Trusted Computing

Flopp oder Durchbruch des TPM-Chips?

Kai-Oliver Detken

Die Trusted-Computing-Technik (TC) wurde von der Trusted Computing Group (TCG) spezifiziert und ermöglicht die Kontrolle von Hard- und Software. Notwendig dafür ist ein sogenannten Trusted Platform Module (TPM), das mit Hilfe kryptografischer Verfahren sowohl die Integrität der Softwaredatenstruktur als auch die Hardware messen kann und diese Werte nachprüfbar abspeichert. Dadurch kann wirkungsvoll bei Rechnersystemen und Smartphones nachgewiesen werden, dass die Basis eines Gerätes noch nicht kompromittiert worden ist. Gerade bei mobilen Geräten, die leichter zu attackieren sind, ist eine solche Technik sinnvoll.

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH

Während heutige Laptops bereits häufig mit einem TPM-Chip ausgerüstet sind, kann man ihn in Smartphones bisher suchen. Und das, obwohl die Trusted Computing Group vor fast zehn Jahren ihre Arbeiten aufnahm. Ein guter Zeitpunkt also, um einmal eine Bilanz über Trusted-Computing-Techniken zu ziehen.

Die Trusted Computing Group

Die Trusted Computing Group (TCG, www.trustedcomputinggroup.org) ist eine von der Industrie betriebene Standardisierungsorganisation, die Spezifikationen für Trusted-Computing-Techniken entwickelt. Sie hat im Jahre 2003 die Arbeiten der Trusted Computing Platform Alliance (TCPA) übernommen und setzt diese fort. Ziel ist es, einen offenen, herstellerunabhängigen Standard für Trusted-Computing-Bausteine und Softwareschnittstellen zu spezifizieren. Der Begriff „Trust" wird dabei so definiert, dass es bestimmte Erwartungen an ein Gerät oder eine Software gibt, die sich für einen bestimmten Zweck nach einer vordefinierten Art und Weise verhalten. Dadurch soll es möglich werden, Veränderungen an der Rechner- bzw. Smartphone-Plattform erkennen zu können. Das heißt, es lassen sich sowohl externe Softwareangriffe als auch Veränderungen der Konfiguration, Sicherheitslücken oder schadhafte Anwendungsprogramme ausmachen.

Die TCG fällt Entscheidungen aufgrund von qualifizierten Mehrheiten ihrer Mitglieder. Es werden vier Arten von Mitgliedern unterschieden:

- Adopter: Die Adopters bekommen den Zugriff auf veröffentlichte Spezifikationsentwürfe der TCG und auf teilweise noch nicht veröffentlichte Informationen. Sie besitzen kein Stimmrecht, um über neue Spezifikationen abzustimmen, und sind auch in den Diskussionsrunden nicht anwesend. Der Kostenbeitrag hängt von der Unternehmensgröße ab.
- Associate: Diese Gruppe erhält bereits ein Stimmrecht, was allerdings auf die Arbeitsgruppen begrenzt ist. Sie haben weder eine Möglichkeit, auf den Vorstand Einfluss zu nehmen, noch nehmen sie an den technischen Arbeitsgruppen teil. Ein Zugriff auf veröffentlichte Spezifikationsentwürfe sowie auf teilweise noch nicht veröffentlichte Informationen ist möglich.
- Contributor: Diese Mitglieder dürfen an den Arbeitsgruppen, die neue Spezifikationen entwickeln, teilnehmen und in ihnen mitwirken. Zusätzlich werden zwei Vertreter aus dieser Mitgliedsgruppe gewählt, die im Vorstand vertreten sind, um aktiv Entscheidungen mitzubestimmen. Es darf auf alle Daten zugegriffen werden.
- Promoter: Diese Gruppe verfügt über einen festen Sitz im Vorstand und in den jeweiligen Arbeitsgruppen. Sie entscheiden auch über die Aufnahme neuer Firmen in die Gruppe der Mitglieder. Mitglieder sind unter anderem Infineon, Intel, Microsoft und Cisco Systems. Ihre Zugriffsrechte sind nicht eingeschränkt.

Die Spezifikationen der TCG können in verschiedene Arbeitsgruppen unterteilt werden. Ein Schwerpunkt ist sicherlich das Trusted Platform Module (TPM) inklusive der Sicherheitselemente sowie der TPM Software Stack (TSS). Beide sind in der Trusted-Network-Connect-Architektur (TNC, *Bild 1*) wiederzufinden, die eine Erweiterung der bisherigen Sicherheitsprotokolle darstellt, da sie zusätzlich Informationen über die eingesetzten Policies und Plattformzustände bereithält. Weitere Gruppen beschäftigen sich mit PC-Clients, Infrastruktur und Serversyste-

men. Best-Practice-Angaben werden zudem regelmäßig definiert. Als Hauptkomponenten der TCG kann man den TPM-Chip und den Core-Root-of-Trust-Measurement-Mechanismus (CRTM) bezeichnen.

TNC-Architektur

Die aktuelle Architektur des Trusted Network Connect ist von der TCG in der Spezifikation 1.5 (Revision 3) vom Mai 2012 veröffentlicht worden. In Bild 1 zeigt die verschiedenen Einheiten. Das Zusammenwirken der einzelnen Komponenten wird durch Interfaces realisiert. Neu in der aktuellen TCG-Spezifikation ist der Metadata Access Point (MAP), der die zusätzlichen Sicherheitskomponenten von MAP-Clients mit anbindet.

Die Einheiten besitzen die folgenden Aufgaben:

- Access Requestor (AR): Der AR stellt die Verbindung in ein geschütztes Netz her. Er muss in der TNC-Architektur auf jeden Fall umgesetzt werden.
- Policy Decision Point (PDP): Der PDP entscheidet für die Anfrage des AR, wie die Zugriffsrechte für die Verbindung aussehen. Er muss in der TNC-Architektur ebenfalls umgesetzt werden.
- Policy Enforcement Point (PEP): Der PEP bildet die von dem PDP erhaltene Zugriffsberechtigung des AR ab. Er wird als optional angesehen.
- Metadata Access Point (MAP): Der MAP speichert und liefert Zustandsinformationen über die AR. Er ist ebenfalls optional.
- MAP-Client (MAPC): Die Rolle des MAP-Client beinhaltet das Veröffentlichen oder das Konsumieren der Zustandsinformationen des MAP über die AR. Auch dieser Bereich wird als optional angesehen.

Alle Einheiten und Komponenten in der Architektur sind logische und nicht physische Einheiten oder Komponenten. Ihre Realisierung kann daher in unterschiedlicher Art und Weise erfolgen.

Der AR besteht aus folgenden Komponenten:

- Network Access Requestor (NAR): Der NAR ist eine Einheit (z.B. Softwarekomponente), die die Verbindung zu einem Netz herstellt. Es ist nicht ausgeschlossen, dass auf einem AR mehrere NAR installiert sind, die die Verbindung zu verschiedenen Netzen ermöglichen.
- TNC Client (TNCC): Der TNCC (Softwarekomponente) sammelt die von den IMCs (Integrity Measurement Collector) erhaltenen Daten und sendet diese an den TNC-Server. Sind nicht alle Statusinformationen über die IMCs abrufbar, kann der TNC-Client zusätzlich selbst Informationen über den Status des Systems abrufen.
- Integrity Measurement Collector (IMC): Die IMC sind Softwarekomponenten, die den Status des AR (z.B. aktuelle Patch-Infos, aktuelle Virensignaturen, Softwareversionen oder den Firewall-Status) an den TNCC melden. In der TNC-Architektur ist vorgesehen, dass mehrere IMCs auf einem AR installiert sein und das diese IMCs auch ihre Statusinformationen an mehrere TNCC melden können.

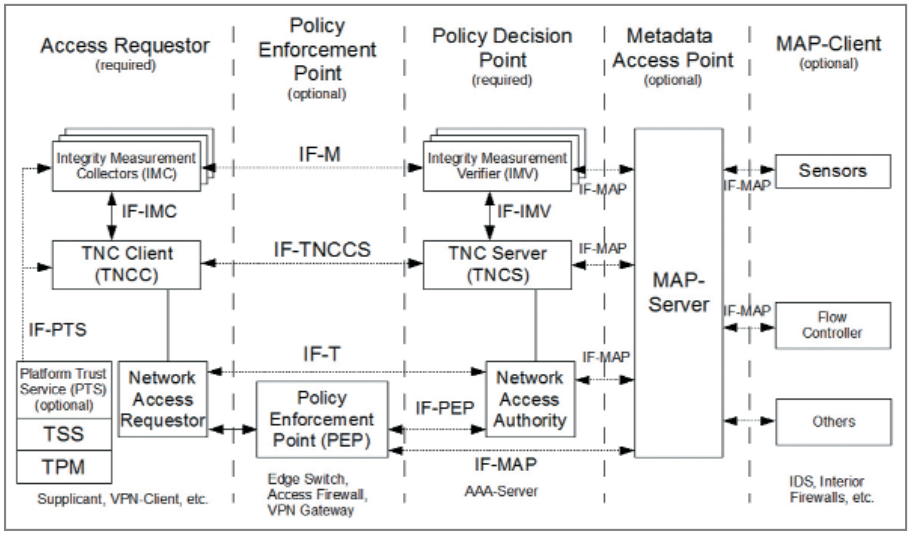

Bild 1: TNC-Architektur (Quelle: Trusted Computing Group: TCG Trusted Network Connect TNC Architecture for Interoperability. Specification Version 1.5, Revision 3, 7. Mai 2012)

- Integrity Measurement Verifier (IMV): Der IMV verifiziert (z.B. mit Hilfe eines Integritätstests) den AR anhand der Daten von den IMCs.

Der MAP-Bereich beinhaltet in der Architektur den MAP-Server (MAPS). Der MAPS speichert und liefert Zustandsinformationen über die Access Requestors (AR). Aufgrund dieser Informationen kann eine Richtlinienentscheidung getroffen und anschließend durchgesetzt werden. Diese Informationen beinhalten Endgeräte- und Benutzeranbindungen, Adressregistrierungen, Authentifizierungsstatus, Übereinstimmungsinformationen über die Endpunktrichtlinien, Endpunktverhalten und Autorisierungsstatus. Weitere Informationen können hinzugefügt werden.

Der MAP-Server ermöglicht Komponenten, die nicht direkt in den Netzzugriffsprozess involviert sind, Richtlinien durchzusetzen. Er ermöglicht es zudem, auch über zusätzliche Komponenten wie Sensoren, die nicht direkt an den AR angebunden sind, Informationen über die Netzaktivität zu veröffentlichen. Diese Zustandsinfor-

mationen könnten wiederum interessant sein für PEP, PDP und andere MAP-Clients (MAPC).
Der MAP-Client veröffentlicht oder konsumiert abschließend die Zustandsinformationen des MAPS über die Access Requestors. Dies wird nicht direkt über die AR vorgenommen, sondern immer über den MAPS hinweg. Der MAPC besteht hauptsächlich aus Flow Controller und Sensor. Während der Flow Controller Entscheidungen zur Netzauslastung vom MAPS durchsetzt, überwacht die Sensorfunktion die Netzaktivität.
Beispiele für Sensoren sind Intrusion-Detection-Systeme (IDS), Antivirensysteme, Layer-3-Überwachung und Applikationsdatenratenscanner. Beispiele für Netzaktivitäten, die von Interesse sein könnten, sind Authentifizierungsaktivitäten, Broadcast-Anfragen für verschiedene Dienste (z.B. DHCP) und die Bekanntmachung von Diensten.

TPM-Anwendungsfallbeispiel

Damit die verschiedenen Einheiten ein höheres Sicherheitsniveau erreichen können, ist als Basis ein Trusted Platform Module (TPM) notwendig. Dies ist ein zusätzlicher Sicherheits-Chip auf der Hauptplatine eines Computers, der kryptografische Schlüssel und Zertifikate speichert, signierte Datenobjekte enthält und Signaturen verifiziert. Der TPM-Chip ist ein passives Element, das erst vom Host-System aktiviert werden muss. Eine Aktivierung erfolgt über entsprechende Applikationen und kann im BIOS auch vom Benutzer jederzeit aus- bzw. eingeschaltet werden.
Bild 2 zeigt die Anwendung von Infineon, die ein zusätzliches virtuelles Laufwerk auf dem Desktop erscheinen lässt. Dieses sog. Personal Secure Drive (PSD) ist verschlüsselt und erscheint nur, wenn man die richtigen Zusatzdaten angibt. Der TPM-Chip kann nun zusätzlich überprüfen, ob es Änderungen an den verschlüsselten Daten gab, die nicht regulär vorgenommen wurden. Das heißt, er überprüft die Integrität der Daten, wodurch eine zusätzliche Sicherheitsstufe erreicht wird.

Neben dem hardwarebasierten TPM-Chip stellt auch die bereits erwähnte BIOS-Erweiterung Core Root of Trust Measurement (CRTM) eine weitere Si-cherheitsfunktionalität zur Verfügung. Sie ermöglicht die Ausführung eines sicheren Boot-Vorgangs und überprüft diesen zusätzlich auf Integrität. Das heißt, der Boot-Vorgang wird mit einer Hash-Funktion gemessen und dann der Messwert sicher im TPM-Chip abgelegt. Dadurch kann man sicher sein, dass man einen sogenannte Secure Boot durchgeführt hat und dass das vorhandene Betriebssystem nicht schon auf der untersten Ebene untergraben wurde. Heutige Betriebssysteme besitzen ohne die TCG-Spe-zifikation diese Möglichkeit nicht, wodurch beispielsweise Virenscanner gegenüber Viren, die unterhalb des Betriebssystems sitzen, machtlos sind.

Bild 2: Benutzerauthentifizierung auf der Infineon-Security-Plattform (Quelle: Infineon)

Dies kann besonders eindrucksvoll anhand von Smartphones demonstriert werden, da diese Geräte ja durchaus kurzfristig in fremde Hände gelangen können. Durch die vorhandene physische Schnittstelle kann ein solches System kompromittiert und mit einer solchen Schadsoftware versehen werden. Der Anwender merkt dies im Anschluss nicht, da das Betriebssystem noch nicht einmal eine Netzverbindung anzeigt. Der Hacker ist dadurch in der Lage, das Smartphone komplett fernzusteuern und alle Informationen, die ihn interessieren, auszulesen.
Um das zu verhindern, ist es wichtig, dass die CRTM-Funktion im Boot-Vorgang des Betriebssystems abgebildet bzw. unterstützt und dass die TPM-Chip-Fähigkeit mit ausgenutzt wird. Eine Anpassung muss allerdings individuell für jedes Betriebssystem erfolgen.

Aussichten für TCG-Spezifikationen

TPMs werden inzwischen von diversen Chip-Herstellern wie z.B. Infineon, Broadcom und Atmel gefertigt. In vielen Laptops und stationären Rechnersystemen sind TPM-Chips auf dem Motherboard vertreten. Leider fehlen solche Chips noch in den meisten heutigen Smartphone-Systemen und Tablet-PCs. Das wäre insofern wünschenswert, weil diese Gerätearten immer leistungsfähiger und zusätzlich stark im beruflichen Umfeld eingesetzt werden. Mit ihnen wird der direkte Zugriff auf Unternehmensdaten ermöglicht, so dass man hier über zusätzliche Schutzmöglichkeiten dringend nachdenken sollte. Die Implementierung eines TPM-Chips würde sich entsprechend anbieten. Leider haben die Marktführer wie Apple und Google aktuell hauptsächlich den Consumer-Markt im Visier.
Nachdem erste TCG-Implementierungen schon fast zehn Jahre her sind, kann die Verbreitung trotzdem immer noch als relativ gering bezeichnet werden. Auch wenn die TPM-Chips bereits in vielen Hardwaresystemen vertreten sind, werden sie doch nur relativ selten eingesetzt. Apple verbaute z.B. auf der Intel-Architektur der MacBooks vorübergehend TPM-Chips, um diese in den aktuellen Modellen dann doch nicht mehr zu berücksichtigen, da anscheinend kein Einsatzfall vorlag. Während in der Forschung das Thema seit etwa drei Jahren angekommen ist und sich diverse Projekte in unterschiedlichen Bereichen mit ihm beschäftigen, z.B. Vogue (**www.vogue-project.de**) und Esukom (**www.esukom.de**), sind praktische Einsätze noch gering. Gerade bei mobilen Endgeräten, die abhanden kommen oder kurzfristig fremdgenutzt werden könnten, ist aber der Einsatz unbedingt zu empfehlen.
Weitere Einsatzgebiete verspricht der noch junge IF-MAP-Standard, der es ermöglichen würde, dass Metadaten unterschiedlicher Komponenten einheitlich zusammengefasst und ausgewertet werden können. Dadurch erhielte man korrelierte Daten, die neue

Informationen über den Sicherheitsstatus eines Systems mit sich brächten. Hersteller wie Juniper Networks, Infoblox oder Enterasys Networks sind gerade dabei, die IF-MAP-Spezifikationen in ihre Produkte aufzunehmen oder bieten bereits Realisierungen an. Zusätzlich gibt es für verschiedene Open-Source-Lösungen bereits entsprechende MAP-Clients, wie z.B. für Android, Snort und Nagios (siehe **www.esukom.de**), wodurch zukünftig mit weiteren Anwendungsfällen zu rechnen ist.

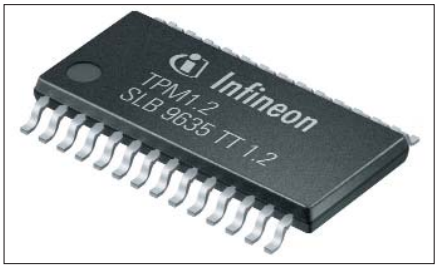

Bild 3: TPM-Chip (Foto: Infineon)

Ein weiteres Hindernis zur Verbreitung von TCG-Spezifikationen könnte aber auch sein, dass die gesamten veröffentlichten TCG-Spezifikationen inzwischen über 1.200 Seiten erreicht haben. Um sich einen Überblick zu verschaffen, ist man daher letztendlich auf externe Literatur angewiesen. Zusätzlich kann ein TPM-Chip bisher nicht auf seine Compliance überprüft werden, also, ob er sich auch an seine Spezifikationen hält. Dies führt in IT-Sicherheitskreisen zu einer gewissen Verunsicherung bzw. Kritik.

Das Schattendasein, das die TCG-Spezifikationen führten, lag aber nicht zuletzt an der Ignorierung durch die führenden Hersteller. Das hat sich inzwischen geändert: Nachdem Microsoft und Cisco Systems zuerst ihre eigenen Wege zur Absicherung von Endsystemen beschritten hatten, traten beide Hersteller der TCG bei und werden nun die Spezifikationen in ihre Produkte einbringen.

Microsoft wird beispielsweise seine Windows-Phone-8-Smartphones zukünftig mit TPM ausrüsten. Die Microsoft-Betriebssysteme Windows Vista und Windows 7 sowie der Windows 2008 Server verwenden den Chip mit der eigenen Laufwerksverschlüsselung BitLocker bereits. Cisco Systems wird seinen bisher proprietären Network-Access-Control-Ansatz (NAC) wohl durch TCG-Spezifikationen standardkonform umsetzen.

Durch den Support dieser Herstellergrößen wird die Verbreitung von TCG-basierten Lösungen stark ansteigen und zusätzliche Anwendungsmöglichkeiten hervorbringen. Man darf also gespannt sein, wie sich das Thema weiter entwickeln wird. *(bk)*