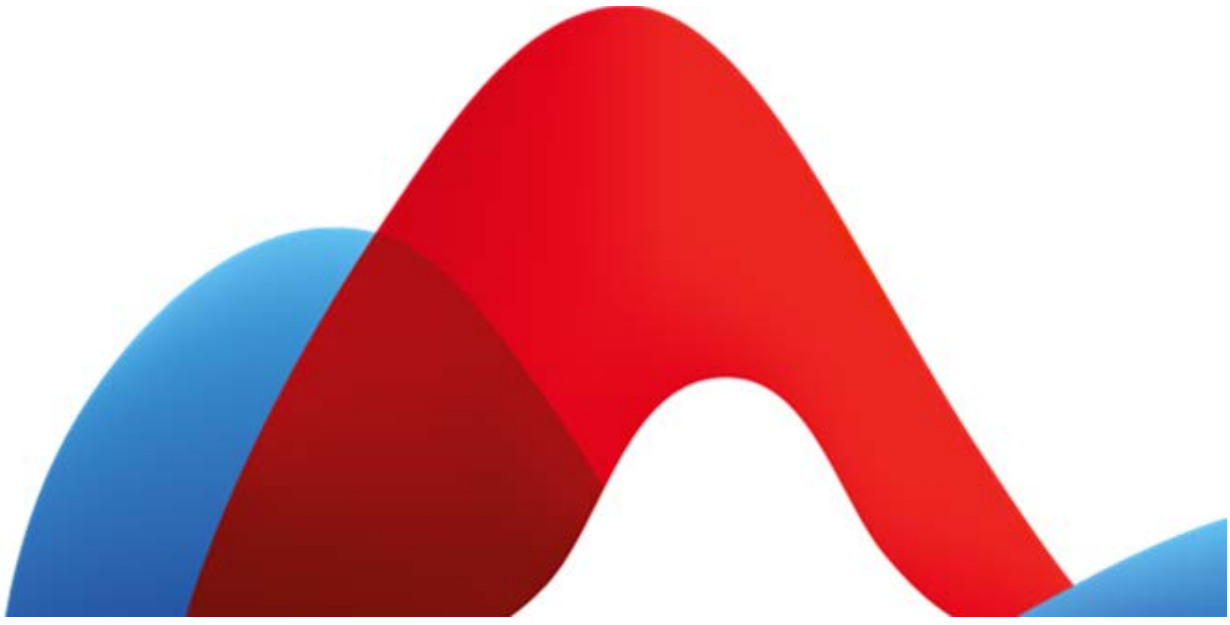
swisscom

Vertrauen und Integrität im Internet der Dinge

Autor
Christof Jungo, Head of Security Architecture, Swisscom AG

Dezember 2015



Inhaltsverzeichnis

Danksagung
Ich möchte mich bei Carolin Latze, Stefan Frei, Martin Rutishauser, Christoph Ernst, Oliver Stampfli, Michael Mäder und Jürg Studerus für ihre Unterstützung bei der Erstellung dieses Dokuments bedanken. Sie haben meinen Text kritisch hinterfragt und selber den einen oder anderen Beitrag geleistet.

1 Integrität und Vertrauen im Internet der Dinge

Dieses Whitepaper präsentiert die Erfahrungen und Einsichten von Swisscom Group Security im Umgang mit dem Internet der Dinge. In Bezug auf die Integrität und das Vertrauen im Internet der Dinge liegt dem Autor an folgenden Feststellungen und Empfehlungen.

1.1 Wichtige Feststellungen

- Im Internet gibt es keine allgemein gültige Möglichkeit, Identitäten zu prüfen
- Der Perimeterschutz wird durch das Ding selbst definiert, extrinsische Sicherheitsmassnahmen sind ressourcenintensiv und nicht praktikabel
- Der Konsument der Dinge hat keinerlei Möglichkeit festzustellen, welche Daten erfasst werden, wem sie gehören und wie diese (weiter-) verwendet werden.
- Die Kombination mehrerer, nicht weiter schützenswerter Informationspakete ergeben unter Umständen schützenswerte Personendaten (z.B. Telemetriedaten eines Herzschrittmachers in Kombination mit dem Namen des Besitzers)
- Der Verbraucher ist heute nicht in der Lage festzustellen, ob die Dinge bereits kompromittiert sind

1.2 Wichtige Empfehlungen

- Ein Umdenken von komplexen, teuren und ineffektiven extrinsischen Sicherheitsmassnahmen zu einfachen, kostengünstigeren intrinsischen Massnahmen muss stattfinden
- Basis-Aufgaben wie sichere Konfiguration, Berechtigungsverwaltung, Softwareaktualisierung und Monitoring werden zunehmend zum Erfolgsfaktor.
- Mit Trusted Computing stehen uns heute bereits technologische Möglichkeiten zur Verfügung um die Integrität und das Vertrauen zu etablieren und auch zu erhalten
- Der Nutzer soll entscheiden, welche der erhobenen Daten er preisgeben möchte.

1.3 Einleitung

Die Steigerung der Lebenserwartung und der Lebensqualität sind zwei wichtige Motivationsfaktoren der Menschheit. Ferner wurden viele Errungenschaften zuerst für militärische Zwecke genutzt, bevor sie der Bildung und Industrie zur Verfügung standen, um anschliessend kommerzialisiert zu werden. Der Zyklus durchläuft grundsätzlich drei Phasen: Lebenserhaltung, Steigerung der Lebensqualität und Unterhaltung. GPS, Mikroprozessoren, Kommunikationsnetze sind nur einige Beispiele für den erwähnten Prozess.
Das Internet durchlief ebenfalls die erwähnten Phasen, jedoch in einer viel kürzeren Zeitspanne. Was früher als militärisches Verteidigungsnetz gebaut wurde, stand später den Universitäten und der Industrie zur Verfügung, bevor es der breiten Masse zugänglich wurde. Das breite Angebot im Internet lässt sich spätestens seit der Einführung des Smartphones auch bequem von überall her und jederzeit konsumieren.
Im Zuge der fortwährenden Miniaturisierung der Elektronik werden immer kleinere leistungsstarke Geräte entwickelt, die messen, überwachen steuern und kommunizieren können. Das Internet der Dinge (IoT) hält dadurch Einzug in alle Bereich unseres Alltags, wie die nachstehende Tabelle zeigt.

	IoT Controller	Basisplattform zur Entwicklung neuer Services.
	Wearables	Einsatz im Fitness und Sportbereich zum Erfassen verhaltensbasierter Daten (Puls, Schritte, Route).
	Medizinische Systeme	Steuerung medizinischer Hilfssysteme anhand erfasster Gesundheitsdaten (Herzschrittmacher, Insulinpumpe, Hörgeräte).
	Systeme für die Geschäftsoptimierung	Verbesserung der Genauigkeit der Lagerverwaltung unter Verwendung von RFID-Daten. Durchführen von sicheren Finanztransaktion.
	Smart Grid / Smart Meter	Intelligente Systeme zur Überwachung und Steuerung der Umgebung (Strom, Temperatur).
	Connected Car, Industrie Sensoren	Integrierter Vernetzung und Steuerung zur Vorhersage von Komponentenausfällen basierend auf Sensordaten sowie Optimierung der Systemeinstellungen (Fahrwerk).

Tabelle 1 - IoT Kategorien

1.4 Veränderung der Rahmenbedingungen

Mit dem Aufkommen des Internets der Dinge wird der Benutzer zunehmend Aufgaben auch gezielt an Geräte delegieren wollen, die mit ihm in Beziehung stehen (Auto, Smartphone, Smart Meter, etc.). In der Industrie übernehmen die Controller vermehrt die Steuerung komplexer Systemabläufe und werden dadurch auch anfälliger und interessanter für Angriffe.
Jedes neu angeschlossene Gerät erhebt Monitoring und Messdaten. Können diese in Zusammenhang zu einer Person gebracht werden – wie bspw. Bewegungsdaten, Gesundheitsdaten, Einkaufsverhalten, etc. -, entstehen sensitive Personendaten. Es ist davon auszugehen, dass das Bedürfnis nach vertrauenswürdigen Geräten massiv zunehmen wird.
Zudem ist die Frage bezüglich des Besitzers der Daten zu klären. Wenn beispielsweise ein Bauunternehmer einen Bagger mit Sensoren ausstatten und Leistungsmerkmale messen will, wem gehören die Daten? Dem Bauunternehmer, der den Bagger benutzt, dem Baggerhersteller oder beiden? Bei den Wearables (AppleWatch, Fitbit) tritt der Benutzer -entsprechenden den allgemeinen Geschäftsbedingungen – das Nutzungsrecht an den Hersteller ab. Ist dem Benutzer dies bewusst?
Die Kontrolle über „meine“ Daten – wo immer sie sind, wie immer sie entstehen, wer immer sie generiert – wird entscheidend sein. Der Nutzer wird selber bestimmen wollen, unter welcher digitalen Identität er einen ICT-Service nutzt und mit wem er seine Daten teilt. Dieser Wunsch wirft zwangsläufig die Frage der Sicherheit und Integrität der einzelnen Dinge auf.

Mit den Dingen ändert sich die Art der Kommunikation fundamental. Das Verständnis des klassischen Perimeterschutzes, (zum Beispiel mit einer Firewall), der von einer geschützten Innenwelt und der ungeschützten Aussenwelt ausgeht, verschwindet. Es weicht dem Bild eines Perimeters, der durch die Objekte selbst definiert ist. Somit hat jedes Objekt für seinen eigenen Schutz zu sorgen.

Verglichen mit einem typischen Unternehmensnetzwerk stellt IoT einzigartige Sicherheitsherausforderungen, darunter auch die folgenden:

Herausforderung	Beschreibung
Eine beispiellose Anzahl und Vielfalt von Geräten verunmöglichen eine zentrale Verwaltung und ein homogenes Umfeld.	Vielen Geräten fehlt die Rechenleistung oder Speicherkapazität, um grundlegende Authentifizierung und Autorisierung zu unterstützen.
Unbeaufsichtigte und nicht verwaltete Geräte , die nur schwierig oder gar nicht physisch zu erreichen sind, um sie zu aktualisieren.	Potentielle Sicherheitsrisiken, die sich ergeben, wenn der Zugriff irrtümlicherweise verweigert bleibt. (z.B.: bei Blaulicht-Organisationen).
Geräte, die jahrelang im Betrieb sein werden und der Lieferant stellt nur selten oder nie Updates zur Verfügung.	Software-only- Sicherheitsmechanismen mit begrenztem Umfang von Sicherheitsfunktionen.
Missbrauch der Identität eines Dings.	Dinge können sich als andere Dinge ausgeben, Betriebsabläufe beeinträchtigen und unberechtigten Zugang zu geschützten Daten erlangen.

Tabelle 2 - Sicherheitsherausforderungen im IoT Umfeld

1.5 Warum wir heute nicht sagen können, ob wir sicher sind

Die Kommunikation im Internet basiert auf implizitem Vertrauen. Es gibt keinerlei gegenseitige Überprüfung der Echtheit der Identität. Der Benutzername und das Passwort reichen in den meisten Fällen für die Authentisierung aus. Wir können davon ausgehen, dass mit der Zunahme der Anzahl der Teilnehmer – und auch des damit einhergehenden Missbrauchs durch Cyberkriminelle – die Vertrauensstellung untereinander an Wichtigkeit gewinnen wird. Die Fragen wer ist wer und wem vertraue ich rücken ins Zentrum.
Die NSA-Affäre rund um die Enthüllungen von Edward Snowden zeigt, dass neben kriminellen Organisationen auch Regierungsbehörden versuchen, mit immer besseren Angriffsmethoden Geräte unter ihre Kontrolle zu bringen. Es ist bekannt, dass es Hintertüren in der Firmware von Hardwarekomponenten wie z.B. Festplattenkontroller[1], Graphikkontroller oder Netzwerkkarten gibt. Gleichzeitig sind die Möglichkeiten für den Endverbraucher sich selber zu schützen stark eingeschränkt. In der Schlussfolgerung können wir davon ausgehen, dass immer mehr Geräte – welche in unserem Besitz sind – nicht mehr unter unserer Kontrolle sind (Viren, Botnetze, Spionage etc.). Um dieser Situation Herr zu werden, wurden in der Vergangenheit verschiedene Initiativen gestartet, um eine Kompromittierung der Systeme zu verhindern.

[1] http://arstechnica.com/information-technology/2015/02/how-hackers-could-attack-hard-drives-to-create-a-pervasive-backdoor/

Initiative	Problem
Signierung von Applikationen und Treibern	Hersteller signieren ihre Applikationen oder die zugehörigen Softwarebibliotheken nicht. Es gibt keine einfache Möglichkeit herauszufinden, ob wir eine authentische Software einsetzen oder eine manipulierte Version.
Signierung von Firmware BIOS, Festplatten, Graphikkarten, Netzwerkkontroller	Jeder Hersteller verwendet seine eigene Signierungsmethode. Es gibt nur selten öffentlich zugängliche Dokumentation zum Signierungserfahren und Möglichkeit für Dritte, die Signatur zu prüfen.
Signaturschlüssel	Public Key Infrastructure (PKI) gehen von einer sicheren Zertifizierungsstelle und vertrauenswürdigen Zeichnern aus. Die Realität hat gezeigt, dass dies eine falsche Annahme ist: - Es gibt keine Möglichkeit zu überprüfen, ob eine Datei von derjenigen Person / Firma signiert wurde, auf welche der Schlüssel ausgestellt wurde. (Zum Beispielkönnte eine Regierungsbehörde oder eine kriminelle Organisation eine Software signieren.) - Angreifer haben Zertifizierungsstellen in der Vergangenheit gehackt (DigiNotar[2], Verisign[3], Comodo[4], Gemalto[5]) und Software-Signaturschlüssel gestohlen. - Es gibt hunderte von Zertifizierungsstellen, welche nicht alle den gleichen Standards folgen. Die Überprüfung der Integrität all dieser Stellen ist unmöglich. Die neue Annahme besteht darin, dass - Codesignaturschlüssel von vielen Softwareanbietern und Zertifizierungsstellen bereits wissentlich oder unwissentlich entwendet wurden - es keine Möglichkeit der unabhängigen Überprüfung von verlorenen Schlüsseln gibt.

Tabelle 3 – Bisherige Initiativen

Trotz aller Sicherheitsmechanismen ist es somit in IT-Infrastrukturen nahezu unmöglich zu bestimmen, ob ein System kompromittiert wurde. Es ist auch praktisch unmöglich, ein infiziertes System zu säubern, da wir nicht wissen, auf welcher Ebene das System infiziert wurde. Ein blosses Neu-Aufsetzen des Betriebssystems nützt nichts, wenn beispielsweise die Firmware des Festplattencontrollers infiziert wurde. Es fehlt ein vertrauenswürdiger Ankerpunkt.

[2] https://en.wikipedia.org/wiki/DigiNotar
[3] https://www.schneier.com/blog/archives/2012/02/verisign_hacked.html
[4] http://www.infoworld.com/article/2623707/hacking/the-real-security-issue-behind-the-comodo-hack.html
[5] http://www.pcmag.com/article2/0,2817,2477363,00.asp

1.6 Wie entsteht Vertrauen?

Vertrauen in zwischenmenschlichen Beziehungen gründet auf der Annahme, dass mir als Individuum nichts zustösst. Ich fühle mich geschützt und geborgen. Dies ist eine reine Sinneswahrnehmung und manifestiert sich erst über die Zeit faktisch in Form von Erlebnissen und Erfahrungen. Das Vertrauen muss folglich aufgebaut und gepflegt werden. Es ist jedoch fragil und kann mir nur einer einzigen negativen Erfahrung zerstört werden.

Übertragen wir dieses Verhalten auf die Sicherheit des Internets der Dinge, so lassen sich folgende Grundsätze ableiten.

a) Identität

   Das Vertrauen ist immer an eine Identität gebunden. Jedes Ding braucht somit eine eineindeutige nicht veränderbare Identität. Es muss sich jederzeit ausweisen können.

b) Positive Absicht

   Das Ding und der gekoppelte Service haben eine positive Absicht. Wenn ich im vornherein schon weiss, dass ein Ding mich direkt oder indirekt schädigt, werde ich es nicht einsetzen (manipulierter Herzschrittmacher, Überwachungsgeräte, welche Daten an Fremde schicken).

c) Vorhersehbarkeit und Transparenz

   Der Funktionsumfang des Services, welcher das Ding anbietet, ist vollumfänglich bekannt. Es gibt keine nicht dokumentierten (geheimen) Funktionen. Die Verhaltensweise des Systems kann jederzeit durch unabhängige Dritte überprüft werden. Unterlaufen Fehler (wie Softwareschwachstellen), so wird eine transparente Aufklärung und Behebung (Coordinated Disclosure[6]) erwartet, damit wir das Vertrauen in den Hersteller nicht verlieren. Versuchte Manipulationen, wie das Fälschen der Abgaswerte bei Volkswagen,[7] führen zum Vertrauensverlust mit enormen ökonomischen Schäden.

d) Reputation

   Je mehr positive Interaktionen es zwischen den Dingen gibt, desto mehr bildet sich ein intelligentes Netzwerk basierend auf Reputation. Die Grundlage für die Feststellung der Vertrauenswürdigkeit und der Reputation ist die Kombination der nachstehenden Punkte:

   - ein Bewertungssystem analog Tripadvisor, Trivago oder HolidayCheck basierend auf Erfahrungen und Meinungen der Gemeinschaft
   - ein technisches Bewertungssystem wie es heute für die Reputation von Domain Name Server und E-Mail Server verwendet wird
   - eine systematische technische Überprüfung durch unabhängige Sicherheitsexperten

e) Kontinuität

   Hersteller, für welche diese Grundsätze Teil ihrer Firmenkultur sind und dies über eine längere Zeit praktizieren, werden in der Gesellschaft als vertrauenswürdig wahrgenommen. Vertrauen wird über Zeit durch authentisches Verhalten erarbeitet.

---

[6] http://www.nzitf.org.nz/pdf/NZITF_Disclosure_Guidelines_2014.pdf
[7] http://www.spiegel.de/auto/aktuell/volkswagen-skandal-durch-gefaelschte-abgaswerte-a-1054193.html

1.7 Von Sicherheitsprodukten zur Produktesicherheit

Heutige IT-Systeme sind ein Verbund von Hardware und Software mit dem Ziel, einen Service so effizient wie möglich anzubieten. Die IT-Industrie hat eine umfassende und komplexe Lieferkette unterschiedlicher Komponenten, wie Design und Fabrikation von Computerchips, Computersysteme, BIOS, Controller Firmware, Betriebssystem, Treiber, Applikationen und Datenbanken. Dazu kommen eine Vielzahl dynamischer Prozesse, wie Datenaustausch mit anderen Systemen, Internetverbindungen, automatische Softwareupdate usw. Der Sicherheitsgrad des Systems wird durch das schwächste Glied in der Kette bestimmt. Ein Sicherheitsdispositiv sollte folglich in der Lage sein, die gesamte Lieferkette zu sichern.

In der heutigen Bauweise der IT-Systeme liegt der Fokus in der Funktionalität und der Verfügbarkeit im Sinne der Ausfallsicherheit. Der Schutz der IT-Systeme und der darauf gespeicherten Daten ist keine Kernaufgabe der Applikationen und wird deshalb an ein Sicherheitsprodukt delegiert. Bei diesem extrinsischen Ansatz, werden zusätzliche Sicherheitskomponenten auf dem Gerät installiert oder aber eine Schutzhülle um das System gebaut. Zum Einsatz kommen Anti-Malware-Software, um IT-Systeme vor bekannten Bedrohungen (Schadsoftware, Spam, usw.) zu schützen oder Zonierungen mittels Firewalls und Application Level Gateways. Wir vertrauen darauf, dass die Produkte nach besten Wissen und Gewissen ihre Aufgaben erfüllen.

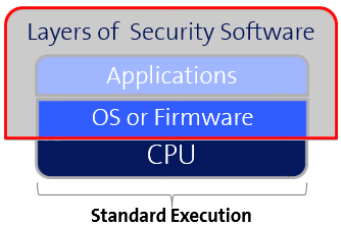


Abbildung 1 Gerät mit extrinsischer Sicherheit

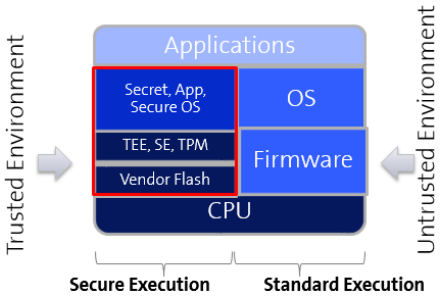


Abbildung 2 Gerät mit intrinsischer Sicherheit

Die Geschichte der Cyberkriminalität zeigt uns auf eine eindrückliche Weise, dass der extrinsische Ansatz –wie oben beschrieben – gravierende Schwächen hat. Er kann die Komplexität der Lieferkette nicht abbilden. Im besten Fall sichert er einzelne Bereiche daraus. Würde er funktionieren, so könnten wir jederzeit die Integrität eines Systems prüfen und wiederherstellen. Viren, Trojaner und sonstige Schadsoftware wären keine Bedrohung mehr. Die Sicherheitsindustrie versucht den Verbraucher vor immer komplexeren Attacken zu schützen, während die Basisintegrität der Plattform unberücksichtigt bleibt.
Dies Vorgehen ist ungenügend und ineffizient, denn wir wissen seit geraumer Zeit, dass Virenerkennung[8] mittels statischen Signaturen nur bereits bekannte Malware reaktiv erkennt und einfach zum Umgehen ist. Das proaktive Erkennen neuer Malware ist extrem ressourcenintensiv und von einer hohen Rate von Fehlalarmen (false positives) geprägt. Beide Ansätze schützen nicht vor bereits bei Lieferung eingebauter Malware oder Hintertüren.

[8] http://techzoom.net/Publications/Papers/failurecorrelation
http://www.forbes.com/sites/andygreenberg/2010/08/17/study-shows-programs-designed-to-catch-hackers-exploits-miss-nearly-half/

Das Kernproblem des fehlenden vertrauenswürdigen Ankerpunkts existiert nicht erst seit dem Internet der Dinge. Es ist bei jedem IT System – Mobiltelefon, Serversystemen, Laptop, Desktops, Host – vorhanden. Bis anhin konnte es mit extrinsischen Sicherheitsmassnahmen überlagert werden, da genügend Performance vorhanden war. Ressourcenintensive Sicherheitsprodukte sind auf IoT-Geräten schwieriger realisierbar, da die Ressourcen der Funktion des Dings zur Verfügung stehen sollen bei gleichzeitig geringem Stromverbrauch.

Ein Umdenken in der Industrie ist gefordert. Die Sicherheit und Integrität darf nicht weiter an eine externe Stelle delegiert werden, sondern muss Bestandteil jedes Elements der Lieferkette werden.
Bei der intrinsischen Sicherheit hat jedes IT-System für sich die Möglichkeit, jederzeit seine Integrität zu prüfen. Sollte die Prüfung fehlschlagen, so muss ein Selbstheilungsprozess ausgeführt werden, welcher das System wieder in einen definierten Zustand zurückführt. Alternativ kann genügend Redundanz aufgebaut werden, so dass ein bei der Prüfung durchgefallenes s System durch ein neues ersetzt werden kann.
Um die Integrität der kompletten Lieferkette eines Systems zu prüfen, ist der Hersteller gefordert Sicherheitsfunktionen nachvollziehbar für Dritte einzubauen. Jeder Hersteller bestätigt anhand von fälschungssicheren Signaturen, welche auf seiner Webseite publiziert sind, dass eine bestimmte Komponente (Hardware oder Software) durch ihn hergestellt wurde. Die Komponente entspricht dem vordefinierten Funktionsumfang und enthält keine undokumentierten Funktionen. So kann festgestellt werden, ob bei Erhalt der Lieferung, bei jedem Systemstart oder bei einem Sicherheitsvorfall authentische Hardware und Softwarekomponenten vorhanden sind oder eingesetzt wurden.

Ebene	**Geforderte Sicherheitsfunktion**
Identität	Jedes IT-System muss mit einer fälschungssicheren eineindeutigen Identität mittels Zertifikaten ausgestattet werden. Die Zertifizierungsstellen müssen höchsten Ansprüchen entsprechen.
Prozessoren und Controller	Feststellung und Bestätigung der Echtheit / Authentizität des Prozessors und der Controller für Memory, Graphikkarte, Storage, Peripherie (USB, etc.), Kommunikation (Ethernet, WLAN, Bluetooth, GSM, etc.).
BIOS / UEFI und Controller Firmware	Feststellung und Bestätigung der Echtheit der Softwareversion für BIOS / UEFI, Graphikkarte, Storage, Peripherie und Kommunikation
Betriebssystem, Treiber, Middleware und Applikationen	Feststellung und Bestätigung der Echtheit der Softwareversion.

Tabelle 4 Prüfen der Integrität

Mit Secure Boot und Remote Attestation stehen uns die entsprechenden Möglichkeiten zur Verfügung, diese erste Prüfung der Integrität sicherzustellen. Die Hauptaufgaben, welche durch die Trusted Computing Group definiert wurde sind:

- Die Bestätigung der Echtheit der Hardwareplattform und der verwendeten Systemsoftware / Firmware
- Sicher stellen, dass ein authentisches (echtes, nicht manipuliertes) Betriebssystem in einer vertrauenswürdigen Umgebung startet, um dann selber vertrauenswürdig zu werden
- Bereitstellen zusätzlicher Sicherheitsfunktionen auf einem vertrauenswürdigen Betriebssystem, welche ansonsten nicht zur Verfügung stehen

Diese Technologie verwendet ein Trusted Platform Module (TPM)[9]. Ein TPM Chip stellt eine überprüfbare Identität und das sichere Ausführen von kryptographischen Funktionen, so wie das sichere Hinterlegen von Schlüsseln zur Verfügung. Verschiedene Hersteller wie Intel, Infineon, Atmel oder NXP bieten entsprechende Module an.

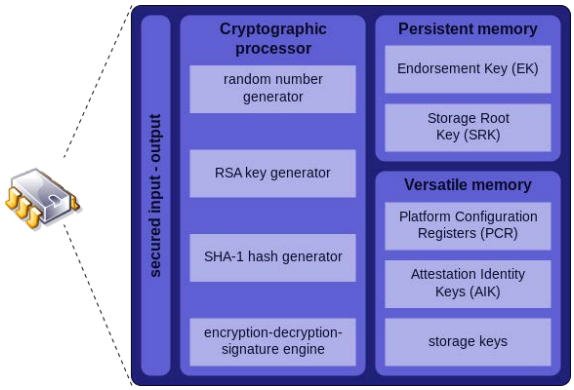


Abbildung 3 Trusted Platform Module v1.2 [10]

Durch die Verwendung eines TPM Chips kann auf der untersten Stufe sichergestellt werden, dass das System nur mit authentischer Hardware und Firmware[11] betrieben wird. Schlägt die Überprüfung fehl, so startet das System nicht und es wird ein Fehler ausgegeben. Im Anhang Attestierung ist der Startprozess skizziert. Dieser Attestierungsprozess kann entlang der gesamten Serviceerbringungskette stattfinden – durchgängig von der Überprüfung der Hardware bis hin zu Service Applikationen.

[9] https://en.wikipedia.org/wiki/Trusted_Platform_Module
[10] https://en.wikipedia.org/wiki/Trusted_Platform_Module#/media/File:TPM.svg
[11] http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf

1.8 Was tut Swisscom?

Das Internet der Dinge ist immer noch in den Kinderschuhen. Unternehmenskunden und Endbenutzer beginnen erst zu verstehen, welche Vorteile das Internet der Dinge bietet. Die Auswirkungen auf die Sicherheit sind weitestgehend unbekannt. Das Internet der Dinge, geniesst derzeit ein hohes Interesse – das Auftreten von signifikanten Sicherheitsvorfällen ist nur eine Frage der Zeit.

Bis Trusted Computing im Internet der Dinge zu einem festen Bestandteil geworden ist, arbeitet Swisscom mit IoT Gateways, um wichtige Industrie - Controller zu schützen. Die IoT Gateways haben die entsprechende Rechenleistung, damit extrinsische Sicherheitsfunktionen wie beispielsweise Firewalls angeboten werden können.

Swisscom ist aktives Mitglied der Trusted Computing Group (TCG)[12] und befasst sich seit Jahren mit dem Thema Trusted Computing. In einer intensiven Entwicklungszusammenarbeit mit Intel und Universitäten aus dem In- und Ausland hat Swisscom diesen Ansatz für Serversysteme industrialisiert. Swisscom setzt diese Technologie erfolgreich in der Cloud-Infrastruktur ein.

Die Sicherstellung der Identität und Integrität von IoT-Geräten, sowie die Sicherheit ihrer Datenspeicherung und Kommunikation werden zum zentralen Erfolgsfaktor. Nur damit können Unternehmen und Verbraucher von den Möglichkeiten des Internets der Dinge profitieren ohne unnötige Risiken einzugehen.

[12] http://www.trustedcomputinggroup.org

2 Anhang

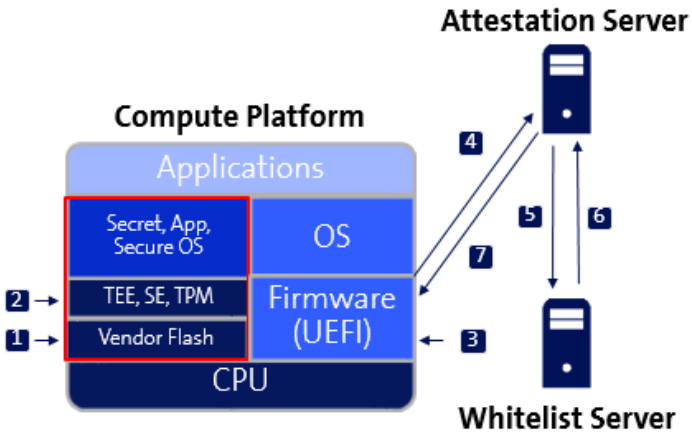
2.1 Glossar

Attestierung von Produkten	Die qualitativ einwandfreie Beweisbarkeit, Identifikation, Rückverfolgbarkeit und Dokumentation der Produkte.
Authentizität[13]	Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein.
Application Level Gateway[14]	Das Application Layer Gateway (auch bekannt unter den Namen ALG oder Application-Level Gateway) stellt eine Sicherheitskomponente in einem Computernetzwerk dar.
Controller[15]	Als Controller (englisch für Steuergerät oder Steuereinheit) werden elektronische Einheiten der Computer-Hardware bezeichnet, die bestimmte Vorgänge steuern.
Integrität[16]	Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.
IoT	Internet of Things, Internet der Dinge
Kompromittierung[17]	Ein System wird als kompromittiert betrachtet, wenn Daten manipuliert sein könnten und wenn der Eigentümer (oder Administrator) des Systems keine Kontrolle über die korrekte Funktionsweise oder den korrekten Inhalt mehr hat, beziehungsweise ein Angreifer ein anderes Ziel der Manipulation erreicht hat.
Malware[18]	Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und Malware werden häufig synonym benutzt. Malware ist ein Kunstwort, abgeleitet aus "malicious software" und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen.
Zertifizierungsstelle für digitale Zertifikate	In der Informationssicherheit ist eine Zertifizierungsstelle (englisch certificate authority oder certification authority, kurz CA) eine Organisation, die digitale Zertifikate herausgibt.

[13] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html
[14] https://de.wikipedia.org/wiki/Application_Layer_Gateway
[15] https://de.wikipedia.org/wiki/Controller_(Hardware)
[16] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html
[17] https://de.wikipedia.org/wiki/Technische_Kompromittierung
[18] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html

2.2 Attestierung

Der Attestierungsprozess sieht vor, dass die Compute Platform erst den TPM Chip initialisiert, um anschliessend die entsprechenden Hardware und Software zu überprüfen. Das nachstehende Prinzipschema zeigt den Ablauf einer Attestierung.



1. Intialisierung des Hersteller-Programms
2. Microcode intialisiert Startsequenz
3. Protokollierung der Startsequenz im TPM Modul inkl. Protokollsignierung. Mittels Launch Control Protocol (LCP) und den Werten im TXT[19] kann das System bereits in der Startphase angehalten werden.
4. Nach erfolgreichem Start des Betriebssystems wird die Protokollsignatur mit der Attestierungsstelle synchronisiert
5. Attestierungsstelle gleicht Signatur mit Referenzwerten ab
6. Integrität des Systems ist bestätigt oder widerlegt
7. Integrität geprüft oder System wird logisch aus dem Netzwerk entfernt

Abbildung 4 - Attestierungsprozess für die Startsequenz eines Systems

Auf Stufe des Betriebssystems können dieselben Tests durchgeführt werden wie auf Stufe der Hardware. Betriebssystemkomponenten wie Betriebssystemkern (Kernel) und seine Treiber wie auch Treiber von Drittanbietern für Graphikkarte, Peripherie oder Storage können somit überprüft und bestätigt werden.

[19] Trusted Execution Technologie (TXT) http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/malware-reduction-general-technology.html