Sitzung des DIHK-Ausschusses Telekommunikation und neue Dienste
13. Mai 2004

Trusted Computing

Andreas Neumann

Zentrum für Europäische
Integrationsforschung (ZEI), Bonn

Trusted Computing *(Andreas Neumann)*

Konzept des Trusted Computing (grob vereinfacht):

- Trusted Platform Module (TPM) als fest an eine Rechnerplattform gebundenes Hardwaresicherheitsmodul, spezifiziert von der Trusted Computing Group (TCG)
- TPM erfüllt drei zentrale Funktionen (Authentifizierungs-, Kryptographie- und Mess-/Überwachungsfunktion)
- Software kann TPM nutzen, um eine „Kette der Vertrauenswürdigkeit“ zu schaffen und auf diese Weise Systemintegrität sicherstellen

⇒ Betriebssystem von zentraler Bedeutung

- Besonderheit: Fernattestierung (Remote Platform State Attestation) erlaubt Bestätigung, dass sich Plattform in einem bestimmten Zustand befindet (potentielle Einsatzgebiete wären u. a. elektronischer Geschäftsverkehr und DRM)

⇒ Trusted-Computing-Konzept ist nicht auf PCs beschränkt, sondern auch auf PDAs, Mobiltelefone, Set-Top-Boxen, Video- und DVD-Abspielgeräte etc. übertragbar

Trusted Computing *(Andreas Neumann)*

NGSCB (Next-Generation Secure Computing Base):

- Microsofts Ansatz für ein vertrauenswürdiges Betriebssystem (früher als „Palladium“ bekannt)
- Integration in nächste „Windows“-Version („Longhorn“) geplant
- Ursprünglich: „Nexus“ als Trusted Operating Root, in dem sicher abgeschirmte „Nexus Computing Agents“ (NCAs) laufen („Linke Hand/rechte Hand“-Konzept)
- NGSCB benötigt Hardwarefunktionalitäten, die über die TCG-Spezifikationen hinausgehen (sichere Datenpfade von und zum Nutzer etc.)

La Grande (Intel)/Secure Execution Mode (SEM) (AMD):

- Mikroprozessortechnologie mit gegenüber den TCG-Spezifikationen erweiterten Sicherheitsfunktionalitäten
- Potentielle Hardwarebasis für NGSCB

Trusted Computing *(Andreas Neumann)*

Gefahren für den unbeschränkten Wettbewerb:

- Wettbewerbsbeschränkende Vereinbarungen zwischen mehreren Unternehmen bzw. abgestimmte Verhaltensweisen

⇒ Gefahr durch Kartelle *Artikel 81 EG*

- Entstehen marktbeherrschender Positionen, die es einem Unternehmen ermöglichen, sich der Kontrolle durch den Wettbewerb zu entziehen und Marktbedingungen frei zu bestimmen

⇒ Gefahr durch Marktbeherrscher *Artikel 82 EG*

Trusted Computing *(Andreas Neumann)*

Wettbewerbsrechtliche Bedenken gegen TCG (1):

- Art. 81 Abs. 1 EG erfasst auch Vereinbarungen, die lediglich die Wettbewerbsmöglichkeiten Dritter beeinträchtigen
- Netzwerkeffekte können TCG-Konformität zur faktischen Marktzugangsbedingung machen
- Wettbewerbsvorteile durch TCG-Mitgliedschaft:
  - Einfluss auf Spezifikationen, Erlangung technischen Wissens, früherer Zugriff auf Spezifikationen
  - Nur TCG-Mitglieder haben gemäß der TCG-Satzung einen *Anspruch* auf Lizenzierung von Patenten, die für TCG-Produkte erforderlich sind, zu vernünftigen und nicht diskriminierenden Bedingungen

  ⇒ Zentrale Bedeutung der Mitgliedschaftsbedingungen für etwaige wettbewerbliche Auswirkungen

Trusted Computing *(Andreas Neumann)*

Wettbewerbsrechtliche Bedenken gegen TCG (2):

- Keine Abhängigkeit der Mitgliedsgebühren von der finanziellen Leistungsfähigkeit bzw. anderen wirtschaftlichen Kenngrößen des Mitgliedsunternehmens (im Gegensatz zu zahlreichen anerkannten Standardisierungsorganisationen)
- Niedrigste Mitgliedskategorie (Adopter Member) partizipiert nur sehr gering an Vorteilen der Mitgliedschaft (im Wesentlichen beschränkt auf Teilnahme an der Lizenzpolitik)
- Lizenzinhaber sind regelmäßig marktstarke Mitgliedsunternehmen (finanzieller Transfer zu Lasten der KMU durch Lizenzgebühren)

⇒ Wettbewerbsbeschränkung gegenüber KMU

- Wettbewerbsvorsprung der Gründungsmitglieder: Wesentliche Entscheidungen der ursprünglichen TCPA-Spezifikationen und der TCG-Spezifikationen wurden jeweils in der Frühphase der Organisation getroffen
- Grundsätzliches Problem: nicht kommerzielle, quelloffene Software (Open Source)

Trusted Computing *(Andreas Neumann)*

Wettbewerbsrechtliche Bedenken gegen NGSCB:

- Behinderungspotential gegenüber Wettbewerbern auf Anwendungsmärkten durch Kontrolle über NGSCB-API (Schnittstellenproblematik)
- Marktmachtausübung auf vorgelagerten Hardwaremärkten:
  - Prominente Rolle in TCPA/TCG
  - Ausrichtung von La Grande auf NGSCB – Gefahr einer „gemeinsamen vertikalen Marktbeherrschung“ (Art. 81 EG *und* Art. 82 EG)?
  - Faktische Notwendigkeit, dass Trusted-Computing-Hardware kompatibel mit NGSCB ist – Aushebelung des transparenten, offenen und nicht diskriminierenden Standardisierungsprozesses durch Anpassungsdruck auf TCG?
- Schaffung neuer Interdependenzen mit Inhalteebene: Nach EuGH-Rechtsprechung kann ein Verstoß gegen Art. 82 EG bei Vorliegen besonderer Umstände auch durch ein Verhalten begründet werden, das lediglich einen Markt betrifft, der mit dem beherrschten Markt nur „verbunden“ ist (erhöhtes Missbrauchspotential und erhöhte Kontrolldichte)

Trusted Computing *(Andreas Neumann)*

Wettbewerbsrechtliche Bedenken bzgl. institutioneller Aspekte:

- Das Konzept vertrauenswürdiger Systemumgebungen sieht an zahlreichen Stellen die Einbindung von Zertifizierungsinstanzen vor (TPME, PE, CE, VE, Privacy CA, zukünftig: NGSCBE?)
- Beschränkungen des Zugangs zum Zertifizierungsmarkt können gegen Art. 81 Abs. 1 EG oder Art. 82 EG verstoßen:
  - Zulassung nur bestimmter Unternehmen
  - Beeinflussung der Zertifizierungsbedingungen
- Problem der Geschäfts- und Betriebsgeheimnisse im Falle der Weitergabe von Bauplänen/Quelltexten

⇒ Dezentrale Zertifizierungsinfrastrukturen!

Trusted Computing *(Andreas Neumann)*

Neue technische Entwicklungen (1): TPM-Spezifikationen 1.2

- Direkte anonyme Bestätigung
- Schlüsselmigration
- Löschen des Endorsement-Schlüssels
- Lokalität
- Delegation
- Transportschutz und General-Purpose-IO
- Monotone Zähler und Uhren
- Nicht flüchtiger Speicher
- Kontextsicherung und Wiederherstellung

Trusted Computing *(Andreas Neumann)*

Neue technische Entwicklungen (2): NGSCB

- WinHEC 2004: partielle Neuausrichtung des NGSCB-Konzepts, allerdings keine Beendigung des Projekts(!)
- Aufgabe des „Linke Hand/rechte Hand“-Konzepts
- Grund: erheblicher Aufwand für die Anpassung bestehender Anwendungen (insbesondere auch von Drittherstellern)
- Abgeschottete Bereiche („Compartments“) als sichere (Teil-) Umgebungen innerhalb des restlichen Systems (virtuelle Maschinen?)

Trusted Computing *(Andreas Neumann)*

Neue rechtliche Entwicklungen (1): Stellungnahme der Bundesregierung zu TCG/NGSCB

- Inhaltliche Verantwortung bei BMWA/BMI: sowohl wirtschaftspolitische als auch sicherheitstechnische Aspekte (im Folgenden nur wirtschaftspolitische Forderungen)
- Anforderung an TCG – faire Lizenzpolitik:
  - Keine Ausgrenzung von Nichtmitgliedern, Freistellung nicht kommerzieller Open-Source-Projekte
  - Ermöglichung der kostenfreie Nutzung, Modifikation und Weitergabe der spezifizierten Treibersoftware (Trusted Software Stack, TSS)
  - Offenlegung relevanter Schutzrechte durch Mitglieder und Lizenzierung nach GSR-Politik
  - Klärung der Möglichkeit, einen Technologiepool einzurichten
- Anforderung an TCG – nicht diskriminierende Informationspolitik:
  - Einführung einer unentgeltlichen Mitgliedschaft mit Möglichkeit des zeitnahen Zugriffs auf notwendige Informationen (für nicht kommerzielle Projekte ohne Kosten)
  - Sicherstellung ausgewogener Interessenvertretung innerhalb der TCG

Trusted Computing *(Andreas Neumann)*

Neue rechtliche Entwicklungen (1): Stellungnahme der Bundesregierung zu TCG/NGSCB

- Anforderung an TCG – keine Schaffung von Marktzugangsschranken:
  - Keine Schaffung oder Verstärkung marktbeherrschender Stellungen
  - Keine Schaffung von Marktzutrittshemmnissen
  - Schaffung einer gemeinsamen Schlichtungsstelle von TCG sowie Branchen- und anderen Verbänden für Beschwerden über mögliche Diskriminierung
- Anforderung an TCG – technologische Offenheit:
  - TPM muss systemoffen sein
  - Interoperabilität von TCG- mit Nicht-TCG-Systemen muss sichergestellt sein
  - Keine einseitige Bevorzugung einzelner Mitgliedsunternehmen durch Spezifikationen
- Anforderung an NGSCB:
  - Offene und transparente Informationspolitik
  - Keine Diskriminierung durch Lizenzbedingungen
  - NGSCB-fähiges Betriebssystem muss auch Nicht-NGSCB-Anwendungen ausführen
  - Bei Nutzung für DRM-Zwecke Vorrang einer Offline- vor einer Online-Prüfung

Trusted Computing *(Andreas Neumann)*

Neue rechtliche Entwicklungen (2): Arbeitspapier der Art. 29-Datenschutzgruppe vom 23. Januar 2004

- Primär datenschutzrechtliche und -technische Erwägungen (nachfolgend nur wettbewerbsrechtlich relevante Erwägungen)
- Erhöhung der Sicherheit in Unternehmensumgebungen, aber Zweifel am Nutzen für den Verbraucher (ambivalentes Nutzenpotential)
- Zweifel an faktischer Relevanz der Wahlfreiheit beim Einsatz des TPM (Opt-In) im Falle der Etablierung eines De-facto-Standards (Auswirkungen auf Datenschutz und Meinungsäußerungsfreiheit, aber auch auf Wettbewerb – vgl. Hinweis von *Stefan Bechtold*)
- Entscheidung über Verwendung direkter anonymer Bestätigung erfolgt auf Anwendungsebene (Anwendung entscheidet über Zertifizierungsinfrastruktur)

Trusted Computing *(Andreas Neumann)*

Neue rechtliche Entwicklungen (3): Microsoft-Entscheidung der Kommission vom 24. März 2004

- Marktmachtmissbrauch durch Nichtoffenlegung von Schnittstellen für den Dialog zwischen „Windows“ und nicht von Microsoft stammenden Arbeitsgruppenservern
- Marktmachtmissbrauch durch Koppelung des „Media Player“ an „Windows“
- Folge des Marktmachtmissbrauchs:
  - Senkung der Innovationsbereitschaft
  - Beschränkung des Wettbewerbs
  - Verringerung der Auswahl und Erhöhung der Preise zu Lasten der Verbraucher
  - Gefahr der Kontrolle benachbarter Märkte im Bereich der digitalen Medien
- Angeordnete Abhilfemaßnahmen/Rechtsfolgen:
  - Offenlegung der Arbeitsgruppenserver-API (allerdings Anspruch auf angemessene Vergütung für geschützte APIs)
  - Angebot einer vom „Media Player“ entbündelten „Windows“-Version
  - Geldbuße (497 Mio. EUR)

Trusted Computing *(Andreas Neumann)*

Neue rechtliche Entwicklungen (4): Technologietransfer-Leitlinien der Kommission vom 27. April 2004

- Gedanke des Technologiepools zur Lösung wettbewerbsrechtlicher und praktischer Probleme im Bereich der Lizenzvereinbarungen:
  - Begriff: Vereinbarungen, bei denen zwei oder mehr Parteien ein Technologiepaket zusammenstellen, das nicht nur an die Mitglieder des Pools, sondern auch an Dritte in Lizenz vergeben wird
  - Wettbewerbsbeschränkende Wirkung: gemeinsamer Absatz der verbundenen Technologien, Beschränkung des Innovationswettbewerbs bei Unterstützung eines Industriestandards
  - Wettbewerbsfördernde Wirkung: Senkung von Transaktionskosten (insbesondere für KMU)
  - ⇒ Pools mit (nur) wesentlichen Technologien sind wettbewerbspolitisch wünschenswert
  - Gefahr wettbewerbsschädlicher Wirkungen wächst mit Marktstellung des Pools
  - Pools mit starker Marktstellung sollten offen sein und Gleichbehandlung gewährleisten
  - Keine übermäßige Abschottung fremder Technologien und keine Einschränkung der Einrichtung alternativer Pools

Trusted Computing *(Andreas Neumann)*

Neue rechtliche Entwicklungen (5): IMS-Health-Entscheidung des EuGH vom 29. April 2004

- Weigerung zur Erteilung einer Lizenz durch den Inhaber eines ausschließlichen Rechts kann – unter außergewöhnlichen Umständen – ein missbräuchliches Verhalten im Sinne von Art. 82 EG sein

- Außergewöhnliche Umstände liegen unter folgenden Bedingungen vor:
  - Weigerung muss das Auftreten eines neuen Erzeugnisses verhindern, nach dem eine potentielle Nachfrage der Verbraucher besteht
  - Weigerung darf nicht aus sachlichen Gründen gerechtfertigt sein
  - Weigerung muss geeignet sein, jeglichen Wettbewerb auf einem abgeleiteten Markt auszuschließen (potentieller oder auch nur hypothetischer Markt reicht; erforderlich ist lediglich Unterscheidung zwischen zwei Produktionsstufen, die durch das nachgefragte Erzeugnis – z. B. API – miteinander verbunden sind)

Vielen Dank für die Aufmerksamkeit!

Für weitere Informationen:

Andreas Neumann

Zentrum für Europäische Integrationsforschung, Abteilung A

Walter-Flex-Str. 3, 53113 Bonn

Tel.: 02 28 / 73 49 33 Fax: 02 28 / 73 18 93

E-Mail: an@andreasneumann.de

WWW: http://www.andreasneumann.de / http://www.tkrecht.de

Trusted Computing *(Andreas Neumann)*

Weiterführende Literatur:

Koenig/Neumann/Katzschmann (Hrsg.), Trusted Computing – Technik, Recht und gesellschaftspolitische Implikationen vertrauenswürdiger Systemumgebungen, 2004

Weiterführende WWW-Quelle:

http://cyberlaw.stanford.edu/blogs/bechtold/tcblog.shtml

Wichtiger Hinweis:

„The Board views the endemic use of PowerPoint briefing slides instead of technical papers as an illustration of the problematic methods of technical communication at NASA."

-- Columbia Accident Investigation Board, Final Report of 26 August 2003, S. 191, <http://anon.nasa-global.speedera.net/anon.nasa-global/CAIB/CAIB_lowres_chapter7.pdf>

Anhang (1): Artikel 81 EG

(1) Mit dem Gemeinsamen Markt unvereinbar und verboten sind alle **Vereinbarungen zwischen Unternehmen, Beschlüsse von Unternehmensvereinigungen und aufeinander abgestimmte Verhaltensweisen**, welche den Handel zwischen Mitgliedstaaten zu beeinträchtigen geeignet sind und **eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs** innerhalb des Gemeinsamen Marktes **bezwecken oder bewirken**, ...

Anhang (2): Artikel 81 EG

(3) Die Bestimmungen des Absatzes 1 können für nicht anwendbar erklärt werden auf

- Vereinbarungen ... zwischen Unternehmen,

...

die unter **angemessener Beteiligung der Verbraucher** an dem entstehenden Gewinn zur Verbesserung der Warenerzeugung oder -verteilung oder **zur Förderung des technischen oder wirtschaftlichen Fortschritts** beitragen, ohne dass den beteiligten Unternehmen

a) Beschränkungen auferlegt werden, die für die Verwirklichung dieser Ziele nicht unerlässlich sind, oder

b) Möglichkeiten eröffnet werden, für einen wesentlichen Teil der betreffenden Waren den Wettbewerb auszuschalten.

Anhang (3): Artikel 82 EG

Mit dem Gemeinsamen Markt unvereinbar und **verboten ist die missbräuchliche Ausnutzung einer beherrschenden Stellung** auf dem Gemeinsamen Markt oder auf einem wesentlichen Teil desselben durch ein oder mehrere Unternehmen, soweit dies dazu führen kann, den Handel zwischen Mitgliedstaaten zu beeinträchtigen.
...