

Oliver Grimm
Hauptstraße 5
98554 Benshausen
e-Mail: post ,at' olivergrimm.com

**Microsoft NGSCB -
Chancen und Risiken neuer Sicherheitsinitiativen**

**Projektarbeit
an der Fakultät für Wirtschaftswissenschaften
der Technischen Universität Ilmenau**

**Fachgebiet Informationsmanagement
Betreuer: Dipl.-Wirtsch.-Inf. Daniel Fischer**

1. Einleitung	5
1.1. Problemstellung.....	5
1.2. Zielsetzung	6
1.3. Vorgehensweise und Aufbau	6
2. Die Rolle des Internets und daraus entstehende Risiken.....	7
3. DRM – Digital Right Management	8
4. Sicherheitsziele der Informationsverarbeitung.....	9
5. Palladium / NGSCB	13
5.1. Ziele von Microsoft NGSCB	14
5.1.1. NGSCB- Security Model.....	14
5.1.2. NGSCB und DRM	16
5.1.3. Resümee der Ziele	17
5.2. Hardwarevoraussetzungen	17
5.3. Komponenten, Struktur und Funktionsweise	18
5.3.1. NGSCB-Komponenten	18
5.3.2. Funktionsweise	21
5.4. Chancen und Risiken von Microsoft NGSCB	24
5.4.1. Vorteile & Chancen	24
5.4.2. Nachteile und Risiken.....	26
6. Ausblick.....	27
7. Literaturverzeichnis / Quellenangaben.....	29

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CPU	Central Processing Unit
DMA	Direct Memory Access
DoS	Denial of Service
DRM	Digital Right Management
EFS	Encryption File System
HAL	Hardware Abstraction Layer
HMAC	Hash-based Message Authentication Code
I/O	Input/Output
ID	Identification
IEC	International Electrotechnical Commission
IPC	Interprocess Communicatio
IRM	Information Rights Management
ISO	International Organization for Standardization
LHS	Left Hand Side
ME	Millennium Edition
MS-DOS	Microsoft-Disk Operating System
NAL	Nexus Abstraction Layer
NCA	Nexus Computing Agent
NGSCB	Next Generation Computing Base for Windows
PDF	Portable Document Format
PKSC	Public Key Crypto Standards
RAM	Random Access Memory
RHS	Right Hand Side
RMS	Right Management System
SSC	Security Support Component
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Alliance
TPM	Trusted Platform Module
TSP	Trusted Service Provider
TUE	Trusted Userinterface Engine

Abbildungsverzeichnis

Abbildung 3-1: DRM am Beispiel von Windows Media Rights Manager	9
Abbildung 4-1: Elemente von Sicherheit	11
Abbildung 4-2: Sicherheitskonzepte und deren Wechselbeziehungen	13
Abbildung 5-1: Komponenten im Aufbau von NGSCB	18
Abbildung 5-2: Interaktionen der NGSCB-Komponenten.....	21
Abbildung 5-3: Austausch zwischen Standard- und Nexus-Mode.....	22
Abbildung 5-4: Datenfluß vom Secure Input bis zum Secure Output.....	23

1. Einleitung

1.1. Problemstellung

Der Vertrieb von digitalen Gütern nimmt rasant zu: Musikstücke werden als MP3-Dateien mehr oder weniger legal zum Download angeboten, Dokumente oder sogar ganze Bücher (sog. eBooks) stehen im Internet zur Verfügung. Aber den vielen Vorteilen dieses Vertriebsweges sowohl für Firmen als auch für die Nutzer stehen auch Nachteile gegenüber: Einmal „in Verkehr gebracht“ ist der Weiterverbreitung des Dokumentes/der Datei meist keine Grenzen gesetzt. Die Datei kann beliebig oft kopiert und weitergegeben werden, ohne daß der Urheber etwas davon erfährt oder etwas dagegen unternehmen kann.

Abhilfe bei diesen Problemen soll das sogenannte Digital-Right-Management (DRM) schaffen. Diese DRM-Systeme sind derzeit zum Beispiel in den benutzten Playern oder Readern implementiert (z. B. das Microsoft-Format Windows-Media in Verbindung mit dem MediaPlayer oder die Rechtebeschränkung in PDF-Files mit Hilfe von Adobe Acrobat). Einen neuen Weg will die TCG¹ (vorher bekannt als TCPA (Trusted Computing Platform Alliance)) gehen.² TCG ist die Abkürzung für Trusted Computing Group, ein von AMD, IBM, Intel, HP sowie Microsoft gegründetes Konsortium mit dem Ziel, eine vertrauenswürdige Computerplattform zu schaffen. Mit Hilfe des TPM (Trusted Platform Module) und von ‚Next Generation Secure Computing Base for Windows‘, kurz NGSCB (Projekt von Microsoft zur Umsetzung des DRM-Ansatzes im Betriebssystem, welches unter dem Namen ‚Palladium‘ bekannt wurde), soll es möglich sein, dass der Urheber von digitalen Dokumenten die Verbreitung dieser unter Kontrolle halten bzw. einschränken kann. Der PC soll durch diese Technologie für den Nutzer sicherer werden und Urhebern ein Digital-Right-Management ermöglichen: Musikstücke, die im Internet als MP3-Dateien erworben wurden, können dann nur noch auf dem entsprechenden Rechner abgespielt werden, Urheber von Dokumenten können bestimmen, wer das Dokument öffnen oder ändern darf.

¹ <http://www.trustedcomputing.org>

² Vgl. Himmlein / Ganz im Vertrauen-TCG / c't 9/2003, S. 52

Sichere Systeme werden für die Nutzung des Computers und des Internets immer relevanter. Viele sensible und schutzwürdige Daten werden mit Hilfe von PC-Systemen bearbeitet und verwaltet, so daß der Wunsch vieler Nutzer nach einer sicheren Plattform immer größer wird. Aus diesem Grund arbeiten Soft- und Hardwarehersteller ständig an neuen Sicherheitsstrategien. Auch TCG und ‚Next-Generation Secure Computing Base for Windows‘ sollen zur Erreichung der neuen Sicherheitsziele beitragen. So kann z. B. mit Hilfe von TCG dem System eine eindeutige ID gegeben werden, mit derer man das System identifizieren kann. Auch ist das Authentifizieren [griech., lat.: die Echtheit bezeugen, beglaubigen] von Daten möglich, wodurch zum Beispiel e-Mails ohne entsprechendes Zertifikat automatisch als SPAM erkannt werden können.

Aber durch die genannten Systeme können auch Nachteile entstehen: So ist zum Beispiel eine ständige Überwachung des Nutzers möglich, ohne daß dieser davon etwas merkt. Dies führt derzeit zu einer heftigen Diskussion in Zeitschriften und im Internet.

1.2. Zielsetzung

Ziel der Projektarbeit ist es, die neuen Sicherheitsinitiativen näher zu betrachten. Es soll die Funktionsweise bzw. der Aufbau von Microsoft-NGSCB beschrieben und Vor- und Nachteile aufgezeigt werden. Weiterhin soll dargestellt werden, welche Beiträge das Konzept zur Erreichung der allgemeinen Sicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit, Authentifikation, Zugriffskontrolle, Unabstreitbarkeit) leistet.

1.3. Vorgehensweise und Aufbau

Nachdem zunächst die allgemeinen Sicherheitsziele genannt und erläutert werden, sollen mit Hilfe von Internetrecherchen und Literaturlauswertungen die grundlegenden Gedanken und Ziele des Digital-Right-Management, Trusted Computing und anderer Sicherheitsinitiativen dargestellt werden und wodurch diese Ziele erreicht werden sollen. Anschließend soll auf die Ziele von Microsoft-NGSCB eingegangen werden. Im weiteren Verlauf sollen die technische Umsetzung und die Funktionsweise erläutert, und die Vor- und Nachteile gegenübergestellt werden.

2. Die Rolle des Internets und daraus entstehende Risiken

Das Internet gewinnt sowohl im privaten als auch im geschäftlichen Bereich der Menschen immer mehr an Bedeutung. So gab es beispielsweise im Mai 2002 26,7 Millionen Internetnutzer in Deutschland.³ Das entspricht 41,7% der (über 14jährigen) Bevölkerung. Doch je größer die Anzahl der Nutzer ist, desto größer wird auch die Anzahl der Gefahren und Risiken, die durch das Internet entstehen. Weiterhin spielen rechtliche Aspekte eine größer werdende Rolle (DRM – Digital Right Management). Täglich werden laut einer Studie des amerikanischen Marktforschungsunternehmens Viant Corporation⁴ ca. 600.000 Filme aus dem Internet heruntergeladen. Bei MP3⁵-Dateien dürfte die Zahl wohl noch deutlich höher liegen. Diese Tatsache beschert der Film- und Musikindustrie hohe Umsatzverluste, weshalb diese ein großes Interesse daran hat, gegen den illegalen Download sowie die Nutzung von nicht rechtmäßig erworbenen Kopien vorzugehen bzw. diesen zu kontrollieren. Durch die immer weiter steigende Anzahl der Internetnutzer beschleunigt sich auch die Verbreitung von Computerviren, Trojanern und anderer böswilliger Programme. Möglich wird diese rasante Verbreitung teilweise erst durch Sicherheitslücken in Betriebssystemen. Besonders die bei den privaten Anwendern weit verbreiteten Betriebssysteme Windows 95, 98 und ME basieren noch auf MS-DOS und sind dadurch besonders anfällig. Aber auch die NT-Betriebssysteme (Windows-NT, Windows 2000, Windows XP) sind Attacken gegenüber anfällig, wie die Verbreitung des e-Mail-Wurms W32.Blaster im August 2003 verdeutlicht.⁶ Ermöglicht hat diese rasante Verbreitung eine Sicherheitslücke in den Windows-Betriebssystemen NT4, 2000 sowie XP. Microsoft schreibt zu diesem Sachverhalt: „Es handelt sich bei dieser Sicherheitsanfälligkeit um einen Pufferüberlauf. Wenn ein Angreifer diese Schwachstelle erfolgreich ausnutzen kann, kann er die vollständige Kontrolle über einen Remotecomputer erlangen.“⁷ Heise.de schätzt die Anzahl der weltweit betroffenen Rechner dieses Virus auf 500.000. Durch den Ausfall von Rechnern und Servern entsteht ein großer wirtschaftlicher Schaden. Vermutlich ist für den Stromausfall vom August 2003 in großen Teilen Nordamerikas der Wurm

³ Vgl. Emnid / Onliner-Atlas

⁴ Vgl. Heise / Tauschbörsen

⁵ MP3: Kompressionsverfahren für Audiodateien

⁶ Vgl. Heise / W32.Blaster

⁷ Vgl. Microsoft / Microsoft Security Bulletin MS03-026

fall vom August 2003 in großen Teilen Nordamerikas der Wurm W32.Lovsan verantwortlich.⁸ Nach einer Studie des Sicherheitsunternehmens Kaspersky Labs hat allein der Anfang dieses Jahres 2003 verbreitete Virus Klez einen Schaden von neun Milliarden US-Dollar verursacht.⁹ Ein weiteres Ärgernis für Privatnutzer aber auch für Firmen sind die sogenannten SPAM-Mails.¹⁰ Dabei handelt es sich um unaufgefordert zugesandte Werbemails. Oft sind die Absender dieser Mails nicht ermittelbar. Durch die immer größer werdende Anzahl dieses SPAMS kommt es nicht nur zu einer höheren Belästigung der Anwender, sondern auch zu Störungen des Datenverkehrs im Internet.

3. DRM – Digital Right Management

Unter DRM versteht man Systeme die verhindern sollen, daß Anwender nicht-bezahlte digitale Werke konsumieren, oder Inhalte bestimmter Dokumente verändern können. Es handelt sich also um ein umfassendes Vertriebskonzept für digitale Güter. Hauptinteressenten dieser Technologien dürften die Film-, Musik- und Softwareindustrie sein.¹¹ Die Firma Adobe schreibt zum Thema Softwarepiraterie auf ihren Internetseiten: „Bei einer Piraterie-Rate von 25% sind zum Beispiel die wirtschaftlichen Auswirkungen in den USA erheblich: 1999 hat Piraterie die US-Wirtschaft 3,2 Milliarden Dollar in fehlenden Steuereinnahmen und 100.000 Arbeitsplätze in der Software- und verwandten Branchen gekostet.“¹² Aus diesen Gründen besteht ein großes Interesse von Herstellern digitaler Güter an DRM-Systemen. Die Entwicklung solcher Systeme wird immer weiter vorangetrieben. Microsoft setzt die Gedanken des DRM beispielsweise in Technologien wie RMS (Right Management System) oder dem Windows Media Right Manager um. RMS ist für Firmen geeignet, um die Verwendung von Dokumenten sowie internen Unterlagen zu kontrollieren.¹³ Der Media Right Manager von Windows soll die Interes-

⁸ Vgl. Bachfeld / IT-Sicherheit

⁹ Vgl. Auding / Computerviren in Manager-Magazin

¹⁰ Vgl. hierzu auch Pew Internet & American Life Project / Spam-Report

¹¹ Vgl. Himmelein / Der digitale Knebel / c't 15/2002, S. 18

¹² Vgl. Adobe / Softwarepiraterie

¹³ Vgl. Heise / DRM-Client

sen von Herstellern digitaler Audio- und Videodateien durchsetzen sowie den Vertrieb dieser Güter revolutionieren.¹⁴ In der Abbildung 3-1 ist dieser schematisch dargestellt.

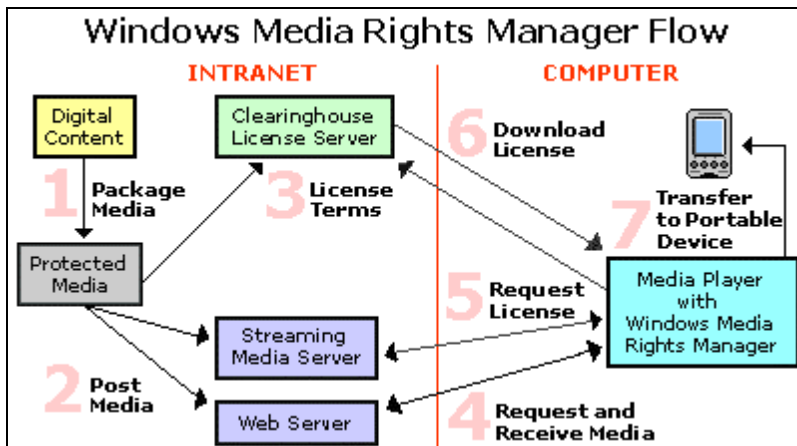


Abbildung 3-1: DRM am Beispiel von Windows Media Rights Manager¹⁵

Erläuterungen zur Grafik:

- (1) Verpacken und Verschlüsselung
- (2) Absatz/Verkauf
- (3) Einrichten des Servers für den Vertrieb der Lizenzen
- (4-6) Erwerb der Lizenz
- (7) Abspielen der Media File

4. Sicherheitsziele der Informationsverarbeitung

Zu den allgemeinen Hauptsicherheitszielen zählen:¹⁶

- Integrität (integrity)
- Verfügbarkeit (availability)
- Vertraulichkeit (confidentiality)

¹⁴ Vgl. Heise / DRM für Dokumente

¹⁵ Vgl. Microsoft / Windows Media Rights Manager

¹⁶ Vgl. BSI / Grundschutzhandbuch / Seite 19

Weitere Ziele sind beispielsweise:¹⁷

- Authentizität (authentication)
- Zugriffskontrolle, Autorisierung (access control)
- Unabstreitbarkeit, Verbindlichkeit (non-repudiation)

Unter **Integrität** versteht man die Forderung, daß sicherheitsrelevante Elemente nicht unautorisiert verändert werden können.¹⁸ Dies betrifft sowohl physische Elemente (Hardware [Festplatte, Arbeitsspeicher u.s.w.]) und Peripherie des Computers) als auch die logischen Elemente (immaterielle Elemente wie Daten, Grafiken, Texte, Betriebssysteme und Anwendungsprogramme). Die Integrität ist gewährleistet, wenn das entsprechende Element vollständig, unverfälscht und korrekt sind.¹⁹ Es muß gesichert werden, daß unerwünschte Veränderungen sowohl durch Datendefekte, als auch durch mutwillige Verfälschung eindeutig erkennbar werden. Eine Möglichkeit diese Forderung zu erfüllen ist zum Beispiel die digitale Signatur für e-Mails, um sicherzustellen, daß der Inhalt nicht nachträglich verändert wurde. Die Digitale Signatur trägt außerdem zusätzlich zur Authentizität bei.

Authentizität ist die Echtheit, Zuverlässigkeit und Glaubwürdigkeit einer Mitteilung. Zur Gewährleistung der Authentizität schreiben in bestimmten Fällen Gesetzte zum Beispiel eine notarielle Beglaubigung vor. Im elektronischen Datenverkehr kann die Authentifizierung beispielsweise durch digitale Wasserzeichen oder durch die digitale Signatur ausgeführt werden. Authentizität ist die Voraussetzung für die Verbindlichkeit.

Der Begriff **Verfügbarkeit** beschreibt den Zustand einer Ressource vorhanden zu sein, wenn diese benötigt wird. Die Verfügbarkeit ist gewährleistet, wenn die Betriebsbereitschaft und die Funktionalität jederzeit gegeben ist, d.h., wenn keine unberechtigte Beeinträchtigung der Funktionalität stattfindet. Sie kann beispielsweise durch unberechtigte Veränderungen von Hard-, Software und Informationen oder durch unbefugte Nut-

¹⁷ Vgl. Fischer / Sicherheitsmanagement in der IV / Teil: „Sicherheit im Mobile Business“ / Seite 15

¹⁸ Vgl. Stelzer / Sicherheitsstrategien / Seite 32

¹⁹ Vgl. Stelzer / Sicherheitsstrategien / Seite 34

zung von Computerressourcen beeinträchtigt werden.²⁰ Verfügbarkeit und Integrität können sich teilweise überschneiden.

Von *Vertraulichkeit* spricht man, wenn man gewährleisten kann, daß bestimmte Daten und Informationen nur den Personen zur Verfügung stehen, die zu deren Nutzung befugt sind, d.h., wenn man unbefugten Informationsgewinn verhindern kann. Dies kann durch die *Zugriffskontrolle (Autorisierung)* gewährleistet werden. Hierbei werden Datenverarbeitungssysteme gegen unberechtigte Nutzung gesichert.

Durch die *Unabstreitbarkeit/Verbindlichkeit* von Daten kann die Urheberschaft eindeutig ermittelt werden. Dadurch kann gewährleistet werden, daß weder der Autor, noch der Anwender den Versand bzw. den Empfang von Daten und Informationen (E-Mails, Dokumente u.s.w.) abstreiten können. Daten und Datenmanipulationen müssen der verantwortlichen Person eindeutig und sicher zugeordnet werden können.

Die Abbildung 4-1 zeigt, wie Kai Rannenberg die Elemente der Sicherheit darstellt.

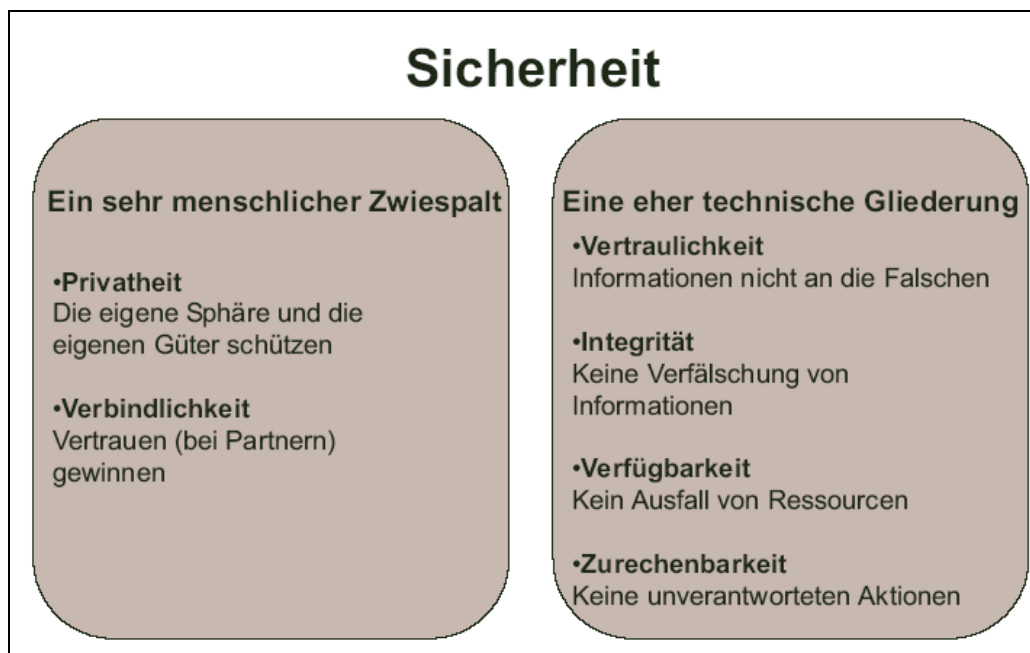


Abbildung 4-1: Elemente von Sicherheit²¹

²⁰ Vgl. Stelzer / Sicherheitsstrategien / Seite 35

²¹ Vgl. Rannenberg / Mehrseitige Sicherheit / Wirtschaftsinformatik 6/2000, S. 489-497

Er unterteilt die Sicherheitsziele in eine menschliche- und eine technische Gliederung. Das Ziel der Unabstreitbarkeit/Vertraulichkeit (hier auch als Zurechenbarkeit bezeichnet) tritt dabei auf beiden Seiten der Einteilung auf.

Zwischen den sicherheitsrelevanten Elementen und den Hauptsicherheitszielen besteht folgender Zusammenhang:

sicherheitsrelevantes Element	Integrität	Verfügbarkeit	Vertraulichkeit
Hardware	unbefugte Manipulationen	Zerstörung, Diebstahl, Defekt, Verschleiß	unberechtigter Zugang zur Hardware (Serverraum o.ä.)
Betriebsmittel	Manipulation des Speicherinhalts	Defekt, Diebstahl	Zugriff auf geschützten Speicherbereich
Software	unbefugte Manipulationen, Viren	Löschung, Programmfehler, Ablauf von Nutzungszeiträumen	Softwarepiraterie
Daten	unbefugte Manipulationen, mutwillige Verfälschung, Datendefekte, Fehleingaben	Löschung, kein Zugriff möglich (z.B. defekte Festplatte)	unbefugte Einsichtnahme, Diebstahl, unbefugtes Kopieren und Weitergeben

Tabelle 4-1: sicherheitsrelevante Elemente und Sicherheitsziele

In den „Common Criteria“²² wird Sicherheit als „der Schutz von Werten“²³ vor Bedrohungen“ verstanden. Bedrohungen sind „Potential für den Mißbrauch von geschützten Werten“.²⁴ In erster Linie sind hier böswillige und andere menschliche Aktivitäten gemeint. Diese sind in der Abbildung 4-2 dargestellt.

²² Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik; entsprechen dem internationalen Standard ISO/IEC 15408

²³ Werte (assets): Informationen oder Betriebsmittel

²⁴ BSI / Common Criteria / Seite 21

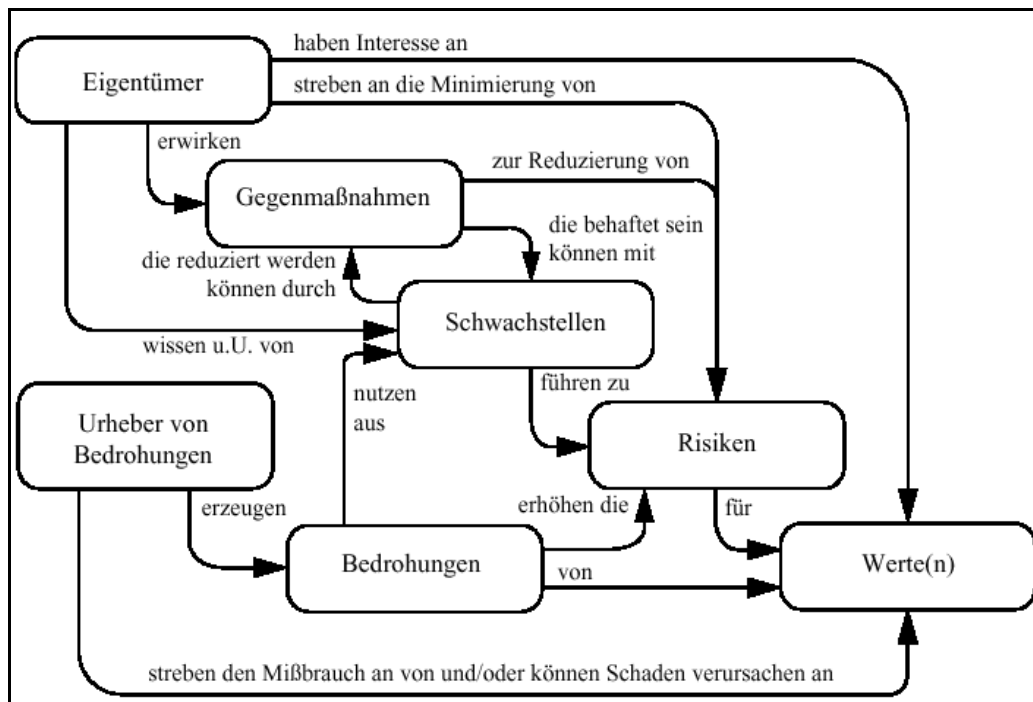


Abbildung 4-2: Sicherheitskonzepte und deren Wechselbeziehungen²⁵

5. Palladium / NGSCB

Bei NGSCB handelt es sich um eine Sicherheitsinitiative von Microsoft, einem der bedeutenden Mitglieder der TCG. Das Unternehmen betont allerdings, daß es sich bei NGSCB nicht um eine Umsetzung der TCG-Spezifikation²⁶ handelt.²⁷ Die Microsoft-Sicherheitsinitiative basiert sowohl auf Software-, als auch auf Hardwareelementen. Ursprünglich unter dem Namen Palladium bekannt geworden, wurde das Projekt Anfang des Jahres 2003 in NGSCB umbenannt. Ursache für diese Maßnahme sind wahrscheinlich die kontroversen Diskussionen, die um Palladium geführt wurden und den Namen aus der Sicht von Microsoft verdorben haben.²⁸ Microsoft will mit dieser Technologie ein „vertrauenswürdigen Betriebssystem“ auf der Basis einer Security Support Component (SSC) erschaffen. Die SSC wird in dem Kapitel 5.2. näher erläutert. NGSCB soll in zukünftige Windows-Versionen integriert werden. Bereits die nächste

²⁵ BSI / Common Criteria / Seite 22

²⁶ TCG / Spezifikation

²⁷ Vgl. Microsoft / NGSCB Technical FAQ

²⁸ Vgl. Webseiten wie z.B. <http://www.notcpa.org>

Version (Codename „Longhorn“), die Windows XP ablösen soll, soll diese Sicherheitskomponenten enthalten. Die Nutzung von NGSCB erfordert Änderungen am Chipsatz am Prozessor sowie an weiteren Hardwarekomponenten (siehe Kapitel 5.2.), um einen geschützten und isolierten Speicherbereich zur Verfügung stellen zu können und um den Datenfluß von der Tastatur zum Computer und vom Computer zum Bildschirm abzusichern. Microsoft sieht NGSCB als eine von zwei Säulen des „Trustworthy Computing“.²⁹ Die zweite Säule sind die Rights Management Services (RMS). RMS wiederum besteht aus Digital Rights Management (DRM) und Information Rights Management (IRM). Die Microsoft-Sicherheitsinitiative NGSCB wird im folgenden näher dargestellt.

5.1. Ziele von Microsoft NGSCB

Durch NGSCB soll verhindert werden, daß ein Programm in den Speicherbereich eines anderen eingreifen kann, wie das bei aktuellen Betriebssystemen noch möglich ist. Es soll dazu dienen, Software vor Software zu schützen. Ziel von NGSCB ist es, sowohl sichere, als auch die „normalen“ Betriebssystemoperationen auf einem Computer nebeneinander laufen zu lassen.³⁰ Grund dafür ist, daß es bei bisherigen Sicherheitsmodellen für Betriebssysteme nicht möglich ist, die Firmware, die Peripheriegeräte, Treiber und Anwenderprogramme so einzuschränken, daß eine angemessene Prozessisolierung möglich ist. Primäre Ziele von NGSCB sind Sicherheit und Systemintegrität.

5.1.1. NGSCB- Security Model

NGSCB baut auf vier wesentlichen Grundsätzen auf („Four Key Features“):³¹

- Sealed Storage („versiegelte Speicherung“)
- Secure Path to and from User (Input/Output)
- Attestation
- Strong Process Isolation

5.1.1.1 Sealed Storage

Durch Sealed Storage wird ermöglicht, Daten verschlüsselt auf der lokalen Festplatte des Computers zu speichern. Dazu bedient sich NGSCB einer speziellen „Security Sup-

²⁹ Vgl. Chip-Online / Microsoft: Digitale Rechte-Verwaltung im Überblick

³⁰ Vgl. Microsoft / NGSCB Security Model

³¹ Vgl. Microsoft / NGSCB Four Key Features

port Component“ kurz SSC und den in dieser Komponente vorhandenen Verschlüsselungstechnologien. Durch diesen Mechanismus kann sichergestellt werden, daß Daten, die auf diese Art und Weise gespeichert wurden, nur durch den NCA³² selber sowie durch andere Programme und Services, die der NCA als vertrauenswürdig identifiziert, eingesehen werden können. Ebenso wird der Zugriff zu den Daten gesperrt, wenn ein anderes Betriebssystem versucht darauf zuzugreifen (z.B. wenn die Festplatte in ein anderen Computer eingebaut wurde).

5.1.1.2 Secure Path to and from User

Um Daten nicht nur innerhalb der Trusted Application³³ als sicher zu gewährleisten, wird mit Hilfe von NGSCB der komplette Datenfluß von den Eingabegeräten (Tastatur, Maus) bis hin zu den Ausgabegeräten (Bildschirm) geschützt, um ein „Abfangen“ der Daten zu verhindern (Spyware, Trojaner). Dazu sind besondere Hardwarekomponenten (Secure Graphic Adaptor, Secure USB-Hub) nötig (siehe Abb. 5-4).

5.1.1.3 Attestation

Bei Attestation handelt sich um einen Mechanismus zur Authentifizierung von Soft- oder Hardware. Programmcode oder Daten können digital signiert werden um dem Empfänger den Ursprung und die Authentizität beweisen zu können. Attestation erlaubt einer Applikation sowohl eine andere Remoteapplikation zu identifizieren, als auch deren Integrität zu verifizieren.

5.1.1.4 Strong Process Isolation

Mit Hilfe des sogenannten „Curtained Memory“ kann ein bestimmter Bereich des Hauptspeichers abgeschottet werden, so daß andere Programme oder das Betriebssystem selber nicht mehr darauf zugreifen können. Dieser Bereich steht dann alleinig der Trusted Application zur Verfügung. Dies ist bei der heutigen Betriebssystem-Architekturen von Windows nicht möglich. Der RAM eines Computers ist in zwei Teile aufgeteilt: Ring-0 und Ring-3.³⁴ Der Ring-0-Bereich ist dem Betriebssystem vorbehalten (Kernel-Modus). Hier sind wichtige Systemfunktionen beinhaltet, wie zum Beispiel

³² NCA: Nexus Computing Agent, siehe Kapitel 5.3.1

³³ Trusted Application (sichere Anwendung): NGSCB-fähige Applikation

³⁴ Vgl. Bünning, Krause / Windows 2000 / Seite 76f

das Speichermanagement, das Scheduling und die Gerätetreiber für die Peripheriehardware. In diesem privilegiertem Ring wird der Kern des gesicherten Modus (Nexus) ablaufen. Im Ring-3 laufen die Anwendungsprogramme (Benutzer-Modus). Diese können jedoch bei dem bisherigen Windows-Betriebssystemen auch Funktionen des Rings-0 aufrufen, zum Beispiel wenn diese zusätzlichen Speicher benötigen. Sollte es bei diesem Vorgang ein Fehler auftreten, oder ein defekter Gerätetreiber im Ring-0 geladen sein, so kann es zu dem bekannten „Windows-Blue-Screen“ kommen.

Weiterhin soll von NGSCB der sogenannte Direct Memory Access (DMA) verhindert werden, so daß keine unautorisierten Programme oder Geräte aus dem „Curtained Memory“ lesen oder in diesen schreiben können. Alle Daten, die beispielsweise von der Festplatte in den sicheren Speicherbereich geladen werden sollen, müssen zunächst in das Betriebssystem oder in den normalen Bereich des Speichers eingelesen werden, um dann über einen NCA in den geschützten Bereich weitergeleitet werden. Durch diesen Mechanismus kann sichergestellt werden, daß die Trusted Application, die in dem geschützten Speicherbereich läuft, weder von anderen Programmen noch vom Betriebssystem manipuliert werden kann.

5.1.2. NGSCB und DRM

Bill Gates³⁵ erklärte zu Beginn der NGSCB-Initiative, daß der eigentliche Grund für die Entwicklung die Verbesserung und die Durchsetzung von Digital-Right-Management (DRM) war:

„We came at this thinking about music, but then we realized that e-mail and documents were ar more interesting domains“³⁶

Tatsächlich sprechen viele Tatsachen dafür, daß mit den Konzepten von TCG und NGSCB die Interessen der Musik-, Film- und Softwareindustrie umgesetzt werden sollen. DRM-Systeme könnten mit Hilfe dieser neuen Technologien wesentlich effektiver arbeiten. So wäre es beispielsweise möglich, im Zusammenhang mit dem SCC beim Herunterladen einer legal gekauften Musikdatei diese mit einem eindeutigen Schlüssel

³⁵ Chairman and Chief-Software-Architect der Microsoft Corporation

³⁶ Green / Präsentation zu TCPA S. 21

zu versehen, so daß diese Datei nur noch von dem Windows-Media-Player auf diesem Rechner als „sichere Datei“ identifiziert wird und somit auf keinem anderen Rechner lauffähig ist. Deshalb ist es auch nicht überraschend, daß das Microsoft-Patent 6,330,670 vom 08. Januar 1999 unter dem Namen „Digital Rights Management Operating System“ registriert ist.³⁷

5.1.3. Resümee der Ziele

Das offizielle Ziel von NGSCB (in Verbindung mit der TCG) ist es, eine vertrauenswürdige Computerumgebung für die Sicherheit des Nutzers bereitzustellen. Kritiker sprechen aber auch von ganz anderen Zielen: Durchsetzung des Digital-Rights-Managements, Verhinderung von Raubkopien, die Entwicklung von neuen teuren Abrechnungsmodellen für digitale Inhalte und die Verdrängung von unerwünschter Hardware- und Software-Konkurrenz.³⁸

5.2. Hardwarevoraussetzungen

Für die Nutzung der neuen NGSCB-Technologie ist eine neue Hardware gemäß der TCG-Spezifikation nötig. So müssen Änderungen am Chipsatz des Computers und am Hauptprozessor vorgenommen werden. Dies ist jedoch nachträglich bei herkömmlichen Geräten nicht möglich, so daß eine Neuanschaffung nötig ist. Auf der Hauptplatine eines NGSCB-fähigen Rechners ist ein Chip, ähnlich einer Smart-Card, fest aufgelötet. Mit Hilfe dieses zusätzlichen Chips können verschiedene kryptographische Schlüssel gespeichert werden. Diese Technologie wird von der TCG entwickelt. Im Detail sind folgende Hardwarekomponenten nötig, um NGSCB in vollem Umfang nutzen zu können:³⁹

- eine CPU die NGSCB unterstützt
- einen Chipsatz der NGSCB unterstützt
- SCC (Security Support Component)
- sichere Eingabegeräte (Tastatur, Maus)
- sichere Ausgabegeräte (Bildschirm)

³⁷ Vgl. US-Patent-Datenbank <http://www.uspto.gov> ; Patent-Nr.: 6,330,670

³⁸ Vgl. hierzu auch: Plura / Digital Rights Management

³⁹ Vgl. Microsoft / NGSCB Hardware

5.3. Komponenten, Struktur und Funktionsweise

5.3.1. NGSCB-Komponenten

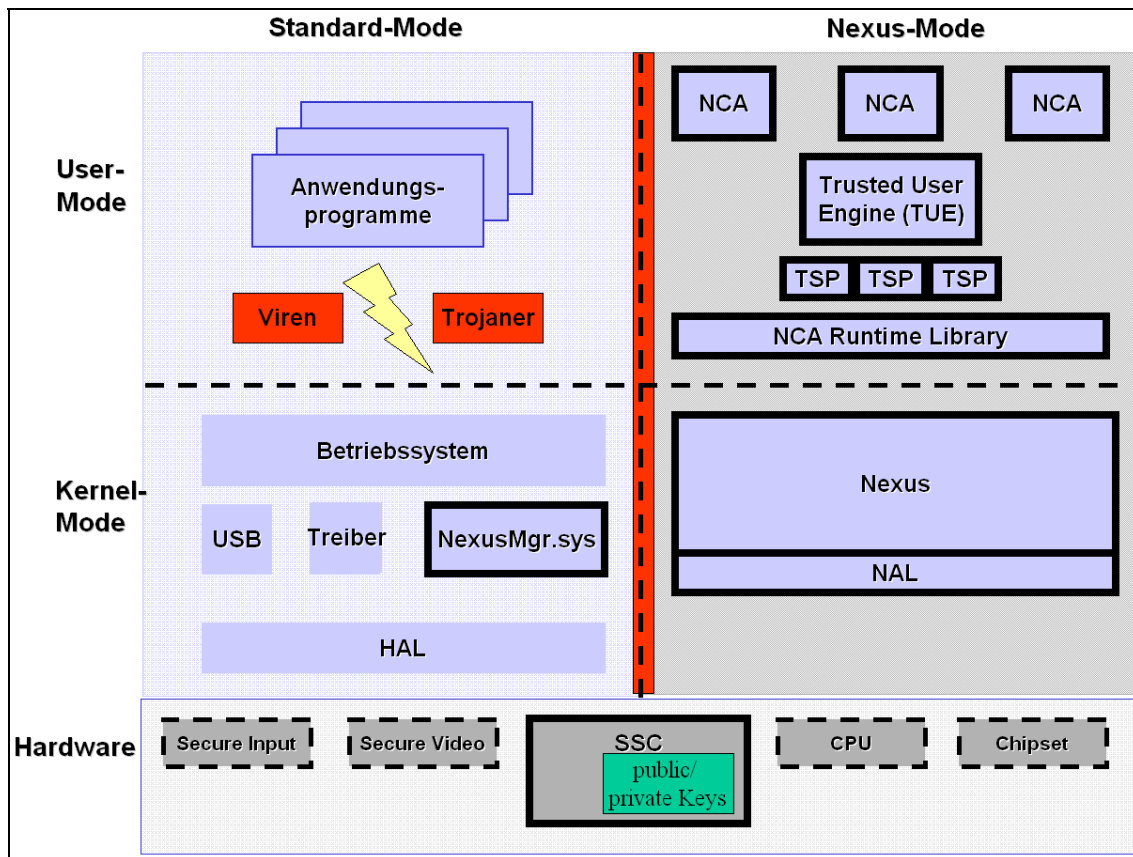


Abbildung 5-1: Komponenten im Aufbau von NGSCB⁴⁰

Wie die Abb. 5-1 verdeutlicht, wird es in einem NGSCB-fähigem Betriebssystem zwei unterschiedliche Sicherheitsmodi geben: den Standard- und den Nexus-Mode. Bei dem Standard-Mode handelt es sich um den Teil, der den heutigen Betriebssystemen entspricht. Dieser wird von Microsoft auch als LHS (Left-Hand-Side) bezeichnet. Bei dem Nexus-Modus handelt es sich um den sicheren Teil (Trusted Mode bzw. RHS (Right-Hand-Side)). Beide sind in der Lage, parallel auf einem Rechner zu laufen. Im Folgenden sollen die wichtigsten Komponenten näher erklärt werden:

⁴⁰ Vgl. Himmlein / Trusted Computing

SSC– Secure-Support-Component

Bei der Secure-Support-Component handelt es sich um ein Hardwarebestandteil nach der TCG-Spezifikation. Die SSC befindet sich auf dem Motherboard des Computers. Zu Beginn soll es sich um eine Art Smart-Card handeln, die auf die CPU aufgelötet wird. Später soll diese dann integriert werden. Hauptaufgaben sind die Speicherung der kryptographischen Schlüssel sowie die Bereitstellung von kryptographischen Operationen. Die SSC enthält ein 2048 Bit langes Schlüsselpaar nach dem PKCS-Standard #1⁴¹, einen weiteren Schlüssel (AES-128⁴²) sowie einen HMAC⁴³-Schlüssel.⁴⁴ Anhand dieses Schlüsselpaars wird von NGSCB ein RSA-Schlüssel⁴⁵ erzeugt, um das System zu authentisieren (Attestation). Beide Schlüssel werden nur innerhalb der SSC verwendet und sind nach außen hin nicht sichtbar.

Nexus

Der Nexus ist der wichtigste Bestandteil von NGSCB. Er läuft im sog. Curtained Memory (siehe Kapitel 5.1.1.4.) ab. Es handelt sich dabei um einen Sicherheitskern („Kernel“), der die sogenannte „Security Hardware“ managt und die Betriebssystemumgebung schützt. Der Nexus ist eine Art eigenes, kleines Betriebssystem, welches aus sehr wenig Quellcode bestehen soll. Genau wie ein richtiges Betriebssystem muß auch ein Nexus gebootet werden. Dies kann jedoch auch zur Laufzeit (also nach dem Start) des Hauptbetriebssystems erfolgen. Genauso kann er vor dem Shutdown des Hauptbetriebssystems wieder heruntergefahren werden. Ein Nexus ist verantwortlich für verschiedene NCA's (siehe nächster Punkt) und stellt Basisfunktionen für diese zur Verfügung. Weiterhin stellt er für NGSCB-Applikationen Services bereit, damit diese im sicheren Bereich des Betriebssystems (RHS) laufen können. Der Nexus besitzt Schnittstellen zum Standard-Betriebssystem, und er wird während des Startvorganges des Computers authentifiziert. Alle I/O-Operationen laufen über die LHS, also den normalen Betriebssystem-Modus. Weitere Eigenschaften des Nexus:⁴⁶

⁴¹ Vgl. RSA / PKCS #1

⁴² Vgl. <http://csrc.nist.gov/CryptoToolkit/aes/> (Abruf: 2003-10-15)

⁴³ HMAC: schlüsselabhängige Einweg-Hash-Funktion

⁴⁴ Vgl. Himmlein / Ganz im Vertrauen

⁴⁵ RSA: asymmetrisches Verschlüsselungsverfahren

⁴⁶ Vgl. Microsoft / NGSCB Security Model

- ermöglicht kryptographische Schlüssel sowie Ver- und Entschlüsselungsinformationen zu speichern
- identifiziert und authentifiziert die NCA's
- überwacht den Zugriff auf Trusted Applications und sichere Ressourcen
- leitet alle nötigen NGSCB-Funktionalitäten

Für den NCA stellt der Nexus die Basis-Services Memory-Mapping, Thread-Management und Interprocess Communication (IPC) zur Verfügung. Ein Bestandteil des Nexus-Kernels ist der Security Reference Monitor. Dieser beinhaltet eine vom Nutzer definierte Liste, welche Programme zu den Trusted Applications gehören sollen. Der Nexus entspricht dem TCG Software Stack (TSS) der TCG-Spezifikation.⁴⁷

NCA – Nexus Computing Agent

Bei dem NCA handelt es sich um eine Applikation, einen Teil einer Applikation oder einen Service, der im Protected-Operating-Environment läuft. Der NCA ist für die Kommunikation mit dem Nexus verantwortlich und wird im User-Modus ausgeführt.

NexusMgr.sys – Nexus-Manager

Sobald NGSCB-Services angefordert werden, wird eine Art Treiber im Standard-Modus (LHS) gestartet. Dabei handelt es sich um den Nexus-Manager (NexusMgr.sys). Dieser ist dafür verantwortlich, den Nexus zu laden sowie Services für diesen sowie andere Programme im Nexus-Mode (RHS) bereitzustellen. Die RHS kann nur über den Nexus-Manager (also über die LHS) mit der Außenwelt kommunizieren.

Weitere Komponenten:

- HAL – Hardware Abstraction Layer
- NAL – Nexus Abstraction Layer
- TSP – Trusted Service Provider
- TUE – Trusted UI Engine

⁴⁷ Vgl. TCG / TCG Software Stack

5.3.2. Funktionsweise

Microsoft stellt die Funktionsweise in Ihrem Whitepaper wie folgt grafisch dar:

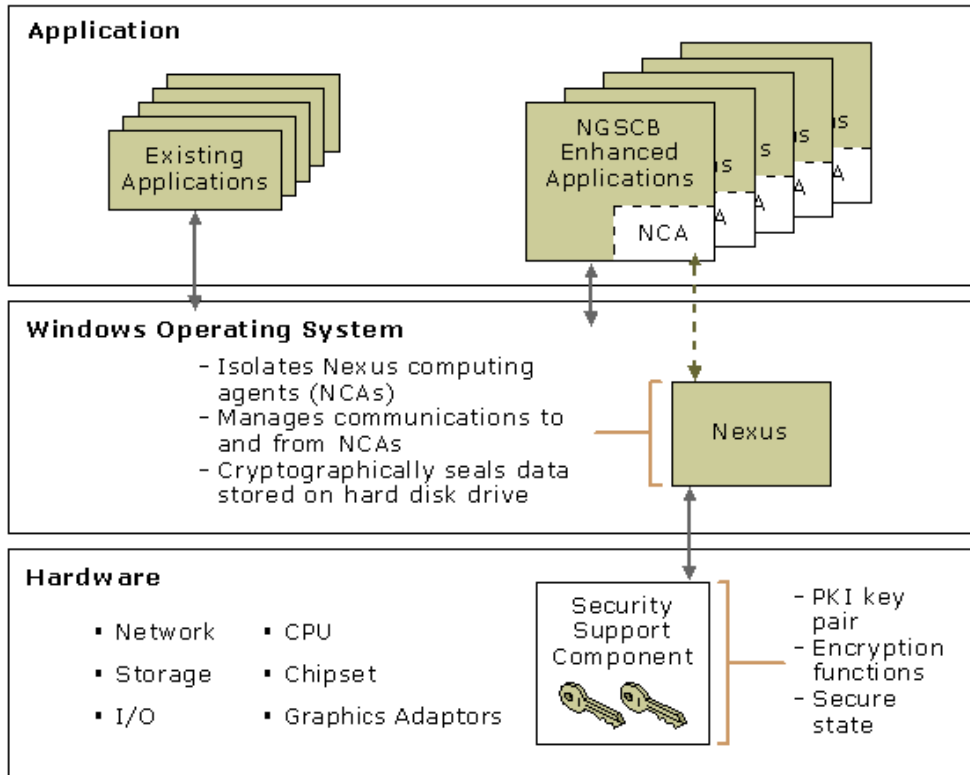


Abbildung 5-2: Interaktionen der NGSCB-Komponenten⁴⁸

Bei Programmen, die im sicheren Modus(RHS), d.h., im abgeschotteten Speicherbereich des Computers laufen, übernimmt der Nexus die Kontrolle. Mit Hilfe der eingesetzten Hardware, insbesondere des TPM-Chips [SSC], kann verifiziert werden, daß es sich bei dem operierenden Nexus auch um den handelt, dem der Nutzer vertraut. Der Nexus des NGSCB-Betriebssystems kann jederzeit gestartet werden. Sobald dieser aktiv ist, ermöglicht er, daß sich sowohl die Hardware- als auch die Softwarekomponenten authentifizieren können. Dadurch, daß sich der Nexus im abgeschotteten Speicherbereich befindet (curtained memory), kann er weder durch andere Programme, noch durch das Betriebssystem selber, manipuliert werden. Dieser Curtained Memory wird ebenso für das Ausführen von sogenannten „Sicheren Applikationen“ (Trusted Application) verwendet. Diese werden dann in speziellen Fenstern (Trusted Windows) am Bildschirm dargestellt, welche durch ein (nicht überschreibbares) Icon eindeutig gekennzeichnet sind. Diese Fenster können nicht durch andere Fenster von Standard-

⁴⁸ Vgl. Microsoft / NGSCB Security Model

Applikationen verdeckt werden. Weiterhin soll sichergestellt werden, daß sich Fenster von verschiedenen Trusted Applications nicht überlappen können.

Wird von dem Rechner verlangt, daß er sich authentifizieren soll (z.B. durch ein anderes Programm oder ein anderes System), so übermittelt er einen Hash des Sicherheitskerns (Nexus), der mit dem Public Key signiert wurde. Dieser Hash-Wert ist ausreichend, um die Vertrauenswürdigkeit des NGSCB-Systems zu beglaubigen.

Durch die Verknüpfung mit der Hardware sind reine Softwareattacken nicht mehr geeignet, um ein NGSCB-System zu überwinden.

Die Ausführung des NCA's und des Nexus erfolgt, genau wie die restlichen Programme des Computers, über eine Zeitscheibe.

Das Aktivieren der NGSCB-Funktion eines Betriebssystems soll lt. Microsoft keine Auswirkungen auf die Funktionsfähigkeit von Programmen haben, die nicht NGSCB-fähig sind. Der Datenaustausch zwischen den beiden Modi von NGSCB (Standard- und Nexus-Mode) erfolgt, wie in Abbildung 5-3 dargestellt, nur über den Nexus-Manager und den Nexus.

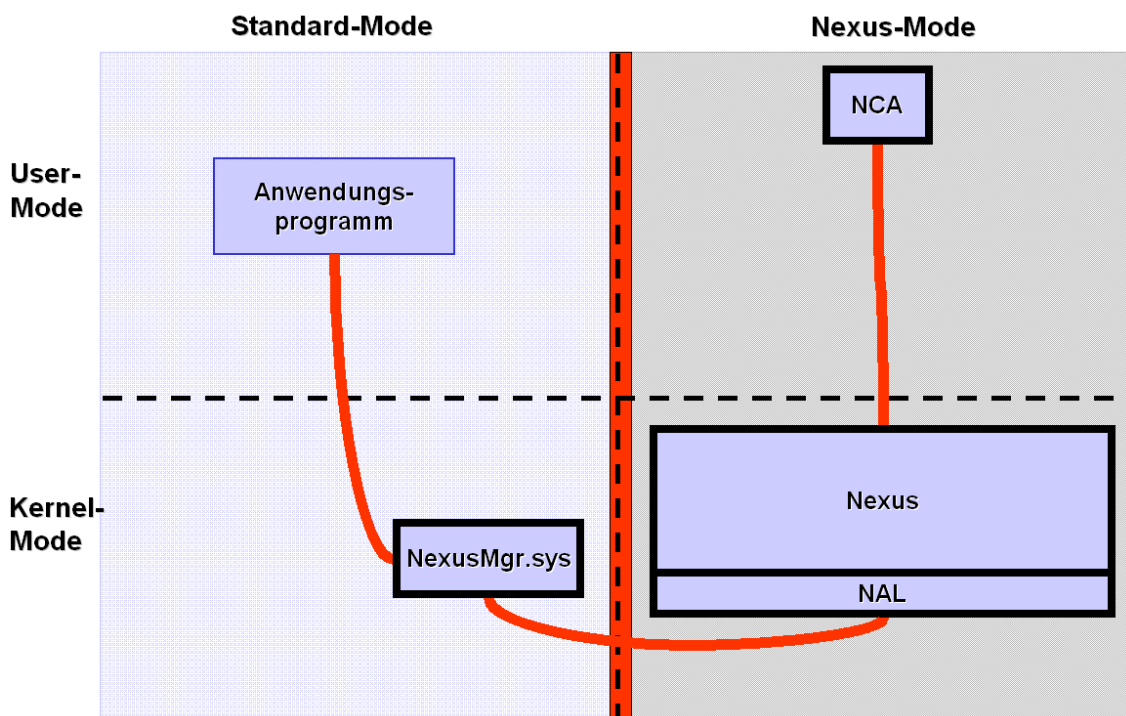


Abbildung 5-3: Austausch zwischen Standard- und Nexus-Mode⁴⁹

⁴⁹ Vgl. Himmlein / Trusted Computing

In der folgenden Abbildung 5-4 ist der Ablauf der sog. sicheren Ein- und Ausgabe (Trusted Input, Trusted Output) erkennbar.

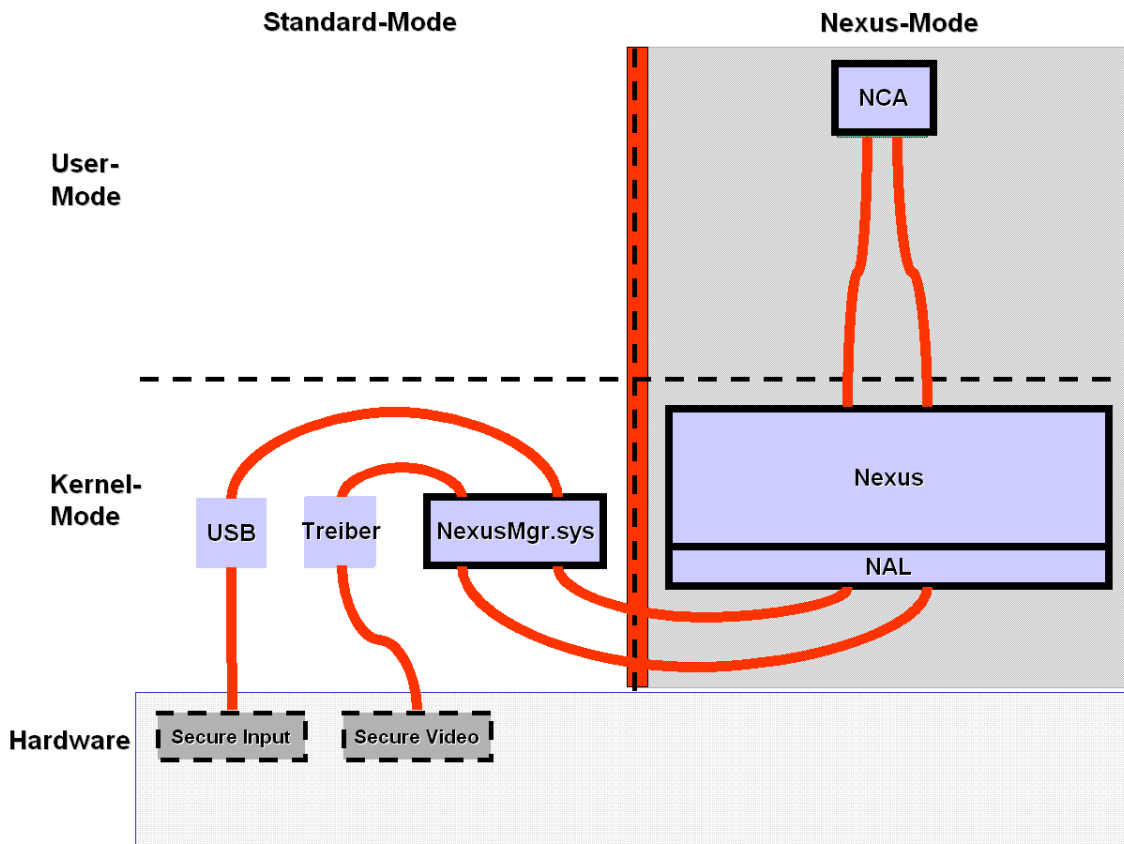


Abbildung 5-4: Datenfluß vom Secure Input bis zum Secure Output⁵⁰

Bei NGSCB handelt es sich also offenbar um eine Art "Sandkasten-Architektur", wie sie von Sun eingeführt wurde (*Virtual Machine*). Hauptunterschied zu dieser Architektur von Sun ist, daß nicht die unsicheren Programme in einer Sandbox ablaufen, sondern der sichere Teil des Betriebssystems. Im Vergleich mit der TCG-Spezifikation, die bereits in den Bootvorgang des Computers eingreift, kann man feststellen daß ein NGSCB-fähiges Betriebssystem sich nur auf diese Sandbox-Funktionen beschränkt.

Um zu gewährleisten, daß das System jederzeit weiß, auf welcher Seite (LHS bzw. RHS) gerade Operationen ausgeführt werden, ist für ein NGSCB-Betriebssystem eine spezielle CPU nötig. Diese muß einen extra Flag⁵¹ unterstützen, mit dessen Hilfe zwischen den beiden Modi umgeschaltet werden kann. Dies wird beispielsweise von einer

⁵⁰ Vgl. Himmlein / Trusted Computing

⁵¹ Flag: Bit oder Variable zur Kennzeichnung eines Zustandes

neuen Generation von INTEL-Chips unterstützt. Diese entsprechen der TCG-Spezifikation und tragen den Namen „La Grande“.⁵²

5.4. Chancen und Risiken von Microsoft NGSCB

5.4.1. Vorteile & Chancen

Microsoft gibt in seinem Whitepaper zum „Security Model“ von NGSCB⁵³ folgende Vorteile für den Nutzer an:

- ***erhöhte und bessere Möglichkeiten für die Kontrolle durch den Nutzer***
Microsoft betont, daß es sich bei NGSCB um ein sogenanntes „Opt-In-System“ handelt. Dies bedeutet, daß der Nutzer selbst entscheiden kann, ob bzw. inwieweit er die zusätzlichen Funktionen auf seinem Computer nutzen will. Standardmäßig sollen die NGSCB-Funktionen bei der Auslieferung von neuen Computern bzw. der Neuinstallation von Betriebssystemen ausgeschaltet sein. Da sowohl die NGSCB-Hardware als auch der Nexus nicht in den Startvorgang des Betriebssystems eingebunden sind, können diese auch keine Programme oder das Betriebssystem selber daran hindern, auf dem Computer zu laufen.
- ***Authentisierte Vorgänge***
NGSCB ermöglicht dem Nutzer, authentifizierte Operationen durchzuführen. So kann beispielsweise sichergestellt werden, daß eine Banking-Software nicht manipuliert wurde, oder die Daten, die mit der Bank ausgetauscht werden, auch wirklich nur von der Banking-Software eingesehen und verarbeitet werden können, und nicht zum Beispiel durch Auslesen des Speichers in unbefugte Hände geraten können (Vertraulichkeit).
- ***überwachter Zugang zu geschützten Ressourcen***
Auf Grundlage von benutzerdefinierten Regeln, die in der sog. NGSCB-Policy-Database hinterlegt sind, können den einzelnen Applikationen Zugriffsrechte auf geschützte Ressourcen gewährt werden. Diese Regeln können vom Nutzer eigenverantwortlich erstellt oder geändert werden.
- ***Plattformintegrität***

⁵² Vgl. Kreml / Hardware lügt nicht / c't 11/2003, S. 20

⁵³ Vgl. Microsoft / NGSCB Security Model

Durch NGSCB soll sichergestellt werden können, daß Manipulationen am System unmöglich sind. Microsoft stellt in seinem White-Paper das Beispiel eines Mitarbeiters einer Firma dar, der sich mit Hilfe seines privaten PC's in das Firmennetzwerk einloggen will. Durch NGSCB soll verhindert werden, daß sowohl Manipulationen am Firmenrechner (z.B. durch böswillige Programme, die der Mitarbeiter unbemerkt auf seinem PC hat), als auch der Zugriff auf private Daten des Mitarbeiters von der Seite des Unternehmens aus, ausgeschlossen sind.

- ***Schutz vor Identitätsmißbrauch, unerlaubten Zugang und sonstigen Attacken***
- ***Weiternutzung bisheriger Applikationen***
- ***Vertrauenswürdigkeit und Integrität der Daten für Applikationen***

Tatsächlich scheint das neue System optimal geeignet zu sein, um private Schlüssel sowie sensitive Daten zu schützen. Dadurch, daß diese Daten verschlüsselt werden, können Angriffe auf diese von außen besser abgewehrt werden. Die Verschlüsselung von Daten kann mit Hilfe der gespeicherten Keys effektiver und sicherer erfolgen. Es wäre möglich, mit einem entsprechend ausgestatteten E-Mail-Programm die Herkunft von Mails zu verifizieren, wodurch SPAM sowie Viren und Trojaner, die sich durch e-Mails weiterverbreiten, unterbunden werden könnten. Paßwörter und andere schützenswerte Inhalte können mit Hilfe von NGSCB sicher verwaltet werden. Dokumente könnten derart geschützt werden, daß nur eine bestimmte Person diese lesen können. So könnte beispielsweise eine Excel-Datei mit konfidenziellen Daten, die aus Versehen an eine falsche Mailadresse gesendet wurde, von dem Empfänger nicht geöffnet werden. In Bezug auf die Hautsicherheitsziele kann man folgendes feststellen:

- ***Integrität***

Durch die Verhinderung des Zugriffs auf geschützte Daten (Sealed Storage) kann sichergestellt werden, daß diese nicht verändert werden können. Somit wird die Integrität des Computers und der verwendeten Daten signifikant erhöht werden. Allerdings besteht das Problem, daß NGSCB zwar sicherstellen kann, daß kein unbefugter Zugriff auf die geschützten Daten besteht, aber diese können nicht davor geschützt werden, daß man diese einfach komplett löscht.
- ***Verfügbarkeit***

Durch NGSCB geschützte Daten und Software können nicht (oder nur schwer) manipuliert werden. Dadurch erhöht sich deren Verfügbarkeit. Allerdings ist zu

bemerken, daß der gesicherten Modus (RHS) auf die Steuerung durch die (unsichere) LHS angewiesen ist. Dadurch können Viren, Trojanern sowie DOS-Attacken die auf die LHS gerichtet sind, die RHS in Mitleidenschaft ziehen (im Hinblick auf deren Verfügbarkeit). Wie bereits unter dem Punkt Integrität genannt, können gesicherte Daten nicht vor dem Löschen geschützt werden. Dies beeinträchtigt die Verfügbarkeit der Daten in hohem Maße.

- ***Vertraulichkeit***

Am meisten wird NGSCB das Ziel der Vertraulichkeit unterstützen. Durch die Technologie der Verschlüsselung und der sicheren Aufbewahrung der dazugehörigen Keys kann gewährleistet werden, daß Informationen auch nur dem Personenkreis zur Verfügung stehen, der zu deren Nutzung legitimiert ist.

Zusammenfassend kann man sagen, daß durch NGSCB eine Verbesserung der Sicherheit in der Informationstechnik zu erwarten ist.

5.4.2. Nachteile und Risiken

Während eines Kongresses des BSI in Bonn zur IT-Sicherheit äußert der Staatssekretär im Innenministerium Göttrik Wewer Kritik an den TCG- und NGSCB-Initiativen.

Es bestehe "die Gefahr, dass diese Technologien den Nutzer in seiner Freiheit beschneiden und dem Nutzer unbemerkt die Kontrolle über seine persönlichen Daten entgleitet".⁵⁴ Durch die Monopolstellung von Microsoft werde die Entwicklung „offener“ Software ausgebremst (freie Software, Open-Source). Weiterhin könnten Einschränkungen im freien Gebrauch von Rechnern die Folge von NGSCB sein. Viele Kritiker befürchten, daß Microsoft mit Hilfe von NGSCB seine Monopolstellung am Softwaremarkt (Betriebssysteme, Office-Anwendungen etc.) weiter ausbauen könnte.⁵⁵ Weiterhin ist bedenklich, daß die neue Sicherheitsinitiative für viele datenschutzfeindliche Zwecke genutzt werden kann und der Anwender des Betriebssystems auf die Sicherheit von NGSCB und dem dazugehörigen SSC vertrauen muß. Die Sicherheit des Systems beruht auf der Annahme, daß es niemandem gelingt, die Kombination aus Hard- und Softwaremechanismen zu überwinden. Doch wer kann schon im Vorfeld garantieren, daß dies nicht der Fall sein wird.

⁵⁴ Schulzki-Haddouti / TCPA- und Palladium-Nachfolger

⁵⁵ Vgl. Heise / Software-Monokultur

Weitere bisher ungelöste technische Probleme:⁵⁶

- Fernwartung
Durch die „Sicher Eingabe“, die zu den Grundzielen von NGSCB gehört, kann keine Fernwartung erfolgen (Secure Path to and from User, siehe Kapitel 5.1.1.2.)
- Behindertengerechte Nutzung
Die Sicherheit der Ein- und Ausgabegeräte ist in der bisherigen Spezifikation nur für die Tastatur, Maus (Trusted Input über USB) und den Monitor (Trusted Output) möglich (siehe Abb. 5-4). Eine behindertengerechte Nutzung des Betriebssystems würde allerdings weitere Kanäle wie z.B. den Audio-Output erfordern.
- Schutz vor Löschung verschlüsselter Daten
- Auslagerung des geschützten Speichers
Beim Stromsparmodus von Computern wird in aktuellen Betriebssystemen der komplette Inhalt des Arbeitsspeichers auf die Festplatte ausgelagert und beim Neustart wieder in diesen zurückgespeichert. Dadurch wären die Daten (auch des geschützten Bereiches) des Arbeitsspeichers auslesbar.

Als weitere ungelöste Probleme sieht Gerhard Himmlein mögliche DoS-Angriffe (Denial-of-Service) sowie die Zertifizierung der Programme. Aber auch unsichere Verschlüsselungsmechanismen können ein Defizit in der neuen Technologie darstellen.⁵⁷

6. Ausblick

Durch die Einführung der NGSCB-Komponente im nächsten Windows-Betriebssystem „Longhorn“ und die dadurch verbundene Abschottung von unsicheren Applikationen wird das Betriebssystem sicherer werden. Trotzdem können bestehende Anwendungen auf der neuen Plattform weitergenutzt werden (Abwärtskompatibilität). Alles das hört sich, abgesehen von dem höheren Mehraufwand, z. B. durch Zertifizierung neuer Hardware und Software und einiger ungelöster Probleme und Anfangsschwierigkeiten, alles sehr positiv an. Aber hinter dem Namen „Sicherheit“ können genauso „Überwa-

⁵⁶ Vgl. Himmlein / Trusted Computing

⁵⁷ Vgl. Heise / Trusted Computing

chung“, „nicht übertragbare Software“, usw. stehen. Mit NGSCB bekommt Microsoft eine Möglichkeit zu verhindern, daß der Nutzer Software verwendet, die nicht legal erworben wurde. Bis zur tatsächlichen Einführung wird noch einige Zeit vergehen in der Microsoft noch viel Informationspolitik betreiben muß, um die zahlreichen Kritiker von NGSCB von der neuen Technologie zu überzeugen. Microsoft versucht unübersehbar den Kunden glauben zu lassen, daß es sich bei NGSCB um eine Technologie handelt, die ausschließlich zum Nutzen des Kunden entwickelt wurde und betont, daß es sich bei NGSCB um ein sogenanntes Opt-In-System handelt, das heißt, daß die zusätzlichen Funktionen bei Auslieferung des Betriebssystems ausgeschaltet sind, und erst durch den Nutzer aktiviert werden (wenn er dies wünscht). Sollte sich allerdings NGSCB als Quasi-Standard bei Softwareprodukten durchsetzen so wird man durch das Nicht-Aktivieren von NGSCB-Funktionen von bestimmten Diensten ausgeschlossen – ähnlich wie bei Cookies auf bestimmten Webseiten. Es wird dann ein „DRM-für-Jedermann“ geben. Jeder kann seine Texte, Bilder oder sonstige Dokumente schützen. Informationen, die bisher frei zugänglich im Internet zur Verfügung stehen, könnten dann durch Copyrights geschützt werden und ließen sich nicht mehr auf jedem Computer öffnen. Das heutige Informationszeitalter basiert jedoch auf dem freien Fluß von Informationen. Somit hat NGSCB (in Verbindung mit DRM und den TCG-Spezifikationen) das Potential diese Informationsgesellschaft negativ zu beeinflussen.

7. Literaturverzeichnis / Quellenangaben

BSI / Common Criteria /

Bundesamt für Sicherheit in der Informationstechnik: Common Criteria

Teil 1: Einführung und allgemeines Modell

<http://www.bsi.bund.de/cc/>

Abruf: 2003-08-27 [Q01]⁵⁸

Auding / Computerviren /

Iris Auding: Unsichtbar und höllisch gefährlich

in: Manager-Magazin

<http://www.manager-magazin.de/ebusiness/cebit/0,2828,240376,00.html>

Abruf: 2003-08-25 [Q02]

Himmelein / Der digitale Knebel /

Gerald Himmelein: Der digitale Knebel

in c't 15/2002, S. 18

Plura / Digital Rights Management /

Michael Plura: Der PC mit den zwei Gesichtern

in: c't 24/2002, S. 186

Heise / DRM-Client /

Heise-Newsticker / Microsoft veröffentlicht DRM-Client

<http://www.heise.de/newsticker/data/anw-05.09.03-001/>

Abruf: 2003-10-28 [Q03]

Heise / DRM für Dokumente /

Heise-Newsticker: Microsofts DRM für Dokumente und Firmen-Unterlagen

<http://www.heise.de/newsticker/data/jk-23.02.03-003/>

Abruf: 2003-10-28 [Q04]

⁵⁸ Die Zahl in den eckigen Klammern gibt das Verzeichnis der gespeicherten Onlinequelle auf der beiliegenden CD an ([Q..]).

NIST / Firmen-Webseite /

Institute of Standards and Technology (NIST) USA

<http://csrc.nist.gov/CryptoToolkit/aes/>

Abruf: 2003-10-26 [Q05]

Himmlein / Ganz im Vertrauen /

Gerald Himmlein: Ganz im Vertrauen - Microsoft betont die Privatsphäre

in: c't 8/2003, S. 33

Himmelein / Ganz im Vertrauen-TCG /

Gerald Himmlein: Ganz im Vertrauen-TCPA ist tot, es lebe die TCG

in c't 9/2003, S. 52

BSI / Grundschatzhandbuch /

Bundesamt für Sicherheit in der Informationstechnik:: IT-Grundschatzhandbuch

Stand: 4.Ergänzungslieferung, Mai 2002

Krempl / Hardware lügt nicht /

Stefan Krempl: Hardware lügt nicht

in c't 11/2003, S. 20

Bachfeld / IT-Sicherheit (Heise-Newsticker) /

Daniel Bachfeld: IT-Sicherheit in der US-Stromversorgung

<http://www.heise.de/ct/03/18/034/default.shtml>

Abruf: 2003-08-25 [Q06]

Rannenberg / Mehrseitige Sicherheit /

Kai Rannenberg: Mehrseitige Sicherheit - Schutz für Unternehmen und ihre
Partner im Internet

in: Wirtschaftsinformatik Nr. 42 (2000), S. 489-497

Chip-Online / Microsoft: Digitale Rechte-Verwaltung im Überblick /

http://www.chip.de/news/c_news_10245909.html

Abruf: 2003-10-21 [Q07]

Microsoft / Microsoft Security Bulletin MS03-026 /

Microsoft Corporation: Microsoft Security Bulletin MS03-026

Onlineartikel: <http://www.microsoft.com/germany/ms/technetservicedesk/bulletin/bulletinms03-026.htm>

Abruf: 2003-08-13 [Q08]

Microsoft / NGSCB-Whitepaper /

Microsoft Corporation: NGSCB: Trusted Computing Base and Software Authentication

http://www.microsoft.com/resources/ngscb/documents/ngscb_tcb.doc

Abruf: 2003-05-15 [Q09]

Microsoft / NGSCB Four Key Features /

Microsoft Corporation: The Next-Generation Secure Computing Base: Four Key Features

http://www.microsoft.com/resources/ngscb/four_features.msp

Abruf: 2003-08-20 [Q10]

Microsoft / NGSCB Hardware /

Microsoft Corporation : Hardware Platform for the NGSCB

<http://www.microsoft.com/resources/ngscb/documents/NGSCBhardware.doc>

Abruf: 2003-05-15 [Q11]

Microsoft / NGSCB Security Model /

Microsoft Corporation: Security Model for the Next-Generation Secure Computing Base

<http://www.microsoft.com/resources/ngscb/productinfo.msp>

Abruf: 2003-08-20 [Q12]

Microsoft / NGSCB Technical FAQ /

Microsoft Corporation: Microsoft Next Generation Secure Computing Base - Technical FAQ

<http://www.microsoft.com/technet/security/news/NGSCB.asp>

Abruf: 2003-08-20 [Q13]

Hermanns, Mühlhaeuser / notcpa.org /

Jannis Hermanns, Christian Mühlhaeuser (Augsburg), Webseite notcpa.org

<http://www.notcpa.org>

Abruf: 2003-10-28 [Q14]

Emnid / Onliner-Atlas /

TNS Emnid: Onliner-Atlas 2002 – Eine Topographie des digitalen Grabens durch Deutschland

Downloadseite:

<http://www.emind.emnid.de/news/studien.html>

direkter Link:

<http://www.emind.emnid.de/downloads/studien/200212101Atlas2002.pdf>

Abruf: 2003-08-14 [Q15]

RSA / PKCS #1 /

RSA Security Inc.: PKCS #1 - RSA Cryptography Standard

<http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html>

Abruf: 2003-10-26 [Q16]

Green / Präsentation zu TCPA /

Lucky Green: „Trusted Computing Platform Alliance: The Mother(board) of all Big Brothers“

http://www.cypherpunks.to/TCPA_DEFCON_10.pdf

Abruf: 2003-10-09 [Q17]

Fischer / Sicherheitsmanagement in der IV /

Daniel Fischer: Skript zur Vorlesung „Sicherheitsmanagement in der IV“
Teil „Sicherheit im Mobile Business“

Version: 2003-01-15

Stelzer / Sicherheitsstrategien /

Dirk Stelzer: Sicherheitsstrategien in der Informationsverarbeitung - Ein wissensbasiertes, objektorientiertes Beratungssystem für die Risikoanalyse.

Braunschweig - Wiesbaden 1993

Heise / Software-Monokultur /

Heise-Newsticker: IT-Verband kritisiert Software-Monokultur durch Microsoft

<http://www.heise.de/newsticker/data/anw-24.09.03-006/>

Abruf: 2003-10-20 [Q18]

Adobe / Softwarepiraterie /

Adobe Systems GmbH: Konsequenzen von Softwarepiraterie

www.adobe.de/aboutadobe/antipiracy/consequences.html

Abruf: 2003-08-25 [Q19]

Pew Internet & American Life Project / Spam-Report /

http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf

Abruf: 2003-10-26 [Q20]

TCG / Spezifikation /

Trusted Computing Group: TCG-Spezifikation

https://www.trustedcomputinggroup.org/downloads/tcg_pc_specification_1_0.pdf

Abruf: 2003-10-26 [Q21]

Heise / Tauschbörsen /

Heise-Newsticker: „Spider-Man" und "Star Wars: Episode II" lassen Tauschbörsen brummen

<http://www.heise.de/newsticker/data/daa-31.05.02-000/>

Abruf: 2003-08-14 [Q22]

TCG / TCG Software Stack /

Trusted Computing Group: TCG Software Stack (TSS) Specification

https://www.trustedcomputinggroup.org/downloads/TSS_Version_1.1.pdf

Abruf: 2003-10-26 [Q23]

Schulzki-Haddouti / TCPA- und Palladium-Nachfolger /

Christiane Schulzki-Haddouti: Innenministerium kritisiert TCPA- und
Palladium-Nachfolger

<http://www.heise.de/newsticker/data/anw-14.05.03-001/default.shtml>

Abruf: 2003-09-12 [Q24]

Heise / Trusted Computing /

Heise-Newsticker: Kein Vertrauen in Trusted Computing

<http://www.heise.de/newsticker/data/jk-08.08.03-004/>

Abruf: 2003-08-08 [Q25]

Himmlein / Trusted Computing /

Gerald Himmlein: Trusted Computing - Ein kurzer Spaziergang (45 Minuten)

<http://www.heise.de/ct/Redaktion/ghi/tc/linuxtagTClinked.html>

Abruf: 2003-10-09 [Q26]

Heise / W32.Blaster /

Heise-Newsticker: W32.Blaster befällt Hunderttausende von PCs

<http://www.heise.de/newsticker/data/dab-13.08.03-000/>

Abruf: 2003-08-13 [Q27]

Bünning, Krause / Windows 2000 /

Uwe Bünning, Jörg Krause: Windows 2000 im professionellen Einsatz

Grundlagen und Strategien für den Einsatz am Arbeitsplatz und im Netzwerk

Carl Hanser Verlag

Berlin – September 2002

Microsoft / Windows Media Rights Manager /

Microsoft Corporation: Architecture of Windows Media Rights Manager

www.microsoft.com/windows/windowsmedia/WM7/DRM/architecture.aspx

Abruf: 2003-10-20 [Q28]