Universität Hamburg
Fachbereich Informatik

Seminarbeit

Einführung in die TCPA Spezifikationen

Michel Messerschmidt

7. Februar 2003

1 Überblick

1.1 Was ist die TCPA ?

Die “Trusted Computer Platform Alliance” (TCPA) ist ein Zusammenschluß mehrerer Unternehmen der Hardware- und Software-Industrie. Seit ihrer Gründung durch die Unternehmen Compaq, HP, IBM, Intel und Microsoft im Jahr 1999 ist die Zahl der Mitglieder bis Anfang 2003 vermutlich auf ca. 200 Unternehmen gestiegen. Die Mitgliederliste sowie die genaue Zahl der beteiligten Unternehmen werden jedoch geheimgehalten.

Die TCPA versteht sich als eine Unternehmensallianz mit dem Ziel, das Vertrauen in Computersysteme zu erhöhen.

Dazu werden mehrere Spezifikationen erarbeitet, die dieses Ziel technisch definieren und Standards für die Einbindung geeigneter Komponenten in heutige Computersystem definieren. Weiterhin soll die Implementierung sicherer Systeme unterstützt sowie die Verbreitung und Verwendung der geschaffenen Standards gefördert werden.

Zur Zeit existieren folgende öffentlich einsehbare Spezifikationen:

- Main Specification, Version 1.1b
- TCPA PC Specific Implementation Specification, Version 1.00
- Trusted Platform Module - Protection Profile, Version 1.9.7

Diese werden im folgenden näher betrachtet.

1.2 Definition der “Trusted Platform”

Ein vertrauenswürdiges System (“Trusted Platform”) ist durch das Vorhandensein eines so genannten “Trusted Buildung Block” (TBB) gekennzeichnet. Dieser wiederum besteht aus einem zusätzlichen vertrauenswürdigen Teilsystem, dem “Trusted Platform Module” (TPM), einer vertrauenswürdigen Initialisierungsfunktion, dem “Core Root of Trust for Measurement” (CRTM) sowie der Verbindung dieser beiden Komponenten. Da der CRTM bei jedem Einschalten bzw. Reset die Kontrolle erhalten muss, um einen vertrauenswürdigen Bootvorgang zu gewährleisten, muss diese Komponente Teil des ursprünglichen Systems sein.

Zusätzlich werden noch so genannte “Trusted Platform Support Services” (TSS) definiert. Die Funktionalität der “Trusted Platform Support Services” kann zwar durchaus für einige Funktionen des TPM notwendig sein, die “Trusted Platform Support Services” selber müssen jedoch nicht zwangsläufig vertrauenswürdig sein, da Fehlfunktionen erkannt werden können. Die verfügbaren Spezifikationen enthalten nur wenig über die “Trusted Platform Support Services”. Es gibt zwar einen Verweis auf eine eigene Spezifikation dieser Komponente, dies ist jedoch (falls sie existiert) nicht öffentlich zugänglich.

Diese allgemeinen Definitionen lassen zunächst offen, auf welche Weise diese Komponenten realisiert werden sollen. Dies wird jedoch an anderen Stellen in den Spezifikationen implizit eingeschränkt (etwa durch die Forderung eines “physical presence” Zustands und der Unmöglichkeit bestimmte Funktionen per Software zu aktivieren).

1.3 Hardware-Integration

Die grundlegende, notwendige Änderung der Hardware-Architektur ist die Einbindung des TPM. Es wird eine eindeutige Zuordnung eines TPM zu einem System (also vermutlich Mainboard, CPU, BIOS-EEPROM, Mainboard-Controller) gefordert. Dies kann entweder durch physikalische Anbindung an das Mainboard oder durch logische Anbindung mittels einer üblichen Schnittstelle (z. B. USB) und kryptographische Absicherung (z. B. durch ein gemeinsames Geheimnis des TPM und dem Mainboard) realisiert werden.

Alle bisher verfügbaren “Trusted Platform” Module sind als separater, fest aufgelöteter Chip auf dem Mainboard realisiert, der mittels dem LPC-Bus (“Low Pin Count”-Bus) an das System angebunden wird.

Das TPM selber ist weniger ein Krypto-Koprozessor als vielmehr ein kleines, nahezu autonomes System mit eigenem Prozessor, RAM, EEPROM, ROM sowie natürlich den Funktionen eines Krypto-Koprozessors (Kryptographische Algorithmen, Zufallszahlengenerator und Timer). Außerdem kann optional ein physikalische Schutz des Moduls vorhanden sein (“Tamper detection”).

1.4 Software-Integration

Wie sich der Hardwarebeschreibung bereits entnehmen lässt, ist jedes TPM ein weitgehend autonomes System und enthält somit auch ein eigenes Betriebssystem (TPM OS), das als Firmware bzw. Software des TPM dessen Funktionen dem Gesamtsystem zur Verfügung stellt und gleichzeitig jeden Zugriff auf das TPM kontrolliert[1]. Somit ist das TPM OS eine der beiden Komponenten, deren korrekte Funktion für die Vertrauenswürdigkeit des Gesamtsystems ausschlaggebend ist.

[1] Teile des TPM OS können dabei auch als ROM realisiert sein

Die andere entscheidende Komponente ist das CRTM. Dieses ist (auf PC-Systemen mit i386-Architektur) zwangsläufig Teil des BIOS. Die PC-spezifische Spezifikation legt dazu zwei mögliche Realisierungen fest:

- Das BIOS ist (wie bisher üblich) eine Komponente. In diesem Fall wird das gesamte BIOS als CRTM betrachtet
- Das BIOS besteht aus zwei Teilen, dem Boot-BIOS und dem POST-BIOS. Hier ist nur das Boot-BIOS das CRTM (und muss entsprechend geschützt werden), während das POST-BIOS bereits die nächste Komponente im Bootvorgang darstellt.

Außerdem muss das das BIOS einen TPM-Treiber enthalten, der für die Kommunikation mit dem TPM verantwortlich ist.

Nach dem Bootvorgang werden die TPM Funktionen vermutlich über die “Trusted Platform Support Services” genutzt, deren unterste Schicht wiederum einen TPM-Treiber enthält. Weitere Informationen darüber sind wie bereits erwähnt noch nicht öffentlich verfügbar.

2 Funktionalität

Die TCPA Spezifikationen enthalten folgende Dienste, die dem vertrauenswürdigen System zur Verfügung gestellt werden:

- “Measurement” - Ermittelung und Schutz der System-Integrität
- “Trusted Storage” - Geschützter Speicher
- “Reporting” - Zustandsauskünfte über das vertrauenswürdige System. Diese Funktion wird hier nicht behandelt, da dies für diese Arbeit zu umfangreich wäre. Kurz zusammengefasst handelt es sich um die Möglichkeit, den Systemzustand von einem anderen System (z. B. über ein Netzwerk) abzufragen und daraus auf die Vertrauenswürdigkeit des abgefragten Systems zu schließen.

Um diese Dienste zur Verfügung zu stellen ist die Verwendung verschiedener kryptographischer Technologien erforderlich. Um ein Mindestmaß an Vertrauen in die Algorithmen sowie der Interoperabilität verschiedener Systeme zu gewährleisten werden die zu verwendenden Technologien in der “Main Specification” genau festgelegt. Folgende Funktionen müssen im TPM implementiert sein und dürfen nicht von anderer (nicht vertrauenswürdiger) Software abhängig sein:

- Zufallszahlengenerator
- Hashfunktionen: SHA-1, HMAC
- Asymmetrische Ver-/Entschlüsselung: RSA
- Asymmetrische Schlüsselgenerierung: RSA mit 512, 1024 und 2048 Bit

Zusätzlich sollen die “Trusted Platform Support Services” ein symmetrische Ver-/Entschlüsselung mittels 3DES bereitstellen.

Des weiteren muss das TPM folgende Funktionen enthalten:

- Schlüsselspeicherung
- Schlüsselverwaltung
- Selbsttest
- Identifikation und Authentifizierung (des Besitzers und der Nutzer)
- Zugriffskontrollen

2.1 Integrität

Das Vertrauen in das System kann nur gewährleistet sein, wenn die Initialisierung des Systems vertrauenswürdig ist. Dies ist die Aufgabe des CRTM, das somit immer (Einschalten, Reset) zuerst die Kontrolle über das System erhalten muss.

Der CRTM speichert dann sein Versionsnummer und ein Integritätswert für die nächste auszuführende Komponente im TPM, bevor es die Kontrolle an diese Komponente übergibt. Jede weitere Komponente speichert ebenfalls einen Integritätswert für die jeweils nachfolgende Komponente im TPM, bevor diese die Kontrolle über das System erhält. Auf diese Weise wird das initiale Vertrauen in den CRTM von einer Komponente zur nächsten weitergereicht (“Chain of trust”).

Integritätswerte sind in der Regel Hashwerte der jeweiligen Komponente, die mittels der vertrauenswürdigen Funktionen des TPM erzeugt werden. In der “TCPA PC Specific Implementation Specification” wird für die meisten am Bootvorgang beteiligten Komponenten detailliert festgelegt, welche Komponenten-Bestandteile in welchem Schritt gemessen werden müssen. Die letzte auf diese Art festgelegte Komponente ist der “Initial Program Loader”, also in der Regel der “Master Boot Record” einer Festplatte, Diskette oder CD.

Da das TPM nicht über unbegrenzten Speicher verfügt, werden die Integritätswerte nicht alle separat gespeichert, sondern in mehreren Registern (für die verschiedenen Stufen des Bootvorgangs). Müssen mehrere Integritätswerte im selben Register gespeichert werden, werden die alten Werte nicht überschrieben sondern mit den neuen Werte verkettet.

Auf diese Weise kann jeder neu ermittelte Systemzustand auf Übereinstimmung mit gespeicherten früheren Systemzuständen geprüft werden. Bei Nichtübereinstimmung können dann die entsprechenden TPM-Funktionen deaktiviert werden.

2.2 Geschützter Speicher

Das TPM muss die geschützte Speicherung sowohl von persistenten wie von nicht-persistenten Daten ermöglichen.

Der geschützte Speicher kann für kryptographische Schlüssel, Integritätsdaten, Benutzerdaten und Konfigurationsdaten genutzt werden.

Der Speicher muss sich innerhalb des TPM befinden und es darf nur von der TPM-Soft-/Firmware direkt darauf zugegriffen werden, um ein unbefugtes Auslesen zu verhindern. Ein Schutz vor physikalischem Zugriff ist jedoch nicht mandatorisch.

Je nach Art der Inhalte geben die entsprechenden TPM-Funktionen diese aber nur abgesichert (signiert, verschlüsselt) weiter. Einige Inhalte können nur über privilegierte Funktionen verwendet werden, die eine Authentifizierung (z. B. des TPM-Besitzers) erfordern. Außerdem existieren

Inhalte, die nur innerhalb des TPM verwendet werden dürfen und die deshalb von außerhalb des TPM nicht zugreifbar sind.

Jedes TPM muss unter anderem folgende persistente Daten enthalten:

- Endorsement Key
  - dient zur eindeutigen Identifizierung des TPM (und somit auch des gesamten Systems)
  - kann nur einmal erzeugt werden (in der Regel bei der Herstellung des TPM) und kann dann nicht mehr geändert oder gelöscht werden
- Storage Root Key
  - schützt alle anderen gespeicherten Schlüssel
  - wird im TPM generiert, darf nur intern verwendet werden und ist nicht exportierbar ("non-migratable")
  - wird genau dann erzeugt, wenn dem TPM ein Besitzer zugewiesen wird und ist implizit (durch die entsprechenden TPM-Funktionen) an diesen gebunden.
- Manufacturer's Public Key
  - öffentlicher Schlüssel des TPM-Herstellers
  - wird für die TPM Maintenance Funktionen benutzt (Übertragung der "non-migratable keys" auf ein anderes TPM)
- TPME Identity Key
  - Nutzen unbekannt, da es keine weitere Erwähnung gibt (vermutlich ein weiterer Hersteller-Schlüssel)
- Owner Authorization Data
  - Daten, um den TPM-Besitzer authentifizieren zu können

2.2.1 Schlüsselspeicher

Zur sicheren Speicherung kryptographischer Schlüssel wird eine Schlüsselhierachie aufgebaut, bei der die Sicherheit des obersten Schlüssels (dem "Storage Root Key") die Sicherheit aller anderen Schlüssel garantiert. Dazu wird jeder andere Schlüssel mit dem jeweils darüber liegenden Schlüssel verschlüsselt bevor er gespeichert wird (und entsprechend beim Auslesen wieder entschlüsselt bevor er verwendet wird).

Zusätzlich wird jedem Schlüssel ein Schlüsseltyp zugeordnet, der die mit diesem Schlüssel möglichen Operationen einschränkt. So gibt es z. B. Schlüssel, die nur zum Signieren verwendet werden dürfen, während andere nur zum Verschlüsseln anderer Schlüssel dienen.

Alle Schlüssel werden außerdem entsprechend ihrer Aufgabe in exportierbar (“migratable”) und nicht exportierbar (“non-migratable”) unterteilt [1].

[1] “Exportierbar” bezieht sich dabei auf einen Export aus dem TPM

3 Probleme

3.1 Integrität

Es gibt keine Möglichkeit festzustellen, ob eine Systemänderung gewollt oder ungewollt ist. Somit bleibt die Frage des Vertrauens in die Systemintegrität nach einer Änderung ungelöst oder wird eventuell sogar immer negativ entschieden, was mit einer heutzutage üblichen Nutzung nicht vereinbar ist.

Das Vertrauen in den CRTM ist entscheidend für das Vertrauen in das Gesamtsystem. Deshalb ist eine Änderung (bzw. Update) dieser Komponente kritisch für die Vertrauenswürdigkeit des gesamten Systems. Leider sind Updates des CRTM zwar vorgesehen aber nicht näher spezifiziert (auch nicht in der “TCPA PC Specific Implementation Specification”), so das hier bereits eine potentielle Schwäche des Systems vorhanden ist, deren Ausnutzung durch die vorliegenden Spezifikationen nicht verhindert werden kann.

3.2 Geschützter Speicher

Die datenschutzrechtliche Frage, ob der TPM-Besitzer (und somit auch der “Storage Root Key”) gelöscht bzw. ein neuer Besitzer zugewiesen werden kann, lässt sich leider nicht eindeutig beantworten. Zwar existieren Funktionen zum Löschen des Besitzers und zum neuen “Installieren” eines Besitzers, diese sind jedoch deaktivierbar. Zwar lässt sich diese Deaktivierung wieder aufheben, allerdings kann dies durch ein entsprechend entworfenes BIOS bzw. CRTM durchaus verhindert werden.

Gerade bei sicherheitskritischen Daten ist die Frage der Datensicherung und gegebenenfalls -wiederherstellung (Backup, Recovery) nicht vernachlässigbar. Dies wird in den vorliegenden Spezifikationen kaum berücksichtigt.

Laut “Trusted Platform Module - Protection Profile” kann auf gespeicherte Inhalte nur dann wieder zugegriffen werden, wenn dasselbe TPM, derselbe Schlüssel und derselbe Systemzustand vorhanden sind.

Nicht exportierbare Schlüssel (“non-migratable keys”) können (z. B. bei einem Hardware-Upgrade) nur durch Kooperation mit dem TPM-Hersteller in ein anderes baugleiches TPM übertragen werden, wenn der TPM-Hersteller diese optionale Funktionalität überhaupt unterstützt.

3.3 Allgemeine Probleme

Das TPM kann nicht komplett deaktiviert werden. Folgende Funktionen lassen sich nicht deaktivieren:

- Das Ermitteln und Speichern der Integritätsdaten
- Statusabfrage des TPM
- Selbsttest

Dies eröffnet unter anderem die Möglichkeit, das beliebige Software die Existenz eines TPM auf jedem System eindeutig feststellen kann.

Es existiert eine nicht näher spezifizierte Upgrade-Funktion für das TPM, der somit ähnliche potentielle Schwächen wie für den CRTM eröffnet.

3.4 Fazit

Vertraulichkeit und Integrität von Daten sowie die Integrität des Computersystems werden durch kryptographische Verfahren gestärkt. Die Spezifikationen haben aber Schwächen bzw. Freiheiten, die Angriffsmöglichkeiten in den Implementationen erlauben.

Es werden PKI-ähnliche Strukturen genutzt, ohne alle Konsequenzen zu berücksichtigen und die dafür notwendigen Funktionen (backup, key revocation, key recovery) vorzusehen.

Die “kryptographische Aufrüstung” des Computersystems lässt sich auch mit Smartcards verwirklichen. Die Notwendigkeit einer eineindeutigen Abbildung des TPM (und des “Endorsement key”) auf das Gesamtsystem ist, gerade unter Datenschutz-Aspekten, nicht nachvollziehbar.

Sicherheitskonzepte und -begriffe werden teilweise eher schlagwortartig verwendet statt vollständig und nachvollziehbar umgesetzt zu werden. Zum Teil werden Begriffe dem allgemeinen Verständnis widersprechend definiert, wodurch leicht ein falsches Verständnis der Spezifikationen resultierten kann (Beispiel: der Begriff “immutable” in [PCSpec, S. 12]).

Insgesamt wird die Abhängigkeit vom TPM-Hersteller verstärkt, ohne dass dadurch ein klar erkennbarer Vorteil für den Besitzer oder Nutzer des Systems erkennbar wäre.

Literaturverzeichnis

[TCPASpec] Trusted Computing Platform Alliance: ”Main Specification Version 1.1b”, 2002-02-22, http://www.trustedcomputing.org/docs/mainv1_1b.pdf

[PCSpec] Trusted Computing Platform Alliance: ”TCPA PC Specific Implementation Specification Version 1.00”, 2001-09-09, http://www.trustedcomputing.org/docs/TCPA_PCSpecificSpecification_v100.pdf

[TPM-PP] Trusted Computing Platform Alliance: ”Trusted Platform Module - Protection Profile Version 1.9.7”, 2002-07-01, http://www.trustedcomputing.org/docs/TCPA_TPM_PP_1_9_7.pdf

[TCPA-WP] Trusted Computing Platform Alliance: ”TCPA Security and Internet Business: Vital Issues for IT”, August 2000, http://www.trustedcomputing.org/docs/TCPA_IT_WP.pdf