Trusted Computing

Proseminar SS05
IT-Sicherheit

Johannes Hoffmann und Johannes Neubauer

Universität Dortmund

Zusammenfassung. Die Trusted Computing Initiative ist ein Zusammenschluss mehrerer Soft- und Hardwarehersteller, die sich zum Ziel gesetzt haben, Computersysteme sicherer zu machen. Es wird allgemein angenommen, dass Hardware schwerer zu manipulieren ist als Software. Vorhandene hardwaregestützte Sicherheitsmechanismen, wie z.B. Smartcards haben sich nicht durchsetzen können, da die Nutzung zu kompliziert und umständlich ist. Dies soll - mithilfe von Trusted Computing - durch die Verlagerung von Sicherheitsmechanismen in eine geschützte Hardwareumgebung, auf möglichst vielen Systemen, erreicht werden. Neue Softwarestandards sollen darauf aufbauend, komplexe und flexible Sicherheitsdienste anbieten können.

1 Überblick

Trusted Computing (TC) ist ein neuer Ansatz - seit 1999 unter der Trusted Computing Platform Alliance (TCPA) - Computerumgebungen sicherer zu machen. Diese Ausarbeitung beschäftigt sich mit der Struktur der Trusted Computing Group und gibt einen Einblick in die Geschichte von Trusted Computing. Des weiteren wird ein Einblick in die Architektur der Trusted Computing Platform, einige Anwendungsmöglichkeiten, sowie einen Ausblick auf die Zukunft von Trusted Computing gegeben.

1.1 Motivation und Anforderungen

Die Idee zu Trusted Computing ist nicht durch eine neue Sicherheitsanforderung enstanden, sondern durch das Fehlen einer adäquaten Sicherheitsarchitektur in herkömmlichen Systemen. Somit beschäftigt sich die Trusted Computing Initiative ähnlich wie andere Sicherheitskonzepte mit Problemen wie der Sicherstellung der Integrität und Vertraulichkeit von digitalen Objekten (wie z.B. einem Word-Dokument), der Informations-, Daten- und Funktionssicherheit von Systemen, sowie der Durchsetzung von Datenschutzrichtlinien, der lokalen Gesetzgebung, auf Plattformen. Nicht Teil der Anforderungen an eine TC Plattform ist die Authentifizierung von Subjekten, sondern die Verifikation der Authentizität des Systems gegenüber Dritten. Hierbei spielt die Authentifikation von Personen oder Diensten nur implizit eine Rolle.

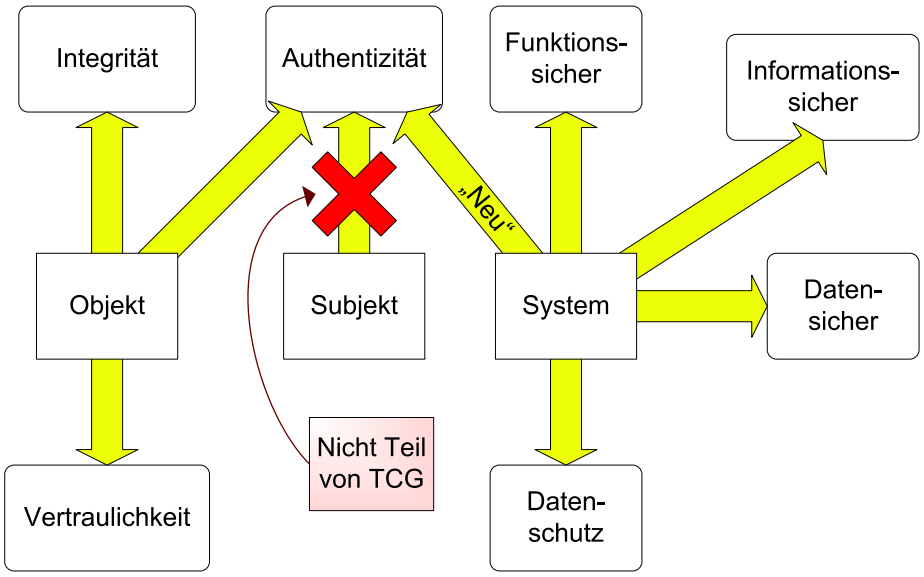

Abb. 1. Anforderungen an eine TC Platform. Authentifikation von *Subjekten* ist nur implizit gefordert.

Wichtigste Einsatzmöglichkeiten von Trusted Computing sind:

- die weltweite Durchsetzung von Copyright- und Urheberrechten, auch in Schwellenländern, in denen entsprechende Gesetze nicht existieren,
- die Eindämmung von Angriffen auf Computersysteme, wie z.B. Trojaner, Würmer, Viren und Spam-Mail,
- die Erhöhung des Vertrauens in Online-Transaktionsdienste,
- die Verbesserung des Komforts von Diensten bei gleichbleibendem oder sogar gesteigertem Sicherheitsniveau (Single-sign on Systeme),
- die Steigerung der Sicherheit in Rechnersystemen, indem sie vor ihrem Nutzer geschützt werden.

Bei der Motivation zu einer Initiative, wie TC, spielen besonders die Interessen der Förderer eine Rolle, was in diesem Fall große Hard- und Softwarekonzerne wie IBM, Intel und Microsoft sind. Die Motivation der Hardwarehersteller ist offensichtlich, da neue Sicherheitstechniken auf Hardwarebasis mit der Produktion und dem Verkauf neuer Hardware Hand in Hand gehen. Auch Softwarehersteller wie Microsoft haben daran ein Interesse, da TC, wie in Abschnitt 3 noch genauer erklärt wird, sich auch dazu eignet, Digital Rights Management (DRM) durchzusetzen und neue Marketingmöglichkeiten für Softwareprodukte eröffnet.

1.2 Technische Maßnahmen

Eine vertrauenswürdige Sicherheitsarchitektur muss ineinander greifende Hard-, Firm- und Software-Sicherheitskonzepte vereinen. Die Hardware stellt vertrauenswürdige und nicht umgehbare Basisfunktionen dem Betriebsystem einerseits und den Applikationen andererseits zur Verfügung. Sie sind die Grundlage für die Bereitstellung komplexerer Dienste. Dabei müssen strategische Entscheidungen (Policies) strikt von den Basismechanismen getrennt werden, um flexibel bleiben zu können. Diese Forderung könnte soweit gehen, dass für jedes Objekt (z.B. ein Word-Dokument) eine eigene Policy - wo darf das Dokument wann und wie verwendet werden - festgelegt wird. Dienste zur Durchsetzung von Sicherheitsstrategien sind daher auf der Betriebssystem-, bzw. Applikationsebene anzusiedeln.

1.3 Unterschied zu herkömmlichen Sicherheitsstrategien

Es gibt bereits viele Ansätze, Systeme abzusichern. Diese Versuche werden allerdings durch verschiedene Einflüsse erschwert. Ein Großteil der Nutzer von Computersystemen, dazu zählen nicht nur die Privatnutzer, ist zu bequem, um die derzeitigen Möglichkeiten zur Absicherung von Systemen auszuschöpfen. Dazu zählen Sicherheitstechniken, wie digitale Signaturen, Verschlüsselung von persönlichen Daten auf einer Plattform, sowie bei der Versendung zwischen Plattformen. Auch Firewalls, Virenscanner und Smartcards werden zu wenig eingesetzt. Sicherheitsupdates von Firm- und Software werden, wenn überhaupt, nur unregelmäßig durchgeführt. Sicherheitdienste, die bereits im Betriebssystem integriert sind bzw. auf die programmiersprachliche Ebene verlagert werden, bieten keinen lückenlosen Schutz. DMA-Geräte haben beispielsweise direkten Zugriff auf den Speicher und können daher die Kontrollen der CPU umgehen. Andere Hardwarekomponenten, wie z.B. Grafik- und Soundkarten, können, aus Performanzgründen, ohne Kontrollen durch das Betriebs- oder Laufzeitsystem agieren. Hier setzt TC ein. Es wird allgemein angenommen, dass die Manipulation von Hardware schwieriger ist als die von Software. TC soll in Zukunft eine auf (fast) allen Rechnersystemen verfügbare sichere Hardwareumgebung zur Verfügung stellen. Dies soll die Nutzung von Sicherheitskonzepten wie Signaturen und Verschlüsselung, sowie die sichere Speicherung von Schlüsseln und sicherheitskritischen Daten, ohne den Komfort zu senken, ermöglichen.

Eine weitere Problematik ist, dass die Durchsetzung von Copyright- und Urheberrechten auf einer Computerplattform nicht möglich ist, wenn der Besitzer die volle Kontrolle darüber besitzt. Der Sender eines digitalen Objektes verliert die Kontrolle darüber, sobald es den Rechner des Empfängers erreicht, unter Umständen sogar schon vorher durch den Zugriff von Dritten. Das Ziel von TC geht demnach einen Schritt weiter als das herkömmlicher Strategien. Es gilt nicht nur den Schutz des Systems gegen Angriffe von ausserhalb, sondern auch Schutz vor dem Besitzer zu gewährleisten. In der Terminologie der Trusted Computing Group (TCG) wird so aus einem klassischen System ein Trusted System.

1.4 Geschichte

Schon vor der Trusted Computing Initiative gab es Ansätze zu hardwaregesicherten Computerumgebungen. Der Bootvorgang in einen sicheren, definierten Zustand war bereits Bestandteil der frühesten Rechnern. Der ROM (Read Only Memory) befand sich im BIOS, und eine Festplatte, die ein Virus hätte befallen können, gab es nicht. Schon früh gab es Überlegungen, wie Sicherheitsmechanismen in Hardware verlagert werden können, und in der Konsumelektronik ist dies schon lange keine Neuheit mehr. Tragbare MP3 Player schützen so beispielsweise ihre Geräte vor fremden Musikinhalten (Digital Rights Management), und DVDs werden verschlüsselt, um sie vor Kopierversuchen zu schützen. Spielekonsolenhersteller verschlüsseln den Systembus ihrer Geräte. Das soll die Installation eines anderen Betriebssystems erschweren, damit die subventionierte Hardware nur dazu genutzt werden kann, die Spiele des Herstellers darauf zu spielen.

1993 Die U.S Regierung entwickelte 1993 unter der Leitung der NSA den Clipper Chip. Dabei handelte es sich um einen Verschlüsselungschip für Telefonverbindungen, er sollte aber auch in andere Konsumelektronik, wie Computer, Handys und ähnliche eingebaut werden. Durch einen Zufall kam heraus, dass sich die NSA eine Hintertür (Back-Door) in das Verschlüsselungsverfahren eingebaut hatte, um weiterhin Telefone abhören zu können. Der Chip wurde von der Öffentlichkeit nicht akzeptiert, und so kam es nie zur Produktion. Allerdings liegen bereits Pläne für den Clipper Chip 2 und 3 vor.

Mitte der Neunziger Intel begann Mitte der neunziger Jahre Prozessoren mit Seriennummern zu produzieren. Geplant war, bis zum Jahr 2000, die Funktionalität des Trusted Plattform Modules (TPM) in die CPUs zu integrieren. Diesem Projekt fehlte ebenfalls die Akzeptanz in der Öffentlichkeit. Später hat Intel die TCPA und die TCG mitgegründet und damit einen neuen Anlauf zu einer sicheren Hard-

1999 wareumgebung gestartet. Die Trusted Computing Platform Alliance wurde 1999 von Intel, Microsoft, IBM, Compaq und HP gegründet. Bis 2003 veröffentlichen sie mehrere Spezifikationen der Trusted Computing Plattform (TCP). Aufgrund der Größe von 200 Mitgliedern und einer starren und unflexiblen Struktur wurde die TCPA 2003 von der Trusted Computing Group (TCG) abgelöst. Im selben Jahr erscheint die Spezifikation Version 1.2, die bis heute aktuell ist. In ihr wurden einige Zugeständnisse an die Kritiker von TC gemacht. Es wurden unter anderem Maßnahmen zur Pseudonomisierung einer Trusted Computing Plattform gegenüber Dritten eingeführt, zur Erschwerung von Profiling.

2003 Ebenfalls im Jahr 2003 stellte Microsoft Palladium vor, ein Projekt, das in die nächsten Windows Betriebssysteme integriert werden sollte und die Funktionen der TC Plattform nutzt. Dieses Projekt wurde von verschiedenen Regierungen, dem BSI (Bundesamt für Sicherheit in der Informatik), der Free Software Foundation und anderen kritisiert. Microsoft reagierte mit einer Umbenennung in Next Secure Computing Base (NGSCB). Bis 2005 musste Microsoft jedoch

2006 die Funktionen zurückschrauben. Für 2006 ist die Auslieferung von Windows Longhorn, mit einem im Funktionsumfang eingeschränkten NGSCB, das unter

anderem einen sicheren Bootvorgang (Secure Start) - mit einer neuen Version des verschlüsselten Dateisystems von Microsoft - implementiert, geplant. Die TCG plant weitere Projekte. Dieses Jahr ist zum Beispiel die Spezifikation der Trusted Network Connection (TNC) Architektur veröffentlicht worden, die die Kommunikation in unsicheren Netzen sicherer machen soll. Es gibt bereits viele Systeme, die das TPM integriert haben, wie z.B. IBM Notebooks.

1.5 Struktur der Trusted Computing Group

Die Trusted Computing Group (TCG) löste 2003 die TCPA ab. Die TCPA hatte kurz vor seiner Auflösung ca. 200 Mitglieder. Der Grund für den Neuanfang war, dass Entscheidungen unter allen Mitgliedern einstimmig gefällt werden mussten. Das war den großen Firmen der Organisation zu starr und unflexibel.

Die TCG hat mittlerweile ca. 96 Mitglieder. Es hat jedoch nicht jede Firma Stimmberechtigung, und es Bedarf lediglich einer zwei Drittel Mehrheit, um einen Beschluss zu fassen. Die TCG ist in drei Gruppen aufgeteilt. Die Promoter sind fördernde Unternehmen, die die höchsten Beiträge zahlen und auch die meisten Rechte besitzen. Sie haben nicht nur eine Stimme, sondern zusätzlich einen Sitz im Board of Directors - dem Vorstand. Contributer sind mitgestaltende Unternehmen, die ebenfalls stimmberechtigt sind. Zwei, aus allen Mitgliedern dieser Gruppe gewählte Firmen haben einen Sitz im Vorstand. Die Adopter haben kaum Rechte. Sie dürfen nicht an den Sitzungen der Arbeitsgruppe teilnehmen, zahlen dafür auch nur den geringsten Beitrag.

Promoter

Contributor

Adopter

2004 hat die TCG zwei Programme ins Leben gerufen. Zum einen das Industry Liaison Programm zur Zusammenarbeit mit der Industrie. Hierbei handelt es sich um die Möglichkeit, sich als Nichtregierungsorganisation für einen Platz in der Arbeitsgruppe zu bewerben, ohne Mitgliedsbeiträge zahlen zu müssen. Zum anderen das Advisory Council, einem Beirat aus fünf unabhängigen Fachleuten, die einerseits beratende Funktion, bei der Verifikation von Sicherheitslösungen der TCG, haben und andererseits die Rechte des Anwenders schützen sollen.

Industry Liaison

Advisory Council

2 Umsetzung

Die Trusted Computing Platform (TCP) implementiert das TCG Subsystem, bestehend aus dem Trusted Platform Module (TPM), der Root of Trust for Measurement (RTM) und dem Trusted Software Stack (TSS). Das Subsystem stellt die Basismechanismen für das Betriebsystem und die Applikationen zur Verfügung. Es verhält sich passiv, reagiert lediglich auf Kommandos. Das TPM implementiert unter anderem die Root of Trust for Storage und Reporting (RTS und RTR). Idealerweise wird auch die RTM vom TPM implementiert. Sie kann aber auch in das BIOS integriert werden. Die Hardware der TCP bietet im Groben die Funktionen einer Smartcard. Zu den Aufgaben der TC-Hardware gehören:

- Die Generierung von asymmetrischen und symmetrischen Schlüsseln.

– Die Hashwertberechnung und Signaturerstellung (Signing bzw. Sealed Signing).
– Die asymmetrische und symmetrische Verschlüsselung von Daten (Binding, Sealing).
– Die Verschlüsselung kryptographischer Schlüssel, um sie in Key-BLOBS (Binary Large Objects) auszulagern (Wrapping).
– Die sichere Speicherung (in shielded Register) von Hashwerten, die über die Konfigurationsdaten der Plattform berechnet wurden. Der Zugriff auf diese Hashwerte ist nur für Sicherheitsdienste (z.B. Signieren, Verschlüsseln) bzw. TPM-Kommandos (protected Capabilities) erlaubt.
– Die Erstellung von signierten Auskünften (Reporting) über diese Werte an authorisierte Stellen.
– Ein spezieller Schlüssel (Endorsement Key), zur Bestätigung der Korrektheit von Identitätsschlüsseln (AIKs, siehe Abschnitt 3). Nur vertrauenswürdige Stellen dürfen erfahren, zu welchem TPM ein AIK gehört, um Profiling zu verhindern.
– Funktionen zur Inbesitznahme (TPM_TakeOwnership), Aktivierung und Deaktivierung des TPM.
– Ein Vertrauenswürdiger Zeitgeber (Timer), für die Festlegung und Prüfung von Gültigkeitsdaten.

2.1 Trusted Platform Module

Das Trusted Platform Module (TPM) ist das Herz der TC Plattform. Technisch gesehen ist es ein *passiver* 8-Bit RISC Prozessor, der mit 33 MHz getaktet ist. Er berechnet einen 2048 Bit RSA Schlüssel in ungefähr $\frac{1}{2}$s. Zusätzlich hat er einen flüchtigen und nicht flüchtigen Speicher und bietet verschiedene kryptografische Algorithmen an.

TPM-Architektur

Input/Output

Die I/O-Komponente ist für die Kommunikation zwischen den Komponenten des TPM und der Außenwelt zuständig. Sie leitet Nachrichten an die internen Bausteine weiter und führt Kodierungen durch, die die Kommunikation über interne und externe Busse ermöglicht.

PCR

Platform Configuration Register (PCR) sind geschützte (shielded) Register. Sie dienen der vertrauenswürdigen Speicherung von 160-Bit Hashwerten über gemessene Konfigurationswerte. Die Spezifikation schreibt 16 derartige Register vor. Sie werden normalerweise im flüchtigen (volatile) Speicher des TPMs gehalten. Sie können auch in den nicht-flüchtigen Speicher geladen werden, das ist allerdings untypisch und erfordert die Bereinigung der Register bei jedem Startvorgang. Die Root of Trust for Storage verwaltet die Daten in den PCRs. Ein Zugriff ist nur für Sicherheitsdienste über bestimmte Befehle (protected Capabilities) möglich. Da in einer TC Plattform die Notwendigkeit besteht, beliebig viele Hashwerte abzuspeichern, ist es möglich, Werte inkrementell in die

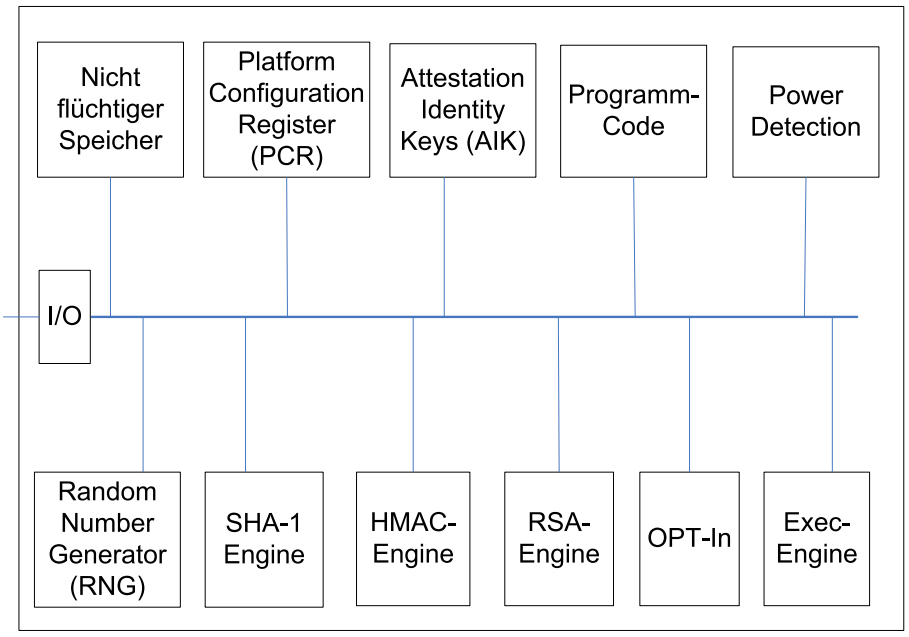

Abb. 2. Komponenten des Trusted Platform Modules.

PCRs abzulegen. Dabei wird der bereits vorhandene Wert aus dem i-ten Register ausgelesen und mit dem neuen Wert verknüpft. Der Hashwert über diesen kombinierten Wert wird als neuer Wert in das Register übertragen.

$$PCR_i^{neu} = HASH(PCR_i^{alt}|Updatewert) \quad (1)$$

AIK

Attestation Identity Keys (AIKs, siehe Abschnitt 2.4) sind pseudonomisierende Schlüssel, die ausschließlich zum Signieren von Inhalten, denen das TPM vertraut, verwendet werden - zum Beispiel Hashwerten aus den geschüzten Registern (PCR) des TPM. Dieser Schlüsseltyp ist in der Spezifikation v1.2 hinzugekommen. Es kann mehrere AIKs auf einer Plattform geben, sie dürfen die Plattform jedoch niemals verlassen (nicht migrierbar).

Programmcode

Der Programmcode implementiert die Firmware zur Messung von Systemkonfigurationen und Plattformgeräten, mit anderen Worten die RTM (siehe Abschnitt 2.2). Dieser Teil des TPM kann auch im BIOS implementiert werden, ist aber laut TCG Spezifikation idealerweise im TPM integriert. Bei der Messung von Werten wird der SHA-1 Algorithmus verwendet, um Hashwerte über die Ergebnisse zu bilden und vom RTS auf vertrauenswürdige Weise in die PCR Register zu speichern.

Power Detection

Die Power Detection Komponente überwacht, während des gesamten Betriebs, den Energiezustand des TPMs. Wird eine unzureichende Energieversorgung gemessen, kann das TPM alle weiteren Kommandos abweisen. Bei einem

Neustart übernimmt die Power Detection die Aufgabe einen Self-Check durchzuführen, bevor das TPM Befehle annimmt. Geht das System in den Standby- oder Ruhezustand, ist dieses Modul für die Auslagerung der Daten aus dem flüchtigen Speicher zuständig. Bei der Rückkehr in den Betriebszustand müssen sie wieder geladen werden.

Krypto-Funktionen

Der Random Number Generator (RNG) unterstützt die Generierung symmetrischer und asymmetrischer Schlüssel. Des Weiteren wird er bei der Erzeugung von Nonces eingesetzt, die zur Erschwerung von Replayangriffen bei verschiedenen kryptografischen Verfahren verwendet werden. Diese Komponente ist auch von außen ansprechbar. Der 160 Bit SHA-1 Generator ist ebenfalls in das TPM integriert. Er macht die Berechnung von Hashwerten über Systemkonfigurationen, bereits während des Bootvorgangs (siehe Abschnitt 2.6), erst möglich. Er ist ebenfalls von Diensten außerhalb des TPM nutzbar. Die HMAC-Engine erzeugt 160 Bit Message Authentication Codes. Dabei handelt es sich um ein Signaturähnliches Verfahren, bei dem ein geheimer Schlüssel in den Hashwert einer Nachricht eingebunden wird, der nur den Parteien bekannt ist, die an der Kommunikation beteiligt sind. Zur Überprüfung einer Signatur, sowie zur Erstellung dieser Signatur, wird der geheime Schlüssel benötigt. Dieses Verfahren ist nicht sehr sicher, vor allem da mindestens zwei Parteien den Schlüssel benötigen und somit keine eindeutige Zuordnung der Signatur möglich ist, aber es ist weniger rechenaufwändig als die Erstellung einer Signatur, die auf einem asymmetrischen Verschlüsselungsverfahren basiert. Das HMAC-Verfahren wird beispielsweise bei Sessions zwischen einer Applikation und dem TPM verwendet (siehe Abschnitt 2.3). Die RSA-Engine umfasst Funktionen zur Generierung von symmetrischen und asymmetrischen Schlüsseln, ist für die RSA-Ver- und Entschlüsselung, sowie für die Erzeugung von RSA-Signaturen zuständig. Die Validierung von Signaturen ist aus Performanzgründen nicht im TPM implementiert. Die Spezifikation erlaubt, dass das TPM auch andere Verschlüsselungsverfahren unterstützt, das RSA-Verfahren ist jedoch obligatorisch.

Flüchtiger und Nicht-Flüchtiger Speicher

volatile

Im flüchtigen Speicher befinden sich die Key Slots und die Platform Configuration Register. Die Key Slots dienen als sicherer Schlüssel-Cache für die RTS (siehe Abschnitt 2.2). Der Befehl LoadKey() läd einen Schlüssel in den Speicher, während der Befehl EvictKey() einen Schlüssel auslagert (Wrapping). Die Verwaltung zwischen dem externen Speicher und dem Schlüssel-Cache übernimmt der Key Cache Manager, der von dem Trusted Software Stack implementiert wird. Ein Schlüssel wird bei der Auslagerung mit einem Storage-Key kodiert, so dass auch nicht migrierbare Schlüssel ausgelagert werden können. Dieses Verfahren wird in Abschnitt 2.2 genauer behandelt. Die PCRs dienen, wie bereits in Abschnitt 2.1 erwähnt, zur Speicherung von 160 Bit SHA-1 Hashwerten, die zur vertrauenswürdigen Attestierung von Systemkonfigurationen benötigt werden.

non-volatile

Der Nicht-flüchtige Speicher enthält die 160 Bit Data Integrity Register (DIR), den Endorsement Key (EK), den Storage Root Key (SRK), das Owner Auth Secret und die Attestation Identity Keys. Die Data Integrity Register

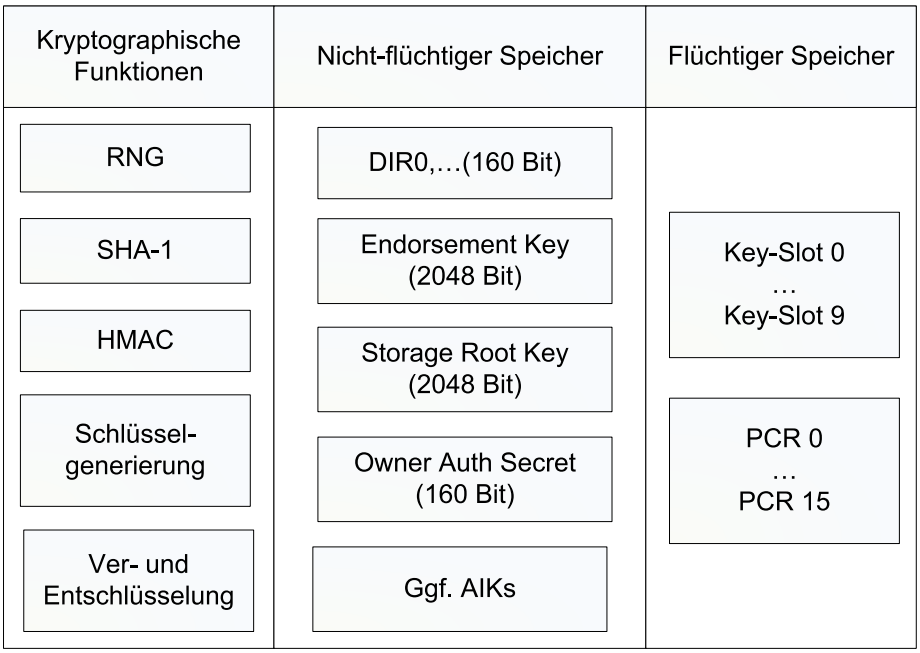

Abb. 3. Flüchtiger und Nicht-flüchtiger Speicher des TPM.

beinhalten sicherheitskritische Daten, wie zum Beispiel das Endorsement Zertifikat. Normalerweise ist ein Zertifikat nicht privacy-sensitiv, da es nur den Public Key eines asymmetrischen Schlüsselpaars beinhaltet. Das Endorsement Zertifikat nimmt eine Sonderrolle ein. Der Endorsement Key wird bei der Herstellung in das TPM geschrieben und ist über die gesamte Lebensdauer des Chips daran gebunden. Daher kann über den Public Endorsement Key Profiling betrieben werden. Der Kritik der Öffentlichkeit an diesem Missstand ist es zu verdanken, dass seit der Spezifikation v1.2 die AIKs eingeführt wurden, die Profiling erschweren sollen. Der EK ist mittlerweile auch austauschbar, allerdings ist diese Funktion in der Praxis nicht applikabel, da dadurch alle Zertifikate der Plattform, die sich auf den Endorsement Key beziehen, ungültig werden und neu erstellt werden müssen (siehe Abschnitt 2.5). Wichtig ist, dass bei der Erstellung von AIKs der öffentliche EK an die Zertifizierungsstelle, die das AIK-Zertifikat signieren soll, ausgegeben werden muss. Die Auswahl der CA sollte sorgfältig ausfallen, denn falls die Certification Authority nicht vertraulich mit dem öffentlichen EK umgeht, kann ein AIK wieder eindeutig dem TPM zugeordnet werden. Der SRK bildet die Wurzel der in Abschnitt 2.2 beschriebenen Schlüsselhierarchie. Er wird bei der Inbesitznahme, die in Abschnitt 2.4 näher beleuchtet wird, erstellt. Das Owner Auth Secret ist ein 160-Bit Hashwert über das Passwort, das bei der Inbesitznahme des TPMs festgelegt wird und das für die Ausführung kritischer

TPM-Befehle wie die Aktivierung und Deaktivierung des TPMs angegeben werden muss.

2.2 Roots of Trust

Die Roots of Trust bilden den Vertrauensanker von TC. Ihnen muss vertraut werden. Die Hardwarekomponenten, die die Roots of Trust implementieren, wie z.B. das TPM müssen laut Spezifikation *EAL3* geprüft sein. Dabei handelt es sich um eine relativ geringe Sicherheitsstufe, bei der die Funktionsweise methodisch getestet wird. Hier setzt häufig die Kritik der Gegner von TC an. Sie sind der Meinung, dass das Vertrauen in die Hardwarekomponenten nicht gerechtfertigt sei. Es handelt sich bei dieser Sicherheitsvorgabe um einen Kompromiss zwischen Kosten und Nutzen. Eine aufwändigere und kostenspieligere Prüfung wäre von den Hardwareherstellern und auch von den Käufern nicht akzeptiert worden.

Es gibt vier verschiedene Roots of Trust, die jeweils unterschiedliche Funktionen übernehmen. Die Root of Trust for Measurement nimmt vertrauenswürdige Messungen von Systemkonfigurationen vor. Die Trusted Building Blocks sind Hardwarekomponenten, die sicherheitskritische Aufgaben erledigen und Verbindungswege zwischen dem Mainboard und den Komponenten des TCG Subsystems. Die Root of Trust for Storage verwaltet vertrauenswürdige Daten innerhalb des TPM. Die Root of Trust for Reporting stellt vertrauenswürdige Bescheinigungen über Daten aus dem TPM gegenüber Dritten aus.

Root of Trust for Measurement (RTM)

Die Root of Trust for Measurement ist ausführbarer Code, der auf zuverlässige Weise die Integrität einer Konfiguration bei Boot-, Reset- und Suspendvorgängen, bestimmen bzw. messen kann. Die Core Root of Trust for Measurement ist der Teil des RTMs, der zu Beginn z.B. des Bootvorganges ausgeführt wird. Die RTM kann im BIOS realisiert werden, ist aber gemäß Spezifikation idealerweise in das TPM integriert. Es nutzt in jedem Fall die SHA-1 Hashfunktion des TPM. Die Messung von Systemzuständen bzw. Konfigurationen erzeugt sogenannte Measurement Events (ME). Bei diesem Vorgang werden zwei verschiedene Typen von Daten erzeugt, einerseits die gemessenen Werte und andererseits Hashwerte darüber. Die Hashwerte werden in den PCRs des TPMs gespeichert und vom RTS verwaltet. Die nicht gehashten Werte werden unverschlüsselt in Stored Measurement Logs - in der Literatur auch häufig Event Logs genannt - gespeichert. Veränderungen an den Logs können anhand der sicher abgespeicherten Hashwerte festgestellt werden, daher stellt die unverschlüsselte Speicherung kein Sicherheitsrisiko dar. Bei einem Bootvorgang (bzw. Reset-, Suspend-) wird eine Vertrauenskette (Chain of Trust) aufgebaut. Ausgehend von dem CRTM und den Trusted Building Blocks, denen vertraut werden muss, wird ein Measurement Flow durchgeführt, so dass jeweils vor der Ausführung von unsicherem Code eine

Vertrauenskette

Messung desselben vorgenommen wird. Dadurch wird aus einer sicheren Konfiguration heraus schrittweise in einen neuen sicheren Zustand übergegangen. Das TCG-Subsystem ist passiv, d.h. hier wird nur protokolliert (monitoring). Eine TC Plattform kann in einen unsicheren Statuts booten. Sie kann jedoch keine Falschaussagen über ihren Zustand machen.

Trusted Building Blocks (TBB)

Bei den Trusted Building Blocks handelt es sich nicht um eine Komponente. Dieser Begriff umfasst alle Hardwarekomponenten des TCG-Subsystems, denen vertraut werden muss, die aber keine direkte Aufgabe für Trusted Computing erfüllen. Das sind unter anderem Verbindungswege und Komponenten, die sicherheitskritischen Code enthalten, bzw. sicherheitskritische Aufgaben übernehmen. Sie gehören nicht direkt zu den Roots of Trust, ihnen muss jedoch vertraut werden.

Beispiel 1. Den Init- und Reset-Funktionen muss vertraut werden, da zu diesem Zeitpunkt die Sicherheitsmechanismen noch nicht aktiv sind.

Beispiel 2. Das TPM hat keinen Einfluss auf seine Konnektivität mit dem Mainboard.

Beispiel 3. Bei der Durchführung wichtiger TPM_Kommandos, soll eine sichere Verbindung zwischen dem Benutzer und dem System gewährleistet werden und dessen physische Anwesenheit überprüft werden können. Dabei soll die Integrität und Vertraulichkeit der Verbindung zwischen Eingabegerät (z.B. Tastatur) und System garantiert werden. Diese sichere Verbindung kann häufig nicht gewährleistet werden und wird daher manchmal durch einen Jumper, oder auch durch Drücken der „fn“-Taste (bei IBM Thinkpads) realisiert. Das Drücken einer bestimmten Taste oder ein Jumper auf dem Mainboard ist kein TBB, sondern eine Notlösung.

Root of Trust for Storage (RTS)

Die Root of Trust for Storage ist für die Verwaltung von Daten, aus dem TPM, verantwortlich. Sie wird durch das TPM implementiert. Sie generiert Schlüssel und verwaltet sie in der Schlüsselhierarchie. Abbildung 4 zeigt, wie die RTS Schlüssel verwaltet. Der Endorsement Key (EK), die Authorization Auth Data und der Storage Root Key (SRK) befinden sich im nicht-flüchtigen Speicher (siehe Abschnitt 2.1 und 2.4). Der Schlüsselcache (Key Slots) befindet sich im flüchtigen Speicher. Nicht alle Schlüssel können im Speicher des TPM gehalten werden, daher ist es möglich mit einem Storage-Key verschlüsselt in sogenannte Key-BLOBs auszulagern. Die Auslagerung (Wrapping) von Key-BLOBS ist hierarchisch aufgebaut. Jeder ausgelagerte Schlüssel ist mit einem Elter-Storage-Key verschlüsselt. Die oberste Hierarchiestufe wird mit dem Storage Root Key verschlüsselt, der sich in dem flüchtigen Speicher des TPM befindet. AIKs werden immer in der obersten Hierarchieebene ausgelagert.

Wrapping, Schlüsselhierarchie

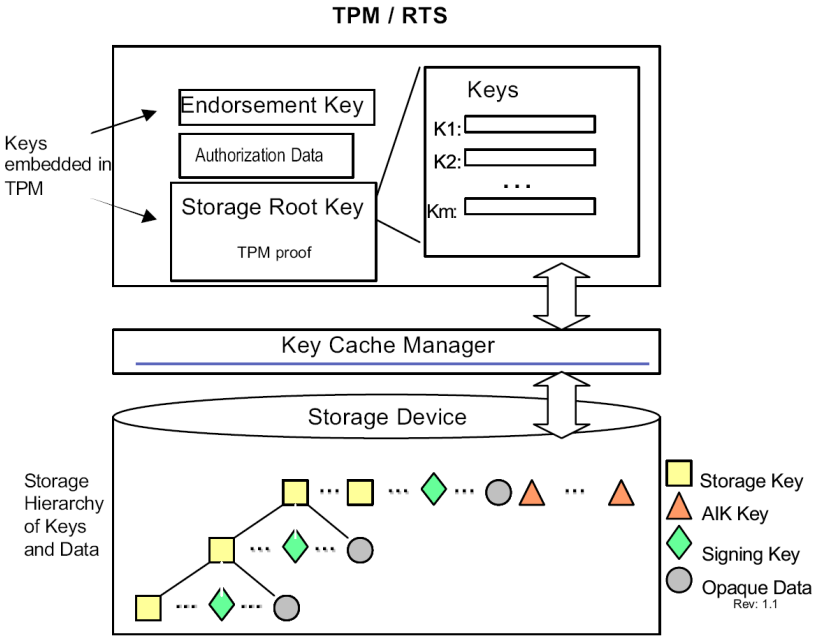

Abb. 4. Schlüsselhierarchie, Root of Trust for Storage und Key Cache Manager

Beispiel 4. Soll ein Schlüssel K_2 aus der zweiten Ebene in den Schlüsselcache geladen werden, so muss erst der Elter-Storage-Key K_1, aus der ersten Hierarchiestufe, mit dem SRK eingelagert werden. Mit dem Storage Key K_1 kann der Schlüssel K_2 entschlüsselt und in einen Key Slot geschrieben werden.

Zusätzlich zur asymetrischen Verschlüsselung durch einen Storage Key wird ein Schlüssel noch symmetrisch mit einem Hash, über eine Passphrase, verschlüsselt, um einen Schlüssel an einen einzelnen Nutzer binden zu können. Auch kleine Datenobjekte können verschlüsselt ausgelagert werden. Die sichere Speicherung von kryptografischen Schlüsseln ausserhalb des TPM ist nicht zu verwechseln mit der Migration von Schlüsseln. Migrierbare Schlüssel können unverschlüsselt ausgelagert werden, um Sie auf einem anderen System verwenden zu können. Sie können z.B. in ein anderes TPM als Legacy Key eingebunden werden (siehe Abschnitt 2.4). Ausgelagerte Schlüssel sind an ein TPM gebunden.

Root of Trust for Reporting (RTR)

Die Root of Trust for Reporting erstellt Bescheinigungen (reporting) über Daten aus dem TPM. Sie ist im TPM implementiert. Es gibt viele Anwendungsszenarios, in denen der Report von Daten, aus dem TPM, eine Rolle spielt. Ein sehr allgemeines Beispiel einer Attestierung ist die Anfrage eines Dienstanbieter an ein TPM, ob es sich in einem vertrauenswürdigen Zustand befindet. An diese

Konfiguration kann ein Dienst - z.B. das Abspielen einer MP3-Datei - gebunden werden (Sealing, siehe Abschnitt 2.4).

Attestierung

Beispiel 5. Der Challenger schickt eine Anfrage an den Agenten der Trusted Computing Plattform. Der Agent holt sich über den TCG Service Provider (siehe Abschnitt 2.3) die Event Logs bzw. SMLs. Die RTR signiert die zugehörigen Hashwerte aus den Platform Configuration Registern mit einem AIK. Das AIK-Zertifikat wird zusammen mit dem Plattformzertifikat (siehe Abschnitt 2.5), den signierten Werten aus den Platform Configuration Registern und den Logs an den Challenger zurückgesendet. Der Challenger kann Änderungen an den Logs mit den signierten Hashwerten aus den PCRs feststellen. Er kann die Vertrauenswürdigkeit der Systemkonfiguration der TCG-Plattform auf unterschiedliche Weise verifizieren. Entweder er überprüft die Werte in den Logs oder er vergleicht die Hashwerte mit Hashwerten, von Servern mit Hashlisten über vertrauenswürdige Komponenten.

2.3 Trusted Software Stack (TSS)

Der Trusted Software Stack bietet eine Schnittstelle zwischen dem TCG-Subsystem und dem Betriebsystem bzw. den Applikationen. Eine beliebige Entität (Prozess, Thread oder Embedded Controller) kann TPM-Befehle absetzen. Die Entität bildet zusammen mit dem TPM, über den Trusted Software Stack, einen sicheren Kommunikationskanal über den die Befehle und die Ergebnisse gesendet werden. Die Kanäle folgen den Semantiken für Session-orientierten Nachrichtenaustausch. Eine Session besteht aus:

Session ID.
Eindeutiger Session-Identifikator.

Nonce.
Zufallswert, der Wiederholungsangriffe erschweren soll. Es wird in jedem Kanal eine neue Nonce verwendet.

Message Digest.
Hashwert über die ausgetauschte Nachricht, der bei jeder Nachricht erneuert wird.

Ephemeral Secret.
Kurzlebiges Geheimnis, zur Bindung einer Nachricht an ein Objekt bzw. um den Nachrichtenverkehr zu verschlüsseln.

Command Validation Protocol

Bei dem Aufbau einer Session wird eine random 160 Bit Passphrase benutzt, die nicht im TPM, sondern von der Entität, die die Kommunikation mit dem TPM aufbaut, generiert wird. Das Protokoll zur Befehlsvalidierung benutzt das HMAC-Verfahren, um eine Session zwischen dem Aufrufer und dem TPM aufzubauen und die Integrität des Datenaustausches zu gewährleisten. Nachrichten werden erst auf beiden Seiten validiert, bevor der nächste Schritt unternommen wird. Alle Komponenten ausserhalb des TPMs inklusive dem TSS werden von dem TPM als nicht vertrauenswürdig eingestuft. Das TPM kann jedoch ein Fehlverhalten feststellen. Abbildung 5 zeigt die Schichtung des TSS. Im Folgenden werden die einzelnen Ebenen des Software Stacks beschrieben.

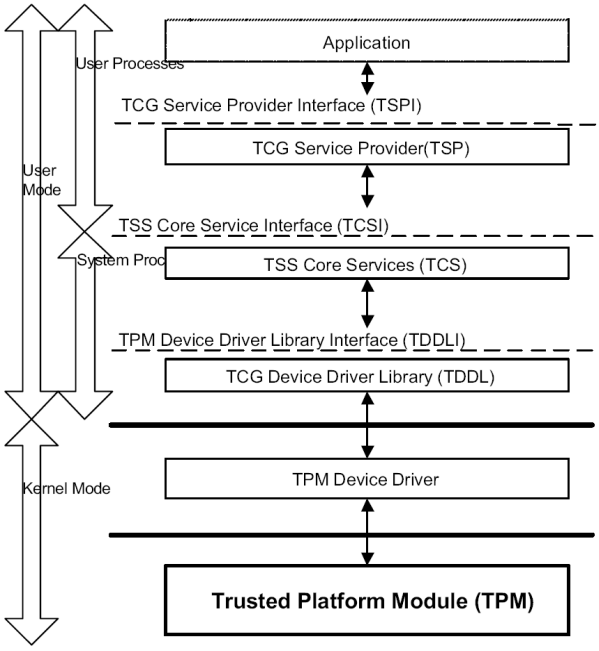

Abb. 5. Ebenen des Trusted Software Stack

Device Driver Library Interface

Das TDDL Interface ist im User Mode angesiedelt. Es setzt auf dem TPM Device Driver auf, der betriebsystemunabhängig implementiert wird. Diese Designentscheidung ermöglicht Flexibilität für die Implementierung des TSS:

- Verschiedene Implementierungen des TCG Software Stacks können mit jedem TPM kommunizieren.
- Es bietet eine betriebssystemunabhängige Schnittstelle für TPM-Applikationen.
- Es erlaubt einem Hersteller einen Software-TPM-Simulator als eine User-Mode-Komponente anzubieten.

TSS Core Service Interface

Das TCS Interface bietet eine Schnittstelle zu einem allgemeinen Satz von Plattformdiensten. Es kann mehrere Service Provider auf einem System geben, der TCS stellt sicher, dass sie sich alle konform verhalten. Er unterstützt vier zentrale Dienste:

Context Management.
Implementiert Multithread-Zugriff auf das TPM.

Credential und Key Management.
Speichert Zertifikate und Schlüssel, die zu der Plattform gehören.

Measurement Event Management.
Verwaltet Stored Measurement Logs (siehe Abschnitt 2.2) und den Zugriff auf PCR-Register.

Parameter Block Generation.
Synchronisiert und verarbeitet TPM-Befehle.

TCG Service Provider Interface

Das TSP Interface arbeitet im selben Addressraum wie die Applikation. Auf dieser Ebene findet die Authorisation zur Nutzung von TPM-Befehlen statt. Dies wird entweder über ein User Interface oder über einen Callback Mechanismus, falls der Aufrufer von Außen zugreift, realisiert.

2.4 Keymanagement

In der TCG-Spezifikation werden mehrere Schlüsseltypen verwendet, um eine sichere Kommunikation und die sichere Speicherung von Daten zu gewährleisten. Diese werden im Folgenden vorgestellt.

Endorsement Key

Der Endorsement Key (EK) ist ein RSA-Schlüsselpaar, hat eine Länge von 2048 Bit und wird bei der Chipherstellung erzeugt. Entweder geschieht dies im TPM, durch das Kommando TPM_CreateEndorsementKey, oder aber außerhalb des Chips. Das generierte Schlüsselpaar wird im letzteren Fall in das TPM exportiert. Dieser Schlüssel stellt eine kritische Komponente dar, da er dem TPM eindeutig zugeordnet ist. Der private Schlüsselanteil kann und darf das TPM niemals verlassen. Er ist im nicht-flüchtigen Speicher abgelegt. Der Zugriff auf den öffentlichen Schlüsselanteil wird nur dem Besitzer gewährt, nachdem eine Zugriffskontrolle stattgefunden hat und dieser die Authentifizierungsdaten nachgewiesen hat.
Der EK wird zur Signierung der im TPM erzeugten Attestion Identity Keys verwendet, sowie zur Bestätigung deren Authentizität. Den zur Überprüfung notwendigen öffentlichen EK muss der Besitzer einer sorgsam gewählten Zertifizierungsstelle (Privacy CA) zu kommen lassen. Mithilfe dieses Schlüssels entsteht eine Bindung zwischen den erzeugten AIK und der TPM-Plattform. Wir werden später in Kapitel 2.5 auf diese Bindung eingehen. Weiterhin wird der Schlüssel bei der Verschlüsselung des Owner Authentication Keys verwendet, um auch diesen an die Plattform zu binden.
Bis zur Version 1.1b war es nicht vorgesehen, den EK zu löschen oder ihn durch einen anderen - neu generierten - zu ersetzen. Aufgrund heftiger Kritik an der TCG durch Datenschutzorganisationen, Regierungen, sowie dem Chaos Computer Club (CCC), ist dieses seit Version 1.2 möglich geworden.

Owner Authentication Key

Besitzübername

Nach dem Erwerb muss die Plattform in Besitz genommen werden damit das TPM eingeschaltet werden kann.
Mit dem Hardware-Befehl TPM_TakeOwnership geschieht dieses. Dabei muss der neue Besitzer eine Passphrase (ownpass) eingeben, welche ihn von nun an identifiziert. Dieser Befehl erwartet als erstes Argument einen 160 Bit SHA-1 Hashwert, welcher aus der eingegeben Passphrase errechnet wird. Dieser Wert wird im nicht-flüchtigen Speicher im TPM abgelegt und zusätzlich noch mit dem öffentlichen EK verschlüsselt. Durch diese Verschlüsselung ist eine Bindung an das TPM gewährleistet, so dass das gehashte Passwort nur auf dieser Plattform gültig ist.
Erfordert ein TPM-Befehl Besitzer-Berechtigung, so muss dieses shared secret nachgewiesen werden, um das Kommando auszuführen. Falls der Chip schon in Besitz genommen wurde, so schlägt der Befehl TPM_TakeOwnership fehl. Ein Besitzerwechsel ist nur durch eine spezielle Reset-Sequenz möglich, welche wiederum die physische Anwesenheit des Besitzers erfordert.

Storage Root Key

Der Storage Root Key (SRK) ist wie der EK ebenfalls ein 2048 RSA Schlüsselpaar. Er wird jedoch erst bei der Besitzübernahme im TPM generiert. Er ist im nicht-flüchtigen Speicher abgelegt und wird, wie der Owner Authentication Key, mit einer Passphrase (srkpass) geschützt. Diese Passphrase wird dem Kommando TPM_TakeOwnership als zweiter Parameter ebenfalls als SHA-1 Hash übergeben.
Der SRK stellt wie bereits erwähnt, die oberste Ebene der Schlüsselhirarchie dar. Er bildet die Wurzel. Mit seinem öffentlichen Anteil werden alle privaten Schlüssel der ersten Hirachiestufe verschlüsselt, wenn sie aus dem TPM ausgelagert werden. Aufgrund dessen ist es möglich, alle Schlüssel (ausser dem EK und dem ownpass) sicher außerhalb des TPM zu verwalten. Zugriff auf die so abgelegten Schlüssel wird dann nur auf der korrekten TPM-Plattform gewährt. Dem Besitzer ist es erlaubt den SRK zu löschen und durch einen anderen zu ersetzen. Durch diese Prozedur gehen jedoch alle Schlüssel in dieser Schlüsselhirarchie verloren, sofern keine gesonderten Sicherheitsmaßnahmen getroffen wurden. Des Weiteren gehen alle Daten verloren, wenn ein Besitzerwechsel vorgenommen wird. Inifineon bietet hier auf seinen TPM-Chips eine Recovery Funktion, um dieses zu verhindern. Wird die Hardware jedoch defekt so sind auch alle mithilfe des TPMs gesicherten Daten verloren.

Schlüsselhirarchie

Das TPM bietet Funktionen zur Erzeugung neuer Schlüssel, oder aber auch um externe Schlüssel zu migrieren, bzw. Abgelegte zu exportieren. Diese werden in der Schlüsselhirarchie abgelegt. Die Eingliederung eines Schlüssels in die Hierarchie benötigt die Angabe eines existierenden Schlüssels, mit dessen öffentlichen Anteil der neue Schlüssel abgelegt werden soll. Danach lässt sich dieser neue Schlüssel in den Speicher laden, die Übereinstimmung der eingegebenen Passphrase mit dem zu dem Elterschlüssel gehörenden vorausgesetzt. Dabei wird

der SHA-1 Algorithmus auf die eingegebene Passphrase angewendet und als symmetrischer Schlüssel für die Entschlüsselung des Elterschlüssels eingesetzt. Dieses Prinzip wird als Wrapping bezeichnet. Zusätzlich muss auch zu jedem eingefügten Schlüssel eine Passphrase hinterlegt werden.

Attestion Identity Key

Die Attestion Identity Keys (AIK) können in beliebiger Anzahl vom Benutzer im TPM mit dem Kommando TPM_MakeIdentity erzeugt werden, sofern das TPM in Besitz genommen wurde. Sie dienen zum Signieren von Daten welche im TPM existieren (z.B. Inhalte aus den PCR-Registern oder Statusinformationen). Sie werden unterhalb des SRK abgelegt. Attestion Identity Keys sind ebenfalls 2048 Bit RSA-Schlüsselpaare, sie müssen jedoch signiert werden damit ihre Gültigkeit überprüft werden kann. Dazu wird bei der Erzeugung ein Zertifikat in Auftrag gegeben, welches der Benutzer anschließend von einer von ihm gewählten Zertifizierungsstelle signieren lassen muss. Dieser Vorgang ist sicherheitskritisch und wird in Kapitel 2.5 näher erläutert.
Für unterschiedliche Anfragen kann der Benutzer verschiedene von ihm erzeugte AIKs benutzen. Dies soll verhindern, dass die Parteien, mit denen man kommuniziert, gezielt Profile erstellen können. Dieses wäre möglich, da ein erzeugter AIK durch den Endorsement Key an eine Plattform gebunden ist. Dem AIK selbst ist diese Bindung jedoch nicht anzusehen. Das Konzept der Anonymisierung mithilfe von AIKs war in frühen Versionen der TCG- bzw. TCPA-Spezifikation nicht vorgesehen. Dieser Umstand wurde jedoch von vielen dritten Parteien bemängelt, da diese die Privacy der Nutzer in Gefahr sahen.

Schlüsselkonzept

Migrierbar

Bei der Generierung von Schlüsseln kann festgelegt werden, ob diese migrierbar sein sollen oder nicht. Das bedeutet, daß diese aus dem TPM exportiert werden können, bzw. in dieses importiert werden können. Dieses Attribut ist fest mit dem Schlüssel verbunden und kann später nicht mehr geändert werden. Ein als nicht migrierbar erzeugter Schlüssel, ist fest an eine spezifische TPM-Plattform gebunden und kann nur an dieser genutzt werden. Andererseits bedeutet dies, dass migrierbare Schlüssel das TPM verlassen können, um z.B. auf einem externen Datenträger abgelegt zu werden. Das ermöglicht die Nutzung des Schlüssels auf verschiedenen Plattformen. Insbesondere ist es auch möglich diesen Schlüssel in ein anderes TPM zu exportieren, z.B. um Daten von einem Desktop-PC auf einem Notebook zu entschlüsseln. Jedoch ist die Sicherheit durch die Hardware dann nicht mehr gegeben, da der Schlüssel das sichere TPM verlassen hat. Signaturschlüssel werden daher immer als nicht-migrierbar deklariert (z.B. AIKs). Ferner sind der Storage Root Key und der Endorsement Key nicht-migrierbar. Bei der Generierung muss ebenfalls festgelegt werden, welche Funktion der Schlüssel erfüllen soll. So kann z.B. mit einem Signaturschlüssel ausschließlich signiert werden, nicht jedoch verschlüsselt.

Zusammenfassend beinhaltet die TCG-Spezifikation 7 Schlüsseltypen:

- Signaturschlüssel werden zum Signieren verwendet und sollten als nicht-migrierbar erzeugt werden. Sie können jedoch auch migrierbar sein. Dies sind asymmetrische Schlüssel.
- Storage Keys sind asymmetrische Schlüssel mit denen Daten oder andere Schlüssel verschlüsselt werden. Diese Daten werden dadurch an die Plattform gebunden. Größere Datenmengen können auf diese Weise sicher außerhalb des TPM gespeichert werden. Sie entlasten somit den begrenzten, sicheren Speicher des TPM
- Identity Keys, bzw. Attestion Identity Keys, dienen zum Signieren und sind immer als nicht-migrierbar deklariert. Mit ihnen dürfen nur Daten signiert werden, die vom TPM selbst stammen (z.B. Werte aus den Platform Configuration Registern).
- Der vom Hersteller erzeugte Endorsement Key ist nicht migrierbar und wird für die Authentifizierung des Besitzers und bei der AIK-Erzeugung benutzt.
- Bind Keys werden verwendet um (kleine) Datenmengen, wie symmetrische Schlüssel, auf einer Plattform zu ver-, und auf einer anderen, zu entschlüsseln (Binding).
- Legacy Keys sind Schlüssel, die außerhalb des TPM erzeugt und später importiert wurden. Sie sind migrierbar.
- Authentication Keys sind symmetrische Schlüssel die in Version 1.2 eingeführt wurden. Mit ihnen erfolgt ein sicherer Datentransfer zwischen dem TPM und dem Betriebssystem bzw. dessen Anwendungen (Kapitel 2.1).

Sealing

Das bereits genannte Binding kann noch einen Schritt weitergeführt werden. Die verschlüsselten Informationen können an einen Systemzustand (PCR-Werte) gebunden werden. Dabei kann es sich um den Zustand handeln, in dem sich der Rechner gerade befindet, oder es wird ein Zustand vorausgesetzt der noch nicht eingetreten ist. Dieses Vorgehen wir als Sealing bezeichnet. Wenn Daten so verschlüsselt werden, dann ist es nur möglich sie zu entschlüsseln wenn a) der gleiche, bei dem Verschlüsselungsprozess vorgefundene, Systemzustand wieder existiert, oder b) sich das System in einem definierten Zustand befindet. Das System muss sich also in vorgegebenen Parametern befinden.
So ist es z.B. möglich Daten sicher abzulegen welche erst in einer Woche wieder entschlüsselt werden können. Befindet sich das System in einem anderem (unbekannten) Systemzustand, wenn es unter Umständen kompromittiert wurde, so schlägt der Befehl zum Entschlüsseln fehl. Zudem kann noch eine Passphrase angegeben werden, welche ebenfalls beim Entschlüsseln eingegeben werden muss.

2.5 Zertifikate

Die TCG definiert 5 Zertifikate (Credentials) welche die Identität einer TPM-Plattform und deren Attestion Identity Keys attestieren. Namentlich sind die-

ses das EK-Credential, Conformance Credential Platform Credential, Validation Credential, sowie das AIK-Credential. Eine besondere Stellung nimmt das AIK-Credential ein, da dieses erst vom Benutzer erzeugt wird. Diese Zertifikate sind Datenstrukturen in ASN.1 Notation und basieren auf X.509 Zertifikat-Strukturen mit zusätzlichen speziellen Datenfeldern.

Endorsement Credential

Dieses Zertifikat wird von dem Hersteller ausgestellt und signiert, der auch den Endorsement Key des TPM erzeugt. Es enthält Informationen wie den Namen des Herstellers, die Versionsnummer des TPM und natürlich den öffentlichen Anteil des EK. Da es sich bei dem Schlüsselanteil um eine sicherheitskritische Komponente des Systems handelt, wird dieses Zertifikat im sicheren nicht-flüchtigen Speicher des TPM abgelegt. Die Einzigartigkeit dieses Schlüssels wurde bereits erwähnt. Es ist daher möglich mithilfe des Zertifikates Rückschlüsse auf den Besitzer zu führen.

Conformance Credential

Mit der Signatur für das Conformance Zertifikat bestätigt der Aussteller, dass das Design und die Implementierung der Trusted Building Blocks der TPM-Plattform der Spezifikation entsprechen. Es kann von jeder beliebigen Instanz ausgestellt werden, welche das System evaluieren kann.

Platform Credential

Das Plattform Zertifikat identifiziert den Hersteller der Plattform sowie einige Eigenschaften der Plattform und verweist auf das Endorsement Zertifikat, sowie auf das Conformance Zertifikat in Form eines MAC-Wertes. Es bescheinigt, dass die Plattform ein TPM enthält, wie es im EK-Zertifikat beschrieben ist. Durch dieses Zertifkat entsteht eine Bindung zwischen dem TPM und der spezifischen Rechner-Plattform. Ausgestellt werden kann dieses Zertifikat von einer beliebigen Instanz mit genügend Glaubwürdigkeit, wie z.B. einem Händler.

Validation Credential

Den Herstellern von (sicherheitskritischen) Komponenten ist es durch dieses Zertifikat möglich, diese auch nachträglich als vertrauenswürdig zu attestieren. Es kann von jeder Instanz ausgestellt werden, die die korrekte Funktionsweise der Komponente verifiziert hat. Einige Beispiele für die es ausgestellt werden kann sind Grafikkarten, Festplatten, Prozessoren, Netzwerkkarten und Tastaturen. Aber auch Software kann so zertifiziert werden.

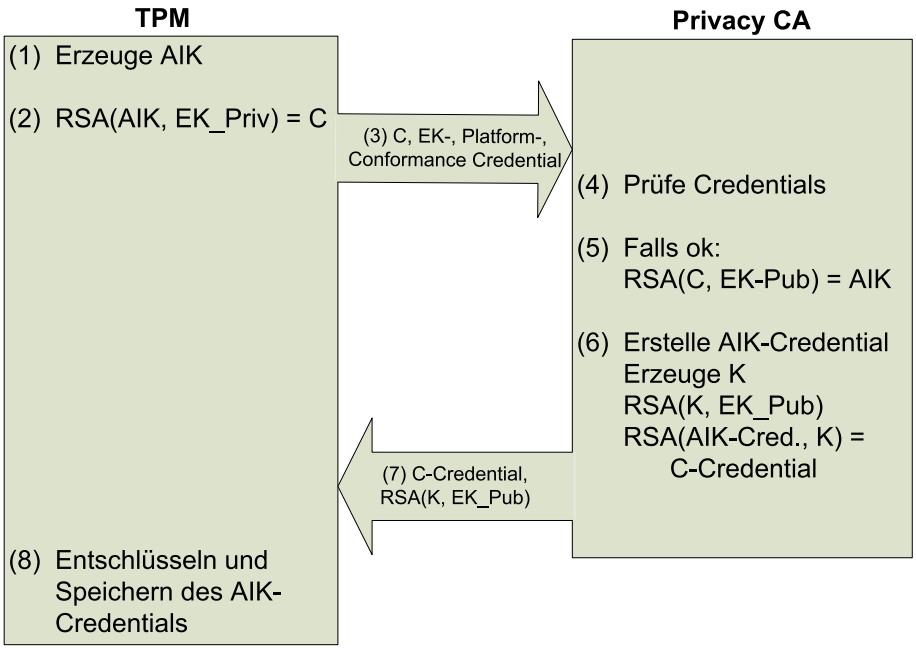

Abb. 6. Signieren eines AIK-Zertifikates

Attestation Identity Credential

Zertifizierungsstelle

Im TPM können beliebig viele Attestion Identity Keys erzeugt werden. Damit diese als glaubwürdig eingestuft werden können, müssen deren Zertifikate von einer glaubwürdigen Instanz signiert werden. Mit der Signatur beglaubigt der Aussteller die Vertrauenswürdigkeit. Bei der Erzeugung eines neuen AIKs wird eine Anfrage an eine, vom Benutzer gewählte, Zertifizierungsstelle (CA) gesandt. Diese Anfrage enthält den öffentlichen Anteil des AIK, das Endorsement Zertifikat sowie das Plattform- und das Conformance Zertifikat. Die CA sollte sorgsam gewählt werden, da diese eine Bindung zwischen dem AIK und der TPM-Plattform vornimmt und dazu den einzigartigen öffentlichen Endorsement Key benutzt. Das kann beim Benutzer zu Privacy Problemen führen. Die Anfrage zur Ausstellung der Signatur übernimmt auf der TPM-Plattform das Betriebssystem. Das TPM selbst regt dieses lediglich durch einen Befehl an. Die Zertifizierungsstelle überprüft zunächst die mitgeschickten Zertifikate. Sind diese noch gültig, so wurde der AIK auf einer korrekt funktionierenden TPM-Plattform erzeugt. Anschließend wird das AIK-Zertifikat mit dem öffentlichen Schlüssel der CA signiert und mit einem Session-Key verschlüsselt an den Antragsteller übertragen. Dieser kann das Zertifikat nun entschlüsseln. Das TPM überprüft die Korrektheit des Zertifikates mit dem Befehl TPM_ActivateIdentity. Abbildung 6 verdeutlicht diesen Ablauf.

2.6 Bootvorgang

Bootstrapping

Bei den aktuellen Rechner-Plattformen läuft der Bootvorgang vereinfacht nach dem folgenden Schema ab. Zunächst wird bei dem Systemstart ein minimaler Bootloader aus einem ROM in den Speicher geladen und ausgeführt. Dieses ROM befindet sich als physikalische Einheit (mounting device) auf dem Motherboard. Dieser Bootloader lädt das BIOS in den Speicher und führt dieses aus. Das BIOS ist meistens als ein gesockelter Chip realisiert, welcher einen Flash-Speicher darstellt. Der Code im BIOS sorgt dafür, dass der eigentliche Bootloader aus dem Master Boot Record der zu bootenden Festplatte in den Speicher geladen und ausgeführt wird. Anschließend werden der Betriebssystemkern und nachfolgend das Betriebssystem gestartet. Dieser Vorgang wird Bootstrapping genannt.
Bei diesem recht einfachen Vorgang können einige Sicherheitsprobleme auftreten. Es ist z.B. möglich, dass der Master Boot Record der Festplatte mit einem Virus infiziert ist, welcher vor dem Kernel ausgeführt wird und so die gleichen Rechte wie dieser besitzt. Zudem kann der Super-Block manipuliert werden, welches zu einer Art Denial-of-Service Angriff führen kann. Ein schadhafter Kernel kann ebenso einfach eingespielt werden. Dies sind nur wenige Risiken, doch sie lassen bereits erkennen, dass ein sicherer Bootvorgang wünschenswert ist.
Ein sicherer Bootvorgang mittels der Konzepte der TCG soll diese Angriffe verhindern. Dazu muss sichergestellt werden, dass das System aus einer sicheren und unmodifizierbaren und vertrauenswürdigen Basis heraus bootet (CRTM). Bei dem Bootvorgang wird in jedem Schritt der aktuelle Konfigurationswert aufgezeichnet und vom TPM protokolliert. In die Messungen fließen unter anderem Firmware-Versionen, Hash-Werte über Komponenten bzw. über deren Firmware, Kontrollnachrichten und Benutzereingaben ein. Es wird eine Vertrauenskette aufgebaut, siehe Kapitel 2.2. Diese gemessenen Werte werden in den PCR-Registern abgelegt und können später vom Betriebssystem ausgelesen und mit bereits bekannten abgeglichen werden. Somit kann das Betriebssystem erkennen, wenn sich das System nicht mehr in einem bekannten (sicheren) Zustand befindet. Da diese Messungen jedoch durch ein passives TPM geschehen, wird keinesfalls verhindert dass ein modifiziertes und evtl. schadhaftes Betriebssystem, bzw. Komponenten von diesem, gestartet werden. Dieser Umstand wird lediglich aufgedeckt. Somit ist der häufig benutze Begriff des „sicheren Bootvorgangs“ nicht nur irreführend, sondern auch falsch.
Die Dienste zur Integritätsberechnung (RTM) kann das Betriebssystem, nachdem es gestartet wurde, selbst benutzen.

3 Anwendungen

3.1 Secure Start

Secure Start wird von Microsoft in Windows Vista (Codename Longhorn) im Jahr 2006 eingeführt. Es soll ein Starten in ein unmodifziertes und vertrauenswürdiges System ermöglichen. Zudem soll es die Sicherheit der Daten bei Diebstahl und Verlust erhöhen. Wird Secure Start verwendet, wird die gesamte

Windows-Partition verschlüsselt. Der Schlüssel wird im TPM sicher abgelegt. Dazu wird ein TPM in der Version 1.2 benötigt. Durch die Verschlüsselung der gesamten Partition werden alle offline-Angriffe abgewehrt, da ein Angreifer keinerlei Zugriff auf die abgelegten Daten erhält. Somit ist eine Manipulation des Systems nicht mehr möglich, wenn das System heruntergefahren ist. Manipulierte Kernel können nicht mehr in das System eingeschleust werden. Bei Verlust bzw. Diebstahl sind die Daten auf der Partition auch vor nicht gewollten Zugriffen geschützt, dieses wären z.B. die Eigenen Dateien (sofern diese nicht auf eine andere Partition ausgelagert wurden), die temporären Dateien, die Auslagerungsdatei sowie die Hibernation-Datei. Aus dem Speicher ausgelagerte Passwörter im Klartext in die Auslagerungsdatei sind nun ebenfalls nicht mehr auslesbar. Dieser Schutz trifft nur auf Systeme zu, welche nicht gestartet sind. Wurde Windows gestartet, so ist die Windows-Partition gemountet und auf alle abgelegten Daten kann zugegriffen werden.

Offline-Angriffe

Als Verschlüsselung wird ein symmetrisches Verfahren gewählt und der verwendete Schlüssel wird innerhalb der Schlüsselhirarchie im TPM abgelegt. Bei einem Systemstart wird der Schlüssel zum Entschlüsseln nur aus dem TPM gelesen, wenn sich das System innerhalb vorgegebener Parameter befindet. Die Verschlüsselung ist für den Benutzer komplett transparent und mit EFS (Encrypted File System) weiterhin kompatibel. Da eine Manipulation des Systems jedoch nicht verhindert werden kann, wenn das System gestartet ist, werden beim Systemstart alle wichtigen Dateien gehasht und der Wert mit bereits bekannten abgeglichen. Somit können auch Online-Manipulationen aufgedeckt werden. Hat sich z.B, ein Wurm in die Registry eingetragen um beim nächsten Startvorgang wieder ausgeführt zu werden, so würde dies bemerkt werden. Der Eintrag ändert den Hash-Wert.
Eine Recovery-Funktion schafft Abhilfe bei Verlust des Passwortes. Es ist möglich jenes im Active Directory abzulegen, welches jedoch den Hardwareschutz des TPM umgeht. Ist das Passwort nicht mehr verfügbar, so sind auch alle Daten auf der Partition verloren.

3.2 Vertrauenswürdigkeit attestieren

Mit einem System welches der TCG-Spezifikation entspricht kann ein Benutzer einem Kommunikationspartner attestieren, dass er seinen Anweisungen und Richtlinien im Umgang mit seinen Daten folge leistet. In einem System ohne TPM müsste der Partner administrative Rechte auf dem anderen System besitzen, um dieses durchzusetzen. Das ist oft nicht möglich bzw. unerwünscht. Die Lösung des Problems stellt ein Betriebssystem dar, welches die Dienste eines TPM einsetzt, um Policies auf Datensätzen durchzusetzen.

Policy

Unter einer Policy versteht man einen Satz von Regeln, der festlegt, wie bestimmte Daten auf einer IT-Plattform behandelt werden müssen.
„Das Kopieren oder Versenden meines Datensatzes XYZ ist nicht gestattet“ könnte eine einfache Security-Policy lauten, welche dann befolgt werden muss.

Auch können bestimmte Programme, sowie Hardwarekomponenten festgelegt werden, welche auf den Datensatz zugreifen dürfen, bzw. diesen bearbeiten dürfen. Als mögliches Einsatzgebiet bietet sich hier natürlich DRM (Digital Rights Management) an. Das Betriebssystem hat diese gesetzten Policies durchzusetzen.

Um den Ablauf der Attestierung zu veranschaulichen, verwenden wir als Synonym für 2 Kommunikationspartner Alice und Bob, wobei Alice einen Datensatz an Bob versenden möchte.
Zunächst fordert Alice von Bob einen Beweis, dass sein TPM korrekt funktioniert und ihre Policies befolgt werden. Da Bob keinen Einfluss auf die Arbeitsweise seines TPM hat, und dieses über den Systemzustand niemals lügt, kann Alice den aktuell herrschenden Systemzustand auf Bobs System erfragen. Erst durch die fehlende vollständige Kontrolle von Bob über sein System kann sichergestellt werden, dass sich Bob gegenüber Alice als vertrauenswürdig ausweisen kann.
Dazu schickt Alice Bob zunächst eine zufällige Zahl, welche Bob anschließend mit einem von ihm gewählten privaten AIK verschlüsselt. Dieser verschlüsselte Wert wird zusammen mit dem zugehörigen AIK-Zertifikat an Alice zurückgeschickt. Alice überprüft nun das Zertifikat auf Gültigkeit, und falls diese besteht, entschlüsselt sie den zurückgeschickten Datensatz. Stimmen beide Zahlen überein, so kann sie sich sicher sein, dass das TPM von Bob korrekt arbeitet. Daraufhin verschlüsselt Alice ihren Datensatz mit Bobs öffentlichen AIK (Binding) und schickt diesen gebunden an Policies an Bob. Bei größeren Datensätzen wird dieser mit einem symmetrischen Verfahren verschlüsselt, und lediglich der Schlüssel mit dem AIK verschlüsselt übertragen. Die Entschlüsselung des Datensatzes kann an eine Systemkonfiguration gebunden sein (Sealing). In diesem Fall werden die aktuellen Hash-Werte in den PCR-Registern mit den geforderten abgeglichen. Werden diese Werte vorgefunden, so gewährt das TPM die Benutzung des SRK und die Entschlüsselung von Alices Datensatz.
Abbildung 7 zeigt die einzelnen Schritte. Nach dem vierten Schritt würde dann der Dienst in Anspruch genommen werden.

3.3 Lückenloser Schutz?

Im Internet werden immer wieder Versprechungen verbreitet, dass mit TC bald alles sicherer wird. Viren, Würmer und Trojaner könnten das System nicht mehr befallen und Spam würde auch endlich ein Ende nehmen. Hundertprozentige Sicherheit ist und bleibt eine Utopie. Das sind falsche Versprechungen und anhand eines kleinen Beispieles soll dieses verdeutlicht werden.

Lovesan-Wurm

Wir betrachten dabei die Vorgehensweise des Lovesan-Wurmes der im Jahre 2003 nachweislich 48.000 Computer befiel. Der Wurm baut zunächst eine Verbindung zu TCP-Port 135 des Opfer-Rechners auf. Hier lauscht der RPC-Dienst von Microsoft, welcher unter anderem Funktionen für das Actice Directory und für die Exchange-Server beinhaltet. Wurde die Verbindung aufgebaut wird ein Buffer-Overflow erzeugt und der so eingeschleuste und ausgeführte Code öffnet eine Remote-Shell auf Port 4444. Anschließend verbreitet sich der Wurm weiter. Der Wurm benötigt dazu lediglich die Kommandos tftp

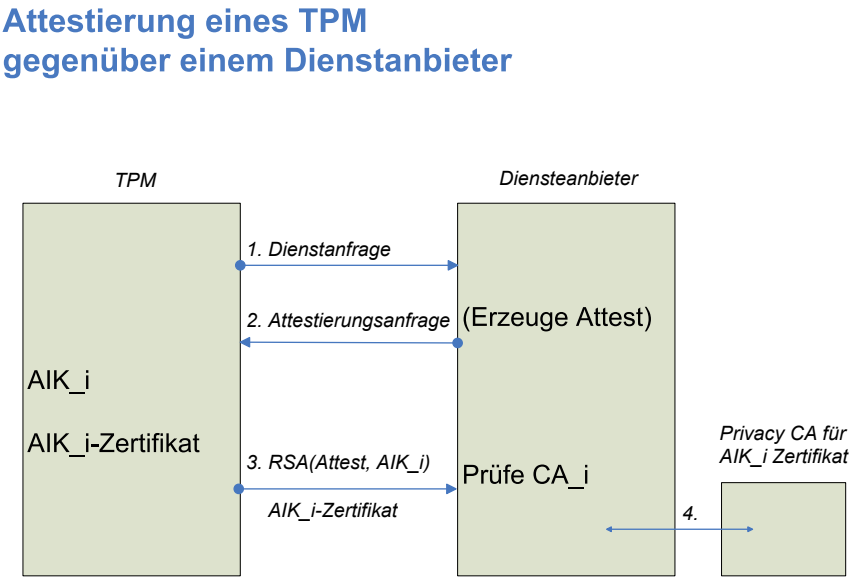

Abb. 7. Attestierung eines TPM gegenüber eines Diensteanbieters

und cmd. Diese beiden Programme sind beide vom Betriebssystem als zulässig deklariert und würden demnach auch auf einer TPM-Plattform ausgeführt. Eine Integritätsüberwachung des TPM schlägt also fehl. Nachdem der Wurm in das System eingedrungen ist versucht dieser, sich in die Windows-Registry einzutragen, um auch beim nächsten Systemstart wieder gestartet zu werden. Dieser Versuch gelingt auch zunächst, wird jedoch bei dem nächsten Starten bemerkt, da die Registry eine sicherheitskritische Komponete darstellt und beim Systemstart überwacht wird. Somit schlägt der Einnistversuch fehl, das Eindringen aber nicht. Ein Wurm, bzw. Virus, der über die Shell alle auffindbaren Dateien löscht könnte seine Schadroutine ohne Hindernisse verrichten.

3.4 Probleme und Gefahren von TC

Die TCG hat zum Ziel, das Arbeiten am Computer sicherer zu machen. Jedoch geht dieses oft nur auf Kosten der Freiheit. Angefangen bei dem Verlust der vollständigen Kontrolle über die Hardware. Viel schlimmer ist jedoch die Möglichkeit, von Dritten kontrolliert zu werden. So können zum einen bereits bei der Erstellung der AIKs Profile der Benutzer erstellt werden. Wenn die Zertifizierungsstellen mit den Diensteanbietern zusammenarbeiten, können sehr detaillierte Benutzerprofile erstellt werden. Neben dem Profiling ist es Dritten auch

Profiling

Privacy

möglich, zu entscheiden was gemacht werden darf und was nicht. So kann ein Content-Anbieter seine Datensätze an bestimmte Software und Hardware binden. Die so gekauften MP3-Dateien im Online-Store ließen sich dann z.B. nur noch mit dem Windows-Media Player abspielen und dieser würde wiederum nur mit zertifizierten Soundkarten kommunizieren, welche nur digitale und verschlüsselte Ausgänge bereitstellt. Ein digitales Kopieren dieser Datei wäre damit nur mit größtem Aufwand möglich und der MP3-Player im Autoradio würde seinen Dienst einstellen. Marktführende Unternehmen könnten Mitstreiter schnell aus dem Rennen werfen, indem sich ihre Dateien nur noch mit ihrer Software öffnen lassen (MS Word vs. OpenOffice.org). Content-Anbietern, wie der MPAA und der RIAA, eröffnen sich interessante neue Möglichkeiten. Jedoch können diese Möglichkeiten den Benutzer sehr stark einschränken.

Raubkopien würden mit sogenannten SRL-Servern (Serial Number Revocation List) unterbunden bzw. erheblich erschwert werden. Bei jedem Start des Programmes überprüft das Betriebssystem zunächst die Seriennummer an einem Server. Befindet sich diese auf einer Black-List, wird der Start verweigert. Gecrackte Programme können anhand von DCL-Servern (Document Revocation List) am Starten gehindert werden. Diese speichern Hash-Werte und können dann mit zu prüfenden Werten verglichen werden. Damit nur noch zertifizierte Hardware zum Einsatz kommt, können HCL-Server (Hardware Certification List) kontaktiert werden.

Diese Server ermöglichen neue Szenarien. Ein Unternehmensleiter könnte so eine ihm schädliche E-Mail von einem Arbeitnehmer im Firmennetzwerk unlesbar machen, indem er sie in die Black-List des DCL-Server einträgt. Kein Client in der Firma würde diese E-Mail noch anzeigen. Einen Schritt weitergedacht wäre globale Zensur möglich. Unbeliebte Dokumente könnten binnen kürzester Zeit weltweit verbannt werden.

Nur wenige Hersteller verbauen in ihrer Hardware TPM-Chips. Doch auch diese Anzahl nimmt stetig zu. Wenn die Module nicht mehr gesockelt verbaut werden, sondern etwa in die CPU oder die Southbridge integriert werden, wäre ein Zugriff so gut wie komplett unterbunden. Sollte die Funktion zum Abschalten aus dem TPM verschwinden, sind oben beschriebene Szenarien schnell realisierbar. Doch um dieses durchzusetzen muss zunächst eine kritische Masse von TPM-Plattformen vertrieben worden sein. Eine andere Möglichkeit TC durchzusetzen wäre es, wenn viel benutzte namhafte Software ein TPM verlangt; so z.B. Microsoft Windows. Dann mag das TPM weiterhin abschaltbar sein, doch wenn jegliche Windows-Versionen den Dienst verweigern, sehen sich Unternehmen vor einer schwierigen Entscheidung. Möglich wäre auch eine gesetzliche Verpflichtung. Debatten für Gesetzesvorschläge wurden in den USA bereits geführt. Sie scheiterten jedoch recht früh.

Probleme

Doch neben diesen düsteren Zukunftsvisionen gibt es auch andere Probleme. So sind alle im TPM abgelegten Daten verloren wenn die Hardware defekt ist. Ein EK-Austausch ist zwar vorgesehen, doch der Ablauf ist nicht spezifiziert. Der neue EK muss zertifiziert werden, und bisher bietet keine Zertifizierungsstelle einen solchen Dienst an. Zudem wird dieser Dienst wohl kaum kostenlos

in Anspruch genommen werden können. Ein weiteres Problem stellen die Integritätschecks des Systems dar. Die heutige Flut an Sicherheitsupdates und Patches wird kaum ein Ende nehmen, und jedes Update ändert den Hash-Wert der geänderten Komponente. Somit muss auch jedes System nach einem Update erst wieder als sicher deklariert werden. Wird der Benutzer zu oft mit diesen Problemen konfrontiert, so mag er auf Kosten der Sicherheit das TPM einfach deaktivieren, um wieder wie gewohnt arbeiten zu können.

3.5 Fazit

Das Ziel der TCG ist sicherlich nicht verkehrt, doch sind noch viele Probleme in Hinsicht auf Benutzbarkeit und Privacy zu lösen. Auch der Umstand dass die Gründer der TCG marktführende Unternehmen mit eigenen Zielen sind, sollte nicht vergessen werden. TPM-Plattformen bieten Firmen viele neue Möglichkeiten in Bezug auf Datenschutz und Zugriffskontrolle. Die Wünsche eines Privatanwenders sind jedoch andere. Ob die Benutzbarkeit eines TPMs diesen gerecht werden kann, muss sich zeigen. Dennoch ist TC ein Schritt hin zu sicheren Systemen und wir müssen zwischen Sicherheit und Kontrollmöglichkeiten abwägen.

Literatur

1. Eckert, C.
   IT-Sicherheit
   Oldenbourg, 3.Aufl, 2004
2. Dr. Siani Pearson u.A.
   trusted computing platforms
   Prentice Hall, 2003
3. Homepage der Trusted Computing Group
   https://www.trustedcomputinggroup.org
4. Bundesamt für Sicherheit in der Informationstechnik
   http://www.bsi.de/sichere_plattformen/index.htm
5. Heise.de
   http://www.heise.de/
6. FAQ zu Trusted Computing von Ross Anderson
   http://moon.hipjoint.de/tcpa-palladium-faq-de.html
7. Microsoft Secure Start
   http://www.microsoft.com/whdc/system/platform/pcdesign/secure-start_exec.mspx