Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1040 Wien, Weyringergasse 35
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

TRUSTED COMPUTING
TECHNOLOGIEBEOBACHTUNG
VERSION 1.0, 16. FEBRUAR 2009

DI Thomas Zefferer – thomas.zefferer@iaik.tugraz.at

Zusammenfassung: Die Technologie „Trusted Computing“ bietet im Bereich der IT Sicherheit interessante neue Konzepte und Methoden an, um vernetzte Systeme für jeden einzelnen Teilnehmer insgesamt vertrauenswürdiger zu machen. Durch die Einführung neuer Komponenten in derzeit übliche Computerplattformen können diese ständig überwacht und vor unerwünschtem Verhalten, wie es beispielsweise durch Schadsoftware verursacht werden könnte, geschützt werden. Neben dem Schutz des eigenen Systems unterstützt Trusted Computing auf diese Weise auch die Möglichkeit, Informationen über den aktuellen Sicherheitszustand entfernter Systeme zu beziehen.
A-SIT beschäftigt sich im Rahmen der Technologiebeobachtung intensiv mit dieser Technologie und versucht, aktuelle Entwicklungen in diesem Bereich früh zu erkennen. Dieses Dokument gibt einen Überblick über den aktuellen Stand der Trusted Computing Technologie. Dies wird ergänzt mit der Beschreibung einiger Forschungsprojekte des A-SIT Mitglieds TU Graz, um einen Blick auf einige wissenschaftliche Herausforderungen in diesem Forschungsgebiet zu geben.

© A-SIT, Partner für Sicherheitsfragen

Inhaltsverzeichnis

Abkürzungsverzeichnis

A-SIT	Zentrum für sichere Informationstechnologie - Austria
API	Application Programming Interface
AIK	Attestation Identity Key
BIOS	Basic Input Output System
DAA	Direct Anonymous Attestation
EFF	Electronic Frontier Foundation
ELAK	Elektronischer Akt
EK	Endorsement Key
FH	Fachhochschule
IAIK	Institut für Angewandte Informationsverarbeitung und Kommunikations-technologie (der TU Graz)
IMEI	International Mobile Equipment Identity
IT	Informationstechnologie
I/O	Input/Output
ISP	Integrity Service Provider
JAR	Java Archive
JCP	Java Community Process
JDK	Java Development Kit
JSR	Java Specification Request
MLTM	Mobile Local-Owner Trusted Module
MRTM	Mobile Remote-Owner Trusted Module
MTM	Mobile Trusted Module
NGSCB	Next-Generation Secure Computing Base
PC	Personal Computer
PCR	Platform Configuration Registers
P-CA	Privacy-Certification Authority
PKI	Public Key Infrastructure
RTM	Root of Trust for Measurement
SRK	Storage Root Key
SWOT	Strengths-Weaknesses-Opportunities-Threats
TSS	TCG Software Stack
TC	Trusted Computing
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Allicance
TPM	Trusted Platform Module
TU Graz	Technische Universität Graz
VM	Virtual Machine
XKMS	XML Key Management Specification Protocol
XML	Extensible Markup Language

1 Einleitung

IT-Systeme kommen heutzutage in unzähligen Bereichen des täglichen Lebens zur Anwendung und werden dabei durchaus auch für sicherheitskritische Aufgabengebiete wie E-Banking oder Anlagensteuerungen verstärkt eingesetzt. Mit der steigenden Mächtigkeit dieser Systeme und deren zunehmender Vernetzung hat jedoch in den letzten Jahren auch die Zahl der Angriffe auf diese Systeme ständig zugenommen. IT-Sicherheit spielt daher ebenfalls in vielen Bereichen eine zunehmend wichtige Rolle, da nur ein ausreichender Schutz dieser Systeme einen sicheren und reibungslosen Betrieb der selbigen gewährleisten kann.

Vor allem in komplexeren vernetzten Systemen wie dem Internet spielt die Sicherheit einzelner Systeme im zunehmenden Maße auch eine wichtige Rolle für andere Teilnehmer desselben Netzwerks. So kann es in bestimmten Anwendungen relevant sein, ob sich ein entferntes System, mit dem eine Verbindung hergestellt und diverse Daten ausgetauscht werden sollen, in einem sicheren bzw. nicht kompromittierten Zustand befindet. Davon kann es beispielsweise abhängen, ob sensible Daten an dieses System übermittelt werden sollen oder nicht.

Bisher gängige Ansätze, die die Sicherheit in computerbasierten Systemen erhöhen sollten, können zwar im begrenzten Maße die Sicherheit einzelner Systeme verbessern, bieten allerdings keinerlei Möglichkeit den aktuellen Grad an Sicherheit anderer entfernter Systeme zu bestimmen. Trusted Computing setzt an diesem Punkt an und stellt Möglichkeiten zur Verfügung, Systeme verlässlich in einem sicheren Zustand zu halten, und diesen auf Anfrage hin auch anderen entfernten Plattformen zu kommunizieren. Damit bietet diese Technologie die Möglichkeit, sichere Computersysteme aufzubauen, in denen sich die einzelnen Teilnehmer gegenseitig vertrauen können. Dieses Konzept bietet eine Vielzahl von Anwendungsmöglichkeiten und stellt einen interessanten Ansatz dar, die generelle Sicherheit von Computernetzen nachhaltig zu erhöhen. A-SIT engagiert sich daher im Rahmen der Technologiebeobachtung intensiv mit dieser Technologie und versucht künftige Entwicklungen auf diesem Sektor nicht nur frühzeitig zu erkennen, sondern auch den eigenen Ansprüchen entsprechend zu gestalten.

Dieses Dokument gibt eine Einführung in die Trusted Computing Technologie. Dazu wird in Abschnitt 2 auf die prinzipiellen Konzepte und Methoden der TC Technologie näher eingegangen und die wichtigsten Komponenten TC basierter Systeme beschrieben. Aus den von Trusted Computing fähigen Systemen zur Verfügung gestellten Funktionalitäten werden daraufhin mögliche Anwendungsgebiete abgeleitet, sowie bereits vorhandene Umsetzungen dieser Technologie beschrieben. Da es sich bei Trusted Computing um eine relativ kontrovers diskutierte Technologie handelt, wird in Abschnitt 2 auch auf diverse Kritikpunkte an dieser Technologie eingegangen.

Abschnitt 3 widmet sich im Anschluss einer Beschreibung der Projekte, über die sich das A-SIT Mitglied Technische Universität Graz im Bereich Trusted Computing engagiert. Der Überblick über diese Forschungsprojekte soll den Stand der Technik über einen Einblick in aktuelle wissenschaftliche Herausforderungen zu Trusted Computing ergänzen. Dazu werden die Projekte „Open TC“, „TOPAS“ und „Secricom“, sowie der Java Specification Request „JSR 321“ und eine Studie, die sich mit einer möglichen Integration der Trusted Computing Technologie in Vorgänge der öffentlichen Verwaltung beschäftigt, vorgestellt.

In Abschnitt 4 werden schließlich die wichtigsten in diesem Dokument erhaltenen Erkenntnisse zusammengefasst.

2 Trusted Computing - Grundlagen

2.1 Motivation

Durch die zunehmende Verbreitung von computer- und netzwerkbasierten Anwendungen in unterschiedlichsten Bereichen des täglichen Lebens steigen auch die Anforderungen an die Sicherheit dieser Systeme. Da bisher keine geeigneten Strategien gefunden werden konnten, um Angriffe auf IT-Systeme zu unterbinden, verursacht der Mangel an verfügbarer Sicherheit jährlich auch große finanzielle oder auch immaterielle Schäden. Da IT-Systeme im zunehmenden Maße auch in sicherheitskritischen Bereichen Anwendung finden, ist eine Gewährleistung der Zuverlässigkeit dieser Systeme und all ihrer Komponenten unumgänglich.

Der übliche Ansatz die Sicherheit eines computerbasierten Systems zu erhöhen besteht in der Regel darin, das unsichere System durch diverse Sicherheitsmaßnahmen von einem potentiellen Angreifer abzuschirmen. Zu diesen Maßnahmen können beispielsweise der Einsatz von Firewalls oder Anti-Viren Software gehören, die es Angreifern erschweren sollen, Zugang zu sicherheitskritischen Systemen zu erlangen und diese für ihre Zwecke zu missbrauchen. Dieser Ansatz bringt jedoch mit sich, dass sich Entwickler solcher Schutzmechanismen in einem ständigen Wettlauf mit den Angreifern befinden, welche ihrerseits laufend neue Methoden entwickeln, um bereits bestehende Schutzmaßnahmen zu umgehen. Dieser Wettlauf ist für jene, die versuchen, bestehende System zu schützen, freilich nicht zu gewinnen, da sämtliche zusätzliche Schutzfunktionen an der Wurzel des Problems – dem unsicheren System an sich – nichts zu ändern vermögen.

Mit dem Ziel diesen Umstand zu ändern, wurde 1999 die Trusted Computing Platform Alliance (TCPA) von den Unternehmen Microsoft[1], IBM[2], Hewlett-Packard[3] und Compaq[4] gegründet. Mittlerweile wurde dieses Konsortium in Trusted Computing Group (TCG) unbenannt und umfasst derzeit etwa 120 Mitglieder. Die TCG [TCG] hat es sich zum Ziel gesetzt, eine Spezifikation zu entwickeln, die den Entwurf, die Implementierung und den Betrieb von Trusted Computing basierten Systemen definiert [TCG-SPECS].

Dieser neue Ansatz soll das Problem unsicherer Systeme an der Wurzel lösen, indem diese ständig in einem wohldefinierten und damit sicheren Zustand gehalten werden. Der Begriff „Trusted“ bedeutet in diesem Zusammenhang, dass sich das System gemäß einer von Herstellerseite vordefinierter Art und Weise verhält und nicht etwa durch Viren oder andere negative Faktoren in seinem Verhalten in irgendeiner Weise beeinflusst wird. Dieser Ansatz gewährleistet unter anderem, dass sich Dritte vergewissern können, dass sich ein entferntes System, mit welchem sie kommunizieren möchten, in einem wohldefinierten und damit sicheren Zustand befindet.

2.2 Grundkonzept

Die prinzipielle Idee hinter Trusted Computing ist es, Systeme ständig in einem bestimmten sicheren Zustand zu halten. Dies umfasst die verwendete Hardware genauso wie installierte Softwarekomponenten, deren Integrität mit Hilfe bekannter kryptographischer Algorithmen ständig überwacht wird. Ziel ist es, etwaige durch diverse Schadsoftware vorgenommene Änderungen an bestimmten Komponenten des Systems sofort zu identifizieren um entsprechend reagieren zu können.

Die dafür benötigte Funktionalität wird hauptsächlich von einer zusätzlichen Hardwarekomponente, dem so genannten Trusted Platform Module (TPM) zu Verfügung gestellt. Dabei handelt sich im Prinzip um einen Chip, der fix mit der Hardware des zu schützenden Systems verbunden ist und

[1] Microsoft: http://www.microsoft.com
[2] IBM: http://www.ibm.com
[3] Hewlett-Packard: http://www.hp.com
[4] Compaq: http://www.compaq.com

sowohl kryptographische Funktionen als auch Speicher zur Hinterlegung sensibler Daten zur Verfügung stellt. Neben dem TPM verfügen so genannte Trusted Platform Subsysteme üblicherweise noch über eine Root of Trust for Measurement (RTM), sowie über einen TCG Software Stack (TSS). Während die RTM Komponente im Prinzip für die Messung der Integrität des Systems verantwortlich und in PC Systemen meist in Form einer durch elektronische Signaturen geschützten BIOS Erweiterung umgesetzt ist, stellt der TSS die auf der Plattform befindliche Software dar, welche das TPM unterstützt und über die Applikationen die Funktionalität des TPM nutzen können. Durch die Ergänzung üblicher Rechnersysteme durch das eben beschriebene Trusted Platform Subsystem werden diese zu Trusted Computing fähigen Plattformen.

Mit Hilfe dieser Kernelemente eines Trusted Computing fähigen Systems ist es möglich, dieses bereits vom Zeitpunkt des Bootens an in einem wohldefinierten Zustand zu halten. Dazu überprüft das TPM bereits zu Beginn des Bootvorgangs die Integrität der installierten Hardwarekomponenten. Nur wenn diese Überprüfung positiv abgeschlossen werden kann, wird der nächste Schritt im Bootprozess initialisiert. Vor einem Zugriff auf das BIOS des Systems wird dieses ebenfalls vom TPM überprüft. Äquivalent dazu werden auch der Bootvorgang selbst, sowie die geladenen Komponenten des Betriebssystems ständig überwacht. Auf diese Weise kann jede Abstraktionsebene auf einen gesicherten Zustand des Systems aufbauen, wodurch eine durchgehende Vertrauenskette (Chain of Trust) und damit ein gesicherter Zustand des laufenden Systems gewährleistet bleibt.

Die Basis dieser Vertrauenskette bildet das TPM, welches entsprechend zertifiziert ist, und welchem im gesamten Konzept von Trusted Computing eine relevante Rolle zuteil wird. Dieses Hardwaremodul soll daher im folgenden Abschnitt genauer betrachtet werden.

2.3 Trusted Platform Module (TPM)

Dem Trusted Platform Module (TPM) wird in der gesamten Architektur von Trusted Computing fähigen Systemen eine besondere Rolle zugewiesen. Das TPM ist ein Kernelement des Trusted Computing, weshalb in diesem Abschnitt die wesentlichsten Begriffe und Funktionen des TPM kurz erklärt werden. Dabei wird von wenigen Grundkenntnissen der Kryptographie, vor allen von Begriffen zur asymmetrischen Verschlüsselung und Signatur ausgegangen.

Im Prinzip handelt es sich beim TPM um eine fix mit der Hauptplatine des Computers verdrahtete Smart-Card, die aber anderes als gewöhnliche Smart-Cards nicht an einen bestimmten Benutzer, sondern an einen gewissen Rechner gebunden ist. Das TPM ist ein passives Modul, woraus folgt, dass sämtliche unterstütze Funktionalität von einer externen Komponente wie zum Beispiel dem Betriebssystem angestoßen werden muss. Das TPM führt von sich aus keine Aktionen durch. Durch die Auslagerung der Funktionalität des TPM auf eine externe Hardwarekomponente ist es besser gegen softwarebasierte Angriffe geschützt als eine alternative reine Softwareimplementierung.

Da das TPM die Wurzel des Vertrauens der gesamten Vertrauenskette darstellt, muss dieses besonders zertifiziert sein, um dessen Integrität und Authentizität gegenüber Dritten nachweisbar zu gestalten. Zu diesem Zweck wird für jedes TPM ein sogenanntes Endorsement Zertifikat ausgestellt, das belegt, dass das TPM von einem autorisierten Hersteller zur Verfügung gestellt wurde. Untrennbar mit dem Endorsement Zertifikat verbunden ist der Endorsement Key, ein 2048 Bit RSA Schlüsselpaar, das meist direkt bei der Herstellung des TPM erstellt und mit diesem verknüpft wird. Der private Teil dieses Schlüssels darf das TPM niemals verlassen. Ergänzend zum Endorsement Zertifikat bescheinigt das Conformance Zertifikat, dass das verwendete TPM den Spezifikationen der TCG entspricht. Weitere Zertifikate, die für den Betrieb einer Trusted Computing fähigen Plattform benötigt werden, sind das sogenannte Plattform Zertifikat, das vom Hersteller der Plattform – z.B. des PCs – ausgestellt wird und bescheinigt, dass alle vorhandenen Komponenten den Spezifikationen der TCG entsprechen und die Plattform über ein entsprechendes TPM verfügt. Weiters gibt es das Validation Zertifikat, das für entsprechende Ein- und Ausgabegeräte deren Konformität zur TCG Spezifikation bescheinigt.

Alle entsprechenden Schlüssel sind im TPM an spezifizierten Stellen hinterlegt. Zusätzlich beinhaltet das TPM einen Storage Root Key (SRK), welcher erstellt wird, sobald das TPM von einem neuen Besitzer übernommen wird. Generell kann jedem TPM immer nur einen Besitzer zugewiesen sein, auch wenn das System, das durch das TPM geschützt ist, potentiell mehrere Benutzer haben kann. Wie auch der Endorsement Key, ist der SRK ein 2048 Bit RSA Schlüsselpaar. Er wird hauptsächlich dazu verwendet, um von ihm weitere benutzte Schlüssel abzuleiten und stellt somit die Wurzel eines Schlüsselbaums dar.

Neben der sicheren Aufbewahrung bzw. Erstellung von kryptographischen Schlüsseln, stellt das TPM folgende Technologien zur Verfügung, die als Schlüsselfunktionen für weitere Anwendungen im Rahmen von Trusted Computing dienen und diverse Anwendungsgebiete eröffnen.

2.3.1 Endorsement Key

Der Endorsement Key wird meist bereits bei der Produktion des TPM festgelegt und kann nachträglich nicht mehr geändert werden. Er kann daher herangezogen werden, um das jeweilige TPM eindeutig zu identifizieren. Zusammen mit dem ebenfalls auf der Plattform vorhandenen Endorsement Zertifikat gewährleistet der Endorsement Key, dass das verwendete TPM nicht emuliert und dadurch umgangen werden kann.

Da es sich beim Endorsement Key um ein 2048 Bit RSA Schlüsselpaar und somit um einen starken kryptographischen Schlüssel handelt, kann dieser auch verwendet werden, um sichere Transaktionen mit dem TPM durchzuführen. So können Daten, die dem Hardwaremodul gesichert übertragen werden sollen, mit dem öffentlichen Teil des Endorsement Keys verschlüsselt werden um so zu gewährleisten, dass diese nur vom TPM, welches über den entsprechenden privaten Schlüssel verfügt, auch wieder entschlüsselt und gelesen werden können.

2.3.2 Sealing

Unter dem Begriff „Sealing“ versteht man eine Bindung von Daten an ein bestimmtes System. Dazu wird ein Hash-Wert der aktuellen Systemkonfiguration gebildet und dieser als Schlüssel zur Verschlüsselung der entsprechenden Daten verwendet. Die auf diese Weise chiffrierten Daten können nur dann wieder entschlüsselt werden, wenn der Hash-Wert korrekt rekonstruiert werden kann. Dies ist nur dem TPM auf dem entsprechenden System, das auch zur Verschlüsselung verwendet wurde, möglich.

2.3.3 Auslagerung (Binding/Wrapping)

Da das TPM als Hardwaremodul ausgeführt ist, unterliegt es gewissen Beschränkungen was sich vor allem in einer limitierten Speicherkapazität niederschlägt. Um dieses Problem zu umgehen, ist es dem TPM möglich, bestimmte Daten wie z.B. zusätzliche Schlüssel an externen Speicherorten wie der Festplatte zu hinterlegen. Diese extern gespeicherten Schlüssel sind ebenfalls in einem Schlüsselbaum organisiert, wobei dessen Wurzel mit einem Schlüssel im TPM verschlüsselt wird.

2.3.4 Bescheinigung (Remote Attestation)

Eine der wichtigsten Funktionen des TPM im Rahmen von Trusted Computing Systemen ist die „Remote Attestation“ was mit „Bescheinigung“ übersetzt werden kann. Sie dient dazu, einem entfernten System auf Anfrage eine zuverlässige Aussage über den aktuellen Zustand und die Fähigkeiten des lokalen Systems zu übermitteln. Basierend auf dieser Aussage kann das entfernte System dann entscheiden, ob es mit dem überprüften System kommunizieren möchte oder nicht.

Zur Bereitstellung dieser Funktionalität dienen unter anderem die Platform Configuration Registers (PCR), über die jedes TPM verfügt. In diesen werden Hash-Werte der aktuellen Hard- und Softwarekonfiguration gespeichert. Jedes TPM muss dabei zumindest 16 dieser Register bereitstellen. Aus Speicherplatzgründen wird in jedem Register eine Sequenz von Hash-Werten über Messergebnisse der aktuellen Konfiguration hinterlegt. Dazu geht in jeden neu gespeicherten Wert auch das bisher aktuelle Ergebnis mit ein. Es entsteht eine Kette von Messwerten des

Systemzustandes, die im TPM sicher hinterlegt sind. Entspricht ein aktuell gemessener Zustand nicht dem erwarteten, so kann die Änderung – etwa durch eine Schadsoftware – erkannt werden.

Anhand der in den PCR hinterlegten Werte, kann eine entfernte Partei Informationen über den aktuellen Zustand des Systems abfragen. Dazu wird der entsprechende Wert vom lokalen TPM signiert und an das entfernte System übermittelt. Da der in dem TPM gespeicherte Endorsement Key dem System eindeutig zugeordnet werden könnte, werden für die Signaturerstellung eigene sogenannte Attestation Identity Keys (AIK) abgeleitet. Hierbei handelt es sich ebenfalls um 2048 Bit lange RSA Schlüsselpaare, die vom TPM selbst in beliebiger Anzahl erstellt werden können.

Das Bescheinigungsverfahren selbst kann über zwei mögliche Ansätze implementiert werden. In der ursprünglich vorgeschlagenen Lösung signiert eine vertrauenswürdige dritte Partei, die sogenannte Privacy-Certification Authority (P-CA), den vom lokalen TPM erstellten AIK und zertifiziert diesen, sofern die entsprechende Plattform alle vorgeschriebenen Richtlinien erfüllt. Dazu sendet das TPM den neu erstellten AIK, sowie diverse Informationen über die Identität des Systems verschlüsselt an eine beliebige P-CA. Diese entschlüsselt die einzelnen Elemente und überprüft die zur Verfügung gestellten Nachweise. Nach erfolgreicher Verifikation stellt die P-CA schließlich ein Platform Identity Certificate aus, das schließlich einem entfernten System auf Anfrage vorgezeigt werden kann um auf diese Weise bestimmte Eigenschaften des lokalen Systems zu bescheinigen.

Das Hauptproblem dieses Ansatzes liegt in der notwendigen Hochverfügbarkeit der P-CA, sowie in dem zentralen Angriffspunkt, den diese Instanz bietet, da sie über die nötigen Informationen verfügt um die zertifizierten AIK den jeweiligen Identitäten zuzuordnen. Aus diesem Grund wurde ein zweites Beglaubigungsverfahren namens Direct Anonymous Attestation (DAA) entwickelt, das auf dem Prinzip der Zero-Knowledge Protokolle beruht und es so ermöglicht, die vertrauenswürdige dritte Partei einzusparen. Mit diesem Verfahren ist möglich, einem entfernten System die Gültigkeit eines erstellten AIK zu zeigen, ohne Details über den entsprechenden Endorsement Key preisgeben zu müssen.

2.3.5 Sicherer Zufallsgenerator

Das TPM implementiert in der Regel auch die Funktionalität eines Zufallsgenerators. Die Erstellung von Zufallszahlen ist für die Sicherheit diverser kryptographischer Verfahren von großer Relevanz und in Software oft nur schwer umzusetzen. Durch die Auslagerung dieser Funktionalität in Hardware wird diesem Problem auf effiziente Weise begegnet.

2.3.6 Sicherer Input/Output

Übliche Computersysteme sind mit dem Problem konfrontiert, dass die Interaktion mit dem Benutzer prinzipiell über ungesicherte Kanäle stattfindet. Auch wenn unter Umständen gewährleistet werden kann, dass sich die verwendete Software selbst vertrauenswürdig verhält, so ist dennoch nicht auszuschließen, dass Benutzereingaben beispielsweise über sogenannte Keyboard Logger aufgezeichnet, bzw. Bildschirmausgaben über Screen Scrapers mitgeschnitten werden.

Trusted Computing fähige Systeme bieten hier Abhilfe, indem sie über die bereits erwähnten Überprüfungen der Integrität feststellen können, ob sich zusätzliche Software im I/O Pfad zum Benutzer befindet, oder ob vorhandene Treiber nachträglich modifiziert wurden. Durch die Anwendung dieser Maßnahmen wird die ursprünglich unsichere Schnittstelle zum Benutzer zu einem sogenannten Trusted Path.

2.3.7 Sichere Ausführung (Memory Curtaining)

Unter dem Begriff „Memory Curtaining“ versteht man die Fähigkeit von Trusted Computing Systemen, bestimmte Speicherbereiche speziell zu schützen. Diese Maßnahmen gehen so weit, dass nicht einmal das Betriebssystem selbst Zugriff auf diese Bereiche hat. Dadurch kann verhindert werden, dass ein böswilliger Angreifer, der die Kontrolle über das Betriebssystem erlangt hat, auf die geschützten Speicherbereiche zugreifen kann. Die auf diese Weise gesicherten

Bereiche können verwendet werden um dort besonders sensible Daten wie zum Beispiel bestimmte Schlüssel abzulegen.

2.4 Mögliche Anwendungsgebiete

Durch die in Abschnitt 2.3 beschriebene Funktionalität von Trusted Computing fähigen Plattformen ergeben sich eine Fülle möglicher Anwendungsgebiete. Im Folgenden sollen einige mögliche Anwendungen exemplarisch skizziert werden.

2.4.1 Digitale Rechteverwaltung

Da die Funktionalität, welche von Trusted Computing zur Verfügung gestellt wird, es entfernten Parteien erlaubt, authentische Informationen über die Systeme von Endbenutzern zu erhalten, eröffnet diese Technologie im Bereich der digitalen Rechteverwaltung neue Möglichkeiten. Es erlaubt Anbietern von Diensten, die Verwendung der zur Verfügung gestellten Produkte besser zu kontrollieren.

Beispielsweise könnte ein Anbieter von Musikdownloads das Konzept der Bescheinigung verwenden, um zu gewährleisten, dass der zur Verfügung gestellte Musiktitel nur in einer vom Anbieter bestimmten Wiedergabesoftware abgespielt werden kann. Durch Sealing könnte verhindert werden, dass der Benutzer die erhaltene Datei auf einem anderen System öffnet und verwendet. Durch das Konzept der Sicheren Ausführung würde verhindert, dass der Benutzer eine uneingeschränkte Kopie der entsprechenden Datei anfertigt. Um weitere Möglichkeiten den Musiktitel zu kopieren auszuschließen, könnte schließlich noch das Konzept des sicheren Input/Outputs zur Anwendung kommen.

Durch Kombination der in Abschnitt 2.3 beschrieben Methoden wäre es dem Anbieter also möglich, nahezu völlige Kontrolle über den zur Verfügung gestellten Musikdownload zu behalten, obwohl sich dieser bereits auf einem anderen System befindet. Neben der Wahrung der Rechte, würde die Anwendung von Trusted Computing für Anbieter auch neue Geschäftsfelder eröffnen, indem beispielsweise bestimmte Rechte an den zur Verfügung gestellten Produkten nur gegen zusätzliche Gebühren vergeben werden könnten.

2.4.2 Schutz vor Identitätsdiebstahl

Trusted Computing könnte in Bereichen, in denen die Identität des Benutzers zweifelsfrei festgestellt werden muss, einen erhöhten Grad an Sicherheit garantieren. Beispielsweise könnten in E-Banking Systemen die entsprechenden Server über das Konzept der Bescheinigung überprüft und eine Verbindung nur bei Vorlage aller gültigen Zertifikate hergestellt werden.

2.4.3 Schutz vor Schadsoftware

Durch die Anwendung von signierter Software könnte verhindert werden, dass Software, die von Dritten verändert und beispielsweise um Spyware-Komponenten erweitert wurde, auf dem gesicherten System zur Anwendung kommt. Des Weiteren wären Anti-Virus Programme denkbar, die durch Angriffe von Viren nicht verändert werden können. Dies wäre jedoch nur zusammen mit einem speziell auf Trusted Computing zugeschnittenen Betriebssystem möglich.

2.4.4 Schutz biometrischer Daten

Ein weiteres interessantes Anwendungsgebiet ergibt sich im Zusammenhang mit biometrischen Daten. Diese Daten sind noch mehr als andere geheime Daten wie Passwörter oder PINs besonders schützenswert, da sie untrennbar mit der entsprechenden Person verknüpft sind. Trusted Computing bietet mit den Konzepten des sicheren Input/Outputs und der sicheren Ausführung entsprechende Methoden, um diese Daten vor Diebstahl und Kompromittierung zu schützen.

2.4.5 Verifikation von Berechnungen in Grid-Systemen

Eine gängige Methode um komplexe Berechnungen wie zum Beispiel jene einer Simulation der Klimaentwicklung durchzuführen besteht darin, diese auf eine relativ große Anzahl an Systemen aufzuteilen. Hierbei kann Rechenleistung von Systemen zur Verfügung gestellt werden, die nicht unter der direkten Kontrolle der die Berechnung durchführenden Organisation stehen. Diese kann daher in der Regel nicht davon ausgehen, dass sich die erhaltenen berechneten Daten in einem unverfälschten Zustand befinden. In der Regel wird versucht, diesen Unsicherheitsfaktor durch genügend Redundanz in den Berechnungen auszugleichen.

Mit Hilfe von Trusted Computing wäre es für die durchführende Organisation möglich, Gewissheit darüber zu erlangen, dass die retournierten Daten den Vorschriften entsprechend berechnet und nicht verfälscht wurden. Dadurch wäre es möglich, einen Großteil der ansonsten benötigten Redundanz einzusparen was zu schnelleren und billigeren Resultaten führt.

2.5 Bereits vorhandene Umsetzungen

Obwohl bereits eine geraume Zeit an der Trusted Computing Spezifikation gearbeitet wird und diese bereits mehr als 1000 Seiten umfasst, gibt es bis dato keine breit nutzbare Plattform, die diese Technologie in allen Facetten umsetzt und zur Verfügung stellt. Nichtsdestotrotz gibt es bereits einige Ansätze, welche zumindest einen Teil der Funktionalität, die von Trusted Computing geboten wird, nutzen.

So haben seit 2004 bereits die meisten namhaften Hersteller Systeme mit integriertem TPM und entsprechender BIOS Unterstützung herausgebracht. Entsprechend der TCG Spezifikation, muss das TPM durch den Benutzer jedoch aktiviert werden, bevor dessen Funktionalität genutzt werden kann.

Auf dem Betriebssystemsektor gibt es mit Microsofts Next-Generation Secure Computing Base (NGSCB) eine Softwarearchitektur, die Teile des TCG Standards implementiert und für aktuelle und zukünftige Windows basierte Betriebssysteme zur Verfügung stellt [NGSCB]. Aktuell gibt es mit Microsoft Windows Vista (Ultimate und Enterprise) ein Betriebssystem, das prinzipiell eine Unterstützung für Trusted Computing fähige Systeme zur Verfügung stellt. Windows Vista verwendet ein eventuell vorhandenes TPM dabei für die Laufwerkverschlüsselung „BitLocker“, die verhindern soll, dass Daten eines gestohlenen Laufwerks ausgelesen werden können [BitLocker]. Dazu implementiert Microsoft Windows Vista eine Integritätsprüfung beim Start des Betriebssystems, welche erfolgreich abgeschlossen werden muss, um eine erfolgreiche Entschlüsselung der Laufwerke zu ermöglichen.

Für Linux gibt es mit Trusted Gentoo [TG] ebenfalls eine Distribution, welche eine entsprechende Unterstützung für Trusted Computing fähige Systeme aufweist. Prinzipiell bietet der Linux Kernel eine Unterstützung für Trusted Computing seit der Version 2.6.13.

2.6 Kritik an Trusted Computing

Trusted Computing ist eine Technologie, die seit ihrer Entstehung sehr kontrovers diskutiert wird. Während Vertreter der Technologie und hier allen voran die TCG die Vorteile von Trusted Computing betreffend einer Erhöhung der erreichbaren Sicherheit in computerbasierten Systemen herausstreichen, verweisen Kritiker auf diverse Nachteile und Bedenken, die sich aus einem Einsatz dieser Technologie ergeben. Im Folgenden sind die wichtigsten Punkte, an denen sich die Kritik an Trusted Computing orientiert, angeführt und näher erläutert.

2.6.1 Machtverschiebung hin zum Hersteller / Anbieter

Ein Hauptkritikpunkt an der Trusted Computing Technologie fußt auf der Tatsache, dass der Eigentümer eines Computersystems einen Teil seiner Macht über sein eigenes System und die auf dem System befindlichen Daten aufgeben muss. Tatsächlich ist es ein Ziel von Trusted Computing, die Sicherheit eines Systems nicht nur für sondern auch vor dem Benutzer selbst zu

schützen, da nur so für Dritte gewährleistet werden kann, dass ein für sie entferntes System auch vertrauenswürdig ist.

Verfechter der TC Technologie argumentieren, dass der Verlust an Kontrolle über das eigene System durch gewonnenes Vertrauen in andere Systeme wieder aufgewogen wird. Da es sich bei jenen Parteien, die ein bestimmtes Vertrauen in entfernte Systeme voraussetzen möchten, in der Regel um Anbieter von Dienstleitungen und weniger um Konsumenten handeln wird, dürfte dieses Argument einem durchschnittlichen Benutzer wenig stichhaltig erscheinen.

In diesem Zusammenhang schlug die Electronic Frontier Foundation (EFF)[5], einer der Hauptkritiker der TC Technologie, die Integration einer sogenannten Owner Override Funktion vor. Diese würde es dem Besitzer eines Systems ermöglichen, einer dritten Partei eine falsche Konfiguration und Identität vorzutäuschen. Nach Ansicht der EFF würde das die meisten Kritikpunkte an TC entkräften, während gleichzeitig alle Vorteile der TC Technologie bestehen bleiben würden. Die TCG kam diesem Vorschlag jedoch nicht nach, da für sie die vor Manipulation geschützte Bescheinigung eine der zentralen Aufgaben des TPM ist.

2.6.2 Behinderung des freien Wettbewerbs

Durch Anwendung der durch TC zur Verfügung gestellten Funktionalität ist es Herstellern von Software möglich, Kunden enger an das eigene Produkt zu binden. Beispielsweise könnten sich Dokumente, die mit einer bestimmten Software erstellt wurden, mit einem Konkurrenzprodukt nicht mehr öffnen lassen. Dieses unter dem Begriff „Kunden-Lock-In“ bekannte Phänomen würde dazu beitragen, dass bestehende Monopole weiter verstärkt und diverse offene Dateiformate nutzlos werden würden. Insgesamt würde dies die Entwicklung des freien Wettbewerbs behindern.

Weitere Nachteile ergeben sich für Open-Source Projekte. Da diese darauf beruhen, dass der Quellcode von Software frei zugänglich und auch adaptierbar ist, ergeben sich hier zwangsläufig Probleme, sobald es zu einer erforderlichen Zertifizierung der Software kommt. Ein ausgestelltes Zertifikat wird zwangsweise ungültig, sobald sich das zugrundeliegende Programm ändert. Generell könnte der gesamte notwendige Vorgang der Zertifizierung und die damit verbundenen Kosten für freie Softwareprojekte aber auch für kleinere Unternehmen eine zusätzliche Hürde darstellen, die deren Erfolg behindern würde.

2.6.3 Verletzung der Privatsphäre

Obwohl zur Identifizierung bzw. Bescheinigung eines Systems ein Schlüssel verwendet wird, der nicht direkt auf die Identität des Benutzer bzw. des Besitzers schließen lässt, kann das Feature der Bescheinigung trotzdem verwendet werden, um indirekt auf die Identität zu schließen. Dies kann besonders dann der Fall sein, wenn der Benutzer über das Internet bestimmte Informationen betreffend seine Identität preisgibt. Zum Beispiel könnte im Zuge eines Registrierungsprozesses neu erstandener Hardware solch eine Information notwendigerweise bekanntgegeben werden.

2.6.4 Spezifikation

Ein weiterer Kritikpunkt an der TC Technologie basiert auf der Tatsache, dass im Prinzip die gesamte Sicherheit von TC Systemen auf dem TPM beruht. Die Spezifikation für dieses ist öffentlich zugänglich und wurde intensiv begutachtet, sodass davon ausgegangen werden kann, dass diese sicher ist. Im Allgemeinen gilt dies jedoch für die einzelnen Implementierungen dieser Spezifikation, die von den diversen Herstellern selbst vorgenommen wird, nicht. Es ist daher nicht auszuschließen, dass einige Umsetzungen der an sich guten Spezifikation Fehler aufweisen, die es wiederum Angreifen ermöglichen könnten das TPM und damit das gesamte TC System zu kompromittieren. Diesem Kritikpunkt wird jedoch die Zertifizierung der TPM entgegen gehalten.

Ein weiteres Problem besteht darin, dass sich die TC Spezifikationen noch immer ändern, was zu Problemen bei der Interoperabilität von Implementierungen verschiedener Anbieter führt.

[5] Electronic Frontier Foundation: http://www.eff.org

Ein Problem im Zusammenhang mit der aktuellen Spezifikation betrifft die Festlegung der zu verwendenden Hash-Algorithmen. Hier wurde seitens der TCG der Algorithmus SHA1, der bereits seit einiger Zeit als nicht mehr sicher gilt, als Standard festgelegt. Da die Berechnung der Hash-Werte ein zentrales Element der Sicherheit der gesamten TC Architektur ist, stellt die Wahl dieses unsicheren Algorithmus ein nicht zu unterschätzendes Risiko dar.

3 Wissenschaftliche Projekte im Bereich „Trusted Computing“

Im Rahmen der Technologiebeobachtung beschäftigt sich A-SIT mit dem Thema Trusted Computing, um relevante Entwicklungen in diesem Bereich früh erkennen und unter Umständen auch den eigenen Vorstellungen entsprechend beeinflussen zu können. Die dazu notwendige Expertise bezieht A-SIT dabei vor allem auch vom A-SIT Mitglied Technische Universität Graz. Die TU Graz engagiert sich in verschiedenen Projekten, in welchen das Thema Trusted Computing von unterschiedlichen Standpunkten und Sichtweisen aus bearbeitet wird. In diesem Abschnitt werden diese Projekte näher vorgestellt, aktuelle wissenschaftliche Fragestellungen rund um Trusted Computing zu illustrieren.

3.1 Open Trusted Computing (Open TC)

Das Open Trusted Computing (Open TC) Konsortium [OpenTC] ist ein internationales Forschungsprojekt, das sich mit der Entwicklung von vertrauenswürdigen Computersystemen basierend auf Open-Source Komponenten beschäftigt. Dabei versucht Open TC Lösungen sowohl für traditionelle Systeme wie Personal Computer als auch für alternative Plattformen wie eingebettete oder mobile Systeme zur Verfügung zu stellen. Besonders letztere haben in letzter Zeit im Zusammenhang mit Trusted Computing an Relevanz gewonnen und verdienen daher eine besondere Aufmerksamkeit.

Ziel des Open TC Konsortiums ist es, ein öffentliches Trusted Computing Framework zu definieren und umzusetzen. Das Framework baut dabei auf Sicherheitsmechanismen auf, die von diversen Schichten des Betriebssystems zur Verfügung gestellt werden. Den zentralen Punkt des gesamten Frameworks bildet das Trusted Platform Module (TPM), das von der TCG spezifiziert wurde und in diversen aktuellen Prozessoren bereits integriert ist.

Um die zu erreichenden Vorteile für die entsprechende Community zu maximieren, werden sämtliche Resultate dieses Projekts als Open-Source Software zur Verfügung gestellt. Dabei wird besonderes Augenmerk auf eine bestmögliche Unterstützung von Linux basierten Systemen gelegt.

Das Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) der TU Graz ist Mitglied in diesem Projekt und konzentriert sich dabei hauptsächlich auf eine Integration der Trusted Computing Technologie in die Java Plattform [TCJava]. Ein weiterer Fokus liegt auf der Erforschung und Weiterentwicklung von TC fähigen Netzwerkkomponenten. Im Folgenden werden die Resultate des IAIK, die sich im Rahmen des Projekts Open TC ergeben haben, zusammenfassend beschrieben.

3.1.1 jTSS – TCG Software Stack for the Java Platform

Die Trusted Computing Group (TCG) zeichnet verantwortlich für die Spezifikation aller im Rahmen von Trusted Computing benötigten Komponenten. Eine dieser zentralen Komponenten ist der TCG Software Stack (TSS), welcher im Prinzip Möglichkeiten für die zur Verwendung von vorhandener TC Hardware nötige Ansteuerung durch Softwarekomponenten implementiert.

Im Rahmen des Projekts Open TC wurde durch das IAIK eine Implementierung des TSS für die Programmiersprache Java entwickelt. Diese unter dem Namen jTSS veröffentlichte Umsetzung bietet dabei eine Java-Implementierung aller spezifizierten Schichten des TSS.

3.1.2 jTSS Wrapper – TSS Wrapper for the Java Platform

Wie bereits in Abschnitt 3.1.1 erwähnt, stellt der TCG Software Stack (TSS) ein zentrales Element Trusted Computing fähiger Systeme dar. Üblicherweise wird der TSS in der Programmiersprache C implementiert, was zu Problemen führt, wenn dieser von anderen Programmiersprachen wie zum Beispiel Java verwendet werden soll.

Aus diesem Grund wurde mit dem jTSS Wrapper eine Möglichkeit geschaffen, unter Verwendung des Konzepts der Sprachanbindung einen in C implementierten TSS auch in Java-Umgebungen nutzen zu können.

Im Gegensatz zu dem in Abschnitt 3.1.1 beschriebenen jTSS stellt der jTSS Wrapper keine eigene Implementierung der TCG Software Stacks dar, sondern bietet eine Schnittstelle zu einer bereits vorhandenen Implementierung in einer anderen Programmiersprache. Die beiden Produkte sind nichtsdestotrotz in der Praxis eng miteinander verknüpft, da der jTSS Wrapper üblicherweise als Add-On in den jTSS integriert ist. Um einen Wechsel zwischen den beiden Instanzen rasch und unkompliziert zu ermöglichen, greifen sowohl der jTSS als auch der jTSS Wrapper auf dieselbe API (TSP Interface oder TSPI) zurück.

3.1.3 jTpmTools – TPM Tools for the Java Platform

Die jTpmTools stellen eine Sammlung von Werkzeugen zur Verfügung, mit denen die prinzipielle Interaktion mit dem Trusted Platform Module (TPM) und dem TCG Software Stack demonstriert werden kann. Mit Hilfe der zur Verfügung gestellten Tools können beispielsweise Platform Configuration Registers (PCR) ausgelesen, Attestation Identity Keys (AIK) erstellt, oder mit einem entfernten Privacy-CA Service interagiert werden.

Folgende Kommandos werden durch jTpmTools unterstützt:

Kommando	Beschreibung
take_owner	Eigentümerschaft über TPM übernehmen.
clear_owner	Eigentümerschaft über TPM aufgeben (wodurch alle durch das TPM gesicherten Daten verloren gehen).
pcr_read	Auslesen der Inhalte der PCR Register.
pcr_extend	Erweitern der PCR Register.
dump_eventlog	Ausgeben der Log-Dateien, die durch die pcr_extend Operation generiert wurden.
read_pubek	Auslesen des öffentlichen Teils des Endorsement Keys.
read_certek	Auslesen des Endorsement Key Zertifikats.
aik_create	Generieren eines AIK Zertifikats durch Simulation eines lokalen Privacy-CA Durchlaufs.
xkms_aik_create	Generieren eines AIK Zertifikats unter Verwendung des XKMS Protokolls.
xkms_aik_locate	Lokalisieren eines AIK Zertifikats unter Verwendung des XKMS Protokolls.
xkms_aik_revoke	Widerrufen eines AIK Zertifikats unter Verwendung des XKMS Protokolls.
xkms_aik_validate	Validieren eines AIK Zertifikats unter Verwendung des XKMS Protokolls.
xkms_ekcert_create	Auslesen des öffentlichen Endorsement Keys und Generierung eines Endorsement Key Zertifikats unter Verwendung des XKMS Protokolls.
xkms_ekcert_validate	Validieren des EK Zertifikats unter Verwendung des XKMS Protokolls.

create_key	Erstellung von TSS Keys, die im nicht flüchtigen Speicher des TSS gesichert werden.
list_keys	Auflisten aller gesicherten Keys im nicht flüchtigen Speicher des TSS.
bind	Binding (Verschlüsseln) einer Datei mit einem TPM Schlüssel.
seal	Sealing (Verschlüsseln unter Einbeziehung der PCR Werte) einer Datei mit einem TPM Schlüssel.
unbind	Unbinding (Entschlüsseln) einer an ein TPM gebundenen Datei.
unseal	Unsealing (Entschlüsseln) einer Datei.
version	Feststellen der Bibliotheksversionen.

Tabelle 1 - Befehlsübersicht

3.1.4 TCcert Tool - Trusted Computing certificate tool

Ein Zusammenschluss mehrerer TC fähiger Systeme eröffnet Vorteile bezüglich der erreichbaren Sicherheit des daraus entstehenden Gesamtsystems. Um eine für den Aufbau solcher komplexeren Zusammenschlüsse von Systemen benötigte TC unterstützende Public-Key Infrastruktur (PKI) einsetzen zu können, sowie diverse Abläufe zwischen den einzelnen TC fähigen Plattformen automatisieren zu können, müssen die verwendeten elektronischen Nachweise (credentials) einem gemeinsamen Standard folgen.

Das vom IAIK entwickelte TCcert Tool unterstützt Anwender und Betreiber solcher komplexen Systeme bei der Erstellung und Verwaltung dieser notwendigen Nachweise. So können beispielsweise diverse Zertifikate, die für die reibungslose Abwicklung von verschiedenen TC basierten Aktionen benötigt werden und von der TCG entsprechend spezifiziert wurden, mit dem TCcert Tool erstellt werden.

3.1.5 PrivacyCA

Wie auch bereits in Abschnitt 3.1.4 erwähnt, bedingt der Zusammenschluss mehrerer die TC Technologie unterstützender Systeme den Einsatz einer speziell auf die Anforderung von Trusted Computing abgestimmten Public-Key Infrastruktur (PKI). So müssen neue, von der TCG eigens für den Einsatz in TC Umgebungen spezifizierte Nachweise (credentials) in bestehende PKI Lösungen integriert, sowie bestehende Prozeduren entsprechend den Bedürfnissen von TC fähigen Systemen angepasst werden.

PrivacyCA stellt eine Implementierung der von der TCG spezifizierten TC unterstützenden PKI dar. Die prototypische Umsetzung hat vor allem zum Ziel Erfahrungen mit Umsetzung und Betrieb derartiger Systeme zu gewinnen und mögliche Probleme im Umgang mit solchen Lösungen zu identifizieren.

3.1.6 TCPVM – Java VM for TCP Implementations

Im Rahmen dieses Teilprojekts wurde der bestehenden OpenJDK Implementierung diverse Funktionalität hinzugefügt, um für bestehende Java Applikationen eine Unterstützung von TC Funktionalität zu gewährleisten. Die Java VM for TCP Implementation unterstützt die Messung von Daten unter Zuhilfenahme eines vorhandenen TPM gemäß den Spezifikationen der TCG. Auf diese Weise wird eine vollständige Integration der Java VM in TC fähige Plattformen gewährleistet.

Die aktuelle Implementierung unterstützt die Messung von Klassen, JAR-Archiven und Konfigurationsdateien zur Laufzeit. Die Möglichkeit die Java VM nur mit bekannten Klassen laufen

zu lassen, stellt ein weiteres Feature der aktuellen Umsetzung dar. Der Integrity Service Provider (ISP), der die für die Durchführung der Messungen verantwortliche Architektur darstellt, kann prinzipiell in zwei Modi betrieben werden. Im sogenannten „VM Modus“ ist der ISP in den Class-Loading Prozess der HotSpot VM integriert, wodurch Klassen und native Bibliotheken zur Ladezeit gemessen werden. Da die Anzahl der Messergebnisse rasch steigen kann, werden diese in der VM zwischengespeichert und nicht einzeln an das TPM übertragen. Dieser Modus ist vor allem für Testzwecke ausgelegt.

Im Gegensatz dazu ist im „Java Modus“ der ISP in die Java Runtime Bibliothek integriert und führt Messungen von Klassen und JAR-Archiven dort zur Ladezeit durch. Die Runtime Klassen selbst, sowie native Bibliotheken des JDK müssen hingegen zuvor bereits vom Betriebssystem gemessen werden.

Der ISP verwendet einen TSS um die Messungen durchzuführen. Die Ergebnisse der Messungen werden entsprechend der TCG Spezifikation in den PCR Registern des TPM gespeichert. Messungen der VM spezifischen Klassen und Bibliotheken werden dabei im PCR#10 hinterlegt, während applikationsspezifische Klassen im PCR#11 gespeichert werden.

3.1.7 XKMS

Für eine erfolgreiche Vernetzung mehrerer TC fähiger Plattformen ist eine entsprechend auf Trusted Computing ausgelegte PKI nötig. Das XML Key Management Specification Protocol (XKMS) ist dabei einer der von der TCG vorgeschlagenen Kandidaten für eine Umsetzung dieser PKI.

Im Rahmen dieses Teilprojekts wurde XKMS daher implementiert um es gegebenenfalls in eine umzusetzende PKI Lösung integrieren zu können.

3.2 Trust Oriented Platform For Advanced Security (TOPAS)

Während Trusted Computing ursprünglich für PC basierte Plattformen konzipiert und spezifiziert wurde, führte die in den letzten Jahren zunehmende Verbreitung von mobilen Geräten zu der Anforderung, die Möglichkeiten von TC auch für diese Geräte nutzbar zu machen. Durch die besonderen Gegebenheiten, die Geräte wie Smartphones oder andere Handhelds mit sich bringen, eröffnen sich im Zusammenhang mit Trusted Computing neue Anwendungsgebiete. Neben der üblichen Funktionalität, die TC auch PC basierten Systemen zur Verfügung stellt, können auch typisch mobile Anwendungen wie zum Beispiel Mobile Ticketing oder Mobile Payment von den Vorteilen eines durch TC geschützten Systems profitieren.

Um eine bestmögliche Unterstützung mobiler Systeme zu gewährleisten, wurde die TCG Mobile Phone Work Group [TCG-MOBILE] ins Leben gerufen, die entsprechende Spezifikationen und Dokumente über Referenzarchitekturen entwickelt, um TC auch für mobile Geräte nutzbar zu machen. Zentrales Element von mobilen TC Systemen bildet das Mobile Trusted Module (MTM), das prinzipiell dem TPM herkömmlicher Systeme entspricht. Da es bezüglich eines mobilen Geräts mehrere Interessensgruppen (Eigentümer, Service Provider, Hersteller) gibt, besteht das MTM üblicherweise aus zwei Elementen und kann auch in reiner Software implementiert werden.

Das Mobile Local-Owner Trusted Module (MLTM) entspricht dabei in etwa einem herkömmlichen TPM, unterstützt jedoch nur ein Subset der TPM Befehle. Wie sein Pendant aus der PC Welt ist es mit einem Endorsement Key ausgestattet und unterstützt die Konzepte der Beglaubigung, des Sealings und des Bindings. Den zweiten Teil eines MTM stellt das Mobile Remote Owner Trusted Module (MRTM) dar, das zusätzlich die Identifizierung des Geräts in Mobilfunknetzen, Updatefunktionen durch Hersteller und Service Provider, oder auch einen geeigneten Schutz der International Mobile Equipment Identity (IMEI) unterstützt.

Im Rahmen des Projekts TOPAS [TOPAS] wird versucht, die Möglichkeiten, die Trusted Computing für mobile Plattformen bietet, auszuloten und damit einhergehende Risiken und Kosten abzuschätzen. Dazu wurde auf einem handelsüblichen Mobiltelefon eine auf Java-Card basierte

Implementierung einer MTM umgesetzt. Basierend auf den im Zuge der Erstellung der Implementierung gewonnen Erfahrungen und den erhaltenen Resultaten können entsprechende Schlussfolgerungen über die Funktionalität und Praktikabilität von TC basierten Lösungen auf mobilen Geräten gewonnen werden.

3.3 JSR 321 – Trusted Computing API for Java

Der TCG Software Stack ist eines der zentralen Elemente einer TC unterstützenden Plattform indem er für Applikationen eine Schnittstelle zur Verfügung stellt, mit der diese die vom System gebotene TC Funktionalität nutzen können. Die vorhandene Spezifikation konzentriert sich dabei auf Applikationen, die in der Programmiersprache C geschrieben sind. Für Anwendungen, die in anderen Sprachen – und hier allen voran in Java – entwickelt wurden, ergeben sich dadurch naturgemäß Probleme mit der Verwendung des vorhandenen TSS.

Ziel dieses Projekts ist es daher, eine Trusted Computing API für Java zu entwickeln, die es Entwicklern zukünftiger Java-Applikationen ermöglichen soll, die Funktionalität der von TC fähigen Systemen zur Verfügung gestellten Funktionalität besser nutzen zu können. Dazu wurde im Rahmen eines offiziellen Java Community Process (JCP) ein Java Specification Request (JSR) mit dem Titel „Trusted Computing API for Java“ eingebracht [JSR321].

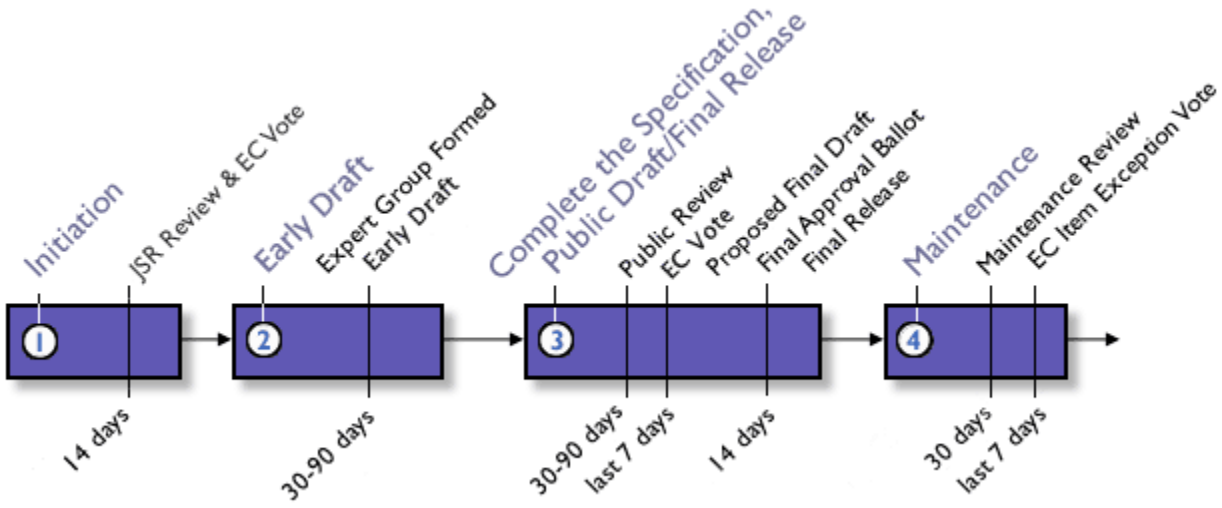

Abbildung 1 – Phasen des JCP Programms [Quelle: www.jcp.org]

Das JCP Programm erlaubt die Definition neuer Industriestandards bei gleichzeitiger Wahrung der Kompatibilität zur Java Technologie. Prinzipiell besteht ein JCP aus den im Folgenden angeführten und in Abbildung 1 gezeigten Phasen.

1) Initiation: Eine Spezifikation wird von einem Community Mitglied initiiert und durch das verantwortliche Exekutivkomitee zur Entwicklung freigegeben.

2) Early Draft: Eine Expertengruppe wird gebildet um einen vorläufigen Entwurf der Spezifikation zu entwickeln, welcher daraufhin der Community und der Öffentlichkeit zur Begutachtung vorgelegt wird.

3) Public Draft: Der vorhandene Entwurf der Spezifikation wird erneut begutachtet. Nach Beendigung der Begutachtungsphase entscheidet das Exekutivkomitee ob die vorhandene Spezifikation weiter bearbeitet werden soll. Wenn diese Entscheidung positiv ausfällt, werden die Referenzimplementierung und das entsprechende Technology Compatibility Kit vervollständigt. Das Exekutivkomitee entscheidet daraufhin noch einmal über die endgültige Annahme der Spezifikation.

4) Maintenance: Die fertig gestellte Spezifikation, Referenzimplementierung und Technology Compatibility Kit werden entsprechend vorhandenem Feedback laufend angepasst und gewartet.

3.4 Secricom

Im Rahmen des Projekt „Secricom (Seamless Communication for Crisis Management)“ [SECRICOM] soll eine Referenzimplementierung einer Sicherheitsplattform entwickelt werden, die eine EU weite Kommunikationsinfrastruktur für Krisenfälle zur Verfügung stellt. Dabei sollen Probleme aktueller Kommunikationssysteme wie schlechte Kompatibilität verschiedener Teillösungen, unzulänglicher Schutz gegen das Abhören von Kommunikation oder Missbrauch, aber auch hohe Betriebskosten gelöst werden. Zusätzlich sollen bestehende Systeme mit neuen Features versehen und dadurch deren Verwendung effizienter und sicherer gestaltet werden.

Ein Ziel von Secricom ist es unter anderem, die zu entwickelnde Infrastruktur und damit auch die verwendeten Kommunikationsgeräte selbst sicher und vertrauenswürdig zu machen. Ein Zurückgreifen auf die von Trusted Computing zur Verfügung gestellte Funktionalität scheint daher naheliegend zu sein. Da sich das gesamte Projekt derzeit noch in einem frühen Stadium befindet, ist die Rolle, welche die TC Technologie in der angestrebten Umsetzung spielen wird, noch nicht restlos geklärt. Es scheint jedoch wahrscheinlich, dass einige TC basierte Konzepte herangezogen werden um die erreichbare Sicherheit der zu implementierenden Lösung zu erhöhen.

3.5 KIRAS Studie: Trusted Computing in der Österr. Verwaltung

Im Rahmen einer vom IAIK der TU Graz in Zusammenarbeit mit Technikon Research[6] und der FH Kärnten[7] durchgeführten Studie wurde untersucht, inwieweit sich die von Trusted Computing zur Verfügung gestellten Konzepte und Technologien in der österreichischen Verwaltung einsetzen lassen um dort einen höheren Grad an Sicherheit zu erreichen. Die erstellte Studie steht unter [KIRAS-TC] zum Download bereit.

In einer am Anfang der Studie durchgeführten SWOT Analyse der TC Technologie wurden die Stärken, Schwächen, Möglichkeiten und Gefahren von Trusted Computing identifiziert und analysiert. Diese decken sich im Prinzip mit jenen Beobachtungen und Schlussfolgerungen, die auch bereits in diesem Dokument ausgeführt wurden. Des Weiteren identifizierte die KIRAS Studie verschiedene Anwendungsgebiete, in denen Trusted Computing potentiell zum Einsatz kommen könnte, und listete Kriterien, die für bzw. gegen den Einsatz dieser Technologie sprechen, auf. Neben der Ausführung einiger Kritikpunkte an TC, welche auch bereits in diesem Dokument dargelegt wurden, versucht die Studie einen möglichen Nutzen, der sich aus der Verwendung von Trusted Computing in der öffentlichen Verwaltung erreichen ließe, abzuschätzen. Zum Abschluss der Einführung in die TC Technologie werden in der Studie verschiedene andere Konzepte wie zum Beispiel die österreichische Bürgerkarte und deren Konzepte jenen von Trusted Computing gegenübergestellt um Vor- und Nachteile der jeweiligen Ansätze zu vergleichen.

Der zweite Teil der Studie beschäftigt sich mit der Strukturierung und den Aufgaben der österreichischen Verwaltung im Allgemeinen. Hier werden speziell die einzelnen Aufgaben und Herausforderungen skizziert, sowie versucht, den aktuellen Status Quo der verwendeten Sicherheitstechnologien in diesem Bereich zu ermitteln. Dazu wurden unter anderem Interviews mit verschiedenen Personen, die in der öffentlichen Verwaltung tätig sind, geführt und deren Antworten ausgewertet.

Im dritten Teil der Studie wurde schließlich versucht, basierend auf den Erkenntnissen der Analyse der TC Technologie und der aktuellen Situation in der österreichischen Verwaltung mögliche geeignete Anwendungsgebiete für Trusted Computing zu finden. Dazu wurden zwei Beispielsszenarien entworfen und skizziert, wie TC einerseits im Bereich des e-Votings – und hier

[6] Technikon Research: http://www.technikon.at
[7] Fachhochschule Kärnten: http://www.fh-kaernten.at

vor allem bei Wahlmaschinen – und andererseits bei der Verwendung des elektronischen Akts (ELAK) zum Einsatz kommen könnte um die gewährleistete Sicherheit zu steigern.

Schließlich kommt die Studie über den Einsatz von Trusted Computing in der öffentlichen Verwaltung zu dem Schluss, dass diese Technologie durchaus das Potential bieten würde, um diverse computerbasierte Vorgänge in der Verwaltung noch sicherer zu gestalten. Der aktuelle Entwicklungsstand von Trusted Computing lässt einen Einsatz von TC in der Praxis jedoch nur mittel- oder langfristig möglich erscheinen. Nichtsdestotrotz empfiehlt die Studie bereits jetzt vorbereitende Maßnahmen für eine zukünftige Einführung der Technologie zu treffen. Dazu gehören einerseits gezielte Schulungen für das technische Personal und für Benutzer, als auch die Durchführung von Pilotprojekten, mit denen die Vorteile von TC demonstriert und zusätzlich Erfahrungswerte für einen späteren Einsatz der Technologie gewonnen werden können. Zu guter letzt empfiehlt die Studie die gezielte Förderung von Forschungsprojekten im Bereich des Trusted Computing um so die Möglichkeit zu wahren, lenkend in die Entwicklung dieser Technologie eingreifen zu können.

4 Zusammenfassung

Im Rahmen der Technologiebeobachtung beschäftigt sich A-SIT mit der Trusted Computing Technologie, um Entwicklungen auf diesem Gebiet vorzeitig erkennen und auch beeinflussen zu können. In diesem Dokument wurden die wichtigsten Konzepte und Methoden von Trusted Computing vorgestellt und Projekte, in die sich die TU Graz einbringt, zusammengefasst. Als Mitglied von A-SIT bildet die damit gewonnene Expertise der TU Graz eine Basis für die A-SIT Technologiebeobachtung im Bereich Trusted Computing.

Trusted Computing ist eine Technologie, die durchaus das Potential besitzt, einige aktuelle Probleme aus dem Bereich der IT-Sicherheit durch die Anwendung neuer Konzepte zu lösen. Vor allem die Möglichkeit, Informationen über den aktuellen Zustand entfernter Systeme auf verlässliche Art und Weise zu beziehen, eröffnet interessante neue Anwendungsgebiete. Ermöglicht werden diese neuen Features durch die Integration neuer Komponenten in bestehende Computersysteme. Das zentrale Element ist dabei das Trusted Platform Module, das einen Großteil der für Trusted Computing Systeme typischen Funktionalität in Hardware umsetzt.

Allerdings gibt es zu dieser Technologie auch durchaus kritische Stimmen, die auf die Gefahren, die sich aus einer zunehmenden Verbreitung von Trusted Computing ergeben, hinweisen. Diese Kritik bezieht sich unter anderem auf eine Verschiebung der Machtverhältnisse betreffend der Kontrolle über die durch Trusted Computing geschützten Systeme. Durch Anwendung der von dieser Technologie vorgeschlagenen Methoden und Konzepte, verliert der Besitzer und Benutzer einer TC fähigen Plattform einen Teil seiner Berechtigungen auf dem eigenen System, während Dritte wie zum Beispiel Anbieter von Diensten zusätzliche Rechte auf dem jeweiligen System erhalten.

Im Rahmen diverser Projekte, über die sich das A-SIT Mitglied TU Graz in dieser Thematik engagiert, wird versucht Entwicklungen im Bereich von Trusted Computing zu erkennen und wenn möglich auch positiv zu beeinflussen. So wird beispielsweise versucht, im Zuge des Projekts Open TC Java basierte Lösungen zu erarbeiten, die dem Umgang mit Trusted Computing im Zusammenhang mit dieser Programmiersprache erleichtern sollen. Aus dem selben Grund wurde über den Java Community Process (JCP) ein Java Specification Request mit dem Titel „Trusted Computing API for Java“ eingebracht, der zum Ziel hat, eine entsprechende Java API zu entwickeln um dadurch die Programmierung von Trusted Computing basierten Applikationen in dieser Programmiersprache zu erleichtern.

Hingegen wird im Projekt „TOPAS“ versucht, den Horizont von Trusted Computing auf mobile Geräte wie zum Beispiel Mobiltelefone auszuweiten. Des Weiteren gibt es Bestrebungen, Konzepte und Methoden der TC Technologie auch in das Projekt „Secricom“, das sich mit dem Entwurf eines sicheren und zuverlässigen Kommunikationssystems für ein EU weites Krisenmanagement beschäftigt, einzubinden. Ergänzend wurde auch im Rahmen einer Studie untersucht, inwieweit sich Trusted Computing Technologien für einen Einsatz in der öffentlichen Verwaltung eignen, um etablierte Vorgänge in diversen Institutionen auf ein höheres Sicherheitsniveau zu heben.

Prinzipiell zeigten die bisher durchgeführten Arbeiten im Bereich von Trusted Computing, dass diese Technologie durchaus das Potential besäße, bestimmte aktuelle Probleme im Bereich der IT Sicherheit zu lösen oder zumindest zu entschärfen. Allerdings lässt der derzeitige Entwicklungsstand der Technologie noch keine breiten Anwendungen zu. Die anhaltenden Weiterentwicklungen auf diesem Gebiet scheinen aber auf eine vielversprechende Zukunft dieser Technologie hinzuweisen, sofern es gelingt die derzeit noch vorhandenen Vorbehalte und Kritikpunkte an Trusted Computing zu entkräften.

Referenzen

[TCG]	Trusted Computing Group:Home, [https://www.trustedcomputinggroup.org/home/], abgerufen am 19.12.2008
[TCG-SPECS]	Trusted Computing Group:Specs, [https://www.trustedcomputinggroup.org/specs/], abgerufen am 19.12.2008
[NGSCB]	Microsoft Next-Generation Secure Computing Base, [http://www.microsoft.com/resources/ngscb/default.mspx], abgerufen am 19.12.2008
[BitLocker]	Microsoft BitLocker Drive Encryption, [http://technet.microsoft.com/en-us/library/cc766200.aspx], abgerufen am 19.12.2008
[TG]	Gentoo Linux -- Trusted Gentoo, [http://www.gentoo.org/news/20050202-trustedgentoo.xml], abgerufen am 19.12.2008
[OpenTC]	Open TC, [http://www.opentc.net/], abgerufen am 19.12.2008
[TCJava]	Trusted Computing fort he Java(tm) Platform, [http://trustedjava.sourceforge.net/], abgerufen am 19.12.2008
[TCG-MOBILE]	Trusted Computing Group:Mobile, [https://www.trustedcomputinggroup.org/groups/mobile], abgerufen am 19.12.2008
[TOPAS]	TOPAS – Trust Oriented Platform For Advanced Security, [http://www.iaik.tugraz.at/content/research/trusted_computing/topas/], abgerufen am 19.12.2008
[JSR321]	The Java Community Process(SM) Program - JSRs: Java Specification Requests - detail JSR# 321, [http://jcp.org/en/jsr/detail?id=321], abgerufen am 19.12.2008
[SECRICOM]	Secricom, [http://www.iaik.tugraz.at/content/research/trusted_computing/Secricom/], abgerufen am 19.12.2008
[KIRAS-TC]	KIRAS Trusted Computing, [http://www.trusted-computing.at/images/kiras_studie_20080303.pdf], abgerufen am 19.12.2008
[BSI-TC]	Trusted Computing, [http://www.bsi.de/sichere_plattformen/trustcomp/], abgerufen am 19.12.2008

Historie

Version	Datum	Kommentar
0.1	12.9.2008	Dokumentstruktur
Ersteller		
Thomas Zefferer		
Version	**Datum**	**Kommentar**
0.9	19.12.2008	Erste Fassung zum Review
Ersteller		
Thomas Zefferer		
Version	**Datum**	**Kommentar**
1.0	16.2.2009	Veröffentlichte Version
Ersteller		
Thomas Zefferer		