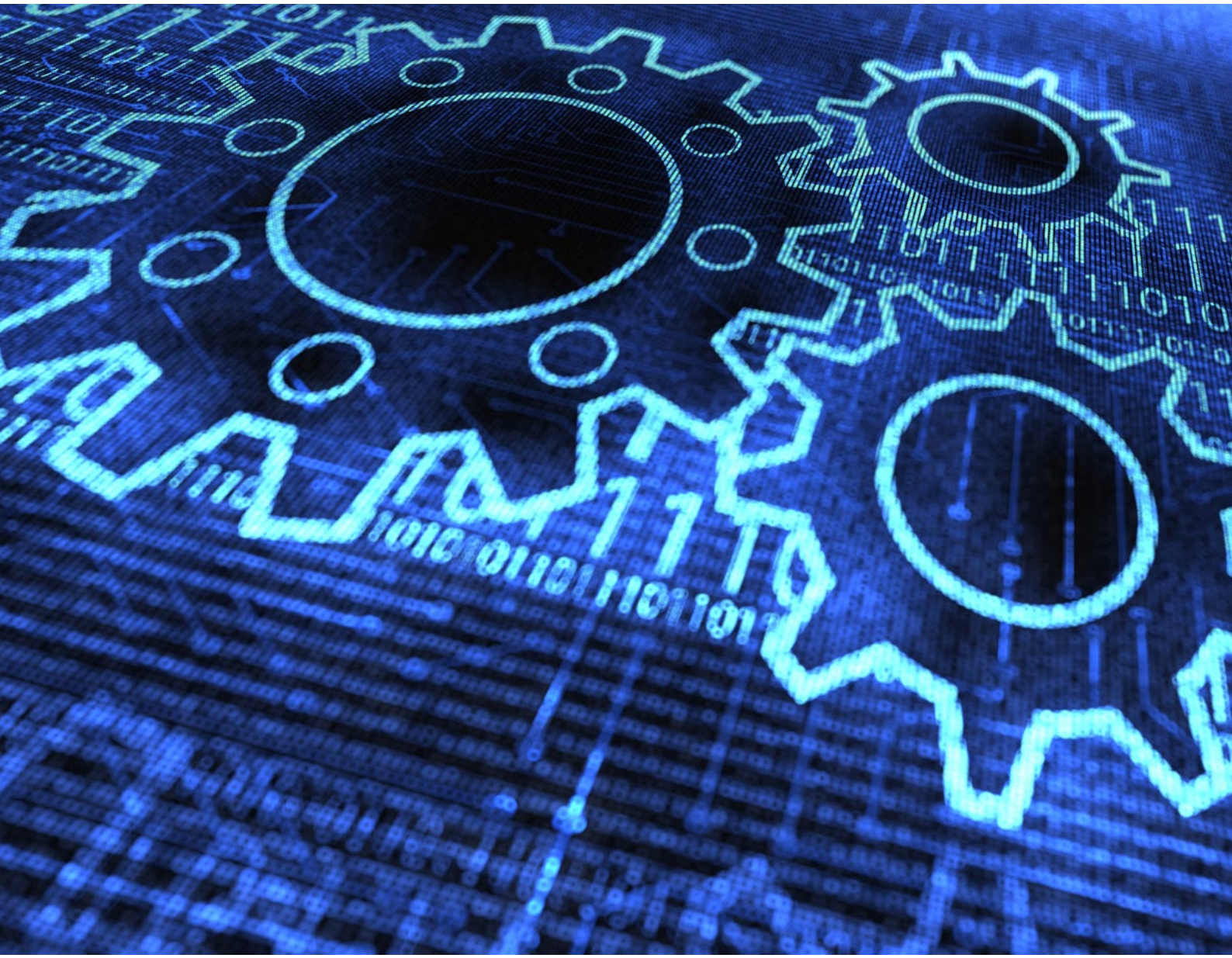
Positionspapier | Task Force

GERÄTEIDENTITÄT UND -INTEGRITÄT IM INTERNET DER DINGE



April 2017

Fraunhofer SIT

VDE

Positionspapier | Task Force

GERÄTEIDENTITÄT UND -INTEGRITÄT IM INTERNET DER DINGE

20. April 2017

Kontakt

Andreas Fuchs
andreas.fuchs@sit.fraunhofer.de

Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75, 64295 Darmstadt

Christian Seipel
christian.seipel@vde.com

DKE Deutsche Kommission Elektrotechnik
Elektronik Informationstechnik in DIN und VDE,
Stresemannallee 15, 60596 Frankfurt am Main

Taskforce Mitglieder

Bernecker, Dr. Otto		München
Bluschke, Andreas	Teleconnect	Dresden
Fuchs, Andreas	Fraunhofer SIT	Darmstadt
Haas, Dr. Christian	Fraunhofer IOSB	Karlsruhe
Harner, Andreas	VDE	Frankfurt am Main
Hartmann, Prof. Dr. Andreas	Hochschule Leipzig	Leipzig
Hartung, Prof. Dr. Frank	Fachhochschule Aachen	Aachen
Hohmuth, Michael	Kernkonzept	Dresden
Jänicke, Dr. Lutz	PHOENIX CONTACT	Blomberg
Katzenbeisser, Prof. Dr. Stefan	Technische Universität Darmstadt	Darmstadt
Kranawetter, Michael	Microsoft Deutschland	Unterschleißheim
Li, Prof. Dr. Quingdang	Qingdao University of Sience	LAOSHAN DISTRICT QUINGDAO
Polian, Prof. Ilia	Universität Passau	Passau
Rolfes, Carsten	Fraunhofer AISEC	Garching
Schanz, Dr. Volker	VDE	Frankfurt am Main
Schnabel, Dr. Ronald	VDE	Frankfurt am Main
Seewald, Maik	Cisco	Hallbergmoos
Seipel, Christian	DKE	Frankfurt am Main
Sikora, Prof. Dr. Axel	Hochschule Offenburg	Offenburg
Sporer, Dr. Thomas	Fraunhofer IDMT	Ilmenau
Stock, Arno	Renesas Electronics	Düsseldorf
Theuerkauf, Klaus	ifak	Magdeburg
Walz, Andreas	Hochschule Offenburg	Offenburg
Wichert, Dr. Reiner	AHS	Weiterstadt
Wieland, Prof. Dr. Sabine	Hochschule Leipzig	Leipzig
Wiggers, Rainer	Vattenfall Europe	Berlin
Wirth, Michael	Microsoft Deutschland	Köln

Inhalt

Kurzdarstellung

Durch die Entwicklung des Internets der Dinge und der in diesem Zusammenhang zunehmenden Vernetzung cyber-physischer Geräte in privaten und öffentlichen Bereichen steigen die Anforderungen an die Informationssicherheit (Security) eingebetteter Systeme maßgeblich. Ein effektiver Schutz vor Missbrauch und Cyberattacken kann nur gewährleistet werden, wenn die Einzelgeräteechtheit gesichert ist. Die Einzelgeräteechtheit umfasst die Identität und Integrität eines Geräts als Komposition von Hardware, Software und Betriebsparametern. Vor diesem Hintergrund wurde die Taskforce „Sichere Geräteidentität und -integrität im Internet der Dinge“ gegründet. Das Ziel der Taskforce ist, die Verbreitung der notwendigen Technologien zu fördern, indem in einem gemeinsamen Forum über die Grenzen der verschiedenen Anwendungsdomänen (z.B. Energie- und Industrieautomation, Verkehrsleittechnik, E-Mobility, Smart-Cities, Industrie 4.0 und weitere) hinweg eine gemeinsame technologische Basis geschaffen wird, die in allen Anwendungsdomänen ein- und umgesetzt werden kann. Das Positionspapier gibt einen Überblick über die Ziele, die sich hierbei ergebenden Anforderungen und Herausforderungen und Potenziale.

1. Einleitung

Zu seinem Amtsantritt im Jahr 2001 ließ sich US-Vizepräsident Dick Cheney die Fernsteuerungsfunktion seines Herzschrittmachers deaktivieren [1]. Dies tat er wohl aus berechtigter Sorge, denn mit dieser Fernsteuerungsfunktion gehen viele Möglichkeiten einher, das Gerät unautorisiert und ohne Wissen oder Mitwirken seines Besitzers zu manipulieren [2].

Im Falle eines Herzschrittmachers sind die Auswirkungen eines Angriffes sehr offensichtlich. Für andere Kleinstcomputer, wie sie mittlerweile massenweise in allen denkbaren Bereichen zum Einsatz kommen, wird die Gefahr jedoch häufig nicht im gleichen Maße wahrgenommen. Dabei zeigt eine ganze Reihe von Cyberattacken auf und durch das sogenannte Internet der Dinge, dass Angriffe auf eingebettete Geräte nicht nur als Sprungbrett für Angriffe auf große, möglicherweise kritische Infrastrukturen genutzt werden können, sondern auch eine an sich zunehmende Gefahr für unsere vernetzte Gesellschaft darstellen [3][12].

Traditionell wurde der Informationssicherheit (engl. Security) großer Rechenanlagen und des Internets mehr Beachtung geschenkt als der Informationssicherheit kleiner und eingebetteter Geräte. Dies ist nicht zuletzt der Tatsache geschuldet, dass die Verbreitung, Fähigkeiten und Konnektivität solcher eingebetteter Geräte lange Zeit weit hinter denen klassischer Computer zurückblieben. Getrieben durch das Internet der Dinge nimmt nun aber nicht nur die Verbreitung eingebetteter Geräte massiv zu, sondern gleichermaßen steigen auch deren Fähigkeiten an; dies gilt sowohl in Bezug auf die vorhandenen Ressourcen (Rechenleistung, Speicher, und nahezu uneingeschränkter Konnektivität) als auch auf deren Möglichkeiten, Einfluss auf ihre physische Umgebung zu nehmen. Dabei gehören Energie- und Industrieautomation, Verkehrsleittechnik, E-Mobility, Smart City, Smart Home, Industrie 4.0 und E-Health wohl zu den bekanntesten Schlagwörtern.

In der Informationssicherheit werden eine Reihe wichtiger Schutzziele definiert, wie z.B. Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit und Nichtabstreitbarkeit. Zu deren Sicherstellung gibt es eine ganze Reihe erprobter Ansätze, welche größtenteils die digitale Identität der beteiligten Kommunikationspartner verwenden, deren Integrität jedoch bislang in der Regel nicht mit einbeziehen. Im Internet der Dinge ist es heute jedoch noch wichtiger die Einzelgeräteechtheit aus der Ferne überprüfen zu können. Diese besteht aus der Identität und Integrität von Hardware und Software, sowie der Betriebsparameter der Geräte. Neben der Manipulation von Betriebsparametern über unzureichend gesicherte Schnittstellen sind insbesondere die Manipulation der Firmware oder das Imitieren eines Gerätes einer der einfachsten Angriffspfade.

Die Gefahren reichen von der Persistierung eines Angriffs, d.h. der dauerhaften Einnistung z.B. eines Trojaners, bis zur Extraktion von privaten Daten. Die Angriffsmethodiken erstrecken sich von Angriff über das Netzwerk, die Nutzung von lokalen Wartungsschnittstellen bis hin zum Austausch von Geräten. Entsprechend wird sich zeigen, dass Geräteidentität und -integrität als Komposition der Identität und Integrität von Hardware, Software und Betriebsparametern verstanden werden muss.

Vergessen werden sollte allerdings nicht, dass grundsätzlich jedes IKT-System und jede IKT-Komponente Angriffspotentiale bietet, die mehr oder wenig versierte Angreifer mit entsprechendem Aufwand ausnutzen können. Einen allumfassenden Schutz gegen Cyberangriffe gibt es ebenso wenig, wie es diesen gegen Straftaten in der physischen Welt gibt. Daher muss das Ziel die Entwicklung und Anwendung

von Schutzstrategien sein, die die Erfolgswahrscheinlichkeit bzw. die negativen Auswirkungen von erwarteten Angriffen mit vertretbarem Aufwand so stark verringern, dass sie für die potentiellen Angreifer uninteressant werden und somit das Risiko akzeptierbar wird. Ein weiterer Aspekt ist der Umgang mit erfolgten Angriffen und Möglichkeiten der Wiederherstellung eines sicheren Zustands.

In diesem Positionspapier werden im Umfeld von Geräteidentität und Geräteintegrität im Internet der Dinge Anwendungsszenarien beispielhaft aufgezeigt (Kapitel 2), Anforderungen und Voraussetzungen beschrieben (Kapitel 3), Konzepte und Ansätze präsentiert (Kapitel 4) und Herausforderungen dargelegt (Kapitel 5). Abschließend werden die Ziele dieser Taskforce formuliert (Kapitel 6) und ein Fazit gegeben (Kapitel 7).

2. Anwendungsszenarien

Die Bedeutung einer sicheren Geräteidentität und -integrität ist grundsätzlich an keine spezielle Anwendungsdomäne gekoppelt, sondern stellt sich vielmehr als ein universeller Baustein der Sicherheit in einer umfassend vernetzten Welt dar. Die technischen Herausforderungen sind dabei jeweils sehr ähnlich gelagert und unterscheiden sich im Wesentlichen nur in ihrer Risikobewertung und der Angriffsreaktion.

Zur Illustration der Motivation von Angreifern sowie der hiervon ausgehenden Gefahren seien im Folgenden beispielhaft die Bereiche der Smart City und der Industrie 4.0 angeführt. Dabei kann es sich um direkte Gefahren – bei denen der Schaden auf dem angegriffenen Gerät stattfindet – oder indirekte Gefahren – bei denen ein gekapertes Gerät etwa als Angriffstool in Botnetzen verwendet wird – handeln.

2.1. Smart Cities

Die Smart City zeichnet sich vor allem dadurch aus, dass intelligente Systeme genutzt werden, um die Lebensqualität der Bürger zu erhöhen und Ressourcen effektiver und effizienter zu nutzen. Dazu werden die Elemente der urbanen Infrastruktur derart vernetzt, dass eine automatisierte Optimierung ihres Zusammenspiels möglich wird.

Eine vernetzte Smart City basiert jedoch in weiten Teilen auf Informationen und Daten von kleinsten Sensoren in Parkhäusern und Parkbuchten, an Ladesäulen, in Straßen und anderen wichtigen Punkten. Konnte man früher nur persönlich vor Ort in das städtische Geschehen eingreifen, so genügt in der Smart City das Fälschen oder Manipulieren von Sensordaten über das Internet, um sich z.B. aus der Ferne einen Parkplatz freizuhalten und sich damit einen Vorteil oder Anderen einen Nachteil zu verschaffen.

Dass solche Szenarien nicht undenkbar sind, zeigt z.B. der Fall eines Schülers, der mit der heimischen, programmierbaren TV-Fernbedienung kritische Funktionen, wie das Stellen einer Weiche der S-Bahn per Infrarotsignal, auslösen konnte [13]. Offensichtlich ist damit auch die körperliche Unversehrtheit von Menschen betroffen. Während der Schüler wohl aus Spieltrieb handelte und dabei keinen ernsten

Schaden anrichten wollte, sind die möglichen Auswirkungen von politisch, wirtschaftlich oder gar terroristisch motivierten Angriffen sehr ernst zu nehmen [14]. So könnte z.B. die Verkehrsleitfunktionen einer Smart City manipuliert werden, um während eines Raubüberfalls oder eines terroristischen Anschlags Zufahrtswege zu blockieren oder um eine Panik zu erzeugen und Polizeieinsätze und Rettungsmaßnahmen zu erschweren.

Damit die Idee der Smart City Akzeptanz und Umsetzung finden kann ist es unerlässlich, dass die Identität und Integrität der Geräte aus der Ferne verifiziert werden kann. Das trifft insbesondere auch auf die kleinsten Geräte zu, welche das Gesamtsystem mit ggf. kritischen Daten versorgen.

2.2. Industrie 4.0

„Industrie 4.0“ ist das Synonym für eine durchgängige Digitalisierung und tiefgreifende Vernetzung von industriellen Anlagen sowie Produktions- und Handelsprozessen. Neben neuen Möglichkeiten, Produktionsabläufe und Lieferketten deutlich effizienter und flexibler zu gestalten und dabei große Wettbewerbsvorteile zu erreichen, ergeben sich jedoch auch große Gefahren, die nicht zuletzt in unmittelbarem Zusammenhang mit der (Un-)Sicherheit von eingebetteten Geräten stehen.

Ein prominentes Beispiel eines erkannten Angriffs auf industrielle Anlagen ist Stuxnet, bei dem ein System zur Überwachung und Steuerung von Zentrifugen-Motoren angegriffen wurde [21]. Angriffe, bei denen Daten illegal kopiert werden und Geschäftsgeheimnisse an die Konkurrenz abfließen, bleiben hingegen sehr oft unentdeckt oder erfahren keine öffentliche Aufmerksamkeit [15]. Nach Schätzung von Bitkom beträgt der Anteil angegriffener Unternehmen 69% und es entsteht der deutschen Wirtschaft jedes Jahr ein Schaden von 22 Milliarden Euro [22]. Der Abfluss deutscher Ingenieursleistungen in Form von Produktionsverfahren und -konfigurationen in Länder mit günstigeren Arbeitskräften und geringeren Energiekosten stellen letztlich den Verlust wesentlicher Vorteile deutscher Produkte und Produktion dar.

Die Potenziale von Industrie 4.0 werden sich nur dann nutzen lassen, wenn die zugrunde liegende Infrastruktur in ausreichendem Maße sicherstellen kann, dass sich die Vertrauensverhältnisse zwischen einzelnen Akteuren der physischen Welt auch auf den Cyberspace abbilden lassen. Dabei muss der Identität und Integrität von Geräten besondere Aufmerksamkeit zukommen.

3. Anforderungen und Voraussetzungen

3.1. Vertrauenswürdige Funktionalität

Die Sicherheit von IKT-Geräten beginnt bei der Konzeption und Entwicklung ihrer Hardware- und Softwarekomponenten. Hierbei muss sichergestellt werden, dass das Produkt die erwartete Funktionalität aufweist und insbesondere frei von ungewollter Funktionalität ist. Diesem Ziel können jedoch einige Umstände und Interessen entgegenwirken. So erschweren die zunehmende Komplexität von

Software und Hardware auf der einen und der zunehmende Preis- und Zeitdruck auf der anderen Seite das Entwickeln von sicheren und verlässlichen Komponenten und Geräten. Probleme werden häufig erst beim Kunden bzw. Endanwender entdeckt. Hier können z.B. die Normenreihen VDI/VDE 2182, ISO/IEC 25000, ISO/IEC 62443, ISO/IEC 27000 oder ISO/IEC 15408, als Leitfaden für die Sicherstellung einer hohen Qualität dienen.

Jedoch unterscheidet sich häufig auch die Erwartung des Kunden bzw. Endanwenders an die Funktionalität eines Gerätes von der des Herstellers oder Anbieters. Es gibt unzählige Beispiele von gelieferten Systemen, die zusätzliche Funktionen aufweisen, die dem Benutzer nicht bekannt waren. Dies beginnt bei intransparenten Zugriffen auf die Cloud, bei der personenbezogene Daten übertragen werden, um einen vermeintlich besseren Service zu liefern, geht über Kassenterminals, die in krimineller Absicht Bankkartendaten ins Internet übertragen bis hin zu Audiotechnologien, die als Wanzen missbraucht werden können [4][5][6].

Eine wesentliche Voraussetzung für das Vertrauen in das Internet der Dinge ist daher die Überprüfbarkeit der Funktionalität von Geräten. Das kann nach verschiedenen Herangehensweisen durchgeführt werden – entweder über die Transparenz gemäß des neuen Standard-Datenschutzmodells [11] oder anhand von Zertifizierungen von Software, Prozessen oder Funktionalitäten.

Ähnliche Herausforderungen finden sich auch im Bereich der Hardwaresicherheit. Die Gefahren von Hardwaretrojanern sind insbesondere aufgrund der erschwerten Detektierbarkeit ein aktuelles Forschungsfeld. Hard- und Software ist zudem das Problem der Lieferkettenintegrität gemein.

Offensichtlich ist jedoch auch, dass z.B. die reine Existenz einer vertrauenswürdigen Komponente nicht ausreicht. Vielmehr muss es ausgehend von Komponenten mit vertrauenswürdiger Funktionalität auch eine Möglichkeit geben, sicherzustellen, dass diese im konkreten Fall tatsächlich auch zum Einsatz kommen. Die Selbstauskunft einer Komponente, insbesondere einer Softwarekomponente, lässt sich in der Regel leicht fälschen. Dies gilt umso mehr, da in Szenarien des Internets der Dinge der Angreifer physischen Zugriff auf die Geräte haben kann, während die Überprüfung aus der Ferne geschehen muss.

3.2. Datenschutz

Das Internet der Dinge bringt vor allem ein Mehr an Sensoren und intelligenten Systemen, welche zuvor nicht verfügbaren Daten automatisiert verarbeiten. Es gibt viele Unternehmen, deren Geschäftsmodell in der Sammlung möglichst umfangreicher Daten besteht. Daten als Rohstoff der Zukunft werden auch zur weiteren Wertschöpfung genutzt werden; über direkte Endkundenbelange (z.B. Versicherungen, Autohersteller, Gesundheitsbranche) bis hin zum Mining von Erkenntnissen aus Prozessdaten. Ziel muss es sein, dass persönliche Daten unter der Souveränität des Eigentümers verbleiben. In der Smart City oder Industrie 4.0 sind dort anfallende Daten zwar größtenteils nicht personenbezogen, aber sehr wohl kritisch für den Geschäftserfolg. Mit diesen Daten muss daher genauso sorgsam umgegangen werden.

Eng verknüpft mit dem Datenschutz ist das Prinzip der Datensparsamkeit. Zur Erbringung eines (gewollten) Dienstes sollten nur jene Daten übermittelt werden, die unbedingt notwendig sind. Wo möglich sollten Daten nur anonymisiert (oder ggf. pseudonymisiert) weitergegeben werden. Die Einhaltung dieser Prinzipien sollte bereits im Entwicklungsprozess berücksichtigt werden (Privacy-by-Design). Ansätze dies umzusetzen existieren bereits, etwa mit ABC4Trust [7].

3.3. Skalierbarkeit

Das Internet der Dinge wird Milliarden von Geräten umfassen. Hieraus ergeben sich hohe Anforderungen an die Skalierbarkeit und Massentauglichkeit des Nachweises der Einzelgeräteechtheit, sprich der Geräteidentität und -integrität. Dazu zählen insbesondere eine automatisierte Verwaltung, eine anwenderfreundliche Konfiguration der Geräte sowie eine Unterstützung über den gesamten Lebenszyklus der Geräte hinweg.

Dabei muss insbesondere der Entwicklung genüge getan werden, dass Updatezyklen und Fehlerbeseitigungen in immer kürzeren Abständen erfolgen müssen. Dies muss insbesondere in großen Stückzahlen im Feld möglich sein, ohne dass hierbei unzumutbarer Mehraufwand oder ein Angriffspotenzial für den Normalbetrieb entsteht. Standards und Industrienormen erleichtern diesen Vorgang.

3.4. Verfügbarkeit

Wenn Geräte mit sicherheitsrelevanter Funktionalität, also z.B. physische Aktoren, involviert sind, stellt sich die Frage der Verfügbarkeit und des Umgangs mit Fehlerfällen. Hier zeigen sich deutlich die wechselseitigen Abhängigkeiten zwischen der funktionalen Sicherheit (Safety) und der Informationssicherheit (Security). Insbesondere darf z.B. eine nicht erfolgreich überprüfbare Geräteidentität nicht dazu führen, dass eine Anlage komplett ausfällt oder die funktionale Sicherheit des Gesamtsystems in irgendeiner Weise beeinträchtigt wird [16].

4. Konzepte und Ansätze

Die Geräteinformationssicherheit hängt auf der einen Seite ab von Prozessen und Konfigurationen der Geräte in der Fertigung und im Betrieb (vgl. ISO/IEC 27000) sowie auf der anderen Seite von der Einzelgeräteechtheit. Als Ausgangspunkt für Einzelgeräteechtheit dient die folgende Definition: Eine Einzelgeräteechtheit ist die einzigartige und nicht duplizierbare Summe jener Identitäts- und Integritätseigenschaften eines Gerätes, welche das erwartete und vertraute Geräteverhalten hervorbringen, sowie eine Unterscheidbarkeit gleichartiger Geräte erlaubt. Kurz:

> Einzelgeräteechtheit = Geräteidentität & -integrität
> = Hardware + Software + Betriebsparameter

Die Charakteristik eines modernen computergestützten Geräts setzt sich also aus drei hauptsächlichen Aspekten zusammen: der Hardware, der Software (im Kontext eingebetteter Geräte oft auch als Firmware bezeichnet) und dem Teil seiner Betriebsparameter, der die Funktionalität des Gerätes charakterisiert. Abweichungen bei jedem dieser Aspekte können in Bezug auf das Gesamtgerät einen immensen Unterschied darstellen und die Einzelgeräteechtheit verfälschen.

Der Austausch von Hardware kann beispielsweise, selbst wenn die gleiche Software darauf läuft, den Unterschied zwischen zuverlässiger, geprüfter Hardware für den Einsatz in kritischen Systemen und einem billigen Imitat von minderer Qualität und hoher Ausfallwahrscheinlichkeit ausmachen. Der Austausch von Software kann bei gleicher Hardware aus einer Wasserwerksteuerung eine Schwimmbadsteuerung und umgekehrt machen. Das Ändern von Betriebsparameter kann beispielsweise aus einem Firewallsystem einen Router ohne Sicherheitsfunktionen machen. Ebenfalls vorstellbar ist, dass der Hersteller eines Gerätes das Freischalten von Funktionalität gegen Bezahlung ermöglicht, ohne dass hierzu die Software aktualisiert wird. Dies würde dann über die Konfiguration geschehen und ggf. ein völlig anderes Geräteverhalten hervorbringen.

Aus der obigen Definition bleibt die Frage, welche der vielfältigen Betriebsparametern für die Bestimmung der Geräteechtheit relevant sind. Dies lässt sich wohl nicht ohne eine Betrachtung des konkreten Anwendungsfalls beantworten und erfordert eine genaue Analyse des Einflusses der jeweiligen Parameter.

4.1. Hardwareidentitäten

Eine Hardwareidentität wird in der Regel durch ein eindeutiges Identifikationsmerkmal umgesetzt, üblicherweise ein kryptographischer Schlüssel. Das wichtigste Ziel hierbei ist die Unklonbarkeit dieses Identifikationsmerkmals, sprich die Vervielfältigung dieses Identifikationsmerkmals zu verhindern, um dessen Exklusivität und somit die eindeutige Hardwareidentität zu gewährleisten.

In der Vergangenheit wurde zur Bereitstellung von Geräteidentitäten in einer Vielzahl von Domänen auf reine Software-Methoden gesetzt. Dabei wird ein kryptographischer Schlüssel z.B. auf der Festplatte oder in einem nicht flüchtigem Speicher (Flash/EEPROM) des Geräts abgelegt und für kryptographische Berechnungen im Rahmen eines Identitätsnachweises in den Speicher der CPU geladen. Hier bestehen jedoch zwei maßgebliche Probleme. Erstens ist eine Festplatte oder ein Flash/EEPROM in der Regel nicht vor dem Zugriff eines Angreifers geschützt, der physisch mit dem Gerät interagieren kann. Ein Angreifer kann somit relativ einfach den betreffenden Baustein aus dem Gerät entnehmen, sich Zugriff verschaffen und den Schlüssel, und damit die Hardwareidentität des Gerätes, duplizieren. Zum Zweiten ist der Schlüssel nicht hinreichend vor netzwerkbasierten Angriffen geschützt. Es ist weitreichend bekannt, dass eine vollständige Fehlerfreiheit von Software bei der Komplexität heutiger Systeme nicht erreicht werden kann. Dies wurde z.B. eindrucksvoll durch den Heartbleed-Bug in OpenSSL demonstriert, der es Angreifern ermöglichte, kryptographische Schlüssel aus der Ferne zu extrahieren.

Vor diesem Hintergrund erscheint die Nutzung spezieller Hardwareerweiterungen notwendig, welche sowohl den kryptographischen Hardwareidentitäts-Schlüssel vor ungewollten Zugriffen abschirm, als auch die kryptographischen Berechnungen, die den zugehörigen Schlüssel verwenden; seien dies Entschlüsselungen, Signaturerzeugungen, Schlüsselaustausch oder auch nur Schlüsselableitungen.

Durch den korrekten Einsatz und softwareseitige Einbindung solcher Module kann der Angriffsaufwand für den überwiegenden Teil von Angriffen auf die Hardwareidentität auf ein in der Regel unprofitables Maß gebracht werden. Voraussetzung für den sicheren Einsatz sind jedoch entsprechende, vorzugsweise zertifizierte Produktions- und Verwaltungsprozesse, die insbesondere das initiale Erzeugen und Einbringen von Schlüsseln bzw. das Erzeugen zugehöriger Identitätszertifikate absichern.

4.2. Softwareidentitäten und Betriebsparameter

Bei der Softwareidentität und den Betriebsparametern wird ein ganz anderes Ziel verfolgt als bei der Hardwareidentität. Im Gegensatz zur Hardware ist es bei Software völlig normal und auch gewünscht, dass dieselbe Version (und damit die gleiche Identität) in einer Vielzahl gleichartiger Geräte zum Einsatz kommt. Im Fall von Software wird das Ziel der Integrität verfolgt. Dabei soll sichergestellt werden, dass die erwartete Software auf dem Gerät zum Einsatz kommt und nicht eine veränderte Version.

Der bekannteste Mechanismus in diesem Zusammenhang, Secure Boot genannt, verhindert das Starten von illegitimer Software. Mithilfe eines auf dem Gerät hinterlegten kryptographischen Schlüssels oder Referenzwertes wird vor dem Starten der Software deren kryptographische Signatur überprüft.

Zur Feststellung der Softwareidentität hilft Secure Boot jedoch nur bedingt und auch nur dann, wenn bekannt ist, dass ein bestimmtes Gerät diese Technologie aktiv einsetzt. Die Sicherheitsbewertung der Software wird bei Secure Boot von der signierenden Instanz, d.h. zumeist dem Softwarehersteller, im Voraus durchgeführt. Durch diese Indirektion ist es für einen Kommunikationspartner später nicht mehr möglich festzustellen, welche Software in welcher Version genau auf dem Gerät läuft. Selbst der Hersteller kann seine Bewertung, welche Software vertrauenswürdig ist, nicht mehr ohne weiteres zurückziehen. Letzteres stellt insbesondere in Bezug auf Software-Update-Verfahren ein großes Problem dar. Eine einmal signierte Softwareversion bleibt trotz des Erscheinens einer neuen Softwareversion gültig. Dies kann ein Angreifer bspw. in sogenannten „Downgrade-Attacken" nutzen, um veraltete Software mit bekannten Sicherheitslücken unbemerkt auf einem Gerät einzuspielen und dann ebendiese Sicherheitslücken auszunutzen.

Festzustellen ist zudem, dass mit Secure Boot die Kontrolle eines Gerätes nahezu vollständig der Zertifikate erteilenden Instanz, oftmals also dem Hersteller obliegt. Dadurch hat ein Gerätebesitzer nur noch sehr eingeschränkte Möglichkeiten, ein Gerät eigenständig mit Software zu versorgen oder über die Supportdauer des Herstellers hinaus eigene Sicherheitsupdates einzuspielen.

Eine zweite Technologie die auch sehr gut in Verbindung mit Secure Boot eingesetzt werden kann, ist das sogenannte Measured Boot. Dabei wird die Software vor dem Start „gemessen", d.h. eine Zahl berechnet, welche die Software in ihrer aktuellen Konfiguration eindeutig repräsentiert. Der entsprechende Wert wird dann in einem nicht manipulierbaren Speicher abgelegt, während der Start der Software weder behindert noch verhindert wird. Solche Messungen können im Gegensatz zu Secure Boot auch bzgl. relevanter Betriebsparameter betreffend der Funktionen des Gerätes getätigt werden.

Um diesen „Messwert“ als Softwareidentität nutzen zu können, muss er gegenüber einem Dritten verifiziert werden können. Der entsprechende Vorgang wird als Software-Attestation oder auch Remote-Attestation bezeichnet. Er kann z.B. auf einer vorhandenen Hardwareidentität basieren, welche entweder zur Signierung des Messwertes genutzt wird (explizite Attestation) oder deren Nutzung durch eine Hardwarekomponente nur dann freigegeben wird, wenn bestimmte, „erlaubte“ Messwerte vorliegen (implizite Attestation).

Mit Hilfe der genannten Verfahren lassen sich die Soft- und Hardwareidentität und -integrität eines Geräts und damit dessen Einzelgeräteechtheit sicher feststellen und beim Aufbau von Netzwerkverbindungen oder auch nur zum Monitoring von Geräten in einem größeren System verwenden.

5. Herausforderungen

Für die genannten Konzepte existieren bereits heute einige Lösungsansätze und Standards. So definiert beispielsweise die Trusted Computing Group mit dem Trusted Platform Module (TPM) einen Standard für ein Hardwaresicherheitsmodul, das Secure Boot und Measured Boot unterstützt, sowie mit der Device Identity Composition Engine (DICE) ein Verfahren zum Ableiten von einfachen Identitäten in Kleinstsystemen. Auch werden Basistechnologien laufend verbessert; bei Physical Unclonable Functions (PUFs) findet eine rasante Entwicklung statt [18] und völlig neue Authentifikationsverfahren etwa für Sensoren werden entwickelt [19][20].

Auf der anderen Seite zeigt sich allerdings auch, dass die existierenden Technologien noch nicht genügen, um die Umsetzung sicherer Geräteidentitäten und -integritäten in einem breiteren Anwendungskontext zu ermöglichen. Das Verständnis um die Komposition eines Gerätes und seiner Identitätsaspekte fehlt in vielen Anwendungskontexten bisher grundsätzlich. Für die Weiterentwicklung der Technologien zur Geräteidentität und -integrität werden daher eine Reihe weitergehender Probleme zu adressieren sein.

Auf der technologischen und konzeptionellen Seite bestehen noch viele Problemfelder bei der Integration entsprechender Ansätze in die Anwendungsebene und das Gesamtsystem. Insbesondere das Management von Geräteidentitäten und der zugrunde liegenden Hardware, Software und Betriebsparameter bedarf sowohl neuer und weiterentwickelter Konzepte als auch der Integration mit bestehenden Werkzeugen zum Gerätemanagement und in Lieferketten. Die genannten Verfahren zur Remote Attestation müssen mit den vorhandenen Funktionsprotokollen verwoben werden, sodass Identitätsfeststellungen verlässlich erfolgen können.

Klar ist aber auch, dass weit mehr als die Spezifikation von Basistechnologien notwendig ist. Ein simples Zusammenstecken vorhandener Lösungen schafft schnell kritische Schnittstellen zwischen den einzelnen, eigentlich sicheren Bestandteilen. Ein System mit schwach angebundenen Sicherheitschips bietet beispielsweise eine andere Angriffsfläche als ein System, bei dem die Sicherheitskomponente entsprechend in das Gesamtsicherheitskonzept integriert ist [17].

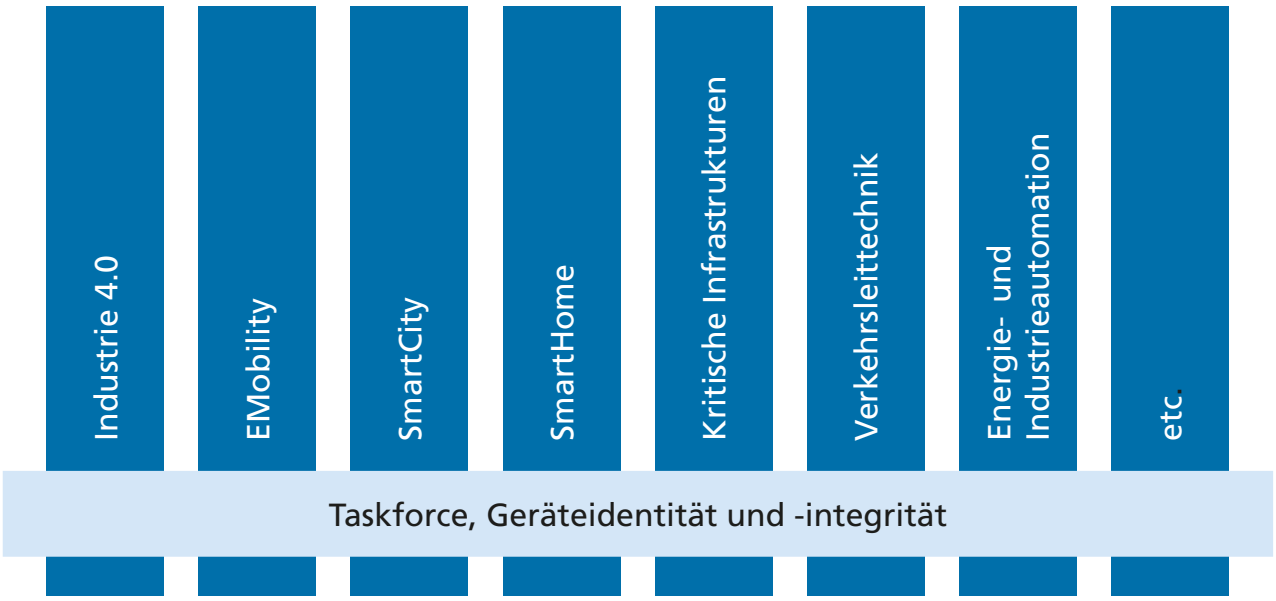
Auch das Zusammenspiel aus Safety und Security scheint im Kontext noch nicht ausreichend betrachtet worden zu sein. Ein gemeinsames und domänenübergreifendes Modell zur Abwägung dieser Eigenschaften in verschiedenen Anwendungsfällen würde die Vergleichbarkeit und Wiederverwendbarkeit von Lösungen deutlich verbessern.

Auf der ökonomischen Seite besteht die Fragestellung nach Anreizen zum Einsatz der beschriebenen Technologien. Die Wahrnehmung der Kritikalität von eingebetteten Systemen, der Auswirkungen von Schadensfällen und der zunehmenden Risiken der Vernetzung auf der einen Seite sind noch nicht auf dem gleichen Stand wie die Anreize der Funktionsausweitung und Vernetzung von Systemen auf der anderen Seite. Die Sensibilisierung von Anwendern wie Herstellern sowie die Etablierung von Technologien zur sicheren Geräteidentitäten als Qualitätsmerkmal werden die Basis für eine Durchdringung des Markts mit diesen Technologien sein. Dabei müssen diese Technologien anwendungsdomänenübergreifend mit gemeinsamen Schnittstellen und Protokollen entwickelt werden, um durch die Bündelung von Entwicklungsressourcen die Kosten zu minimieren.

Auf gesellschaftlicher Ebene sind ebenfalls noch Fragestellungen aufzulösen. So kann Geräteidentität einerseits dem Gerätebesitzer mehr Kontrolle und Sicherheit bieten. Auf der anderen Seite können solche Lösungen mit einem gewissen Verlust der Souveränität und einer zusätzlichen Abhängigkeit zum Hersteller einhergehen. Auch steht eine überprüfbare Identität von Geräten gewissen Belangen des Datenschutzes und der Privatsphäre gegenüber. Hier offenbart sich letztlich ein Spannungsfeld zwischen Informationssicherheit, Privatsphäre und Souveränität, das einer gesellschaftlich-politischen Debatte bedarf.

Schließlich müssen Entwickler, Ingenieure, Systemarchitekten, Manager und Kunden ein Verständnis für die Grundbegriffe dieser Technologie und die Notwendigkeit ihres bestimmungsgemäßen Einsatzes entwickeln. Bei der Zusammenführung von Technologien aus Einzelbereichen, der Unterrichtung und Aufklärung von beteiligten Akteuren und der Koordination und Synchronisation von neuen Entwicklungen über die Grenzen traditioneller Anwendungsdomänen hinaus, muss aktiv gearbeitet werden.

6. Ziele und Rolle der Taskforce



Das Ziel der Taskforce besteht darin, den Technologien zur Einzelgeräteechtheit, sprich der Geräteidentität und –integrität, bestehend aus Hardware, Software und Betriebsparametern, zur Anwendung im gesamten Bereich des Internets der Dinge auch über alle industriellen Anwendungsdomänen und kritische Infrastrukturen hinweg zu verhelfen. Für eine optimale Förderung dieser Entwicklung wird die Taskforce domänenübergreifend agieren.

Die Rolle der Taskforce besteht dabei insbesondere aus drei Hauptaufgaben:

(i) der Aggregation und Konsolidierung von Anforderungen,

(ii) der Identifikation und ggf. Entwicklung von Lösungen und

(iii) der Verbreitung und Multiplikation von Technologien.

Die Aggregation von Anforderungen aus den verschiedenen Anwendungsdomänen stellt den ersten Schritt im Fluss der Aufgaben der Taskforce dar. Dabei werden durch die beteiligten Experten Anforderungen zusammengetragen und in konsolidierter Weise zusammengestellt.

Die Identifikation und ggf. Entwicklung von Lösungen stellt den zweiten Schritt dar. Für die gesammelten Anforderungen werden hier Lösungen bzw. das Nichtvorhandensein von Lösungen identifiziert und in Form eines Kompendiums gesammelt. Auch neue Lösungen können hier ggf. im Rahmen der Taskforce und auch in Kollaboration mit anderen Gremien entwickelt werden.

Letztlich werden diese Lösungen und das Kompendium wieder in die Anwendungsdomänen zurückgespielt. Die Taskforce wird als Multiplikator dieser Technologien dienen, indem die identifizierten Lösungen in den Anwendungsdomänen verbreitet werden.

Der Prozess wird ein zyklischer Prozess sein, bei dem in jedem Schritt parallel gearbeitet werden kann. So wird bei der Rückspielung von Lösungen in die Anwendungsdomänen das Verständnis der Technologie steigen und neue Anforderungen, die bisher nicht bedacht wurden, können identifiziert werden. Auch wird es in verschiedenen Domänen regelmäßig zu Weiterentwicklungen kommen, die in das Kompendium an Lösungen zur Geräteidentität und -integrität aufgenommen werden können, um sie auch anderen Anwendungsdomänen näher zu bringen.

Mit dem vorliegenden Positionspapier soll das Verständnis der Aufgaben der Taskforce und der betrachteten Technologien dargestellt werden. Es dient in der Folge dazu, weitere Mitglieder für die Mitarbeit zu gewinnen und mit verwandten Gremien aus den Anwendungssektoren Partnerschaften zu bilden und die domänenübergreifende Lösungsentwicklung zu unterstützen.

7. Fazit

Kleine und vernetzte Computersysteme werden unsere Gesellschaft immer weiter durchdringen und zunehmend selbstständig agieren. Aufgrund der Wechselwirkungen zwischen den Geräten im Internet der Dinge entsteht dabei ein Gesamtsystem hoher Komplexität. Die verteilten Infrastrukturen beinhalten sehr viele vernetzte Geräte und Besitzer, die dezentral miteinander kollaborieren müssen.

Als zentrales Element ist es in jedem Fall unerlässlich, dass sich Geräte zu jedem Zeitpunkt zuverlässig authentisieren und ihre Integrität – und Einzelgeräteechtheit – nachweisen können, d.h. eine sichere Geräteidentität und -integrität besitzen. Dies umfasst die Verknüpfung von nachweisbar authentischer Hardware und Software sowie funktionsbestimmender Betriebsparameter. Jede Manipulation all dieser Komponenten muss erkennbar sein.

Die hierfür notwendigen Basistechnologien existieren bereits in verschiedenen Formen, jedoch bestehen noch große Lücken bei der Integration dieser Technologien in die Anwendungsebene und die Gerätemanagementprozesse. Ein Bewusstsein für die hier dargelegten Probleme und Herausforderungen sowie ein Verständnis für mögliche Lösungsansätze muss weiter ausgebaut werden. Letztlich müssen Entwickler, Ingenieure, Systemarchitekten, Manager und Kunden ein Verständnis für die Grundbegriffe dieser Technologien entwickeln. An der Zusammenführung von Technologien aus Einzelbereichen, der Unterrichtung und Aufklärung von beteiligten Akteuren und der Koordination und Synchronisation von neuen Entwicklungen über die Grenzen traditioneller Anwendungsdomänen hinaus, muss aktiv gearbeitet werden. Dabei müssen auch die ökonomischen Aspekte der behandelten Risiken, neuen Chancen und mögliche Geschäftsmodelle betrachtet werden.

Die Taskforce hat sich das Ziel gesetzt, die Verbreitung von Technologien für sichere Einzelgeräteechtheit, sprich Geräteidentitäten und Integrität als Komposition von Hardware, Software und Betriebsparametern zu fördern. Dabei dient die Taskforce als anwendungsdomänenübergreifendes Instrument um Synergien herzustellen. Ähnlich wie bei anderen Basistechnologien muss es auch im Bereich der Einzelgeräteechtheit, aus Geräteidentität und Integrität, das Ziel sein, eine anwendungsunabhängige technologische Basis zu schaffen. Die Integration in die Anwendungsdomänen, deren Prozesse und Lebenszyklen, stellt dabei eine zentrale Herausforderung dar.

Referenzen

[1] SPIEGEL Online, „Früherer US-Vize Cheney fürchtet sich vor Anschlag auf seinen Herzschrittmacher“, 19.10.2013

[2] D. Halperin et al., „Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses,“ 2008 IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA, 2008, pp. 129-142.

[3] ZDNet, „Störungen bei Spotify und Twitter: IoT-Botnet für massiven DDoS-Angriff benutzt“, 24.10.2016

[4] http://www.heise.de/newsticker/meldung/Verbraucherschuetzer-klagen-Samsung-TV-uebertraegt-Daten-ungefragt-2878594.html

[5] http://www.heise.de/newsticker/meldung/Manipulierte-Kreditkartenleser-funken-Daten-nach-Pakistan-210821.html

[6] http://www.storyleak.com/tor-developer-fears-nsa-interception-amazon-purchase/

[7] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/ARM%20Security%20Technology.pdf

[8] https://os.inf.tu-dresden.de/papers_ps/nizza.pdf

[9] http://www.heise.de/newsticker/meldung/VW-Chef-Markteinstieg-von-Google-und-Apple-begruessenswert-aber-ohne-Daten-2576824.html

[10] https://www.abc4trust.eu/

[11] https://www.datenschutz-mv.de/datenschutz/sdm/sdm.html

[12] BSI: Die Lage der IT-Sicherheit in Deutschland 2014 |3.3.1 APT-Angriff auf Industrieanlagen in Deutschland

[13] Heise Security: TV-Fernbedienung lässt Züge entgleisen 2008 https://www.heise.de/security/meldung/TV-Fernbedienung-laesst-Zuege-entgleisen-Update-177790.html

[14] BBC News, Are smart city transport systems vulnerable to hackers? http://www.bbc.com/news/business-36854293

[15] BSI: Die Lage der IT-Sicherheit in Deutschland 2015 |2.2.3 Gezielte Angriffe – APT

[16] IEC 62443 „Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models“

[17] B. Kauer „OSLO: Improving the security of Trusted Computing“, 2007, p3

[18] U. Rührmair, S. Devadas, and F. Koushanfar. “Security based on physical unclonability and disorder”. Introduction to Hardware Security and Trust. Springer, 2012, pp. 65–102.

[19] M. Potkonjak, S. Meguerdichian and J. L. Wong, „Trusted sensors and remote sensing,“ Sensors, 2010, pp. 1104–1107.

[20] Ulrich Rührmair et al. „Virtual Proofs of Reality and their Physical Implementation.“ IEEE Symp. Security and Privacy, 2015, pp. 70–85.

[21] Sandro Gaycken, „Stuxnet, Wer war's? Und wozu?“ Zeit Online, 2010, http://www.zeit.de/2010/48/Computerwurm-Stuxnet.

[22] Bitkom, „Industrie im Visier von Cyberkriminellen und Nachrichtendiensten.“ 2016, https://www.bitkom.org/Presse/Presseinformation/Industrie-im-Visier-von-Cyberkriminellen-und-Nachrichtendiensten.html.