAP)	102
8.2.3	Cisco Network Admission Control (NAC)	103
8.2.4	Property-Based Attestation	104
8.2.5	WS-Attestation	105
8.2.6	Sicherheit des Attestation-Protokolls	108
8.3	Trusted Software Stack (TSS)	110
8.3.1	TrouSerS	110
8.3.2	Trusted Java	111
8.3.3	TPM/J	111
8.4	Protected Execution	111
8.4.1	Terra Architecture	113
8.4.2	Nizza Architecture	115
8.4.3	Perseus Architecture	118
8.4.4	Xen-Hypervisor-Erweiterungen	120
8.5	Trusted Graphical User Interface (Trusted-GUI)	122
8.5.1	Dynamic Security Skins	122
8.5.2	Nitpicker – Overlay Window Management	123
<b>9</b>	<b>Trusted-Computing-Systeme</b>	127
9.1	European Multilaterally Secure Computing Base	127
9.2	Open Trusted Computing	128
9.3	Intel Virtual Appliances/RedHat Embedded IT Software (EIT)	128
<b>10</b>	<b>Fazit</b>	131
<b>11</b>	<b>Trusted Computing mit Windows Vista</b>	133
11.1	Die Geschichte von Windows Vista	134
11.2	Sicherheitsfunktionen in Windows Vista	135
11.3	Windows Vista TPM Support	136
11.4	Secure Startup und Full Volume Encryption (FVE) – BitLocker	137
11.5	Kernel Integrity Checks/Driver Signing (nur 64-Bit-Versionen)	140
11.6	Windows Resource Protection (WRP)	143
11.7	PatchGuard (nur 64-Bit-Versionen)	144
11.8	User Account Control	144
11.8.1	User Account Protection (UAP)	145

- 11.8.2 Mandatory Integrity Control (MIC) ..... 147
- 11.8.3 Secure Desktop (Trusted Path) ..... 148
- 11.8.4 UI Privilege Isolation (UIPI) ..... 150
- 11.9 Windows Service Hardening ..... 150
- 11.10 Zusammenfassung und Schlussfolgerung ..... 151
- Literaturverzeichnis ..... 153
- Sachverzeichnis ..... 159**

# Abbildungsverzeichnis

2.1	CPU-Ringe .....	6
2.2	Verwendung der CPU-Ringe .....	6
2.3	Windows und CPU-Ringe .....	7
2.4	Zusätzlicher CPU-Ring .....	9
3.1	Trusted Computing System .....	20
3.2	Trusted Computing Base .....	22
4.1	PC-Referenzarchitektur .....	26
4.2	Trusted Building Block .....	28
4.3	Referenzarchitektur mit TPM .....	30
4.4	Blockschaltbild eines TPM .....	31
4.5	TPM-Komponenten .....	31
4.6	TPM-Lebenszyklus .....	40
4.7	Zustände des TPM .....	42
4.8	Zustandsübergänge des TPM .....	42
4.9	TPM-Eigentümer einrichten und entfernen .....	45
4.10	TPM-Schlüsselobjekt .....	47
4.11	TPM-Schlüsselhierarchie [TCG2004] .....	48
4.12	TPM-Schlüssel-Ladevorgang [TCG2004] .....	49
4.13	Update der PCR .....	51
4.14	Chain of Trust [TCG2004] .....	53
4.15	Static Chain of Trust [TCG2005] .....	54
4.16	Remote Attestation .....	56
4.17	AIK-Erzeugung .....	59
4.18	Plattform-Zertifikate und deren Beziehungen [TCG2004] .....	62
5.1	Intel-Trusted-Execution-Technologie .....	66
5.2	Intel TXT – Secure Launch .....	67
5.3	AMD Presidio .....	68

6.1	Remote Attestation .....	75
6.2	Trusted Software Stack [TCG2006-2] .....	76
6.3	TSS Core Services [TCG2006-2] .....	77
6.4	TSS-Einsatzszenarien [TCG2006-2] .....	79
7.1	Ausstellung der Plattform-Zertifikate .....	85
7.2	Signatur eines AIK .....	86
7.3	PKI Remote Attestation .....	86
7.4	PKI-Subject Key Attestation Evidence Extension .....	87
7.5	Trusted Computing PKI .....	88
8.1	AEGIS-Architektur .....	92
8.2	Copilot-Architektur .....	94
8.3	Trusted Grub .....	95
8.4	Integrity Measurement Architecture [Sailer2004] .....	97
8.5	Prüfsummenerzeugung mit BIND .....	100
8.6	Trusted Network Connect [TCG2006] .....	101
8.7	Network Access Protection .....	102
8.8	WS-Attestation Architektur [Munetoh2005] .....	106
8.9	WS-Attestation mit WS-Trust .....	108
8.10	Remote-Attestation-Protokoll .....	109
8.11	Erweitertes Remote-Attestation-Protokoll .....	109
8.12	Terra-Architektur .....	114
8.13	Nizza-Architektur .....	116
8.14	Perseus-Architektur .....	118
8.15	Perseus-Architektur mit Xen .....	119
8.16	Perseus-Architektur mit Xen II .....	120
8.17	Overlay Window Management .....	124
8.18	Overlay Window Management #2 .....	125
9.1	Intel Virtual Appliances .....	129
11.1	NGSCB .....	134
11.2	Sicherheitsfunktionen in Windows Vista .....	135
11.3	TPM-Dienste in Windows Vista .....	136
11.4	Secure Startup .....	137
11.5	BitLocker-Schlüsselverwaltung .....	139
11.6	Driver Signing in Windows Vista .....	141
11.7	Unterbrechung der Chain of Trust .....	142