



Trusted Computing Whitepaper

Prof. Dr. Helmut Reimer, TeleTrusT
Markus Linnemann, Institut für Internet-Sicherheit, FH Gelsenkirchen
Michael Hartmann, SAP AG

30.03.2007

Motivation

Ziel dieses Whitepapers ist es, unter den aktuellen und potenziellen TeleTrusT-Mitgliedern ein Grundverständnis der Trusted-Computing-Technologie zu etablieren und mögliche Anwendungsfelder exemplarisch aufzuzeigen. Es dient als Diskussionsgrundlage für den kommenden Trusted-Computing-Workshop der AG2. Im Rahmen des AG2-Workshops sollen zur Vorbereitung auf den IWS (Jährlicher interner TeleTrusT-Workshop) konkrete Betätigungsfelder für TeleTrusT (TTT) im Bereich des Trusted Computing identifiziert werden.

Einleitung

Die Entwicklung im IT-Bereich schreitet um ein Vielfaches schneller voran als beispielsweise in der Automobilindustrie. Die Komplexität aller informationstechnologischen Systeme steigt, getrieben durch immer neue Anforderungen der Informations- und Wissensgesellschaft, ständig weiter an. Dies führt zu einer überproportionalen Erhöhung der Fehleranfälligkeit von Systemen. Diesem Umstand wird durch zahlreiche Patches und Sicherheitsupdates Ausdruck verliehen.

Hinzu kommt die steigende Kriminalität bei Angriffen. Malware wird in Ihrem Funktionsumfang permanent intelligenter und hat ebenfalls die Vorteile der globalen Vernetzung für sich entdeckt. Hinter den Angriffen stehen nicht nur Personen, die Sicherheitslücken aufdecken wollen, sondern vermehrt organisierte Kriminalität.

In diesem Spannungsfeld stellt der Erhalt der Vertrauenswürdigkeit der IT-Infrastruktur eine kontinuierliche Herausforderung dar, da durch die immer stärkere Vernetzung auch vermehrt sicherheitskritische Prozesse elektronisch abgebildet werden.

Im realen Leben bildet sich Vertrauen normalerweise zwischen Personen oder Parteien durch ihr kontinuierlich erwartungskonformes Verhalten heraus. Falls sich die Parteien nicht kennen, werden vertrauenswürdige Dritte herangezogen, die relevante Informationen über die andere Partei geben können. Dies kann im einfachsten Fall die Empfehlung eines Freundes sein, dem wir vertrauen, oder auch die Erklärung einer Institution, die über einen längeren Zeitraum ihre Vertrauenswürdigkeit unter Beweis gestellt hat. Wie z.B. die Stiftung Warentest, die Aussagen über Produkteigenschaften vorgibt, der Staat, welcher Ausweisdokumente herausgibt und so eine Aussage über die Identität einer Person zulässt, oder aber auch der TÜV, der die TÜV-Plaketten für Kraftfahrzeuge vergibt und so eine Aussage über deren Verkehrstauglichkeit macht.

Um das Vertrauen in IT-Systeme zu erhöhen, gilt es, die Vertrauensbeziehungen zwischen den Eigentümern der IT-Systeme (den Personen) auf die IT-Systeme herunterzubrechen. Nach Möglichkeit sollten vertrauenswürdige Beziehungen zwischen Mensch und IT-System genauso etabliert werden, wie zwischen den IT-Systemen untereinander, selbst wenn keine (direkte) Vertrauensbeziehung zwischen den Eigentümern gegeben ist. Hier kann die Trusted-Computing-Technologie einen entscheidenden Beitrag leisten, indem sie die das Verhalten von IT Systemen leichter verifizierbar macht.

TC markiert den Anfang einer neuen Entwicklungsphase. Damit verbunden ist die Tendenz, vorhandenes Know-how wie in vielen Entwicklungsphasen der IT zur Entwicklung von Einzellösungen in den Bereichen Technologie, Infrastruktur, Geräte und Anwendungen zu nutzen. Die jeweilige Einzellösung für sich könnte als „die beste“ Lösung gelten. Die meisten sind allerdings auch proprietär. Interoperabilität von Produkten und Services und damit auch Herstellerunabhängigkeit waren und sind somit nicht gegeben.

Um strukturelle, nicht interoperable Fehlentwicklungen zu verhindern, bietet TeleTrust seine aktive Mitwirkung bei der Entwicklung sicherer IT-Architekturen durch Anwendung einer vertrauenswürdigen Trusted-Computing-Technologie für sichere Geräteplattformen an. Mit ISIS-MTT hat TeleTrust schon einmal eine Erfolgsgeschichte zum Thema Interoperabilität geschrieben. Das gebündelte Know-how der TTT-Mitglieder und vorliegende Forschungs- und Entwicklungsergebnisse können die Anwendung des TC-Konzeptes in Komponenten der heterogenen IT-Infrastrukturen wirksam fördern. Die von TeleTrust stets unterstützten europäischen Lösungsansätze und die Kompetenz der an ihrer Entwicklung Beteiligten bieten eine passende Ergänzung internationaler Konzepte.

Was bedeutet Vertrauen in der IT?

In der Informationstechnologie bildet sich Vertrauen ebenso wie im realen Leben durch kontinuierlich erwartungskonformes Verhalten heraus – allerdings unter geänderten Rahmenbedingungen.

Einem IT-System kann ich z.B. vertrauen, wenn das IT-System von einem vertrauenswürdigen Eigentümer (Person, Institution, o.ä.) kontrolliert wird und dieser auch über die erforderliche technische Kompetenz verfügt, das Verhalten des IT-Systems konform zu meinen Erwartungen zu steuern.

Interessant wird es, wenn ich einem System vertrauen möchte, zu dessen Eigentümer ich (noch) keine solche Vertrauensbeziehung habe oder mir der Eigentümer gänzlich unbekannt ist. Dann muss die Vertrauensbeziehung direkt zum System etabliert werden, welches mich überzeugen muss, dass es sich erwartungskonform verhält, bevor ich seine Dienste in Anspruch nehme. Hier fehlt bisher eine allgemein als vertrauenswürdig akzeptierte Instanz, die eine Aussage über die Eigenschaften des Systems macht.

Durch Technologien wie digitale Signaturen lässt sich zwar eine vertrauenswürdige Kommunikation zwischen zwei sich gegenseitig bekannten Parteien herstellen, aber das Verhalten eines fremden Systems und der vertrauenswürdige Umgang mit Daten lassen sich in herkömmlichen IT-Systemen nicht garantieren.

Systeme der heutigen Generation in Verbindung mit Ihren Betriebssystemen können ein erwartungskonformes Verhalten nicht garantieren, aber durchaus fälschlich vortäuschen. Dies bildet eine potenzielle Gefahr.

Eine nachweisbare Beziehung zwischen System und Anwender – sprich eine Benutzer-Authentifizierung – ist also nicht ausreichend. Für eine entsprechende vertrauenswürdige Beziehung muss eine Geräteauthentifizierung, beziehungsweise Geräteintegritätsprüfung durchführbar sein, die einen Nachweis über ein spezielles Verhalten ermöglicht.

Dieser Schritt ist absolut notwendig, da geschäftliche Beziehungen auch auf einer reinen Gerätekommunikation – ohne den direkten Einfluss von Personen – basieren können und der Lebenszyklus von Daten bestimmbar sein muss.

Ein Beispiel hierfür bilden Web-Services. Nur wenn sich ein Rechnersystem mit seinen relevanten Komponenten authentifizieren kann und dabei einen ermittelten vertrauenswürdigen Zustand nachweist (Integrität), kann gewährleistet werden, dass sich das System so verhält, wie es für eine vertrauenswürdige und sichere Kommunikation notwendig ist.

Vertrauenswürdige Systeme → Trusted Computing

Grundsätzlich sollen die Angebote, die sich durch neue technologische Ansätze ergeben, nicht eingeschränkt werden; insbesondere dann nicht, wenn eine höhere Sicherheit und damit Vertrauenswürdigkeit erreichbar ist. Vielmehr müssen neue Konzepte gefunden werden,

um die neuen Technologien und Infrastrukturen effektiv zu schützen. Vertrauenswürdige Systeme fallen unter das Schlagwort Trusted Computing. In diesem Bereich engagiert sich besonders die Trusted Computing Group (TCG), die mit offenen Spezifikationen Grundlagen für die vertrauensvolle Verarbeitung von Daten auf einer Vielzahl von Plattformen (Mobile, Desktop, embedded, ...) bereits ermöglicht. Einen besonderen Stellenwert besitzt die Spezifikation eines sicheren Hardwarechips, dem so genannten Trusted Platform Module (TPM – im Folgenden auch Sicherheitschip). Dieses Modul ermöglicht einen „Root of Trust“¹ der die Basis für einen „Chain of Trust“² in einem System bilden kann. Dieser TPM-Chip ist heute bereits in der Mehrzahl der neu beschafften IT-Systeme standardmäßig integriert. Dadurch kann kurz- bis mittelfristig von einer flächendeckenden Verfügbarkeit ausgegangen werden. Aktuelle Betriebssysteme und Anwendungen nutzen bereits (wenn auch noch nicht in vollem Umfang) die Möglichkeiten der vorhandenen TPM-Chips.

Ein grundsätzliches Ziel der Anwendung der TPM-Funktionalität ist der Nachweis der Integrität von IT-System-Komponenten zur Unterstützung der Vertrauensbildung. Die Chips selber sind passiver Natur und werden softwareseitig angesprochen. Ein optimaler Einsatz dieser Technologie wird durch vertrauenswürdige Software und Betriebssysteme erreicht. Herkömmliche Betriebssysteme können aufgrund der hohen Fehleranfälligkeit und der ihnen eigenen Struktur (monolithisch oder hybrid) den Ansprüchen an eine solche Sicherheitsplattform nicht genügen.

Zu einem vertrauenswürdigen System gehört also die Kombination von Hardwaremodulen und sicherer Software, um eine Plattformensicherheit zu erreichen, die den bereits heute vorliegenden Anforderungen entspricht.

Funktionalitäten

Als grundlegende Eigenschaft ermöglicht der Sicherheitschip das sichere Registrieren einer Systemkonfiguration, beginnend beim Bootvorgang, wobei der Chip nicht das Messen übernimmt sondern lediglich die Messwerte in seinem Register abgelegt werden. Die Messwerte erstrecken sich vom BIOS über den Bootloader bis hin zu den einzelnen Applikationen. Über Virtualisierungstechnologien ist es in diesem Zusammenhang möglich, die Applikationen oder Betriebssysteme strikt von einander zu trennen. Die Messwerte der relevanten Komponenten, wozu auch Hardwarekomponenten gehören, können nun mit Referenzwerten verglichen werden, die beispielsweise vom Herausgeber festgelegt wurden. Damit kann eine Applikation überprüfen, ob der Zustand des Systems vertrauenswürdig ist, sprich sich gemäß den Vorgaben verhält; oder es kann überprüft werden, ob eine Applikation unverändert und damit vertrauenswürdig ist. Zusätzlich bietet der Chip verschiedene kryptographische Funktionen und einen Schlüsselspeicher. Über einen eigenen Schlüssel lässt sich das TPM direkt identifizieren. Allerdings greifen Mechanismen, die trotzdem datenschutzrechtlichen Ansprüchen genügen.

Wenn beispielsweise ein Anwender dazu verpflichtet ist, die von ihm verantworteten Daten vor fremden Zugriff zu schützen, gilt das auch, wenn er die Daten an ein anderes Rechnersystem übergibt. In diesem Fall ist die Gewissheit darüber, dass die Daten dort ebenfalls sicher und gemäß den eigenen Vorstellungen behandelt werden, eine Grundvoraussetzung. Durch das Binden von Daten an eine zuvor gemessene und definierte Systemkonfiguration können diese nur noch verwendet werden, wenn das System exakt den Zustand aufweist, der für die Verarbeitung der Daten gefordert wird. Diesen Vorgang nennt man Sealing.

Daraus resultiert eine weitere Funktion, die die Beglaubigung der Rechnersystemintegrität gewährleistet. Mit Hilfe dieser so genannten Attestierung kann der Zustand eines fremden Rechnersystems überprüft werden, bevor Daten an dieses System übergeben werden. Die Messdaten des entfernten Systems werden mit den geforderten Werten verglichen. Dies

¹ Wurzel eines vertrauenswürdigen Systems. Die Sicherheit und Vertrauenswürdigkeit wird auf eine Instanz herunter gebrochen, die eine vertrauenswürdige Verarbeitung aller Vorgänge ab dem Startpunkt eines Systems garantiert und kontrolliert.

² Weitere vertrauenswürdige Vorgänge ausgehend vom Root of Trust verbunden zu einer Kette bilden den Chain of Trust. Ein Beispiel bildet der aufeinander aufbauende Bootvorgang eines Systems.

kann beispielsweise über eine Dritte Partei erfolgen. Das System mit den korrekten Messwerten wird Daten exakt so verwenden, wie vom Herausgeber erwartet und damit die Vertrauenswürdigkeit gewährleisten. Über diese Funktion ist eine gegenseitige Authentifizierung von Systemen ohne den Einfluss eines Menschen möglich.

Anwendungsbeispiele

Trusted Computing besitzt besonderes Potenzial beim Einsatz in offenen Netzen, z.B. in Konstellationen wie GRID-Computing, Peer-to-Peer, Web-Services und der Kommunikation zwischen verschiedenen Unternehmen. Hier kann nicht von einem gemeinsamen Sicherheitsniveau als Vertrauensbasis für alle Beteiligten ausgegangen werden. Eine vertrauenswürdige Plattform, auf der sich die beteiligten technischen Komponenten gegenseitig zuverlässig ihre Identität und Konfiguration attestieren, bringt eine für den Erhalt der Vertrauensbasis notwendige Transparenz.

Beim Online-Banking beispielsweise kann der Bankenserver identifiziert und auf Integrität geprüft werden. Server-Angriffe würden anhand der Messwerte der Konfiguration erkannt werden, und als Folge würde der Client keine Verbindung zum Server herstellen.

Auch die traditionellen Client-Server-Beziehungen in Unternehmen entwickeln sich. Der immer stärker ausgebaute Zugriff „von außen“ auf die Unternehmensdaten durch mobile Geräte stellt neue Anforderungen an die Sicherheit der unternehmensinternen Datenhaltung und Kommunikation. Trusted Computing kann hier einen wirksamen Beitrag zur Sicherstellung der Vertrauenswürdigkeit des Gesamtsystems leisten, indem die Identität und integrale Konfiguration externer Geräte zuverlässig überprüft und vom Prüfergebnis der Zugang zum Firmennetz abhängig gemacht werden kann. Wird beispielsweise eine Festplatte aus einem mobilen Gerät gestohlen und mit ihr in einem anderen Gerät der Zugriff auf die Daten der Festplatte oder der Zugang zum Firmennetz versucht, so wird dies erfolglos bleiben. Dies ist nach dem derzeitigen Stand von Wissen und Technik nur in der ursprünglichen, unveränderten Konstellation möglich. Diese einfache Aussage begegnet wirkungsvoll der wachsenden Komplexität des IT-Gesamtsystems und schafft Transparenz als wesentliche Voraussetzung für das Vertrauen.

Daten können durch weitere Softwaremechanismen zusätzliche Regeln für den Umgang mit diesen Daten erhalten. Darüber lassen sich ERM-Funktionen (Enterprise Rights Management) etablieren. Die Anwendungsgebiete für die Trusted Computing Technologie erweitern sich permanent.

Neue Strukturen – Infrastrukturelle Einbindung

Obwohl sich durch die „Direct Anonymous Attestation“ Integritätstests zwischen technischen Komponenten (mit TPMs) auch ohne „vertrauenswürdige dritte Instanz“ ausführen lassen, bieten sich auch PKIs weiterhin für die Überprüfung der Systemintegrität „fremder Systeme“ (mit TPMs) an. Allerdings erfordert die Umsetzung der Trusted-Computing-Konzepte Infrastrukturen mit erweiterten Funktionalitäten.

Zur TC-Technologie gehört neben den TPMs auch vertrauenswürdige Software. Die höhere Sicherheit basiert auf der Kombination von Hardwaresicherheit zusätzlich zur Softwaresicherheit, die entsprechend nutzbar gemacht werden muss.

Um die Technologie möglichst interoperabel und großflächig einsetzen zu können, müssen Migrationsprozesse initiiert werden, die stets auf international verbreiteten und anerkannten Standards beruhen und die möglichst bereits vorhandene Geräte als Beitrag zum Erhalt von Investitionssicherheit mit einschließen. Es muss dabei analysiert werden, welche Global Player eine treibende Rolle für diese Technologie innehaben und welche zusätzlichen Einrichtungen benötigt werden.

TTT kann sich mit seiner langjährigen Erfahrung – beispielsweise mit der European Bridge-CA und mit ISIS-MTT – einbringen, um unternehmens- und organisationsübergreifende Vertrauensbeziehungen, Interoperabilität und Standardkonformität zu unterstützen.

Grenzen und Ergänzungen von Trusted Computing

Trusted Computing hat viel Potential für mehr Sicherheit und Vertrauenswürdigkeit, wird aber nicht uneingeschränkt positiv betrachtet. Die Funktionen insbesondere des TPMs bergen zumindest theoretisch auch Risiken, die a) datenschutzrechtlich bedenklich sind und b) die Diskriminierung von Anbietern zulassen.

Zu a) Jedes TPM ist theoretisch direkt identifizierbar. Damit sind auch dem Anwender seine im TPM gespeicherten Daten eindeutig zuzuordnen. Sind diese Daten hinreichend personenbezogen und damit datenschutzrechtlich relevant, kann dies bei unzulässiger Verwendung zu Datenschutzproblemen führen.

Zu b) Wie bereits dargestellt, funktionieren Anwendungen auf der Basis von TC nur in der zuvor definierten Konstellation. So kann die Verwendung einer bestimmten Software (z.B. Betriebssystem) vorgeschrieben sein.

Umso wichtiger ist die korrekte Zertifizierung dieser Module, die bestätigt, dass sie spezifikationskonform hergestellt wurden. In diesem Punkt muss wieder eine Verbindlichkeit im realen Leben geschaffen werden, damit die positiven Funktionen vertrauenswürdig genutzt werden können.

Die Trusted Computing Technologie ergänzt die bereits etablierten Technologien zur Benutzerauthentisierung (SmartCard, Biometrie, u.ä.) und ermöglicht zu den Aussagen über die Benutzer zusätzlich Aussagen über die verwendeten Systeme, mit denen die Benutzer arbeiten.

Fazit

Trusted Computing Technologien ermöglichen vollkommen neue Vertrauensbeziehungen und erschließen damit permanent neue Anwendungsgebiete. Daten, Beziehungen und Kommunikation können in einem heterogenen Umfeld abgesicherten und so vertrauenswürdig gestaltet werden. Hochschulen und Unternehmen forschen und implementieren diese Technologie bereits.

Die aktuellen Forschungs- und Entwicklungsaktivitäten konzentrieren sich noch stark auf das jeweils individuelle System und den Nachweis der Systemintegrität gegenüber einem anderen System. Großer Gestaltungsspielraum ist noch hinsichtlich Standardisierung von Datenformaten, Services und Infrastrukturkomponenten vorhanden, um Vertrauensbeziehungen zwischen unbekanntem Systemen zu schaffen und diese leicht administrierbar und kostengünstig zu realisieren.

Zum optimalen Einsatz ist es nun notwendig, die Infrastruktur zu schaffen und weitere Anwendungsgebiete zu erschließen.