Landesbeauftragter für den Datenschutz
Mecklenburg-Vorpommern 31. März 2003

TCPA, Palladium und DRM

In der Fachpresse, auf Websites anerkannter IT-Sicherheitsexperten und in diversen Mailinglisten und Chatrooms wird zur Zeit intensiv über TCPA (Trusted Computing Platform Alliance), das Microsoft-Projekt Palladium und Digital Rights Management (DRM) diskutiert. Durch die Polemik in der Presse und durch die vielen Anti-TCPA-Kampagnen ist das Bild auf die TCPA jedoch stark verzerrt. Technische Sachverhalte werden zum Teil falsch dargestellt oder sind zumindest weitgehend spekulativ. TCPA wird gegenwärtig fast ausschließlich mit einem datenschutz-unfreundlichen DRM gleichgesetzt.

In den letzten Wochen und Monaten erhielten auch die Datenschutzbeauftragten des Bundes und der Länder viele Anfragen von Bürgerinnen und Bürgern zu TCPA und Palladium, in denen die Sorge zum Ausdruck kommt, dass eine unkontrollierte und selbstbestimmte Nutzung von Personalcomputern durch Projekte wie TCPA und Palladium künftig in Frage gestellt werden könnte. Sowohl die Presse als auch die Bürgerinnen und Bürger erwarten, dass sich die Datenschützer zu dem Thema äußern.

Vor diesem Hintergrund hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Arbeitskreis „Technische und organisatorische Datenschutzfragen“ beauftragt, sich mit dem Thema zu befassen. Der Arbeitskreis hat daraufhin einen Entschließungsentwurf ausgearbeitet, in dem die Risiken der o. g. Projekte skizziert und entsprechende Empfehlungen an Hersteller von Informations- und Kommunikationstechnik formuliert werden.

Der vorliegende Kurzbericht soll weiterführende Erläuterungen zum Entschließungsentwurf des Arbeitskreises geben, indem die wesentlichen Merkmale der TCPA-Technologie skizziert, das Verhältnis zwischen TCPA, Palladium und DRM aufgezeigt und verschiedene datenschutzrechtliche Aspekte bei der Verwendung von TCPA-Technologien erläutert werden.

Der Text basiert auf dem ausführlichen und technisch wesentlich detaillierteren Vermerk des LDA Brandenburg vom 17. Februar 2003.

Was ist TCPA?

Die TCPA ist eine Vereinigung führender Hard- und Softwarehersteller und Telekommunikationsausrüster. Sie hat die Spezifikation für einen Sicherheitschip erarbeitet, welcher die Anforderungen aller TCPA-Mitglieder erfüllt. Der Chip ist nicht nur für den Einsatz in PCs konzipiert, sondern auch für PDAs, Mobilfunktelefone usw. gedacht. Für den PC wurde jedoch eine weitere, spezielle Spezifikation erarbeitet. Sie ergänzt die klassische PC-Architektur um einen speziellen Sicherheitschip, das sogenannte Trusted Computing Modul (TPM).

Das TPM führt zahlreiche Funktionen aus, die das Vertrauen in die Sicherheit des PC stärken sollen. Unter anderem existieren Funktionen zur Verwaltung kryptographischer Schlüssel, zum sicheren Booten eines PC, zur Authentisierung, zur Protokollierung, zur Initialisierung und für weitere Managementaufgaben. Das TPM stellt dabei eine ausschließlich passive Komponente dar, die das Betriebssystem des PC beispielsweise bei kryptographischen Funktionen unterstützt. Für die Nutzung dieser Funktionen sind ein spezielles BIOS und ein angepasstes Betriebssystem nötig.

Für die datenschutzrechtliche Bewertung ist insbesondere der Zusammenhang zwischen TPM und Betriebssystem wichtig. Das TPM ist zwar die hardwaretechnische Basis zur Umsetzung der TCPA-Spezifikationen. Wie jedoch die oben genannten Funktionen genutzt werden, hängt wesentlich vom Betriebssystem ab.

Die Schnittstelle zum Betriebssystem ist der Trusted Platform Support Service (TSS). Der TSS stellt u. a. einen begrenzten geschützten Speicher zur Verfügung, der z. B. biometrische Daten enthalten kann, um den Bootvorgang zu schützen (vergleichbar einem Boot-Passwort).

Es gibt bereits erste Realisierungen des TPM. Chiphersteller wie Intel, Infineon und National Semiconductor liefern schon entsprechende Prozessoren und IBM beispielsweise bietet erste PCs und Notebooks an, in denen das TPM eingebaut ist.

Anwendungsszenarien der TCPA-Technologie

Es gibt eine ganze Reihe von Anwendungsszenarien für TCPA-konforme Hardware, die aus der Sicht des Datenschutzes zum Teil zu begrüßen sind:

Hardwareunterstütze Kryptographie:
- Asymmetrische Verschlüsselung (RSA)
- Berechnung und Verifizierung von Signaturen
- Berechnung von Hashfunktionen (SHA-1, MD-5)
- Berechnung von Zufallszahlen (TRNG)

Unterstützung von sicheren Protokollen:
- SSL – Secure Socket Layer (Protokoll zum Authentifizieren und Verschlüsseln, vorwiegend in den Bereichen Internet und Intranet)
- IPSec – Internet Protocol Security (Protokoll, dass den gesicherten Transport von Daten in IP-basierten Netzwerken gewährleistet)
- S-MIME (Standard zur Übertragung verschlüsselter und signierter E-Mails)
- WLAN-Verschlüsselung (Verschlüsselung in drahtlosen Netzen)

Schutz von Daten:

- Kryptographische Schlüssel können an ein TPM gebunden werden, so dass eine Entschlüsselung nur bei erfolgreicher Authentifizierung (PIN, Passphrase) **und** Zugang zum TPM möglich ist.
- Die Entschlüsselung von Daten kann an einen bestimmten Zustand der Hardware gekoppelt werden, um die Entschlüsselung von Daten nach einem Einbruch zu erschweren.
- Durch das TPM kann das Passwortmanagement erleichtert werden. Die Passwörter werden im geschützten Speicher des TPM abgelegt und durch einen Manager verwaltet und „vorgezeigt".

Plattform- und Anwender-Authentifizierung:

- Unter UNIX sind bestimmte Operationen nur an der Console im Rechenzentrum erlaubt. Durch den Einsatz sicherer Hardware und durch die Authentifizierung dieser Hardware kann die Consolen-Definition auch auf Terminals außerhalb des RZ erweitert werden, weil diese Terminals dann als ebenso sicher wie die Console gelten.
- Beim Fernzugriff auf Daten beispielsweise in einer Behörde kann ein zusätzliches Sicherheits-Level etabliert werden: die Authentifizierung des Home-PCs und ein Nachweis, falls in diesen Home-PC nicht eingebrochen wurde.

Business to Environment - B2E

- Die Sicherheit von VPN-Lösungen kann durch die Überprüfung der Integrität der eingesetzten Hardware erhöht werden.
- Durch die Sicherstellung der Integrität von Remote-Servern kann verhindert werden, dass eine Datenübertragung an ein kompromittiertes System erfolgt.

Digitale Signaturen unter Pseudonym

- Bei der Kommunikation zwischen Verwaltung, Wirtschaft und Bürger können Anwender digitale Signaturen insbesondere auch unter einem Pseudonym erzeugen um beispielsweise sicherstellen, dass Transaktionen von Dritten nicht verfälscht wurden. Dies setzt wie in allen PKI-Umgebungen eine verstrauenswürdige Stelle (Privacy CA, Trusted Third Party – TTP) voraus, der alle Parteien vertrauen müssen.

Vorteile der TCPA-Technologie aus der Sicht des Datenschutzes

Durch TCPA-konforme PCs können Private Keys und sensitive Daten von Anwendern wahrscheinlich besser geschützt werden, als durch jedes andere bislang am Markt verfügbare Konzept. Durch die mögliche Versiegelung verschlüsselter Daten (die Entschlüsslung ist nur bei einer vorher definierten Konfiguration möglich) können von außen erfolgende Angriffe besser abgewehrt werden. Die Datensicherheit bei der Nutzung von virtuellen LANs, Fernzugriffsmechanismen und drahtlosen Netzen kann erhöht werden. Die TCPA-Spezifikationen sind unabhängig vom jeweiligen Betriebssystem und offen für jede Plattform. Durch TCPA-konforme Technik kann der Wunsch nach einer generellen Verschlüsselung übertragener und gespeicherter Daten leichter umgesetzt werden. In PKI-Umgebungen können digitale Signaturen unter Verwendung eines Pseudonyms etwa zur Sicherung von Transaktionen eingesetzt werden.

Nachteile der TCPA-Technologie aus der Sicht des Datenschutzes

Jedes TPM ist durch einen eineindeutigen Schlüssel (Endorsement Key) gekennzeichnet. Durch entsprechend sichere Authorisierungsmechanismen kann eine feste Zuordnung des Nutzers zum TPM und somit zum jeweiligen PC erreicht werden. Die TCPA-Spezifikationen sehen die Bildung von anonymen Identitäten vor, die aus datenschutzrechtlicher Sicht mit Pseudonymen zu vergleichen sind. Diese Pseudonyme (Attestation Identity Key) werden unter Nutzung des TPM-spezifischen Schlüssels erzeugt. Ein Nutzer kann mehrere Pseudonyme erzeugen, die dann verschiedene Identitäten repräsentieren. Ohne Kenntnis des TPM-spezifischen Schlüssels kann aus dem Pseudonym nicht auf das dazugehörige TPM geschlossen werden. Die gewünschte Vertrauenswürdigkeit des Pseudonyms kann – wie in allen PKI-Umgebungen – nur durch die Zertifizierung von einer vertrauenswürdigen Stelle (Privacy CA oder Trusted Third Party – TTP) sichergestellt werden. Die Vertrauenswürdigkeit ist von besonderer Bedeutung, da diese Stelle das Pseudonym auflösen und eine Relation zwischen Pseudonym (Anwender) und TPM (Rechner) herstellen kann. Zu kritisieren ist bislang, dass die TCPA die Vertrauenswürdigkeit einfach voraussetzt, obwohl bisher nicht klar ist, welche Stellen dies sein sollen und auf welche Weise Vertrauenswürdigkeit hergestellt werden soll.

Eine weitgehender Datenschutz kann zur Zeit nur erreicht werden, wenn die Möglichkeit der TCPA-Spezifikation genutzt wird, den TPM-spezifischen Schlüssel zu deaktivieren. Bei den ersten Anwendungen TCPA-konformer Hardware spielen Schlüssel und Pseudonym zwar noch keine Rolle. Bei künftigen Anwendungen zur Kommunikation zwischen Verwaltung, Wirtschaft und Bürger werden diese Schlüssel jedoch eine größerer Bedeutung erlangen. Obwohl Hersteller wie Intel bereits erste Ideen zur Nutzung der Pseudonyme entwickelt haben, gibt es gegenwärtig weder vertrauenswürdige Stellen und noch Standards, wie diese Schlüssel im Internet benutzt werden können oder sollen.

TCPA und Privacy

Die TCPA hat bereits lobenswerte Bemühungen unternommen, um datenschutzrechtliche Belange zu berücksichtigen. Folgende Beispiele sollen dies verdeutlichen:

- Die TCPA-Spezifikationen sind offen und lizenzfrei nutzbar.
- Die TCPA-Funktionalität besteht auf opt-in Basis. Das TPM-Modul muss durch den Anwender „eingeschaltet“, in Besitz genommen und aktiviert werden.
- Das TPM-Modul lässt sich vollkommen zurücksetzten bzw. abschalten.
- Der Anwender kann die vollständige Migration seiner durch das TPM geschützten Daten auf ein zweites TPM erlauben oder permanent unterbinden.
- Der mit dem TPM verbundene Endorsement Key hat eine stark eingeschränkte Funktionalität. Er wird nur für die Etablierung der Zuordnung zu einem Benutzer (establish Ownership) und zur Beantragung der Zertifikate von Pseudonymen (Attestation Identity Keys) verwendet.
- Um einen umfassenderen Datenschutz zu gewährleisten, kann der Zugriff auf den Endorsement Key unterbunden werden.
- Es werden Pseudonyme verwendet, damit nicht jedermann den Anwender dem zugrundeliegenden Endorsement Key (d. h. dem TPM) zuordnen kann.
- Der Anwender kann seine Private Keys schützen sowie sensitive Daten versiegeln.
- TCPA-konforme Hardware muss auf der EAL3-Stufe (Common Criteria Version 2.1, ISO/IEC 15408) sicherheitsüberprüft werden.

Neben den oben genannten Nachteilen ist aus der Sicht des Datenschutzes ein weiterer Aspekt zu kritisieren:
Die Herstellers vergeben für jedes TPM eine sogenannte Serial Number, die für das jeweilige TPM einmalig sein kann. Die TCPA wünscht sich hier zwar lediglich eine Seriennummer für eine ganze Modellreihe, überlässt diese Entscheidung aber dem Hersteller. Es besteht die Gefahr, dass Nutzer über diese Seriennummer identifiziert werden können, beispielsweise im Zusammenhang mit den oben beschriebenen Mechanismen zur Zuordnung des Nutzers zum TPM. Das könnte möglicherweise zu einer aus datenschutzrechtlicher Sicht abzulehnenden Nutzerkontrolle führen. Eine abschließende Bewertung dieser Details ist jedoch noch nicht möglich, da bisher nicht klar ist, ob und ggf. auf welche Weise und zu welchem Zweck die Seriennummer das TPM verlässt.

Was hat Palladium mit TCPA zu tun?

Weiter oben wurde bereits erwähnt, dass das TPM zwar die hardwaretechnische Basis zur Umsetzung der TCPA-Spezifikationen ist, die Realisierung der Sicherheitsfunktionen jedoch maßgeblich vom Betriebssystem abhängt, das auf der TCPA-Spezifikation aufsetzt. Fälschlicher Weise wird bisher fast ausschließlich das Microsoft-Projekt Palladium mit TCPA in Verbindung gebracht. Es ist jedoch anzunehmen, dass auch für andere Betriebssysteme – beispielsweise für LINUX – TCPA-konforme Komponenten entwickelt werden, um auch dort die neuen Sicherheitsfunktionen nutzen zu können.

Mit dem Palladium-Projekt will Microsoft ein „vertrauenswürdiges Betriebssystem“ auf der Basis einer Security Support Component (SSC) etablieren (Microsoft will für Palladium allerdings künftig die Bezeichnung “Next Generation Secure Computing Base for Windows” (NGSCBFW) verwenden, da der bisherige Codename „tarnished“ (getrübt) sei.) Mit der ersten Palladium-Windows-Version (Microsoft verwendet hierfür den Codenamen „Longhorn“) ist im Jahr 2005 zu rechnen.

Nachdem eine Verbindung von TCPA und Palladium lange Zeit abgestritten wurde, hat Microsoft mittlerweile jedoch bestätigt, dass ein TPM-Chip zumindest als Anker für Palladium dienen werde. Man kann jedoch Palladium nicht einfach als Umsetzung der TCPA-Technologie ansehen. Palladium geht weit über die Spezifikationen des aktuellen Standards (Version 1.1b) der TCPA hinaus, und verlangt Modifikationen am Prozessor und am Chipsatz sowie geschützte Datenpfade zwischen dem entsprechend isolierten und geschützten Speicher, dem Keyboard bzw. der Maus und der Graphikkarte/Display. Derzeit überarbeitet die TCPA ihre Spezifikationen, insbesondere um mit der neuen Version 1.2 Microsofts Ansprüche zu befriedigen.

Immerhin hat Microsoft angekündigt, den Quellcode zu Palladium und zu der zugrunde liegenden Trusted Computing Base (TCB) offen zu legen. Frühesten dann wird man sich ein klares Bild über die „Next Generation Secure Computing Base for Windows“ machen und die Möglichkeiten zur Einhaltung datenschutzrechtlicher Bestimmungen bewerten können.

Bisher gehen die offiziellen Informationen von Microsoft jedoch über ein Whitepaper nicht hinaus, so dass die mit dem Palladium-Projekt verfolgten Absichten unklar sind. Obwohl führende Köpfe von Microsoft erklären, dass man „...kein Interesse an der Bindung digitaler Inhalte habe...“ ist es doch sehr wahrscheinlich, dass die Microsoft-Patente zu DRM-Betriebssystemen umgesetzt werden sollen. Die Konzeption von Palladium lässt den Schluss zu, dass künftig bestimmte Anwendungen nur unter bestimmten Bedingungen lauffähig sein werden, etwa in einem besonders geschützten Palladium-Trusted-Mode. Die Sicherheit dieser

Anwendungen könnte dann zwingend oder optional durch ein Zertifikat bescheinigt werden. Noch ist völlig offen, ob Microsoft selbst die Rolle des Zertifizierers übernehmen will oder andere TTPs entsprechendes Vertrauen gewährleisten können. In jedem Fall wird sich der Nutzer wiederum auf vertrauenswürdige Stellen verlassen müssen.

Was hat Digital Rights Management mit TCPA zu tun?

Was ist Digital Rights Management (DRM)?

DRM-Systeme sollen grundsätzlich
- die Nicht-Konsumierbarkeit nicht bezahlter Inhalte gewährleisten (Vertraulichkeit),
- die Inhalte vor unautorisierter Veränderung schützen (Integrität der Daten),
- die Identifizierbarkeit urheberrechtlich geschützter Werke und deren Urheber gewährleisten (Authentizität der Daten) und
- die Anfertigung illegaler Kopien verhindern (Verfügbarkeit).

Im DRM-Bereich finden Kerntechniken der IT-Sicherheit Anwendung:
- *Verschlüsselung:* Um individualisierte und kostenpflichtige Dienste vor unberechtigter Nutzung zu schützen, müssen die übertragenen Inhalte verschlüsselt sein.
- *Schutz durch manipulationssichere Hardware:* Sicherheitsmechanismen verwenden (meist kryptographische) Geheimnisse, deren Kenntnis die Voraussetzung für die Nutzung der Inhalte ist. Die einzige derzeit halbwegs sichere Methode zur Aufbewahrung der Geheimnisse ist so genannte Tamper-Resistant (manipulationssichere) Hardware.
- *Schutz durch Software-Kapselung:* Können die zu schützenden Inhalte auf einem handelsüblichen PC nicht durch Tamper-Resistant Hardware geschützt werden, muss wenigstens die Ausführungsumgebung, in der das Rechte-Management erfolgt, gegen böswillige fremde Software (Trojanische Pferde, Sniffing- und Hacker-Software) geschützt sein. Ein Softwareschutz gegen Angriffe durch den Betreiber und Besitzer des Rechners ist dagegen bisher praktisch aussichtslos.

In den Debatten zu TCPA und Palladium entsteht der oft Eindruck, dass DRM-Systeme prinzipiell datenschutzunfreundlich sind und den Anwender entmündigen. Das muss nicht automatisch so sein, auch wenn viele DRM-Techniken dies implizieren.

Mit einem Digital Rights Management verspricht sich vor allem die Unterhaltungsindustrie die Durchsetzung ihrer Interessen und einen wirksamen Kopierschutz. In den USA gibt es z. B. einen Gesetzentwurf “Consumer Broadband and Digital Television Promotion Act”, der die Verwendung von Geräten mit DRM-Funktionalität vorschreibt. Solche Änderungen des Urheberrechts hängen von der Verfügbarkeit und Sicherheit entsprechender Technologien ab. Es gibt allerdings derzeit keine wirklich manipulationssichere Hardware. Auch die aktuellen Spezifikationen der TCPA erfüllen die Anforderungen an Tamper-Resistenz nicht.

TCPA und DRM

Ein Großteil der von TCPA-Kritikern beschriebenen DRM-Szenarien lassen sich mit TCPA-konformer Hardware nur dann umsetzen, wenn zusätzlich sowohl das BIOS als auch das Betriebssystem zusätzliche DRM-Funktionen erhalten.

Die Spezifikationen des TCPA-Chip gehen zumindest in der Version 1.1b nur von Angriffen von Außen (durch Software) aus. Im Protection Profile für die EAL3-Zertifizierung sind kei-

ne Tests vorgesehen, die den Schutz gegen eine Hardware-Analyse (Analyse von Stromverbrauch, Zeit, etc.) vorsehen. Die TCPA nimmt sogar eine Reihe von möglichen „Denial-of-Service“-Attacken in Kauf, um den Datenschutz zu gewährleisten. Ein auf dieser Basis aufgebautes DRM-System wäre leicht zu „knacken“.

Etwas differenzierter wird die demnächst erscheinende Version 1.2 der TCPA-Spezifikationen zu bewerten sein. Es ist zu erwarten, dass weitere datenschutzrechtliche Kritikpunkte benannt werden müssen, weil in der neuen Spezifikation ein verstärkter Schutz gegen mögliche Angriffe durch den Eigentümer des TPM vorgesehen ist und somit die selbstbestimmte Nutzung der eigenen Technik weiter eingeschränkt werden könnte.

Fazit

Die Entwicklung des Internet geht hin zu E-Government, Single-Sign-On-Diensten, Web-Diensten, verteilten Rechnerarchitekturen, Semantischen Netzen usw.. Alle diese Technologien bauen auf der Sicherheit der verwendeten Hard- und Software auf. Die Initiative der TCPA, einen „Root of Trust“ in der PC-Architektur zu etablieren, um zu einem vertrauenswürdiges System beizutragen, ist auch aus datenschutzrechtlicher Sicht grundsätzlich zu begrüßen. Die seitens der Datenschützer seit langem geforderten sicherheitstechnischen Voraussetzungen für Projekte wie z. B. E-Voting könnten auf diese Weise bereitgestellt werden.

Die Gefahr, dass der Datenschutz mit Hilfe TCPA-konformer Hardware ausgehebelt werden kann, ist jedoch groß. Die demnächst erscheinende Version 1.2 der TCPA-Spezifikationen wird die Gefahr noch vergrößern, weil in der neuen Spezifikation ein verstärkter Schutz gegen mögliche Angriffe durch den Eigentümer des TPM vorgesehen ist.

Aufgabe der Datenschützer wird es sein, auch künftig darauf hinzuwirken, dass Nutzer (Private, Firmen, Behörden) die alleinige Kontrolle über ihre Rechner behalten und eine unbeobachtete Nutzung von Hard- und Software ermöglicht wird. Das erfordert vertrauenswürdige, transparente und somit datenschutzfreundliche Technik.

Die Datenschutzbeauftragte des Bundes und der Länder sollten die Entwicklungen um TCPA und Palladium aufmerksam verfolgen und darauf hinwirken, dass

- die Rolle der vertrauenswürdigen Stelle (Privacy CA, TTP o. ä.) geklärt wird,
- das TPM keine hardwarebezogene Seriennummern enthält bzw. sichergestellt wird, das diese nicht ausgelesen und missbräuchlich genutzt werden,
- das Palladium-Projekt von Microsoft auf Verletzungen des Datenschutzrechtes laufend überprüft wird,
- DRM-Systeme verhindert werden, die den Datenschutz unterlaufen und dass
- die von den Datenschützern unterstützte Verbreitung von Open-Source-Software nicht behindert wird.