Trusted Computing / TCPA

Markus Gerstel

Hauptseminar: Digital Rights Management, WS 2005/06
Betreuer: Dr. Stefan Katzenbeisser
Technische Universität München
gerstel@in.tum.de

Zusammenfassung In den letzten Jahren haben die Diskussionen um die Sicherheit von Rechensystemen ständig zugenommen. Größere Sicherheitslücken, Bedrohungen durch Trojaner, Würmer und dergleichen sind mittlerweile an der Tagesordnung. Trusted Computing soll diesen Bedrohungen entgegenwirken und eine solide Basis für Sicherheitsfunktionen im Betriebssystem bieten. Im Folgenden soll ein kurzer Überblick über die TCPA-Plattform und eines darauf aufbauenden Sicherheitskerns anhand des Beispiels von Microsoft Palladium gegeben werden.

Inhaltsverzeichnis

1 Die Trusted Computing Platform Alliance / Trusted Computing Group

Im Oktober 1999 formierte sich eine Interessengemeinschaft unter dem Namen „Trusted Computing Platform Alliance“ (TCPA), mit dem Ziel sichere Geschäftsvorgänge an einem PC zu ermöglichen. Dieses Ziel sollte erreicht werden, indem durch neue Technologien bestehende Angriffsmöglichkeiten in Hard- und Software beseitigt werden. Den Gründungsmitgliedern der TCPA waren unter anderem Compaq, Intel, HP, IBM und Microsoft an.

Das Interesse an der Trusted Computing-Technologie ist so groß, dass der TCPA 2003 bereits über 200 Mitglieder angehörten. Da aber die Satzung jedem Mitglied gleichermaßen ein Veto-Recht zusprach wurde es unmöglich neue Versionen des TCPA-Standards zu verabschieden; dadurch wurde die TCPA handlungsunfähig. Als Folge davon wurde 2003 die TCG (Trusted Computing Group) mit veränderter Satzung gegründet. In der TCG wird zwischen den Mitgliedern unterschieden und nur den *Promoters* wird ein Veto-Recht eingeräumt. Dazu zählen aktuell die Gründungsmitglieder der TCG: AMD, Hewlett-Packard, IBM, Intel Corporation, Microsoft und Sun Microsystems, Inc.

1.1 Ziele von Trusted Computing

Trusted Computing will insbesondere folgende Angriffsklassen verhindern:

- Zugriffsversuche auf Software mit dem Ziel geschützte Speicherbereiche auszulesen oder zu verändern (z.B. mit einem Debugger, aber auch über modifizierte Gerätetreiber und auf Hardware-Ebene mit Direct Memory Access, ferner auch durch Direktzugriff auf die Systemfestplatte an einem anderen Rechner)
- Verstecken oder Ausführen von fremden Code-Segmenten in bestehenden Programmen (Viren und Trojaner, Buffer Overflows)

1.2 Aufbau der TCPA-Architektur

Diese Ziele sollen mit besonderer Hardwareunterstützung erreicht werden: Das Trusted Platform Module (TPM) ist ein eigener Chip auf dem Mainboard, der eine Reihe von kryptographischen Funktionen zur Verfügung stellt. Das TPM kann mit Hilfe des eingebauten Zufallszahlgenerators 2048 Bit RSA-Schlüsselpaare erstellen und diese in einem eingebauten nichtflüchtigen Zertifikats- und Schlüsselspeicher ablegen. Im TPM wird vom Hersteller bereits ein einmaliges Schlüsselpaar, die Endorsement Keys, fest eingebaut. Diese Schlüssel sind als nicht exportierbar markiert und sollen somit den Chip niemals verlassen. Im normalen Betrieb kommen Attestation Identity Keys hinzu, vom Benutzer generierte Schlüsselpaare, die wiederum mit einem im TPM abgelegten Storage Root Key verschlüsselt werden.

Im TPM werden auch Zertifikate gespeichert. Diese sollen die Echtheit des TPMs bestätigen und sollen garantieren dass das System nicht unerlaubt modifiziert worden ist. Das sogenannte Endorsement Zertifikat wird vom TPM-Hersteller direkt eingebrannt. Es ist mit dem Endorsement Key signiert und soll sicherstellen dass das TPM echt und von einem geprüften Hersteller bereitgestellt worden ist. Ein Plattformzertifikat wird vom Plattformhersteller[1] ausgestellt und bindet das TPM an ein Mainboard beziehungsweise an ein System. Ein Conformance Zertifikat garantiert die TCG-Konformität der Kombination TPM und Mainboard/System. Zusätzliche Validation Zertifikate garantieren die Integrität einer oder mehrerer weiterer Systemkomponenten.

Um den sicheren Zustand des Systems zu dokumentieren bietet das TPM außerdem ein sicheres Logging[2] und sogenannte Platform Configuration Register, in denen Ergebnisse von Integritätstests sowie ein Hashwert (SHA-1) der Hardware-Ausstattung abgelegt werden.

Stellt das TPM fest, dass das System sich in einem gesicherten Zustand befindet, kann es sich mit Hilfe der Zertifikate und des Endorsement Keys gegenüber anderen TCG-konformen Plattformen authentifizieren.

Mittelfristig soll das TPM direkt in die CPU integriert werden.

1.3 Secure Bootstrap

Neben dem TPM wird eine BIOS-Erweiterung namens Core Root of Trust Management (CRTM) eingeführt. Diese Erweiterung prüft vor dem eigentlichen Systemstart zunächst sich selbst und anschließend den Programmcode im BIOS. Ein Hashwert des Programmcodes wird im TPM abgelegt und mit dem Wert

[1] Wird der Rechner aus Einzelkomponenten zusammengestellt, ist dies der Mainboardhersteller

[2] Ein Write-Once-Log, an das nur Meldungen angefügt werden können

vom letzten Systemstart verglichen. Danach prüft das BIOS weitere Hardwarekomponenten, den Bootsektor und zu guter Letzt den Betriebssystemloader. Dabei werden Prüfberichte und Hashwerte der einzelnen Hardwarekomponenten im TPM abgelegt. Damit kann der Betriebssystemloader, wenn das System sich aktuell in einem sicheren Zustand befindet, das Betriebssystem selbst prüfen und dann den normalen Bootvorgang fortsetzen.

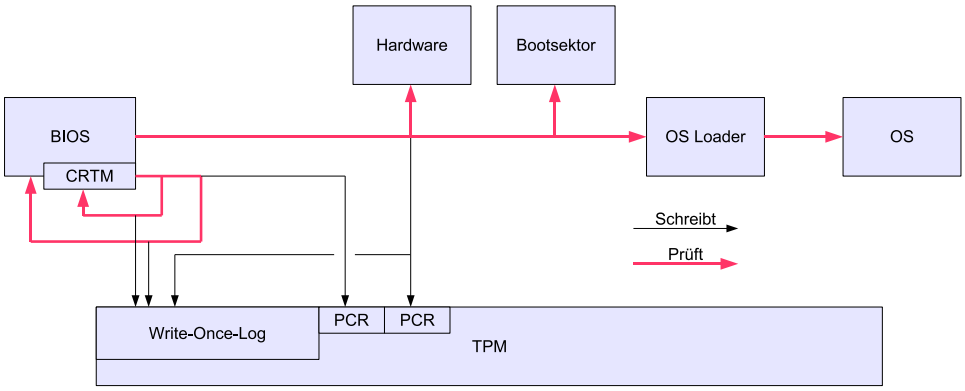

Abbildung 1: Secure Bootstrap

Dieses Verfahren der inkrementellen Prüfung aller Komponenten wird Chain of Trust genannt.

2 Next Generation Secure Computing Base a.k.a. Palladium

Sobald das BIOS die Kontrolle an den Betriebssystemloader übergibt, ist dieser für die weitere Erhaltung des sicheren Systemzustands verantwortlich. Aktuelle Betriebssysteme enthalten aber noch keine Unterstützung für TCPA. Das bereits seit langem angekündigte Microsoft Windows Vista[3] sollte ursprünglich mit dem Sicherheitskern Palladium eine vollständige TCPA-Unterstützung bieten. Microsoft erkannte frühzeitig, dass ein Windows-Nachfolger nur dann verkäuflich ist, wenn er weitgehende Abwärtskompatibilität auf Treiber- und Applikationsebene zum Vorgängersystem Microsoft Windows XP bietet. Um Windows Vista TCPA-konform und sicher zu machen trennte Microsoft Windows in zwei voneinander unabhängige Teilsysteme auf: Das bisher bekannte Windows und den „Nexus“.

[3] Windows Vista wurde unter dem Namen Windows Longhorn entwickelt.

2.1 NGSCB Architektur

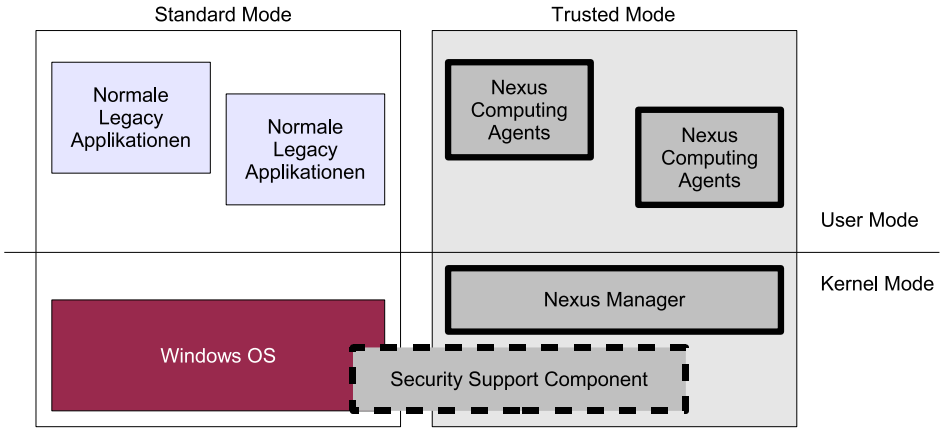

Abbildung 2: Ursprüngliche Architektur von Windows Palladium

Die Idee des Nexus war wie folgt:

- Sichere Programme (nun „Nexus Computing Agents“ genannt) laufen in einem von gewöhnlichen Programmen und anderen Agents speziell isolierten Speicherbereich ab. Diese Technik bezeichnet Microsoft als Strong Process Isolation, einen Seitenschutz im Hauptspeicher gegen Beobachtung und Modifikation.
- Vom Agent auf der Festplatte abgelegte Daten werden vom Betriebssystem ebenfalls vor Zugriff durch andere Programme und Agents geschützt (Sealed Storage).
- Schließlich müssen alle Ein- und Ausgaben von Agents über eine „Security Support Component“ in das ungeschützte Windows durchgereicht werden. Sichere Ein-/Ausgabekanäle direkt zum Benutzer sollen verhindern, dass Tastatureingaben an Agents von anderen Programmen abgefangen werden oder Bildschirmausgaben des Agents von anderen Programmen überlagert werden können.

Diese Technologie wurde von Microsoft erstmals auf der Windows Hardware Engineering Conference 2003 (WinHEC) demonstriert.

2.2 Palladium im Wandel

Ursprünglich hätte Windows Vista mit Palladium 2004 erscheinen sollen. Allerdings waren die strengen Regeln, die Microsoft den Programmierern für Nexus-Agents vorschrieb, unrealistisch. So stellten sich Softwareentwickler auf den Standpunkt, dass Sicherheit hauptsächlich Sache des Betriebssystems sei.

Microsoft nahm daher Abstand von Palladium und stellte auf der WinHEC 2004 eine neue Technologie vor: Die Agents sollten in einer vollständig virtualisierten Umgebung ähnlich eines VMWare- oder Virtual PC-Rechners ablaufen. Neue CPUs mit AMD Pacifica oder Intel Vanderpool Technologie sollten dabei Performance-Verluste verhindern.

Doch bereits auf der WinHEC 2005 änderte sich die Zielvorgabe von Microsoft erneut: Anstatt einer Virtualisierungslösung scheint sich nun Windows Vista auf den in 1.3 beschriebenen sicheren Bootvorgang zu beschränken. Dazu soll eine Verschlüsselung der Systempartition den Zugriff auf das System durch z.B. Ausbau der Festplatte erschweren. Windows Vista soll 2006 erscheinen.

3 Kontroverse - Diskussion um TCPA

Schon bevor der Geschäftsführer der Intel Corporation die Idee der TCPA als „police state in every computer“ bezeichnete, gab es rege Diskussionen für und wider TCPA. Da sich die Kritiken auf verschiedenste Aspekte der Technologie beziehen, und es im Rahmen dieses Seminars nicht möglich ist, auf alle Details einzugehen, soll hier lediglich ein Ausschnitt präsentiert werden:

- Viele Parteien befürchten, dass der Einsatz einer Public Key Infrastructure eine Monopolbildung begünstigt beziehungsweise die bestehenden PKI-Monopole stärkt.
- Sollte in Zukunft die Notwendigkeit bestehen Programme zu zertifizieren, könnten Open Source Projekte und kleine oder mittlere Unternehmen durch prohibitive Zertifizierungskosten vom Softwaremarkt ausgeschlossen werden.
- Daher sehen Juristen TCPA möglicherweise nicht als mit geltendem EU-Wettbewerbsrecht vereinbar.
- Bürgerrechtsvertreter sehen durch Einsatz sogenannter globaler Sperrlisten, die Zugriffe auf Dateien mit bestimmten Hashwerten verweigern, die Möglichkeit zur staatlichen Zensur oder des Eingriffs der verwaltenden Firmen.
- Die Möglichkeit Dokumente oder Material nach Veröffentlichung zurückzuziehen würde vermutlich sehr schnell mißbraucht werden.
- TCPA muss aktuell mit Zustimmung des Benutzers explizit im System aktiviert werden. Dies suggeriert eventuell eine falsche Freiheit.[4] Eventuell entstehen zukünftig Gründe für eine verpflichtende Nutzung von TCPA.
- In den USA haben Content-Anbieter (RIAA/MPAA) bereits versucht den Verkauf von nicht-TCPA-konformen Systemen durch Gesetz unter Strafe zu verbieten: „The penalties proposed for breaking this law would have ranged from 5 to 20 years in prison and fines between $\$50,000$ to \$1 million.“ (SSSCA/CBDTPA)

[4] Analog: Es ist die freie Entscheidung des Fahrers, ob ein Auto mit Benzin betankt werden soll oder nicht.

Literatur

1. Ross Anderson. *Trusted Computing Frequently Asked Questions.* http://www.againsttcpa.com/tcpa-faq-en.html. Stand vom 25.Okt.2005 16:36.
2. Andreas Gapel. *Trusted Computing.* http://wwwspies.in.tum.de/lehre/seminare/WS0304/hauptsem/Ausarbeitung02.pdf, 2003. Hauptseminar Ansätze für Betriebssysteme der Zukunft WS2003/04.
3. Markus Gerstel. *Virtualisierungsansätze mit Schwerpunkt Xen.* http://www13.informatik.tu-muenchen.de/lehre/seminare/WS0506/hauptsem/Ausarbeitung02.pdf, 2005. Hauptseminar Ansätze für Betriebssysteme der Zukunft WS2005/06.
4. Gerald Himmelein. *Ein gutes und ein böses Schloss.* heise Verlag, c't 11/05, S.114.
5. Gerald Himmelein. *WinHEC: Kleine Brötchen statt Big Brother.* http://www.heise.de/newsticker/meldung/59031. Meldung vom 27.Apr.2005 09:26.
6. Christian Koenig. *TCG und NGSCB auf dem Prüfstand des Wettbewerbsrechts.* http://www.tkrecht.de/vortraege/bmwa2003/tc-vortrag-rede20030703.pdf. Symposium T̈rusted Computing Group(̈TCG) des Bundesministeriums für Wirtschaft und Arbeit (BMWA) am Donnerstag, dem 3. Juli 2003, in Berlin.
7. Dirk Kuhlmann and Robert A. Gehring. Trusted platforms, drm, and beyond. In Eberhard Becker, Willms Buhse, Dirk Günnewig, and Niels Rump, editors, *Digital Rights Management*, volume 2770 of *Lecture Notes in Computer Science*, pages 178–205. Springer, 2003.
8. Wikipedia. *Trusted Computing.* http://en.wikipedia.org/wiki/Trusted_computing. Stand vom 22.Nov.2005 04:17.
9. Wikipedia. *Trusted Computing Group.* http://de.wikipedia.org/wiki/Trusted_Computing_Group. Stand vom 25.Okt.2005 16:28.